Awesome Polynomials for Mathematics Competitions

Titu Andreescu
Navid Safaei
Alessandro Ventullo

Awesome Polynomials for Mathematics Competitions

Awesome Polynomials for Mathematics Competitions

Titu Andreescu

Navid Safaei

Alessandro Ventullo

Library of Congress Control Number: 2021939810

ISBN: 978-1-7358315-1-0

9 8 7 6 5 4 3 2 1

www.awesomemath.org

Cover design by Iury Ulzutuev

To my family, for support and understanding.

Titu

To Hamisha, for the sweet memories.

Navid

To the memory of Maria, my beloved grandmother.

Alessandro

Preface

After the well-received book 117 *Polynomial Problems from the AwesomeMath Summer Program*, we decided to publish a second book on polynomials. The evolving landscape that makes up modern mathematical competitions has exposed contestants to polynomials more than ever before. Recently, almost all advanced mathematical competitions have at least one problem on polynomials. Despite this rising importance, only a few problem books bring attention to this topic. Thus, the vast universe that polynomials encapsulate should be more thoroughly investigated.

The following book casts light on this topic from numerous angles. We present important theoretical facts in harmony with their showcased applications, featuring 8 chapters, 252 solved examples, 105 end of chapter problems, all with detailed solutions, as well as 77 additional awesome problems that further enhance the book's exposition. In the first seven chapters, in order to help the reader grasp and master the concepts, we underscore several strategies and lemmas.

Chapter one deals with reciprocal polynomials and their relevant applications. In chapter two we provide a review of complex numbers and present polynomial problems that are closely linked to complex numbers. Reviewing and internalizing this chapter is a key to helping the reader get the most out of subsequent chapters.

Chapter three provides a cogent presentation of elementary ideas about finding unknown polynomials. In chapter four we provide "uniqueness lemmas" and their profound implications. Our primary motivation to expand upon these lemmas was to reduce the difficulties associated with solving a large class of

polynomial equations. The difference between the traditional approaches for solving such problems and the uniqueness lemmas are evident. We included these two lemmas because of their great success in aiding students in our teaching experiences.

Chapter five examines the techniques related to characterizing the roots of polynomials along with long-run behavior. The applications go beyond the realm of quantifying polynomials. In chapter six we provide an in-depth look into Lagrange's Interpolation Formula and present several interesting problems.

Chapter seven sheds light on Newton's formulas and their applications in Algebra and Number Theory and is illustrated by pertinent examples. Finally, in chapter eight, in order to consolidate the learning outcomes of the first seven chapters, we present 77 additional problems proposed by some of the world's most brilliant and creative minds.

The content of this book developed as a result of the union between algebraic ideas and teaching experiences. It is essential to bear in mind that the sophisticated ability to think conceptually, deductively, and sequentially can be achieved through focusing on training materials that are insightful, encourage further thought, and apply to the real world. We invite readers to thoroughly internalize the contents of each chapter.

It is worthy of note that without the exceptional work of Richard Stong, who offered a wealth of ideas and insightful suggestions, this book would not be what it is today. We are also grateful to Peter Boyvalenkov, Alexander Khrabrov, Fedor Petrov, Bayasagalan Banzarach, and Yan Loi Wong for their help.

Titu Andreescu Navid Safaei Alessandro Ventullo

Contents

Part I

Theory, Examples, and Problems

Chapter 1

On the Form $x^d P\left(\frac{1}{x}\right)$

On some occasions, changing the original setting of the problem will make the problem more approachable.
For instance, instead of working with the polynomial $a_d x^d + \ldots + a_0$, we may work with the polynomial $a_0 x^d + \ldots + a_d$. This, may lead us to discover some unseen consequences of the hypotheses. We can easily transform

$$P(x) = a_d x^d + \ldots + a_0 \quad \text{to} \quad a_0 x^d + \ldots + a_d.$$

We just take the polynomial $x^d P\left(\frac{1}{x}\right)$.

1.1 Basic properties

Reciprocal polynomial

Let $P(x) = a_d x^d + \ldots + a_0$. The polynomial

$$x^d P\left(\frac{1}{x}\right) = a_0 x^d + \ldots + a_d$$

is called the *reciprocal polynomial* or *inverse polynomial* of $P(x)$.

From now on, we will call $x^dP\left(\frac{1}{x}\right)$ the reciprocal polynomial.

For example, the reciprocal polynomial of $P(x) = 2x^3 - 3x^2 + 1$ is $x^3 - 3x + 2$. The reciprocal polynomial of $Q(x) = 4x^3 - 3x$ is $-3x^2 + 4$.

In short, the reciprocal polynomial reverses the order of coefficients of the original polynomial.

Sometimes, the reciprocal polynomial has lower degree than the original polynomial. Crudely speaking, it depends on zero-multiplicity of the polynomial. That is, if $P(x)$ is a polynomial of degree d such that 0 is a root with multiplicity r, so $P(x) = x^rQ(x)$ with $Q(0) \neq 0$, we easily find that

$$x^dP\left(\frac{1}{x}\right) = x^dx^{-r}Q\left(\frac{1}{x}\right) = x^{d-r}Q\left(\frac{1}{x}\right).$$

The reciprocal polynomial $x^dP(x) = x^{d-r}Q\left(\frac{1}{x}\right)$ is of degree $d - r$.

Example 1.1. Let $P(x)$ be a polynomial of degree 5 with nonnegative integer coefficients such that for all $x \neq 0$, $P(x) = x^6P\left(\frac{1}{x}\right)$ and $P(2) = 10P(1)$. Find the greatest possible value of $\frac{P(3)}{P(2)}$.

Solution. Let $P(x) = ax^5 + \ldots + c$. If $c \neq 0$, then the polynomial $x^6P\left(\frac{1}{x}\right)$ has degree 6 and it cannot be equal to a polynomial $P(x)$ of degree 5. Hence $c = 0$. Putting $P(x) = xQ(x)$ for some polynomial $Q(x)$ of degree 4, we get

$$P(x) = xQ(x) = x^6P\left(\frac{1}{x}\right) = x^5Q\left(\frac{1}{x}\right).$$

We deduce that $Q(x) = x^4Q\left(\frac{1}{x}\right)$, which gives $Q(x) = ax^4 + bx^3 + cx^2 + bx + a$ for some non-negative integers a, b, c. Moreover, from $P(2) = 10P(1)$, we find

$$2Q(2) = 10Q(1).$$

Thus $17a + 10b + 4c = 5(2a + 2b + c)$, which yields $7a = c$. Moreover,

$$\begin{aligned}\frac{P(3)}{P(2)} = \frac{3Q(3)}{2Q(2)} &= \frac{3(82a + 30b + 9c)}{10(2a + 2b + c)} \\ &= \frac{3(145a + 30b)}{10(9a + 2b)} \\ &= \frac{3(29a + 6b)}{2(9a + 2b)} \\ &= \frac{6a + 3(27a + 6b)}{2(9a + 2b)} \\ &= \frac{9}{2} + \frac{3a}{9a + 2b} \\ &= \frac{9}{2} + \frac{1}{3 + \frac{2b}{3a}}.\end{aligned}$$

Since $\frac{2b}{3a} \geq 0$, then $\frac{9}{2} + \frac{1}{3 + \frac{2b}{3a}} \leq \frac{9}{2} + \frac{1}{3} = \frac{29}{6}$. The equality case occurs for $b = 0$ and the polynomial $P(x) = x(ax^4 + 7ax^2 + a) = ax(x^4 + 7x^2 + 1)$. ■

1.2 Sum of squares of coefficients of a polynomial

Let $P(x) = a_dx^d + \ldots + a_0$. It is instructive to consider the product

$$P(x)P\left(\frac{1}{x}\right) = (a_dx^d + \ldots + a_1x + a_0)(a_dx^{-d} + \ldots + a_1x^{-1} + a_0).$$

The above product is a rational function. The constant term of the above product is of special interest. Constant terms arise from the products of the form $a_rx^r \cdot a_rx^{-r} = a_r^2$. Hence the constant term of the above product is the sum of squares of the coefficients of the polynomial.

Sum of squares of the coefficients of a polynomial

The sum of squares of the coefficients of a polynomial $P(x)$ is the coefficient of the constant term in the product $P(x)P\left(\frac{1}{x}\right)$.

Example 1.2. Let $P_{2n}(x) = (6x^2 + 5x + 1)^n$ and $Q_{2n}(x) = (3x^2 + 7x + 2)^n$. Prove that the sum of squares of the coefficients of $P_{2n}(x)$ and $Q_{2n}(x)$ are the same.

Solution. It is known that the sum of squares of the coefficients of $P_{2n}(x)$ and $Q_{2n}(x)$ are equal to the coefficient of x^0 in the products $P_{2n}(x)P_{2n}\left(\frac{1}{x}\right)$ and $Q_{2n}(x)Q_{2n}\left(\frac{1}{x}\right)$. Note that

$$P_{2n}(x) = (6x^2 + 5x + 1)^n = (3x + 1)^n(2x + 1)^n$$

and

$$Q_{2n}(x) = (3x^2 + 7x + 2)^n = (3x + 1)^n(x + 2)^n.$$

Therefore

$$\begin{aligned} P_{2n}(x)P_{2n}\left(\frac{1}{x}\right) &= (3x+1)^n(2x+1)^n\left(\frac{3}{x}+1\right)^n\left(\frac{2}{x}+1\right)^n \\ &= \frac{(3x+1)^n(2x+1)^n(x+3)^n(x+2)^n}{x^{2n}} \end{aligned}$$

and

$$\begin{aligned} Q_{2n}(x)Q_{2n}\left(\frac{1}{x}\right) &= (3x+1)^n(x+2)^n\left(\frac{3}{x}+1\right)^n\left(\frac{1}{x}+2\right)^n \\ &= \frac{(3x+1)^n(x+2)^n(3+x)^n(2x+1)^n}{x^{2n}}. \end{aligned}$$

Comparing these we see that

$$Q_{2n}(x)Q_{2n}\left(\frac{1}{x}\right) = P_{2n}(x)P_{2n}\left(\frac{1}{x}\right).$$

Thus the coefficient of x^0 is the same in both products. ■

Example 1.3. Assume that for all $x \neq 0$:

$$\left(x + \frac{1}{x} + \sqrt{2}\right)^{12} = \sum_{k=0}^{24} c_k x^{k-12}.$$

Find the value of $\sum_{k=0}^{24}(-1)^k c_k^2$.

Korean Mathematical Olympiad, 2nd Round 2006

Solution. If we use the substitution $x \mapsto -\frac{1}{x}$, we find that

$$\left(x + \frac{1}{x} - \sqrt{2}\right)^{12} = \sum_{k=0}^{24} c_k(-1)^{k-12}x^{12-k} = \sum_{k=0}^{24} c_k(-1)^k x^{12-k}.$$

Multiplying this equality by the original equality, we get

$$\begin{aligned} \left(x + \frac{1}{x} + \sqrt{2}\right)^{12}\left(x + \frac{1}{x} - \sqrt{2}\right)^{12} &= \left(\left(x + \frac{1}{x}\right)^2 - 2\right)^{12} \\ &= \left(x^2 + \frac{1}{x^2}\right)^{12} \\ &= \left(\sum_{k=0}^{24} c_k x^{k-12}\right)\left(\sum_{k=0}^{24}(-1)^k c_k x^{k-12}\right). \end{aligned}$$

Examining the coefficient of x^0 in the last expression, we see that

$$[x^0]\left(\sum_{k=0}^{24} c_k x^{k-12}\right)\left(\sum_{k=0}^{24}(-1)^k c_k x^{k-12}\right) = \sum_{k=0}^{24}(-1)^k c_k^2$$

is exactly the sum we want. Thus the answer is the coefficient of x^0 in

$$\left(x^2 + \frac{1}{x^2}\right)^{12} = \frac{(x^4+1)^{12}}{x^{24}}$$

which is the same as the coefficient of x^{24} in the numerator. Since

$$(x^4 + 1)^{12} = \sum_{k=0}^{12}\binom{12}{k}x^{4k},$$

we obtain that the coefficient of x^{24} is $\binom{12}{6} = 924$, so $\sum_{k=0}^{24}(-1)^k c_k^2 = 924$. ■

1.3 On the roots of $x^d P\left(\frac{1}{x}\right)$

If $r \neq 0$ is a root of a polynomial $P(x)$, then it follows from $P(r) = 0$ that r^{-1} is a root of $x^d P\left(\frac{1}{x}\right)$. That is, the reciprocal polynomial removes zero from the roots of polynomial $P(x)$ and inverts the nonzero roots of $P(x)$. More precisely, we have the following.

Theorem

Let $\{r_1, \ldots, r_d\}$ be the set of nonzero roots of a polynomial $P(x)$ of degree d (taken with multiplicity). The set $\{r_1^{-1}, \ldots, r_d^{-1}\}$ is the set of roots of the reciprocal polynomial of $P(x)$.

Example 1.4. If the polynomial $ax^5 + bx^4 + c$ has exactly three real roots which are distinct, prove that the polynomial $cx^5 + bx + a$ has exactly three distinct real roots.

N. Aghakahanov - Russian Mathematical Olympiad, 3rd Round 2012

Solution. If $r = 0$ is a root of ax^5+bx^4+c, then $c = 0$. Hence the polynomial $ax^5+bx^4 = x^4(ax+b)$ has at most two distinct real roots. Thus the polynomial $ax^5 + bx^4 + c$ has three nonzero distinct real roots r, s, t. Finally, if we put $P(x) = ax^5 + bx^4 + c$, then $cx^5 + bx + a = x^5 P(1/x)$. Hence $1/r$, $1/s$, $1/t$ are all roots of $cx^5 + bx + a$. Furthermore, since the two remaining roots of $P(x)$ are non-real, the remaining roots of $cx^5 + bx + a$ are non-real too. ■

Example 1.5. Let $P(x)$ be the monic polynomial of degree 4 with roots 1, 2, 3, 4. Let $Q(x)$ be the monic polynomial of degree 4 with roots 1, 1/2, 1/3, 1/4. Find $\lim\limits_{x\to 1} \dfrac{P(x)}{Q(x)}$.

First Solution. Since the roots of $Q(x)$ and $P(x)$ are the inverse of each other, we have $Q(x) = Cx^4 P\left(\dfrac{1}{x}\right)$ for some $C \in \mathbb{R}$.

Note that $P(x) = x^4 + \ldots + a$. By Vieta's formulas, we can find that

$$a = 1 \cdot 2 \cdot 3 \cdot 4 = 24.$$

Hence

$$x^4 P\left(\frac{1}{x}\right) = 24x^4 + \ldots + 1.$$

Comparing the coefficient of x^4 in both sides of $Q(x) = Cx^4 P\left(\dfrac{1}{x}\right)$, we deduce that $24C = 1$, that is, $C = 1/24$. Thus $Q(x) = \dfrac{1}{24}x^4 P\left(\dfrac{1}{x}\right)$ and

$$\begin{aligned}
\frac{P(x)}{Q(x)} &= \frac{24P(x)}{x^4 P\left(\frac{1}{x}\right)} \\
&= \frac{24(x-1)(x-2)(x-3)(x-4)}{x^4\left(\frac{1}{x}-1\right)\left(\frac{1}{x}-2\right)\left(\frac{1}{x}-3\right)\left(\frac{1}{x}-4\right)} \\
&= \frac{24(x-1)(x-2)(x-3)(x-4)}{(1-x)(1-2x)(1-3x)(1-4x)} \\
&= -\frac{24(x-2)(x-3)(x-4)}{(1-2x)(1-3x)(1-4x)}
\end{aligned}$$

for all $x \neq 1$. Thus $\lim\limits_{x\to 1} \dfrac{P(x)}{Q(x)} = -24$. ■

Second Solution. From the hypotheses, we know that

$$P(x) = (x-1)(x-2)(x-3)(x-4)$$

and

$$Q(x) = (x-1)\left(x-\frac{1}{2}\right)\left(x-\frac{1}{3}\right)\left(x-\frac{1}{4}\right).$$

Hence,

$$\frac{P(x)}{Q(x)} = \frac{(x-2)(x-3)(x-4)}{\left(x-\frac{1}{2}\right)\left(x-\frac{1}{3}\right)\left(x-\frac{1}{4}\right)}.$$

Setting $x = 1$ in the previous equality, we get $\dfrac{P(1)}{Q(1)} = -24$. ■

Example 1.6. Let

$$P(x) = a_{2d}x^{2d} + a_{2d-1}x^{2d-1} + \ldots + a_1x + a_0$$

be a polynomial with roots $r_1, \ldots, r_{2d}$ such that for all $0 \leq i, j \leq 2d$ we have

$$2^i \frac{a_i}{a_{2d-i}} = 2^j \frac{a_j}{a_{2d-j}}.$$

Let $\sum_{\substack{i,j=1 \\ i \neq j}}^{2d} \frac{r_i}{r_j} = k$. Evaluate the sum of roots of polynomial $P(x)$.

Solution. For $j = d$, we find that $a_i = 2^{d-i}a_{2d-i}$. Hence $2^d a_i = 2^{2d-i}a_{2d-i}$. It follows that

$$2^d P(x) = x^{2d} P\left(\frac{2}{x}\right),$$

since looking at the coefficient of x^i gives exactly this equality. Thus if r is any root of $P(x)$, then $\frac{2}{r}$ is a root too. It is clear that

$$\sum_{\substack{i,j=1 \\ i \neq j}}^{2d} \frac{r_i}{r_j} = \left(\sum_{i=1}^{2d} r_i\right)\left(\sum_{i=1}^{2d} \frac{1}{r_i}\right) - 2d.$$

Moreover,

$$\sum_{i=1}^{2d} \frac{2}{r_i} = \sum_{i=1}^{2d} r_i.$$

Hence

$$k = \sum_{\substack{i,j=1 \\ i \neq j}}^{2d} \frac{r_i}{r_j} = \frac{1}{2}\left(\sum_{i=1}^{2d} r_i\right)^2 - 2d,$$

which gives

$$\sum_{i=1}^{2d} r_i = \pm\sqrt{2(k+2d)}.$$

■

1.4 Self-reciprocal polynomials

If we have a polynomial looking at its reciprocal polynomial may be helpful, but an even more intriguing application of reciprocal polynomials is polynomials that are their own reciprocal, that is, polynomials satisfying

$$P(x) = x^d P\left(\frac{1}{x}\right).$$

Such polynomials are called self-reciprocal polynomials. For example, the polynomial $x^2 + x + 1$ is self-reciprocal.
From the definition, we immediately get one characterization of self-reciprocal polynomials, they are polynomials that have a symmetry in their coefficients $a_d = a_0$, $a_{d-1} = a_1, \ldots$. This makes it easy to decide if a given polynomial is self-reciprocal, However for applications it is often convenient to have a more algebraic description. We will give two constructions of an algebraic characterization. The first is completely elementary, but uses a trick. The second uses the fundamental theorem of algebra.

Example 1.7. Give an algebraic characterization of all self-reciprocal polynomials $P(x)$ with real coefficients of degree d.

First Solution. First consider the case where d is even. In this case, writing

$$P(x) = a_d x^d + \ldots + a_1 x + a_0,$$

we find that $a_{d-i} = a_i$ for all $i = 0, 1, \ldots, \frac{d}{2}$. By factoring out $x^{\frac{d}{2}}$, we find that

$$P(x) = x^{\frac{d}{2}}\left(a_d\left(x^{\frac{d}{2}} + \frac{1}{x^{\frac{d}{2}}}\right) + \ldots + a_{\frac{d}{2}+1}\left(x + \frac{1}{x}\right) + a_{\frac{d}{2}}\right).$$

Since

$$x^{k+1} + \frac{1}{x^{k+1}} = \left(x + \frac{1}{x}\right)\left(x^k + \frac{1}{x^k}\right) - \left(x^{k-1} + \frac{1}{x^{k-1}}\right),$$

we see that $x^k + \frac{1}{x^k}$ can be represented as a polynomial in terms of $x + \frac{1}{x}$. That is, we can write $x^k + \frac{1}{x^k} = T_k\left(x + \frac{1}{x}\right)$ for some polynomial $T_k(x)$ with

real coefficients. (The formula above shows that recursively we can define T_k by $T_0(y) = 2$, $T_1(y) = y$, and $T_{k+1}(y) = yT_k(y) - T_{k-1}(y)$ for $k \geq 1$.) Hence

$$\begin{aligned} P(x) &= x^{\frac{d}{2}}\left(a_d T_{\frac{d}{2}}(x) + a_{d-1}T_{\frac{d}{2}-1}(x) + \ldots + a_{\frac{d}{2}}\right) \\ &= x^{\frac{d}{2}}Q\left(x+\frac{1}{x}\right) \end{aligned}$$

for some polynomial $Q(x)$ with real coefficients.
Now, if d is odd, setting $x = -1$ we find $P(-1) = (-1)^d P(-1) = -P(-1)$ so $P(-1) = 0$. Thus -1 is a root of P and hence we can write $P(x) = (x+1)P_1(x)$ for some polynomial $P_1(x)$ of degree $d-1$. Since P is self-reciprocal, we find that

$$\begin{aligned} (x+1)P_1(x) = P(x) &= x^d P\left(\frac{1}{x}\right) \\ &= x^d\left(\frac{1}{x}+1\right)P_1\left(\frac{1}{x}\right) \\ &= x^{d-1}(x+1)P_1\left(\frac{1}{x}\right) \end{aligned}$$

and hence

$$P_1(x) = x^{d-1}P_1\left(\frac{1}{x}\right),$$

so P_1 is also self-reciprocal. Thus by the even degree case applied to P_1, we see that

$$P(x) = x^{\frac{d-1}{2}}(x+1)R\left(x+\frac{1}{x}\right)$$

for some polynomial $R(x)$. ■

Second Solution. It is clear that 0 is not a root of polynomial $P(x)$ because otherwise the reciprocal polynomial would be of degree at most $d-1$, a contradiction. We have seen that if r is any root of $P(x)$, then $\frac{1}{r}$ is a root of the reciprocal polynomial, hence it is also a root of $P(x)$. It would be tempting at this point to say that we can collect the roots of P into pairs r_i and $\frac{1}{r_i}$. The one complication is that a root $r = \pm 1$ with $r = \frac{1}{r}$ might not be pairable.

Consider the case $r = 1$. Suppose 1 is a root of $P(x)$ with multiplicity k. Then we can write

$$P(x) = (x-1)^k P_1(x), \qquad P_1(1) \neq 0.$$

Since P is self-reciprocal, we find

$$(x-1)^k P_1(x) = x^d\left(\frac{1}{x}-1\right)^k P_1\left(\frac{1}{x}\right) = (-1)^k x^{d-k}(x-1)^k P_1\left(\frac{1}{x}\right)$$

hence

$$P_1(x) = (-1)^k x^{d-k} P_1\left(\frac{1}{x}\right).$$

Putting $x = 1$, we find that $P_1(1) = (-1)^k P_1(1)$. Since $P_1(1) \neq 0$ we conclude that k is even. Thus roots of 1 can be paired.
Thus we may assume the roots of P are -1, say with multiplicity s, and some number of pairs of roots r_i and $\frac{1}{r_i}$, $1 \leq i \leq k$. Since

$$(x-r_i)\left(x-\frac{1}{r_i}\right) = x^2 - \left(r_i + \frac{1}{r_i}\right)x + 1,$$

if we let C denote the leading coefficient of P, we get

$$P(x) = C(x+1)^s \prod_{i=1}^{k}\left(x^2 - \left(r_i+\frac{1}{r_i}\right)x + 1\right).$$

Writing this as

$$P(x) = Cx^k(x+1)^s \prod_{i=1}^{k}\left(x+\frac{1}{x} - \left(r_i+\frac{1}{r_i}\right)\right),$$

we see that the last expression can be written as $x^k(x+1)^s Q\left(x+\frac{1}{x}\right)$ for some polynomial $Q(x)$ with real coefficients of degree k and s, k, d are related by $d = s + 2k$. It is clear that all such polynomials satisfy the condition of the problem. ■

The astute reader will notice that the characterizations given in the two solutions do not quite match, but the difference is minor. Instead of pulling out all roots $r = 1$ of P, we could have paired as many as possible. This would have left us with two cases $s = 0$ or $s = 1$ corresponding to d even and d odd, respectively, and these would match the cases in the first solution. Equivalently, you can think of this as using the identity

$$(x+1)^2 = x\left(x + \frac{1}{x} - 2\right) \text{ to reduce } s.$$

These algebraic characterizations, particularly the second solution above, can be used to give a third characterization of self-reciprocal polynomials in terms of their roots. If $P(x)$ is a self-reciprocal polynomial of even degree, then the roots (taken with multiplicity) can be collected in pairs r, $1/r$, or equivalently we can assume the roots (with multiplicity) are $\{r_1, r_2, \ldots, r_{d/2}, 1/r_1, 1/r_2, \ldots, 1/r_{d/2}\}$. If $P(x)$ has odd degree, then there is one unpaired root of 1 and the remaining roots can be paired.

Self-reciprocal polynomial

Let $P(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0$ be a polynomial. If $P(x)$ satisfies the relation $P(x) = x^d P\left(\frac{1}{x}\right)$, we say that $P(x)$ is a *self-reciprocal polynomial*. Furthermore, if $P(x)$ is a self-reciprocal polynomial, its coefficients satisfy

$$a_k = a_{d-k} \qquad \forall k = 0, 1, \ldots, d$$

and there is a polynomial $Q(x)$ such that

$$P(x) = x^k (x+1)^{d-2k} Q\left(x + \frac{1}{x}\right),$$

where $\deg Q(x) = k$. If the degree d is even, then the roots of $P(x)$, taken with multiplicity, can be written as $\{r_1, r_2, \ldots, r_{d/2}, 1/r_1, 1/r_2, \ldots, 1/r_{d/2}\}$. If d is odd, then they can be written as $\{1, r_1, r_2, \ldots, r_{(d-1)/2}, 1/r_1, 1/r_2, \ldots, 1/r_{(d-1)/2}\}$.

Example 1.8. Characterize all polynomials $P(x)$ of degree d with real coefficients satisfying the following relations:

(i) $P(x) = -x^d P\left(\frac{1}{x}\right)$;

(ii) $P(x) = x^d P\left(-\frac{1}{x}\right)$.

Solution. As in the case of self-reciprocal polynomials, there are two sorts of characterizations we could give, either an explicit characterization in terms of the coefficients or an algebraic characterization.
If we write $P(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, then taking the coefficient of x^k in (i) gives

$$a_k = -a_{d-k} \qquad \forall k = 0, 1, \ldots, d$$

and in (ii) gives

$$a_k = (-1)^{d-k} a_{d-k} \qquad \forall k = 0, 1, \ldots, d.$$

Note that in part (ii), setting k to $d-k$ we also get $a_{d-k} = (-1)^k a_k$ and hence $a_k = (-1)^k a_{d-k}$. Hence d must be even.
We now turn to the algebraic characterizations.

(i) It is clear that $P(1) = 0$. Setting $P(x) = (x-1)^r P_1(x)$, where $P_1(1) \neq 0$, we find that

$$(x-1)^r P_1(x) = (-1)^{r+1} x^{d-r} (x-1)^r P_1\left(\frac{1}{x}\right),$$

i.e.,

$$P_1(x) = (-1)^{r+1} x^{d-r} P_1\left(\frac{1}{x}\right) \qquad \forall x \in \mathbb{R}.$$

Putting $x = 1$, we get $P_1(1) = (-1)^{r+1} P_1(1)$. Since $P_1(1) \neq 0$, we deduce that $r+1$ is even, so $P_1(x) = x^{d-r} P_1\left(\frac{1}{x}\right)$, that is P_1 is a self-reciprocal polynomial of degree $d-r$. From Example 1.7, we conclude that

$$P_1(x) = x^k (x+1)^{d-r-2k} Q\left(x + \frac{1}{x}\right)$$

and hence

$$P(x) = x^k(x-1)^r(x+1)^{d-r-2k}Q\left(x+\frac{1}{x}\right)$$

for some polynomial $Q(x)$ of degree k with real coefficients and some odd positive integer r. It is easy to see that all such polynomials satisfy the problem conditions.

(ii) Using the substitution $x \mapsto -1/x$, we have $P\left(-\frac{1}{x}\right) = \frac{P(x)}{(-1)^d x^d}$.

On the other hand, we know that $P\left(-\frac{1}{x}\right) = \frac{P(x)}{x^d}$. Therefore d is even. Moreover, if r is a root of $P(x)$, then also $-1/r$ is a root with the same multiplicity. As in the second solution to Example 1.7, we can collect the roots not equal to $\pm i$ into pairs r_j and $-\frac{1}{r_j}$, for $1 \le j \le k$. Since P has real coefficients the multiplicities of i and $-i$ as roots must be the same, hence they are $(d-2k)/2$. Since

$$(x-r)\left(x+\frac{1}{r}\right) = x^2 - \left(r-\frac{1}{r}\right)x - 1 = x\left(x-\frac{1}{x}-\left(r-\frac{1}{r}\right)\right),$$

if we let C be the leading coefficient of P, we have

$$\begin{aligned} P(x) &= C(x^2+1)^{(d-2k)/2}\prod_{i=1}^{k}\left(x^2-\left(r_i-\frac{1}{r_i}\right)x-1\right) \\ &= Cx^k(x^2+1)^{(d-2k)/2}\prod_{i=1}^{k}\left(x-\frac{1}{x}-\left(r_i-\frac{1}{r_i}\right)\right) \\ &= Cx^k(x^2+1)^{(d-2k)/2}Q\left(x-\frac{1}{x}\right) \end{aligned}$$

for some polynomial $Q(x)$ of degree k with real coefficients. ■

Example 1.9. Let $P(x) = a_n x^n + \ldots + a_0$ be a nonzero polynomial with complex coefficients and let $\lambda \in \mathbb{C}$.
We say that $P(x)$ is λ-*reciprocal* if $a_{n-i} = \lambda a_i$ for all $i = 0, 1, \ldots, n$.

(i) Prove that if a polynomial is λ-reciprocal, then $\lambda \in \{-1, 1\}$.

(ii) If $P(x)$ is λ-reciprocal and $Q(x)$ is μ-reciprocal, prove that $PQ(x)$ is $\lambda\mu$-reciprocal ($\lambda, \mu \in \{-1, 1\}$).

Marcel Ţena - Gazeta Matematică B 8/2007, *Problem* C:3205

Solution. **(i)** Let $a_i \in \mathbb{C}$ be a nonzero coefficient of $P(x)$. Then

$$a_i = a_{n-(n-i)} = \lambda a_{n-i} = \lambda(\lambda a_i) = \lambda^2 a_i,$$

so $\lambda^2 = 1$, which gives $\lambda \in \{-1, 1\}$.

(ii) It is clear that a polynomial $P(x)$ of degree n is λ-reciprocal if and only if $\lambda P(x) = x^n P\left(\frac{1}{x}\right)$, i.e.,

$$P\left(\frac{1}{x}\right) = \frac{\lambda P(x)}{x^n}.$$

Likewise, a polynomial $Q(x)$ of degree m is μ-reciprocal if and only if

$$Q\left(\frac{1}{x}\right) = \frac{\mu Q(x)}{x^m}.$$

Multiplying side by side the last two equations, we get

$$PQ\left(\frac{1}{x}\right) = P\left(\frac{1}{x}\right)Q\left(\frac{1}{x}\right) = \frac{\lambda\mu P(x)Q(x)}{x^{n+m}} = \frac{\lambda\mu PQ(x)}{x^{n+m}}$$

and since $PQ(x)$ has degree $n+m$, then $PQ(x)$ is $\lambda\mu$-reciprocal. ■

Example 1.10. Assume that the polynomial $P(x) = x^4 + ax^3 + bx^2 + ax + 1$ has two real roots whose product is -1. Find the range of a and b.

Solution. Let r and s be the roots with $rs = -1$ and note that this forces $r \neq \frac{1}{s}$ and since r and s are real, it also forces $r \neq s$. Note that P is a self-reciprocal polynomial of even degree, so the roots can be collected into pairs

of reciprocals. Hence the four roots of P with multiplicity will be $r, s, \frac{1}{r}, \frac{1}{s}$. By Vieta's formulas,

$$r+s+\frac{1}{r}+\frac{1}{s}=-a, \qquad 2+rs+\frac{1}{rs}+\frac{r}{s}+\frac{s}{r}=b.$$

Thus

$$\frac{(r+s)(rs+1)}{rs}=-a, \qquad rs+\frac{(r+s)^2+1}{rs}=b.$$

Since $rs=-1$, we get

$$a=0, \qquad b=-(r+s)^2-2=-\left(r-\frac{1}{r}\right)^2-2\leq -2.$$

Then $P(x)=x^4+bx^2+1$ and $b\leq -2$. ■

Example 1.11. Let $n>1$ be an integer. Prove that the polynomial

$$P(x)=x^n-x^{n-1}-\ldots-x-1$$

has exactly one positive real root.

Solution. Consider the polynomial

$$Q(x)=-x^nP\left(\frac{1}{x}\right)=x^n+x^{n-1}+\ldots+x-1.$$

It is clear that the right-hand side is a strictly increasing function if $x>0$. Therefore it cuts every horizontal line at most once. This means that $Q(x)$ has at most one positive real root and so also $P(x)$ has at most one positive real root. Since $Q(0)=-1<0$ and $Q(1)=n-1>0$, we deduce that $Q(x)$ has exactly one real root in the interval $(0,1)$. Furthermore, since the map $x\mapsto \frac{1}{x}$ doesn't change the sign of the roots, we obtain that the polynomial $P(x)$ has exactly only one positive real root (greater than 1). ■

1.5 Miscellaneous problems

In this section, we provide some relatively hard examples concerning reciprocal polynomials. In most of them, you must consider the following steps.

Strategy

(i) Define the right polynomial.

(ii) Consider its reciprocal polynomial.

(iii) Work on its roots or its coefficients.

Example 1.12. Find all polynomials with real coefficients of the form

$$f(x)=x^{2n}+a_1x^{2n-1}+\ldots+a_{n-1}x^{n+1}+a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+1$$

having $2n$ real roots and such that $|a_i|\leq 2$ for all $i=1,2,\ldots,n$.

Plamen Penchev - Bulgarian Team Selection Test 2015

Solution. Since $f(x)$ is a self-reciprocal polynomial of even degree, we can let $x_1,\ldots,x_n,\frac{1}{x_1},\ldots,\frac{1}{x_n}$ be the roots of $f(x)$. We can write $f(x)=g(x)h(x)$, where

$$g(x)=(x-x_1)\cdot\ldots\cdot(x-x_n)$$

and

$$h(x)=\left(x-\frac{1}{x_1}\right)\cdot\ldots\cdot\left(x-\frac{1}{x_n}\right).$$

Thus by Vieta's formulas

$$g(x)=x^n+b_1x^{n-1}+\ldots+b_{n-1}x+b_n, \qquad h(x)=x^n+\frac{b_{n-1}}{b_n}x^{n-1}+\ldots+\frac{b_1}{b_n}x+\frac{1}{b_n}.$$

Hence

$$|a_n|=\left|b_n+\frac{1}{b_n}+\frac{b_1^2+\ldots+b_{n-1}^2}{b_n}\right|\leq 2,$$

i.e.,

$$-2 \leq b_n + \frac{1}{b_n} + \frac{b_1^2 + \ldots + b_{n-1}^2}{b_n} \leq 2.$$

Hence

$$\left(\sqrt{|b_n|} - \frac{1}{\sqrt{|b_n|}}\right)^2 + \frac{b_1^2 + \ldots + b_{n-1}^2}{|b_n|} \leq 0.$$

So we must have $b_1 = \ldots = b_{n-1} = 0$ and $b_n = \pm 1$. Therefore the only possible polynomials have the form $(x^n \pm 1)^2$, where n is a positive integer. The roots of these are the n-th roots of ∓ 1, which are complex if $n \geq 3$ or if $n = 2$ and we have the upper sign. Thus the only possibilities are $(x-1)^2$, $(x+1)^2$, and $(x^2-1)^2$.
If we interpret the hypothesis of $2n$ real roots as meaning we count the roots with multiplicity, then these are solutions. If we interpret the hypothesis as meaning $2n$ distinct roots, then there are no such polynomials. ■

Example 1.13. Let $a \in \mathbb{Z} \setminus \{0\}$. Prove that $P(x) = x^n + ax^{n-1} + \ldots + ax - 1$ (where all central coefficients are a) is irreducible over $\mathbb{Z}[x]$.

Marian Andronache and Ian Savu - Romanian Team Selection Test 1990

Solution. Note that

$$-x^n P\left(\frac{1}{x}\right) = x^n - ax^{n-1} - \ldots - ax - 1.$$

Hence by working with the negated reciprocal polynomial if necessary, we can assume $a > 0$. Since $P(0) = -1 < 0$ and $P(1) = (n-1)a > 0$, $P(x)$ has at least one real root r in the interval $(0,1)$. Writing

$$P(x) = (x-r)\left(x^{n-1} + b_{n-2}x^{n-2} + \ldots + \frac{1}{r}\right),$$

we can find that $b_{n-2} = r + a, b_{n-3} = rb_{n-2} + a = a + ar + r^2$ and so on. It is easy to see that $1 < b_{n-2} < b_{n-3} < \ldots < \frac{1}{r}$. We need the following lemma.

Lemma 1.1 *Let $Q(x) = a_d x^d + \ldots + a_0$ with $0 < a_d < a_{d-1} < \ldots < a_0$. Then all of the roots of polynomial $Q(x)$ have modulus greater than 1.*

Proof. Note that $(x-1)Q(x) = a_d x^{d+1} + (a_{d-1} - a_d)x^d + \ldots - a_0$. It is clear that $r = 1$ is not a root of $Q(x)$. Suppose that $r \neq 1$ is a root of $Q(x)$. Then

$$a_0 = a_d r^{d+1} + (a_{d-1} - a_d)r^d + \ldots + (a_0 - a_1)r.$$

Thus

$$\begin{aligned} |a_0| &= |a_d r^{d+1} + (a_{d-1} - a_d)r^d + \ldots + (a_0 - a_1)r| \\ &\leq |a_d| \cdot |r|^{d+1} + \ldots + |a_0 - a_1| \cdot |r|. \end{aligned}$$

Assume that $|r| \leq 1$. Then we get

$$a_0 = |a_0| \leq a_d + a_{d-1} - a_d + \ldots + a_0 - a_1 = a_0.$$

Thus we must have equality in every step. This means we have $|r| = 1$ and all the complex numbers $a_d r^d, \ldots, (a_1 - a_2)r^2, (a_0 - a_1)r$ must have the same argument. In particular, $\frac{a_1 - a_2}{a_0 - a_1} r$ must be a positive real number. Hence r must be positive and this together with $|r| = 1$ gives $r = 1$. Since we already saw that $r \neq 1$, this is a contradiction. This completes our proof. ❑

Coming back to our problem, note that applying the Lemma to $\frac{P(x)}{x-r}$ shows that r is the only root of P of modulus at most 1. Assume that $P(x) = Q(x)R(x)$ for some nonconstant polynomials $Q(x)$ and $R(x)$ with integer coefficients. Without loss of generality we can assume that $Q(x)$ and $R(x)$ are monic. Since $Q(0)R(0) = 1$, we conclude that $Q(0) = R(0) = \pm 1$. Thus the product of roots of $Q(x)$ is ∓ 1. Hence Q has at least one root with modulus at most 1. Hence r must be a root of Q. But the same argument could have been made for $R(x)$ and r cannot be a root of both, giving a contradiction. ■

Remark. By the above result, we can prove some hard but interesting problems. The following problem appeared in the American Mathematical Monthly in 1988, which is the particular case of the above problem with $a = -1$.

Prove that the polynomial $P(x) = x^n - x^{n-1} - \ldots - x - 1$ *is irreducible.*

We continue this section with a good number theory problem.

Example 1.14. Let $n \geq 2$ be an integer and let

$$P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + 1$$

be a polynomial with positive integer coefficients such that $a_k = a_{n-k}$ for all $k = 1, 2, \ldots, n-1$. Prove that there exist infinitely many pairs of positive integers (x, y) such that $x \mid P(y)$ and $y \mid P(x)$.

Remus Nicoară - Romanian Team Selection Test 1997

Solution. Since $1 \mid P(P(1))$ and $P(1) \mid P(1)$, we see that $(1, P(1))$ satisfies the conditions. Now, assume (x, y) with $x \leq y$ satisfies the conditions. We will prove that $\left(y, \frac{P(y)}{x}\right)$ also satisfies the problem condition. First, since $x \mid P(y)$, $\frac{P(y)}{x}$ is an integer and clearly $\frac{P(y)}{x} \mid P(y)$. Now we only have to prove that $y \mid P\left(\frac{P(y)}{x}\right)$. Since

$$x \mid P(y) = y^n + a_{n-1}y^{n-1} + \ldots + a_1 y + 1,$$

we conclude that $\gcd(x, y) = 1$. So x has a multiplicative inverse modulo y, i.e., there exists $\frac{1}{x}$ modulo y. Since $P(y) \equiv 1 \pmod{y}$, we find that

$$P\left(\frac{P(y)}{x}\right) \equiv P\left(\frac{1}{x}\right) \pmod{y}.$$

Moreover, the polynomial $P(x)$ satisfies the relation $x^n P\left(\frac{1}{x}\right) = P(x)$. Multiplying both sides of the above congruence by x^n, we get:

$$x^n P\left(\frac{P(y)}{x}\right) \equiv x^n P\left(\frac{1}{x}\right) = P(x) \equiv 0 \pmod{y}.$$

Hence $y \mid x^n P\left(\frac{P(y)}{x}\right)$ and since $\gcd(x, y) = 1$, we obtain that $y \mid P\left(\frac{P(y)}{x}\right)$. So $\left(y, \frac{P(y)}{x}\right)$ is a pair satisfying the condition. Finally note that

$$P(y) \geq 1 + y^n > y^2 \geq xy,$$

so $\frac{P(y)}{x} > y$. Thus we from any pair satisfying the problem condition, we can produced a new such pair with larger maximal entry. Clearly we can iterate this indefinitely to give infinitely many pairs. ■

Next problem has an interesting story. Navid Safaei worked on it during the time he prepared a team for the International Mathematics Competition (IMC), a competition addressed to university students.

Example 1.15. Let $P(x) = dx^d - x^{d-1} - x^{d-2} - \ldots - x - 1$. Prove that $P(x)$ has d distinct roots, and except for the root at 1, all with modulus less than 1.

Solution. Note that

$$(x-1)P(x) = dx^{d+1} - (d+1)x^d + 1.$$

Assume that there exists a root r with multiplicity greater than 1. Then we must have $P(r) = P'(r) = 0$. Therefore by differentiating both sides of the previous equation, we get

$$\begin{aligned}(x-1)P'(x) + P(x) &= d(d+1)x^d - d(d+1)x^{d-1} \\ &= d(d+1)x^{d-1}(x-1).\end{aligned}$$

Putting $x = r$, we find that $r^{d-1}(r-1) = 0$. Hence $r = 0, 1$. It remains only to check $r = 1$, but

$$P'(1) = d^2 - (d-1+d-2+\ldots+1) = d^2 - \frac{d(d-1)}{2} = \frac{d^2+d}{2} > 0.$$

Therefore we have no multiple roots. Now, we will show that all the roots of $P(x)$ except 1 have modulus less than 1. Consider the polynomial

$$-x^d P\left(\frac{1}{x}\right) = x^d + x^{d-1} + \ldots + x - d.$$

We prove that all of the roots $z \neq 1$ of this polynomial satisfy the inequality $|z| > 1$. Assume the contrary. Then there is at least one root such that $|z| \leq 1$. Hence

$$d = z^d + z^{d-1} + \ldots + z,$$

which gives

$$\begin{aligned} d = |z^d + z^{d-1} + \ldots + z| &\leq |z^d| + |z^{d-1}| + \ldots + |z| \\ &= |z|^d + |z|^{d-1} + \ldots + |z| \\ &\leq d. \end{aligned}$$

Thus equality must hold in every step above. For the first inequality this says that $z, z^2, \ldots, z^d$ lie on a ray from the origin. For the second inequality, this says they all have modulus 1. Hence $\frac{z^2}{z} = z$ must be positive real number with modulus 1, therefore $z = 1$ and we are done. ■

1.6 Proposed problems

Problem 1.1. Let $a_1, \ldots, a_n$ be natural numbers whose sum is 2020. Find the least positive real number t such that the equation

$$\sum_{i=1}^{n} \frac{a_i x^i}{1 + x^{2i}} = t.$$

has only one positive real root.

Problem 1.2. Let $a_0 + a_1 x + a_2 x^2 + \ldots + a_{2n} x^{2n}$ be the polynomial obtained expanding $(1 + x + x^2)^n$. Compute:

(i) $a_0 + a_2 + \ldots + a_{2n}$;

(ii) $a_1 + a_3 + \ldots + a_{2n-1}$;

(iii) $a_0 a_1 - a_1 a_2 + a_2 a_3 - \ldots - a_{2n-1} a_{2n}$.

Italian Mathematical Olympiad 1994

Problem 1.3. Let $P(x) = a_n x^n + \ldots + a_0$ be a nonzero polynomial with complex coefficients. We say that $P(x)$ is *reciprocal* if $a_k = a_{n-k}$ for all $k \in \{0, 1, \ldots, n\}$ or $a_k = -a_{n-k}$ for all $k \in \{0, 1, \ldots, n\}$. To each such polynomial we associate the symbol $[P(x)]$ defined as follows: $[P(x)] = 1$ if $a_k = a_{n-k}$ for all $k \in \{0, 1, \ldots, n\}$ and $[P(x)] = -1$ if $a_k = -a_{n-k}$ for all $k \in \{0, 1, \ldots, n\}$.

(a) Prove that if $P(x)$ and $Q(x)$ are reciprocal, then $PQ(x)$ is reciprocal and $[PQ(x)] = [P(x)][Q(x)]$.

(b) Prove that if $P(x)$ and $PQ(x)$ are reciprocal, then $Q(x)$ is reciprocal and $[Q(x)] = \dfrac{[PQ(x)]}{[P(x)]}$.

Marcel Țena - Nicolae Teodorescu Competition 2007

Problem 1.4. A self-reciprocal polynomial

$$P(x) = \sum_{j=0}^{d} a_j x^j$$

satisfies $a_1 = a_{d-1}$, $a_2 = a_{d-2}, \ldots, a_d = a_0$. Consider all the self-reciprocal polynomials with integer coefficients that are factors of $x^{1234} - x^3 - x + 1$. Find the factor that has the largest degree.

Problem 1.5. If the monic polynomial

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

has all its roots $x_1, x_2, \ldots, x_n$ in the interval $[-1, 1]$ and its coefficients satisfy the property $a_{n-i} = a_i$, $i = 0, 1, \ldots, n$, prove that $f(x) = (x+1)^p(x-1)^{2q}$, where $p, q \in \mathbb{N}$ and $p + 2q = n$.

Marcel Țena - Gazeta Matematică B 5/2009, *Problem* 26158

Problem 1.6. Let

$$P(x) = a_{2n}x^{2n} + a_{2n-1}x^{2n-1} + \ldots + a_0$$

such that $a_k = a_{2n-k}$ for $k = 0, 1, \ldots, n$.

(i) Prove that there exists a polynomial Q such that

$$P(x) = x^n Q\left(x + \frac{1}{x}\right).$$

(ii) If $a_0 = a_{2n} = 1$ and $|a_n| < 2$, prove that $P(x)$ has at least one complex root.

Romanian Mathematical Olympiad

Problem 1.7. Let $P(x) = a_d x^d + \ldots + a_1 x + a_0$ and define

$$C(P(x)) = a_d^2 + a_{d-1}^2 + \ldots + a_1^2 + a_0^2.$$

Let $P(x) = 3x^2 + 7x + 2$. Find a polynomial $Q(x)$ with real coefficients such that $Q(0) = 1$ and $C((P(x))^n) = C((Q(x))^n)$ for every positive integer n.

Problem 1.8. Find all positive integers n for which there is a polynomial $P(x)$ with real coefficients satisfying $P(x^{1998} - x^{-1998}) = x^n - x^{-n}, \forall x \neq 0$.

Vietnamese Mathematical Olympiad 1998

Problem 1.9. Let $n \not\equiv 2 \pmod 3$.
Prove that the polynomial $P(x) = x^n + x + 1$ is irreducible over $\mathbb{Z}[x]$.

Problem 1.10. Let n be an even positive integer, and let $c_1, \ldots, c_n$ be real numbers such that

$$\sum_{i=1}^{n} |c_i - 1| < 1.$$

Prove that the polynomial

$$P(x) = 2x^n - c_{n-1}x^{n-1} + c_{n-2}x^{n-2} - \ldots - c_1 x + 2$$

has no real roots.

Po Shen Loh - USA Team Selection Test 2014

Problem 1.11. Let $a_1, \ldots, a_n$ be complex numbers with modulus $r > 0$. Denote by T_s the sum of products of any s numbers from $a_1, \ldots, a_n$. Assume that $T_{n-s} \neq 0$. Prove that $\left|\frac{T_s}{T_{n-s}}\right| = r^{2s-n}$.

Problem 1.12. For a polynomial $P(x) = b_d x^d + \ldots + b_0$, we define the BB-sum of $P(x)$ as the number $b_0b_1 + b_1b_2 + \ldots + b_{d-1}b_d$. Determine whether there exist real numbers r and s such that for every positive integer k, the BB-sum of $(x^2 + rx + s)^k$ is equal to the BB-sum of $(2x^2 + 7x + 3)^k$.

Problem 1.13. Let $P(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0$ be a polynomial of degree $d \geq 3$ with integer coefficients such that $a_k + a_{d-k}$ is even for $k = 1, 2, \ldots, d-1$ and a_0 is also even. If $P(x) = Q(x)R(x)$, where $R(x)$ and $Q(x)$ are nonconstant polynomials with integer coefficients and $\deg Q(x) \leq \deg R(x)$ and all the coefficients of $R(x)$ are odd, show that $P(x)$ has at least one integer root.

Chapter 2

Complex Numbers and Polynomials. Part I

2.1 There are numbers that are not real

The existence of non-real numbers was first discovered by the Italian mathematician Gerolamo Cardano around 1545 in studying cubic equations. However, this new family of numbers was not fully understood until the end of the 18-th century.

The original motivation for complex numbers was solving polynomial equations. (Even if a cubic equation has three real roots, one may need complex numbers to express these roots by radicals.) Dealing with these new numbers was challenging for scholars (partly because of bad notation and incorrect assumptions). Finding a well-defined framework for the arithmetic of complex numbers therefore took a long time and involved many of the biggest names in 17th and 18th century mathematics.

Complex number

Let $a, b \in \mathbb{R}$. A *complex number* is a number of the form $a + ib$, where $i^2 = -1$. We usually denote a complex number by z, i.e.,

$$z = a + ib.$$

If $a = 0$, we say that the number $z = ib$ is an *imaginary number*.

2.2 Basic properties of complex numbers

We denote the set of complex numbers by $\mathbb{C}$, that is

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}, i^2 = -1\}.$$

Definition 2.1 Let $z = a + ib$ be a complex number. The real numbers a and b are said *real part* and *imaginary part* of z, respectively, and we denote

$$a = \mathrm{Re}(z), \qquad b = \mathrm{Im}(z).$$

Definition 2.2 Let $z = a + ib$ and $w = c + id$ be complex numbers. The sum $z + w$ is defined naturally by

$$z + w = (a + ib) + (c + id) = (a + c) + i(b + d)$$

By replacing w with $-w$, we obtain the difference of two complex numbers

$$z - w = (a + ib) - (c + id) = (a - c) + i(b - d)$$

Clearly, $z = a + ib$ is a real number if and only if $b = 0$. It follows that if $z = a + ib$ and $w = c + id$, then

$$z = w \iff z - w = 0 \iff (a - c) + i(b - d) = 0 \iff a = c,\ b = d.$$

Definition 2.3 Let $z = a + ib$ and $w = c + id$ be two complex numbers. The product $z \cdot w$ is defined by using the distributive law and the relation $i^2 = -1$, i.e.,

$$z \cdot w = (a + ib)(c + id) = ac + iad + ibc + i^2bd = (ac - bd) + i(ad + bc)$$

Now, let $z = a + ib \neq 0$ be a complex number. The number

$$\frac{1}{z} = \frac{1}{a + ib} = \frac{1}{a + ib} \cdot \frac{a - ib}{a - ib} = \frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2}$$

is said to be the *inverse* of z. So we can define the quotient of two complex numbers $z = a + ib$ and $w = c + id$ $(w \neq 0)$ as

$$\frac{z}{w} = z \cdot \frac{1}{w} = (a + ib)\left(\frac{c}{c^2 + d^2} - i\frac{d}{c^2 + d^2}\right) = \frac{ac + bd}{c^2 + d^2} + i\frac{bc - ad}{c^2 + d^2}.$$

Definition 2.4 Let $z = a + ib$ be a complex number. We define the *conjugate* of z as

$$\overline{z} = a - ib.$$

Observe that the conjugate $\overline{z}$ of a complex number z when added by z or multiplied by z produces a real number. Indeed, $z + \overline{z} = 2a = 2\mathrm{Re}(z)$ and $z \cdot \overline{z} = a^2 + b^2$.

The complex conjugate is the extension of the conjugate in radical expressions (i.e., $a - b\sqrt{d}$ is the conjugate of $a + b\sqrt{d}$).

Properties of conjugation

For all $z, w \in \mathbb{C}$, we have:
(i) $\overline{z+w} = \overline{z} + \overline{w}$;
(ii) $\overline{z-w} = \overline{z} - \overline{w}$;
(iii) $\overline{zw} = \overline{z} \cdot \overline{w}$;
(iv) $\overline{z^n} = \overline{z}^n$ for all $n \in \mathbb{N}$;
(v) if $z \neq 0$, $\overline{\left(\frac{1}{z}\right)} = \frac{1}{\overline{z}}$;
(vi) if $w \neq 0$, $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$;
(vii) $\overline{(\overline{z})} = z$.

Definition 2.5 Let $z = a + ib$ be a complex number. We define the *modulus* of z as the real number

$$|z| = \sqrt{a^2 + b^2}.$$

The modulus is a multiplicative function (i.e., $|zw| = |z| \cdot |w|$) and, as we will see, is the extension of the absolute value on the real line.

Properties of the modulus

Let $z, w \in \mathbb{C}$. Then:
(i) $-|z| \leq \mathrm{Re}(z) \leq |z|$, $-|z| \leq \mathrm{Im}(z) \leq |z|$;
(ii) $|z| \geq 0$ for all $z \in \mathbb{C}$. Moreover, $|z| = 0$ if and only if $z = 0$;
(iii) $|z| = |-z| = |\overline{z}|$;
(iv) $z\overline{z} = |z|^2$;
(v) $|zw| = |z| \cdot |w|$;
(vi) if $z \neq 0$, then $\left|\frac{1}{z}\right| = \frac{1}{|z|}$;
(vii) if $w \neq 0$, then $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$.

2.3 Using conjugation

Let

$$P(x) = a_d x^d + \ldots + a_0$$

be a polynomial with real coefficients. Since real numbers are there own conjugates, using the properties of the conjugate, we get the following important fact:

$$\begin{aligned} P(\overline{z}) &= a_d\overline{z}^d + \ldots + a_1\overline{z} + a_0 \\ &= \overline{a_d z^d} + \ldots + \overline{a_1 z} + \overline{a_0} \\ &= \overline{a_d z^d + \ldots + a_1 z + a_0} \\ &= \overline{P(z)}. \end{aligned}$$

Proceeding from this fact, we arrive at this great implication:

$$P(z)P(\overline{z}) = P(z)\overline{P(z)} = |P(z)|^2.$$

Example 2.1. Let $P(x)$ be a polynomial with real coefficients. If $P(1+i) = 5 - 6i$, then $P(1-i) = 5 + 6i$.

Example 2.2. Let $\omega = \frac{-1+i\sqrt{3}}{2}$ and $P(x) = ax - b$. Then

$$P(\omega)P(\overline{\omega}) = (a\omega - b)(a\overline{\omega} - b) = a^2\omega \cdot \overline{\omega} - ab(\omega + \overline{\omega}) + b^2.$$

Since $\omega \cdot \overline{\omega} = |\omega|^2 = 1$ and $\omega + \overline{\omega} = -1$, we find that

$$P(\omega)P(\overline{\omega}) = a^2 + ab + b^2.$$

On the other hand $P(\omega) = \frac{-a-2b}{2} + i\left(\frac{a\sqrt{3}}{2}\right)$. Hence

$$|P(\omega)|^2 = \frac{1}{4}(a+2b)^2 + \frac{3}{4}a^2.$$

Thus we find that

$$a^2 + ab + b^2 = \frac{1}{4}(a+2b)^2 + \frac{3}{4}a^2.$$

Example 2.3. Prove following identity:

$$(a^2+ab+b^2)(b^2+bc+c^2)(a^2+ac+c^2)$$

$$=(a^2b+b^2c+c^2a)^2+(b^2a+c^2b+a^2c)^2+(a^2b+b^2c+c^2a)(b^2a+c^2b+a^2c).$$

Solution. Define $P(t)=(ta-b)(tb-c)(tc-a)$. Then by Example 2.2, it follows that

$$P(\omega)P(\overline{\omega})=(a^2+ab+b^2)(b^2+bc+c^2)(a^2+ac+c^2).$$

On the other hand

$$P(t)=abct^3-(a^2b+b^2c+c^2a)t^2+(b^2a+c^2b+a^2c)t-abc.$$

Since $\omega^3=1$, we find that

$$P(\omega)=-(a^2b+b^2c+c^2a)\omega^2+(b^2a+c^2b+a^2c)\omega.$$

Hence using Example 2.2 again

$$\begin{aligned}|P(\omega)|^2 &= |-(a^2b+b^2c+c^2a)\omega^2+(b^2a+c^2b+a^2c)\omega| \\ &= |(b^2a+c^2b+a^2c)-(a^2b+b^2c+c^2a)\omega|^2 \\ &= (a^2b+b^2c+c^2a)^2+(b^2a+c^2b+a^2c)^2 \\ &\quad +(a^2b+b^2c+c^2a)(b^2a+c^2b+a^2c).\end{aligned}$$

■

2.4 Using the modulus, argument, real and imaginary part of a complex number

Your existing knowledge about complex numbers underpins your future readings on this topic.

Example 2.4. Find the complex number ω with modulus 1 which maximizes the modulus of

$$z=(\omega+2)^3(\omega-3)^2.$$

Solution. Let $\omega+\overline{\omega}=2\,\mathrm{Re}(\omega)=t$. Let a be a real number. It is clear that

$$|\omega-a|^2=(\omega-a)(\overline{\omega}-a)=1+a^2-at.$$

Hence

$$|z|^2=(|\omega+2|^2)^3\cdot(|\omega-3|^2)^2=(5+2t)^3\cdot(10-3t)^2.$$

Now, our goal is to maximize $(5+2t)^3\cdot(10-3t)^2$. By AM-GM Inequality, we find that

$$(5+2t)^3\cdot(10-3t)^2\le\left(\frac{3(5+2t)+2(10-3t)}{5}\right)^5=7^5.$$

Thus $|z|\le 7^{\frac{5}{2}}$. The equality occurs when $5+2t=10-3t$, i.e., when $t=1$, yielding $\mathrm{Re}(\omega)=\frac{1}{2}$. This implies that $\omega=\frac{1\pm i\sqrt{3}}{2}$. ■

Example 2.5. Find all complex numbers z with modulus 1 such that

$$\sum_{k=1}^{1006}|z^{2k+1}-z^{2k}|=\sum_{k=1}^{1006}|z^{2k}-z^{2k-2}|.$$

Solution. Note that

$$|z^{2k+1}-z^{2k}|=|z^{2k}|\cdot|z-1|=|z-1|,$$

and

$$|z^{2k}-z^{2k-2}|=|z^{2k-2}|\cdot|z^2-1|=|z^2-1|.$$

Therefore the statement of the problem is reduced to finding z such that

$$|z-1|=|z^2-1|=|z-1|\cdot|z+1|.$$

Thus we need either $|z-1|=0$ (which gives $z=1$) or $|z+1|=1$. Since z has modulus 1, we have $\overline{z}=1/z$. Therefore

$$|z+1|^2=(z+1)\left(\frac{1}{z}+1\right)=2+z+\frac{1}{z}$$

and therefore this becomes $z^2+z+1=0$, hence $z=\frac{-1\pm i\sqrt{3}}{2}$. Thus we have three solutions: $z=1$, $\frac{-1\pm i\sqrt{3}}{2}$.
There is also a geometric solution to the last step of this problem using the interpretation of the complex numbers as the plane discussed in the next section. The numbers of modulus 1 are the unit circle centered at 0 and the solutions to $|z+1|=1$ is the unit circle centered at -1. The intersection of these circles is the two points $z=\frac{-1\pm i\sqrt{3}}{2}$. ■

Example 2.6. Let z be a complex number such that $\left|\frac{z+i}{1+z}\right|=1$. Prove that

$$|z^{2010}+iz^{2009}+\ldots+i^{2009}z+i^{2010}|=|z^{2010}+z^{2009}+\ldots+z+1|.$$

Solution. Let S be the set of points in the complex plane such that $|z+i|=|1+z|$. It is clear that all the points of S have the same distance from the points $-i$ and -1. Thus S is the perpendicular bisector of the segment connecting the points -1 and $-i$ in the complex plane. Hence

$$S=\{z\in\mathbb{C}\mid z=x(1+i),x\in\mathbb{R}\}.$$

Moreover,

$$|z^{2010}+iz^{2009}+\ldots+i^{2009}z+i^{2010}|=\left|\frac{z^{2011}-i^{2011}}{z-i}\right|,$$

and

$$|z^{2010}+z^{2009}+\ldots+z+1|=\left|\frac{z^{2011}-1}{z-1}\right|.$$

Since $z\in S$, we find that $|z-i|=|z-1|$. Thus it suffices to prove that

$$|z^{2011}-i^{2011}|=|z^{2011}-1|,$$

i.e.,

$$|z^{2011}+i|=|z^{2011}-1|.$$

Note that

$$\begin{aligned} z^{2011} &= (x(1+i))^{2011}\\ &= x^{2011}(1+i)^3((1+i)^4)^{502}\\ &= x^{2011}\cdot 2(i-1)(-4)^{502}\\ &= 2^{1005}\cdot x^{2011}\cdot(i-1). \end{aligned}$$

Hence $z^{2011}\in R=\{z\in\mathbb{C}\mid z=y(i-1),y\in\mathbb{R}\}$. It is obvious that all points in the set R have the property $|r-1|=|r+i|$.
Hence $|z^{2011}+i|=|z^{2011}-1|$. ■

Example 2.7. Find all complex numbers $z=a+bi$, where a,b are rational numbers and $z^n=1$ for some positive integer n.

Solution. Let $a=\frac{p}{q}$, $b=\frac{r}{s}$, with integers p,q,r,s, such that $q,s\geq 1$, $\gcd(p,q)=\gcd(r,s)=1$. Let $\gcd(q,s)=d$. Then $q=dq_1$, $s=ds_1$ with $\gcd(q_1,s_1)=1$ and

$$(a^2+b^2)^n=|z|^{2n}=1.$$

Hence $a^2+b^2=1$ and $p^2s_1^2+r^2q_1^2=d^2q_1^2s_1^2$. It follows that $s_1^2\mid r^2q_1^2$, thus $s_1=1$. Analogously, $q_1=1$ and so $q=s$. That is, $p^2+r^2=q^2$ with $\gcd(p,q)=\gcd(r,q)=1$. It is easy to deduce that $\gcd(p,r)=1$ and that p,r have different parities. Therefore q is odd. Finally, rewriting the equation $z^n=1$ as $(p+ri)^n=q^n$, we find that $\mathrm{Re}((p+ri)^n)=q^n$. Therefore

$$\begin{aligned} q^n &= p^n-\binom{n}{2}p^{n-2}r^2+\binom{n}{4}p^{n-4}r^4+\ldots\\ &= p^n-\binom{n}{2}p^{n-2}(q^2-p^2)+\binom{n}{4}p^{n-4}(q^2-p^2)^2+\ldots \end{aligned}$$

Reducing this equation modulo q, we find that

$$p^n\left(1-\binom{n}{2}+\binom{n}{4}-\ldots\right)\equiv 0 \pmod q.$$

Moreover,

$$1-\binom{n}{2}+\binom{n}{4}-\ldots=\mathrm{Re}((1+i)^n).$$

Since $z^{4n} = 1$, then $n' = 4n$ also satisfies the given condition, and so by relabeling, we can assume without loss of generality that $4 \mid n$, that is, $n = 4k$ for some positive integer k. Therefore

$$(1+i)^{4k} = ((1+i)^2)^{2k} = (2i)^{2k} = (-4)^k,$$

implying that $p^{4k}(-4)^k \equiv 0 \pmod{q}$. Since q is odd and $\gcd(p,q) = 1$, we find that $q = 1$. Thus $p = \pm 1$, $r = 0$ or $p = 0$, $r = \pm 1$. Hence $z = \pm 1, \pm i$. ■

2.4.1 Trigonometric representation of a complex number

The algebraic approach to the complex numbers is extremely powerful, but there is an alternative geometric approach which is all very useful. This will allow us to apply trigonometry in studying the complex numbers.
Consider a Cartesian coordinate system in the Euclidean plane $\mathbb{R}^2$. To each complex number $z = x+iy$ $(x, y \in \mathbb{R})$ we can associate a unique point $P(x,y) \in \mathbb{R}^2$, usually called the *image* of the complex number z.
In this way, we have defined a bijective map

$$\begin{array}{rccc} f: & \mathbb{C} & \to & \mathbb{R}^2 \\ & x+iy & \mapsto & (x,y). \end{array}$$

If the image of z is the point P, then the complex number z is called the *affix* of the point P. If we write the coordinates of P in terms of polar coordinates, we have

$$\begin{cases} x &= \rho\cos\theta \\ y &= \rho\sin\theta, \end{cases}$$

where $\rho \in [0,\infty)$ is the length of segment OP and $\theta \in [0, 2\pi)$ is the angle that segment OP forms with the positive horizontal axis of the coordinate system.

Definition 2.6 Let $z = x + iy$ be a complex number and let $P(x,y)$ and $O(0,0)$ be two points in the plane. We define *argument* of z, denoted by $\mathrm{Arg}(z)$, the angle that segment OP forms with the positive horizontal axis of the coordinate system, taken counterclockwise.

The argument of z is defined up to multiples of 2π and when it belongs to the interval $[0, 2\pi)$ is called the *principal argument* of z and we denote this by $\arg(z)$. By convention, we say that the argument of $z = 0$ is undefined.

If $z = x + iy$ is a complex number with $|z| = \rho$ and $\arg(z) = \theta$, then we have that $x = \rho\cos\theta$ and $y = \rho\sin\theta$.

Trigonometric representation of a complex number

Let z be a complex number and let $\rho \in [0,\infty)$ be its modulus and $\theta \in [0, 2\pi)$ be its argument. Then

$$z = \rho(\cos\theta + i\sin\theta). \tag{2.1}$$

This is called the *trigonometric representation* of z.

The trigonometric representation of a complex number is useful when we have to multiply or divide two or more complex numbers.

Theorem 2.7 *Let*

$$z = \rho_1(\cos\theta_1 + i\sin\theta_1)$$

and

$$w = \rho_2(\cos\theta_2 + i\sin\theta_2).$$

Then

(i) $zw = \rho_1\rho_2\,(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2))$.

(ii) *If* $w \neq 0$, *then* $\dfrac{z}{w} = \dfrac{\rho_1}{\rho_2}\,(\cos(\theta_1-\theta_2) + i\sin(\theta_1-\theta_2))$.

Proof. Exercise. ❑

As a corollary of this theorem we get the following.

De Moivre's Formula

Let $z = \rho(\cos\theta + i\sin\theta)$ be a complex number. Then

$$z^n = \rho^n(\cos n\theta + i\sin n\theta)$$

for all $n \in \mathbb{N}$. If $z \neq 0$ the formula holds for any $n \in \mathbb{Z}$.

Proof. If $n > 0$, by using (i) of Theorem 2.7 with $z = z_1 = \ldots = z_n$, we get

$$\begin{aligned} z^n &= \underbrace{\rho\cdot\rho\cdot\ldots\cdot\rho}_{n \text{ times}}\left(\cos(\underbrace{\theta+\theta+\ldots+\theta}_{n \text{ times}}) + i\sin(\underbrace{\theta+\theta+\ldots+\theta}_{n \text{ times}})\right) \\ &= \rho^n(\cos n\theta + i\sin n\theta). \end{aligned}$$

If $z \neq 0$, for $n = 0$ the formula is obvious. If $n < 0$, take $-n = m$ in order to have

$$\begin{aligned} z^n = z^{-m} &= \frac{1}{z^m} \\ &= \frac{1}{\rho^m(\cos m\theta + i\sin m\theta)} \\ &= \rho^n(\cos m\theta - i\sin m\theta) \\ &= \rho^n(\cos n\theta + i\sin n\theta). \end{aligned}$$

□

The geometric locus of points satisfying $|z| = 1$ is the circle of radius 1 centered at the origin, called the *unit circle*. All points on the unit circle have the trigonometric representation $z = \cos\theta + i\sin\theta$. All the points inside the unit circle have the trigonometric representation $z = \rho(\cos\theta + i\sin\theta)$ for some $\rho < 1$ and all the points outside the unit circle have the trigonometric representation $\rho(\cos\theta + i\sin\theta)$ for some $\rho > 1$.

Let's see some examples.

Example 2.8. Find the value of $(1+i)^{2019}$ and $(3+i\sqrt{3})^{2019}$.

Solution. Writing

$$1 + i = \frac{1}{\sqrt{2}}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right),$$

we find that

$$(1+i)^{2019} = 2^{-\frac{2019}{2}}\left(\cos\frac{2019\pi}{4} + i\sin\frac{2019\pi}{4}\right).$$

Furthermore, since $\frac{2019\pi}{4} = 252\cdot 2\pi + \frac{3\pi}{4}$, we have

$$\cos\frac{2019\pi}{4} + i\sin\frac{2019\pi}{4} = -\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}.$$

Thus

$$(1+i)^{2019} = 2^{-1010}(-1+i).$$

Similarly,

$$3 + i\sqrt{3} = 2\sqrt{3}\left(\frac{\sqrt{3}}{2} + \frac{i}{2}\right) = 2\sqrt{3}\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right),$$

so

$$\begin{aligned} (3+i\sqrt{3})^{2019} &= 3^{\frac{2019}{2}}\cdot 2^{2019}\left(\cos\frac{2019\pi}{6} + i\sin\frac{2019\pi}{6}\right) \\ &= 3^{\frac{2019}{2}}\cdot 2^{2019}\left(\cos\frac{3\pi}{6} + i\sin\frac{3\pi}{6}\right) \\ &= 3^{\frac{2019}{2}}\cdot 2^{2019}i. \end{aligned}$$

■

Example 2.9. Let $z = \cos 40° + i\sin 40°$. Find the value of

$$|z + 2z^2 + \ldots + 9z^9|^{-1}.$$

AHSME 1984

Solution. It is clear that $z = \cos\frac{2\pi}{9} + i\sin\frac{2\pi}{9}$. Hence $z^9 = 1$.
Set $A = z + 2z^2 + \ldots + 9z^9$. Then

$$z \cdot A = z^2 + 2z^3 + \ldots + 8z^9 + 9z = A - (z + z^2 + \ldots + z^9) + 9z.$$

Note that

$$z + z^2 + \ldots + z^9 = z(1 + z + \ldots + z^8) = z\left(\frac{z^9 - 1}{z - 1}\right) = 0.$$

Hence $z \cdot A = A + 9z$, that is, $A = \frac{9z}{z-1}$. Thus

$$\frac{1}{|A|} = \frac{|z-1|}{9|z|} = \frac{|z-1|}{9}.$$

Observe that

$$z - 1 = \cos\frac{2\pi}{9} - 1 + i\sin\frac{2\pi}{9}.$$

Therefore

$$|z-1|^2 = \left(\cos\frac{2\pi}{9} - 1\right)^2 + \left(\sin\frac{2\pi}{9}\right)^2 = 2 - 2\cos\frac{2\pi}{9} = 4\sin^2\frac{\pi}{9}.$$

Hence $|z-1| = 2\sin\frac{\pi}{9}$, yielding

$$\frac{1}{|A|} = \frac{2}{9}\sin\frac{\pi}{9} = \frac{2}{9}\sin 20°. \qquad \blacksquare$$

Example 2.10. Let $C_1, \ldots, C_n$ be real numbers and let

$$g(\theta) = C_1\cos\theta + C_2\cos 2\theta + \ldots + C_n\cos n\theta.$$

If $g(\theta) > -1$ for all $\theta > 0$, prove that $C_1 + \ldots + C_n \leq n$.

Chinese Team Selection Test 2004

Solution. Let $z = \cos\frac{2\pi}{n+1} + i\sin\frac{2\pi}{n+1}$. Note that this gives

$$z^{n+1} = \cos(2\pi) + i\sin(2\pi) = 1$$

and since $z^{n+1} - 1 = (z-1)(z^n + z^{n-1} + \ldots + 1)$ we further conclude that $z^n + z^{n-1} + \ldots + 1 = 0$. Putting

$$\theta_1 = \frac{2\pi}{n+1}, \quad \theta_2 = \frac{4\pi}{n+1}, \quad \ldots, \quad \theta_n = \frac{2n\pi}{n+1},$$

we find that

$$\begin{aligned} g(\theta_1) &= \mathrm{Re}(C_1 z + C_2 z^2 + \ldots + C_n z^n) \geq -1, \\ g(\theta_2) &= \mathrm{Re}(C_1 z^2 + C_2 z^4 + \ldots + C_n z^{2n}) \geq -1, \\ &\vdots \\ g(\theta_n) &= \mathrm{Re}(C_1 z^n + C_2 z^{2n} + \ldots + C_n z^{n^2}) \geq -1. \end{aligned}$$

By adding the above inequalities, we find that

$$\mathrm{Re}((C_1 + \ldots + C_n)(z + z^2 + \ldots + z^n)) \geq -n.$$

Since $z + z^2 + \ldots + z^n = -1$, we are done. $\blacksquare$

Example 2.11. Let z be a complex number such that $|z+1| > 2$. Prove that $|z^3 + 1| > 1$.

Walter Janous - International Mathematics Competition 2012

Solution. Since

$$|z^3 + 1| = |z+1| \cdot |z^2 - z + 1| > 2|z^2 - z + 1|.$$

It remains to prove that $|z^2 - z + 1| > \frac{1}{2}$. Write $z + 1 = \rho(\cos\alpha + i\sin\alpha)$, where $\rho > 2$. Then

$$z^2 - z + 1 = (z+1)^2 - 3(z+1) + 3 = \rho^2(\cos 2\alpha + i\sin 2\alpha) - 3\rho(\cos\alpha + i\sin\alpha) + 3.$$

Thus

$$|z^2-z+1|^2=\rho^4+9\rho^2+9-(6\rho^3+18\rho)\cos\alpha+6\rho^2(2\cos^2\alpha-1)$$
$$=12\left(\rho\cos\alpha-\frac{\rho^2+3}{4}\right)^2+\frac{1}{4}(\rho^2-3)^2>0+\frac{1}{4}=\frac{1}{4}$$

and we are done. ■

Example 2.12. If $A=\{1,z,\ldots,z^{n-1}\}$,

$$B=\{1,1+z,\ldots,1+z+z^2+\ldots+z^{n-1}\},$$

and

$$z=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n},$$

find the set $A\cap B$.

Marian Tetiva - Shortlisted Problems for Romanian Mathematical Olympiad 2003

Solution. Note that $1\in A\cap B$. Suppose $\omega\neq 1$ is in both A and B. Since ω is in B, we can write

$$\omega=\frac{z^{k+1}-1}{z-1},$$

for some $1\leq k\leq n-1$. Since $z^n=1$ and $|z|=1$, we see that all of the elements of the set A have modulus 1 and all of them have n-th power equal to 1. In particular, since ω is in A, we find that $|\omega|=1$. Thus $\left|\frac{z^{k+1}-1}{z-1}\right|=1$ which implies that $|z^{k+1}-1|=|z-1|$. By De Moivre's Formula, we find that

$$|z^{k+1}-1|=\left|\cos\frac{2(k+1)\pi}{n}-1+i\sin\frac{2(k+1)\pi}{n}\right|$$
$$=2\left|\sin\frac{(k+1)\pi}{n}\right|=2\sin\frac{(k+1)\pi}{n},$$

and

$$|z-1|=\left|\cos\frac{2\pi}{n}-1+i\sin\frac{2\pi}{n}\right|=2\left|\sin\frac{\pi}{n}\right|=2\sin\frac{\pi}{n}.$$

Thus

$$\sin\frac{(k+1)\pi}{n}=\sin\frac{\pi}{n}.$$

Hence

$$\frac{(k+1)\pi}{n}=\pi-\frac{\pi}{n}=\frac{(n-1)\pi}{n}$$

which implies that $k=n-2$. Thus

$$\omega=\frac{z^{k+1}-1}{z-1}=\frac{z^{n-1}-1}{z-1}=\frac{\frac{1}{z}-1}{z-1}=-\frac{1}{z}.$$

However since $\omega\in A$, we must also have $1=\omega^n=\left(-\frac{1}{z}\right)^n=(-1)^n$. Thus n must be even and if n is even it is easy to check that $z^{n/2-1}=-\frac{1}{z}$ is in A. Thus $A\cap B=\{1\}$ if n is odd and $A\cap B=\left\{1,-\frac{1}{z}\right\}$ if n is even. ■

Example 2.13. Let a,b,c be three complex numbers of modulus 1. Prove that

$$\left|\frac{ab}{a^2-b^2}\right|+\left|\frac{bc}{b^2-c^2}\right|+\left|\frac{ac}{c^2-a^2}\right|\geq\sqrt{3}.$$

Michelle Bataille - Crux Mathematicorum

Solution. Clearly, we can assume that a^2,b^2,c^2 are distinct. Let

$$a=\cos\alpha+i\sin\alpha,\quad b=\cos\beta+i\sin\beta,\quad c=\cos\gamma+i\sin\gamma.$$

Then

$$\left|\frac{ab}{a^2-b^2}\right|=\frac{1}{\left|\frac{a}{b}-\frac{b}{a}\right|}$$
$$=\frac{1}{|(\cos(\alpha-\beta)+i\sin(\alpha-\beta))-(\cos(\beta-\alpha)-i\sin(\beta-\alpha))|}$$
$$=\frac{1}{2|\sin(\alpha-\beta)|}.$$

Now we must prove

$$\frac{1}{|\sin(\alpha-\beta)|}+\frac{1}{|\sin(\beta-\gamma)|}+\frac{1}{|\sin(\gamma-\alpha)|}\geq 2\sqrt{3}.$$

Note that by the AM-GM inequality, we have

$$\frac{1}{|\sin(\alpha-\beta)|}+\frac{1}{|\sin(\beta-\gamma)|}+\frac{1}{|\sin(\gamma-\alpha)|} \geq \frac{3}{\sqrt[3]{|\sin(\alpha-\beta)\sin(\beta-\gamma)\sin(\gamma-\alpha)|}}.$$

Note that

$$|\sin(\alpha-\beta)\sin(\beta-\gamma)\sin(\gamma-\alpha)| = |\sin(\alpha-\beta)\sin(\beta-\gamma)\sin(\pi-(\gamma-\alpha))|.$$

Set $X=\alpha-\beta$, $Y=\beta-\gamma$, $Z=\pi-(\gamma-\alpha)$. Then $X+Y+Z=\pi$.
It is a well-known fact[1] that

$$|\sin X\cdot\sin Y\cdot\sin Z| \leq \left(\frac{\sqrt{3}}{2}\right)^3,$$

whenever $X+Y+Z=\pi$. Then

$$\frac{3}{\sqrt[3]{|\sin(\alpha-\beta)\sin(\beta-\gamma)\sin(\gamma-\alpha)|}} \geq 2\sqrt{3}. \qquad \blacksquare$$

2.5 Roots of unity

Definition 2.8 Let z be a complex number. A number ω such that $\omega^n = z$ is called an *n-th root of z.*

We are interested in finding an expression for all the n-th roots of a complex number z.

Theorem 2.9 *Let z be a nonzero complex number, then z has exactly n distinct n-th roots. If we write $z=\rho(\cos\theta+i\sin\theta)$ with $\rho>0$ and $\theta\in[0,2\pi)$, then they are*

$$\omega_k = \sqrt[n]{\rho}\left(\cos\frac{\theta+2k\pi}{n}+i\sin\frac{\theta+2k\pi}{n}\right), \qquad k=0,1,\ldots,n-1. \tag{2.2}$$

[1] For the proof, see the book 112 Geometric inequalities, for example.

Proof. Let $\omega=r(\cos\varphi+i\sin\varphi)$ be an n-th root of z. Then $\omega^n=z$, so

$$r^n(\cos n\varphi+i\sin n\varphi)=\rho(\cos\theta+i\sin\theta).$$

Since two complex numbers are equal if and only if they have the same modulus and the arguments that differ by a multiple of 2π, we have

$$r^n=\rho, \qquad n\varphi=\theta+2k\pi, \qquad k\in\mathbb{Z},$$

whence $r=\sqrt[n]{\rho}$ and $\varphi_k=\dfrac{\theta+2k\pi}{n}$ with $k\in\mathbb{Z}$, i.e.,

$$\omega_k=\sqrt[n]{\rho}\left(\cos\frac{\theta+2k\pi}{n}+i\sin\frac{\theta+2k\pi}{n}\right), \qquad k\in\mathbb{Z}.$$

Since $0\leq\varphi_k<2\pi$ for $k=0,1,\ldots,n-1$, the n-th roots $\omega_0,\omega_1,\ldots,\omega_{n-1}$ are all distinct. Let $k\in\mathbb{Z}$ and let $0\leq r\leq n-1$ be the remainder when k is divided by n. Then $k=nq+r$ with $q\in\mathbb{Z}$ and

$$\varphi_k=\frac{\theta+2(nq+r)\pi}{n}=\frac{\theta+2r\pi}{n}+2q\pi=\varphi_r+2q\pi,$$

so $\omega_k=\omega_r$, i.e., $\omega_k\in\{\omega_0,\omega_1,\ldots,\omega_{n-1}\}$ for all $k\in\mathbb{Z}$. $\square$

Remark. By setting $z=1$ in the theorem, we get the *n-th roots of unity*, i.e., all the solutions to the equation $\omega^n=1$. They are

$$\omega_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}, \qquad k=0,1,\ldots,n-1. \tag{2.3}$$

In the complex plane, the n-th roots of a complex number $z\neq 0$ form the vertices of a regular n-gon with center at the origin. The n-th roots of unity form the vertices of a regular n-gon with center at the origin and with a vertex at the point $(1;0)$.
We can summarize and give some properties of the n-th roots of unity. The proof of these properties is left to the reader.

Roots of Unity

The complex roots of equation $z^n = 1$ are called the *n-th roots of unity.* If

$$U_n = \{z \in \mathbb{C} \mid z^n = 1\} = \left\{\omega_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \,\middle|\, k = 0, 1, \ldots, n-1\right\}$$

is the set of the n-th roots of unity, we have the following properties:

(i) if ω_i, ω_j are n-th roots of unity, then $\omega_i\omega_j$ is an n-th root of unity;

(ii) non-real roots of unity can be partitioned into sets $\left\{\omega_i, \frac{1}{\omega_i}\right\}$;

(iii) for any $\omega \in U_n$ and for any $i, j \in \mathbb{Z}$ such that $i \equiv j \pmod{n}$, we have $\omega^i = \omega^j$.

Definition 2.10 An n-th root of unity is said to be *primitive* if it is not a k-th root of unity for some smaller k, i.e., if

$$z^n = 1, \quad \text{and} \quad z^k \neq 1 \quad \text{for } k = 0, 1, \ldots, n-1.$$

In other words, if ω is an primitive n-th root of unity, then n is the smallest positive integer such that $\omega^n = 1$.

Theorem 2.11 *An n-th root of unity $\omega_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ $(0 \leq k \leq n-1)$ is a primitive n-th root of unity if and only if* $\gcd(k, n) = 1$.

Proof. First, we prove that if ω_k is a primitive n-th root of unity, then $\gcd(k, n) = 1$. It suffices to show that if $\gcd(k, n) = g > 1$, then ω_k is not primitive. In this case we can write $k = gk_1$ for some k_1, and then we compute that

$$\omega_k^{n/g} = (\omega_1^k)^{n/g} = \omega_1^{nk_1} = ((\omega_1)^n)^{k_1} = 1^{k_1} = 1.$$

So ω_k is a (n/g)-th root of unity and since $n/g < n$, ω_k is not primitive.

Now, we assume that $k \in \{0, 1, 2, \ldots, n-1\}$, $\gcd(k, n) = 1$ and we prove that ω_k is a primitive n-th root of unity. Assume on the contrary, that ω_k is not a primitive n-th root of unity. Then there exists $m \in \{1, 2, \ldots, n-1\}$ such that $\omega_k^m = 1$, i.e.,

$$\cos\frac{2km\pi}{n} + i\sin\frac{2km\pi}{n} = 1.$$

It follows that $\frac{2km\pi}{n} = 2t\pi$ for some $t \in \mathbb{Z}$, i.e., $km = nt$. So $n \mid km$. Since $\gcd(k, n) = 1$, by Euclid's Lemma $n \mid m$, but $1 \leq m \leq n-1$, a contradiction.❑

Corollary 2.12 *For each positive integer n there are $\varphi(n)$ primitive n-th roots of unity, where φ is the Euler's totient function.*

Example 2.14. Let $n = 12$. We have

$$\omega = \cos\frac{\pi}{6} + i\sin\frac{\pi}{6}, \ \omega^5 = \cos\frac{5\pi}{6} + i\sin\frac{5\pi}{6},$$

$$\omega^7 = \cos\frac{7\pi}{6} + i\sin\frac{7\pi}{6}, \ \omega^{11} = \cos\frac{11\pi}{6} + i\sin\frac{11\pi}{6}.$$

These are $\varphi(12) = 4$ primitive 12-th roots of unity.

Example 2.15. Let $a_1, \ldots, a_d$ be d nonzero complex numbers, not necessarily distinct. Let k, l be distinct positive integers such that $a_1^k, \ldots, a_d^k$ and $a_1^l, \ldots, a_d^l$ are two identical collections of numbers. Prove that each of $a_1, \ldots, a_d$ is a root of unity.

Solution. The statement of the problem implies that there is a bijection $\sigma : \{1, 2, 3, \ldots\} \to \{1, 2, 3, \ldots\}$ such that $\sigma(j) = m$ implies that $a_j^k = a_m^l$. Consider the sequence $1, \sigma(1), \sigma(\sigma(1)), \ldots$. Since σ is a bijection on a finite set, there are positive integers r, s such that $\sigma^{(r)}(1) = \sigma^{(s)}(1)$, where $0 \leq r < s \leq n-1$ (here we define $\sigma^{(0)}(1) = 1$). Since σ is a bijection, we find that $\sigma^{(s-r)}(1) = 1$. Therefore $a_1^k = a_{\sigma(1)}^l$, $a_{\sigma(1)}^k = a_{\sigma^{(2)}(1)}^l$. Thus $a_1^{k^2} = a_{\sigma^{(2)}(1)}^{l^2}$. Therefore

$$a_1^{k^{s-r}} = a_{\sigma^{(s-r)}(1)}^{l^{s-r}} = a_1^{l^{s-r}}.$$

Since $l \neq k$, we find that there is a positive integer $n = |l^{s-r} - k^{s-r}|$ such that $a_1^n = 1$. Hence a_1 is a root of unity. The same argument proves that each of $a_1, \ldots, a_d$ is a root of unity. ■

Example 2.16. Let $a_1, \ldots, a_n$ be roots of the polynomial $1+x+x^2+\ldots+x^n$. Find the smallest positive integer m such that the numbers $a_1^m, \ldots, a_n^m$ lie on a straight line in the complex plane whenever:

(i) $n = 2011$;

(ii) $n = 2010$.

Solution. (i) Let $P(x) = 1 + x + x^2 + \ldots + x^{2011}$. Then $a_1, \ldots, a_{2011}$ are all roots of polynomial $(x-1)P(x) = x^{2012} - 1$ and thus they have modulus 1. Hence these numbers lie on the unit circle. Since any straight line intersects the circle in at most two points, call them A, B, we can assume that $a_1^m, \ldots, a_{2011}^m$ are either A or B. Then without loss of generality, there are at least 1006 numbers among $a_1^m, \ldots, a_{2011}^m$ that are equal to A and all of them are roots of the polynomial $x^m - A$. Thus $m \geq 1006$. Now we prove that $m = 1006$ is the least possible number. Indeed, since

$$x^{2012} - 1 = (x^{1006} - 1)(x^{1006} + 1),$$

each of the numbers $a_1^{1006}, \ldots, a_{2011}^{1006}$ is either 1 or -1.

(ii) We will show that $a_1^m, \ldots, a_{2010}^m$ all lie on a line if and only if m is a multiple of 2011. Let $P(x) = 1+x+x^2+\ldots+x^{2010}$. Then $a_1, \ldots, a_{2010}$ are all roots of the polynomial $(x-1)P(x) = x^{2011} - 1$ and thus they have modulus 1. More precisely, the roots of the polynomial $P(x)$ are the complex numbers

$$\varepsilon_k = \cos\frac{2k\pi}{2011} + i\sin\frac{2k\pi}{2011}$$

for $k = 1, \ldots, 2010$. If m is a multiple of 2011, then $a_k^m = 1$ for all k, hence the numbers $a_1^m, \ldots, a_{2010}^m$ all coincide and hence lie on a single line. Now suppose m is not a multiple of 2011. Note that since 2011 is a prime, the ε_k are all primitive 2011-th roots of unity. This means that if $\varepsilon_k^r = 1$ for some integer r, then r is divisible by 2011. As in the previous part, if $\varepsilon_1^m, \ldots, \varepsilon_{2010}^m$ all lie on a line, then they take on at most 2 distinct values. Since m is not a multiple of 2011, none of these values can be 1. Further, they cannot be -1 since if $\varepsilon_k^m = -1$, then $-1 = (-1)^{2011} = \varepsilon_k^{2011m} = 1$, a contradiction. Thus the two values are non-real. Since $\varepsilon_{2010} = \overline{\varepsilon_1}$, we have $\varepsilon_{2010}^m = \overline{\varepsilon_1^m}$. Thus these two values must be ε_1^m and $\varepsilon_1^{-m} = \overline{\varepsilon_1^m}$. Hence ε_2^m must be one of these two values, which means that either $\varepsilon_1^{2m} = \varepsilon_2^m = \varepsilon_1^m$ or $\varepsilon_1^{2m} = \varepsilon_2^m = \varepsilon_1^{-m}$. In the first case, we get $\varepsilon_1^m = 1$ and in the second case we get $\varepsilon_1^{3m} = 1$. In either case we conclude that 2011 divides m, a contradiction. ■

2.6 Polynomials with complex roots

After some preliminaries, we have finally arrived at the main part of this chapter. In this section we need to use all the above-mentioned techniques. Moreover, we need full-fledged knowledge about these topics:

(i) divisibility of polynomials;

(ii) concept of root;

(iii) Vieta's formulas;

(iv) if a non-real complex number z is a root of polynomial $P(x)$ with real coefficients then $\overline{z}$ is another root of polynomial $P(x)$. That is, we can partition all non-real complex roots of $P(x)$ into sets $\{z, \overline{z}\}$.

Corollary 2.13 *Fact (iv) implies that a polynomial $P(x)$ with a non-real root z is divisible by*

$$(x - z)(x - \overline{z}) = x^2 - 2\,\mathrm{Re}(z)x + |z|^2.$$

Example 2.17. Let z be a non-real complex number such that $z^3+1=0$. Evaluate:

$$\left(\frac{z}{z-1}\right)^{2018}+\left(\frac{1}{z-1}\right)^{2018}.$$

Solution. Since $z^3+1=(z+1)(z^2-z+1)$ and $z\neq -1$, we have $z^2-z+1=0$. Therefore $z-1=z^2$. Hence

$$\begin{aligned}\left(\frac{z}{z-1}\right)^{2018}+\left(\frac{1}{z-1}\right)^{2018} &= \left(\frac{z}{z^2}\right)^{2018}+\left(\frac{1}{z^2}\right)^{2018}\\ &= \left(\frac{1}{z}\right)^{2018}+\left(\frac{1}{z^2}\right)^{2018}\\ &= \frac{z^{2018}+1}{z^{2\cdot 2018}}.\end{aligned}$$

■

Since $2018\equiv 2 \pmod 3$, we find that

$$z^{2018}=(z^3)^{672}\cdot z^2=(-1)^{672}\cdot z^2=z^2,$$

so this simplifies to

$$\left(\frac{z}{z-1}\right)^{2018}+\left(\frac{1}{z-1}\right)^{2018}=\frac{z^2+1}{z^4}=\frac{z^2+1}{-z}=\frac{z}{-z}=-1.$$

Example 2.18. Let $f(x),g(x),h(x),k(x)$ be polynomials such that

$$\begin{aligned}(x^2+1)h(x)+(x-1)f(x)+(x-2)g(x)&=0,\\ (x^2+1)k(x)+(x+1)f(x)+(x+2)g(x)&=0\end{aligned}$$

for all $x\in\mathbb{C}$. Prove that $f(x),g(x)$ are divisible by x^2+1.

Solution. Putting $x=i$, we find that

$$(i-1)f(i)+(i-2)g(i)=0,\quad (i+1)f(i)+(i+2)g(i)=0.$$

Solving the above system with respect to $f(i),g(i)$, we can easily find that $f(i)=g(i)=0$. Analogously, $f(-i)=g(-i)=0$. Hence $f(x),g(x)$ are both divisible by $x-i$ and $x+i$. That is, $f(x),g(x)$ are both divisible by $(x-i)(x+i)=x^2+1$. ■

Example 2.19. Let $P(x)=x^4+14x^3+52x^2+56x+16$ and let z_1,z_2,z_3,z_4 be the roots of the polynomial $P(x)$. If $\{a,b,c,d\}=\{1,2,3,4\}$, find the minimal value of the expression $|z_az_b+z_cz_d|$.

Solution. Observe that $Q(x)=\frac{1}{16}P(2x)=x^4+7x^3+13x^2+7x+1$ is a self-reciprocal polynomial. If r is a root of $P(x)$, then by setting $x=\frac{r}{2}$, we get that $\frac{r}{2}$ is a root of $Q(x)$ and then that $\frac{2}{r}$ is a root of $Q(x)$. So $\frac{4}{r}$ is a root of $P(x)$. Since $P(0)=16$, $P(-1)=-1$ and $P(-2)=16$, we find that $P(x)$ has two roots on $(-\infty,-2)$. Hence by the remarks above, it also has two roots on $(-2,0)$. Thus all the roots of P are negative. If we write these roots as $z_1\leq z_2\leq z_3\leq z_4<0$, then the rearrangement inequality gives

$$|z_az_b+z_cz_d|\geq\frac{1}{2}(z_1z_4+z_2z_3+z_3z_2+z_4z_1)=z_1z_4+z_2z_3.$$

Since $z_1z_4=z_2z_3=4$, the minimal value is 8. ■

With the next example, we aim to assess your learning outcome from the previous chapter and what you have learned since the beginning of this chapter.

Example 2.20. Find the sum of the moduli of the roots of the polynomial

$$P(x)=20x^8+7ix^7-7ix+20.$$

Solution. If r is a root of the polynomial $P(x)$, then $P(r)=0$. Whence

$$\frac{P(r)}{r^4}=20r^4+7ir^3-\frac{7i}{r^3}+\frac{20}{r^4}=20\left(r^4+\frac{1}{r^4}\right)+7i\left(r^3-\frac{1}{r^3}\right).$$

Now, assume that $r = it$. Then

$$0 = 20\left(r^4 + \frac{1}{r^4}\right) + 7i\left(r^3 - \frac{1}{r^3}\right) = 20\left(t^4 + \frac{1}{t^4}\right) + 7\left(t^3 + \frac{1}{t^3}\right).$$

Let $y = t + \frac{1}{t}$. Then using the polynomials T_3 and T_4 from the first solution to Example 1.7, we get

$$20((y^2-2)^2 - 2) + 7(y^3 - 3y) = 0.$$

Hence

$$20y^4 + 7y^3 - 80y^2 - 21y + 40 = 0.$$

Assume that $Q(y) = 20y^4 + 7y^3 - 80y^2 - 21y + 40$. Note that

$$Q(-2) > 0, \quad Q(-1) < 0, \quad Q(0) > 0, \quad Q(1) < 0, \quad Q(2) > 0.$$

Thus the polynomial $Q(y)$ has 4 real roots all of which are in $(-2, 2)$. If y is one of these roots, then the corresponding values of t satisfy $t + \frac{1}{t} = y$, which we can rewrite as $t^2 - yt + 1 = 0$ and solve to get

$$t = \frac{y}{2} \pm i\sqrt{1 - \frac{y^2}{4}}.$$

Thus for each y we get two values of t, both on the unit circle. Thus we have found 8 roots $r = it$ of P all on the unit circle. Since the polynomial

$$P(x) = 20x^8 + 7ix^7 - 7ix + 20$$

is of degree 8, these are the only roots. Thus we have 8 roots of modulus 1 and the answer is 8. ■

Example 2.21. The polynomial $P(x) = (1 + x + \ldots + x^{17})^2 - x^{17}$ has 34 complex roots of the form

$$z_k = r_k(\cos 2\pi\alpha_k + \sin 2\pi\alpha_k), \quad k = 1, \ldots, 34$$

and $0 < \alpha_1 \leq \ldots \leq \alpha_{34} < 1$. Find the value of

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5.$$

Solution. Summing the geometric series in $P(x)$, we find

$$\begin{aligned} P(x) &= \left(\frac{x^{18}-1}{x-1}\right)^2 - x^{17} = \frac{(x^{18}-1)^2 - x^{17}(x-1)^2}{(x-1)^2} \\ &= \frac{x^{36} - x^{19} - x^{17} + 1}{(x-1)^2} = \frac{(x^{19}-1)(x^{17}-1)}{(x-1)^2}. \end{aligned}$$

Hence

$$(x-1)^2 P(x) = (x^{19}-1)(x^{17}-1).$$

Note that $P(1) \neq 0$, hence the roots of $P(x)$ are the roots of $(x^{19}-1)(x^{17}-1)$, other than 1. Thus the roots of the polynomial $P(x)$ are of the form

$$\cos\frac{2k\pi}{17} + i\sin\frac{2k\pi}{17} \quad \text{or} \quad \cos\frac{2k\pi}{19} + i\sin\frac{2k\pi}{19}.$$

Then $r_k = 1$ for all k and $\alpha_1 = \frac{1}{19}$, $\alpha_2 = \frac{1}{17}$, $\alpha_3 = \frac{2}{19}$, $\alpha_4 = \frac{2}{17}$, and $\alpha_5 = \frac{3}{19}$. Hence

$$\sum_{i=1}^{5} \alpha_i = \frac{159}{323}.$$ ■

Example 2.22. Let

$$P(x) = 24x^{24} + \sum_{j=1}^{23} (24-j)(x^{24-j} + x^{24+j}),$$

and let $z_1, z_2, \ldots, z_r$ be the roots of the polynomial $P(x)$. If $z_k^2 = a_k + ib_k$, find the value of $\sum_{i=1}^{r} |b_k|$.

Solution. Expanding the formula for $P(x)$ we find

$$P(x) = x^{47} + 2x^{46} + 3x^{45} + \cdots + 23x^{25} + 24x^{24} + 23x^{23} + \cdots + 2x^2 + x,$$

hence we compute

$$(x-1)P(x) = x^{48} + x^{47} + \cdots + x^{25} - x^{24} - x^{23} - \cdots - x^2 - x$$

and

$$(x-1)^2P(x) = x^{49} - 2x^{25} + x = x(x^{24}-1)^2.$$

Since $P(1) \neq 0$, we conclude that the roots of P are 0 and the 24-th roots roots of unit except for 1. Since the root at $z = 0$ contributes zero to the desired sum, we can focus on the other 23 roots which are

$$z_k = \cos\frac{k\pi}{12} + i\sin\frac{k\pi}{12},$$

for $k = 1, \ldots, 23$. For these we compute

$$z_k^2 = \cos\frac{k\pi}{6} + i\sin\frac{k\pi}{6}.$$

As k goes from 1 to 23, $\left|\sin\frac{k\pi}{6}\right|$ cycles through the values $\frac{1}{2}$, $\frac{\sqrt{3}}{2}$, 1, $\frac{\sqrt{3}}{2}$, $\frac{1}{2}$, 0 taking each value except the 0 four times. Hence

$$\sum_{i=1}^{r} |b_k| = 8 + 4\sqrt{3}. \qquad \blacksquare$$

Example 2.23. Let $z_1, \ldots, z_{2016} \neq 1$ be the nontrivial roots of the equation $x^{2017} = 1$. Find the value of $\sum_{k=1}^{2016} \frac{1}{1+z_k}$.

Solution. Since all non-real roots of the polynomial $x^{2017} - 1$ can be partitioned as $z_k, \overline{z_k} = \frac{1}{z_k}$, we find that

$$\begin{aligned}
\sum_{k=1}^{2016} \frac{1}{1+z_k} &= \sum_{k=1}^{1008} \left(\frac{1}{1+z_k} + \frac{1}{1+\frac{1}{z_k}} \right) \\
&= \sum_{k=1}^{1008} \left(\frac{1}{1+z_k} + \frac{z_k}{1+z_k} \right) \\
&= \sum_{k=1}^{1008} 1 \\
&= 1008.
\end{aligned}$$

$\blacksquare$

Remark. The previous problem exploited an interesting fact. If z is a complex number on the unit circle, then $\mathrm{Re}\left(\frac{1}{1+z}\right) = \frac{1}{2}$.

Example 2.24. Let z be a complex number such that $z^{23} = 1$. Find the value of $\sum_{k=0}^{22} \frac{1}{z^{2k} + z^k + 1}$.

Solution. Note that since $z^{23} - 1 = (z-1)(z^{22} + z^{21} + \cdots + z + 1)$ and $z \neq 1$ (since it is complex), we have $z^{22} + z^{21} + \cdots + z^2 + z = -1$. More generally, if k is not a multiple of 23, then z^k also satisfies $(z^k)^{23} = z^{23k} = 1$ and is not real. Hence $z^{22k} + z^{21k} + \cdots + z^k = -1$. (A different way to see this is to note that the numbers $k, 2k, \ldots, 22k$ are all nonzero and distinct modulo 23, hence they are in the congruence classes $1, 2, \cdots, 22$ in some order. Hence $z^{22k} + z^{21k} + \cdots + z^k = z^{22} + z^{21} + \cdots + z^2 + z = -1$.) We have

$$\sum_{k=0}^{22} \frac{1}{z^{2k} + z^k + 1} = \frac{1}{3} + \sum_{k=1}^{22} \frac{1}{z^{2k} + z^k + 1} = \frac{1}{3} + \sum_{k=1}^{22} \frac{z^k - 1}{z^{3k} - 1}.$$

Since $z^{24} = z$, we have

$$\sum_{k=0}^{22} \frac{1}{z^{2k} + z^k + 1} = \frac{1}{3} + \sum_{k=1}^{22} \frac{(z^{24})^k - 1}{z^{3k} - 1} = \frac{1}{3} + \sum_{k=1}^{22} \sum_{l=0}^{7} z^{3kl}.$$

Using the computation above, we have

$$\begin{aligned}
\sum_{k=1}^{22} \sum_{l=0}^{7} z^{3kl} &= \sum_{k=1}^{22} 1 + \sum_{k=1}^{22} (z^{3k} + z^{6k} + z^{9k} + z^{12k} + z^{15k} + z^{18k} + z^{21k}) \\
&= 22 + 7 \cdot \sum_{k=1}^{22} z^k \\
&= 22 - 7 \\
&= 15,
\end{aligned}$$

so that

$$\sum_{k=0}^{22} \frac{1}{z^{2k}+z^k+1} = \frac{1}{3}+15 = \frac{46}{3}. \qquad \blacksquare$$

Example 2.25. If $r_1, \ldots, r_{2018}$ are the non-real roots of the equation

$$z^{2019} = 1,$$

compute the value of

$$\frac{r_1+\ldots+r_{2018}+2018}{(1+r_1)\cdot\ldots\cdot(1+r_{2018})}.$$

Solution. Since $z^{2019}-1 = (z-1)(z^{2018}+z^{2017}+\ldots+z+1)$, we find that $r_1, \ldots, r_{2018}$ are roots of $z^{2018}+z^{2017}+\ldots+z+1$. Hence

$$z^{2018}+z^{2017}+\ldots+z+1 = (z-r_1)\cdot\ldots\cdot(z-r_{2018}).$$

Thus Vieta's formula gives $r_1+\ldots+r_{2018} = -1$. Furthermore, putting $z=-1$ in the above equality, we find that

$$\begin{aligned}(-1-r_1)\cdot\ldots\cdot(-1-r_{2018}) &= (1+r_1)\cdot\ldots\cdot(1+r_{2018})\\ &= (-1)^{2018}+(-1)^{2017}+\ldots+(-1)+1\\ &= 1.\end{aligned}$$

Thus

$$\frac{r_1+\ldots+r_{2018}+2018}{(1+r_1)\cdot\ldots\cdot(1+r_{2018})} = \frac{2017}{1} = 2017. \qquad \blacksquare$$

Example 2.26. Let $P(x) = x^5-x^2+1$, $Q(x) = x^2+1$. Denote the roots of $P(x)$ by r_1, r_2, r_3, r_4, r_5. Evaluate the product

$$Q(r_1)Q(r_2)Q(r_3)Q(r_4)Q(r_5).$$

Solution. Write $P(x) = (x-r_1)\cdot\ldots\cdot(x-r_5)$. Then we compute

$$\begin{aligned}Q(r_1)Q(r_2)Q(r_3)Q(r_4)Q(r_5) &= \prod_{j=1}^{5}(r_j+i)\prod_{j=1}^{5}(r_j-i)\\ &= P(-i)P(i)\\ &= |P(i)|^2\\ &= |i+2|^2\\ &= 5.\end{aligned} \qquad \blacksquare$$

Example 2.27. Let $x^4+3x^3+ax^2+bx+c$ be a polynomial with real coefficients which has four real roots in the interval $(-1,1)$. Prove that

$$(1-a+c)^2+(3-b)^2 \geq \left(\frac{5}{4}\right)^8.$$

Nguyen Viet Hung - Mathematical Reflections, Problem U392

Solution. Let $P(x) = x^4+3x^3+ax^2+bx+c$ and let x_1, x_2, x_3, x_4 be the roots of $P(x)$. Then we have

$$P(i) = 1-3i-a+bi+c = (i-x_1)(i-x_2)(i-x_3)(i-x_4)$$

and

$$|P(i)|^2 = (1-a+c)^2+(3-b)^2 = (1+x_1^2)(1+x_2^2)(1+x_3^2)(1+x_4^2).$$

Now, we have to show that

$$(1+x_1^2)(1+x_2^2)(1+x_3^2)(1+x_4^2) \geq \left(\frac{5}{4}\right)^8.$$

This is equivalent to

$$\ln(1+x_1^2)+\ln(1+x_2^2)+\ln(1+x_3^2)+\ln(1+x_4^2) \geq 8\ln\frac{5}{4}.$$

Now, using the fact that the function $g(x) = \ln(1+x^2)$ is convex on the interval $(-1,1)$ and Jensen's inequality, we get

$$\frac{\sum_{k=1}^{4} \ln(1+x_k^2)}{4} \geq \ln\left(1+\left(\frac{\sum_{k=1}^{4} x_k}{4}\right)^2\right),$$

and since $x_1+x_2+x_3+x_4 = -3$, we get the conclusion. ■

Example 2.28. Let $P(x)$ and $Q(x)$ be polynomials such that

$$P(x^3)+Q(x) = P(x)+x^5Q(x) \qquad \forall x.$$

Let $\deg P = 4$ and $P(0) = 0$. Prove that all the nonzero roots of $P(x)$ lie on the unit circle.

Ukrainian Mathematical Olympiad 2010

First Solution. Let $P(x) = a_4x^4+a_3x^3+a_2x^2+a_1x$. We write the original equation as

$$P(x^3)-P(x) = (x^5-1)Q(x).$$

Then

$$P(x^3)-P(x) = a_4(x^{12}-x^4)+a_3(x^9-x^3)+a_2(x^6-x^2)+a_1(x^3-x)$$

is divisible by x^5-1. Since

$$\begin{aligned} x^{12}-x^4 &\equiv x^2-x^4 \pmod{x^5-1},\\ x^9-x^3 &\equiv x^4-x^3 \pmod{x^5-1},\\ x^6-x^2 &\equiv x-x^2 \pmod{x^5-1}, \end{aligned}$$

we get that

$$a_4(x^2-x^4)+a_3(x^4-x^3)+a_2(x-x^2)+a_1(x^3-x)$$

is divisible by x^5-1. Thus

$$(a_3-a_4)x^4+(a_1-a_3)x^3+(a_4-a_2)x^2+(a_2-a_1)x$$

is divisible by x^5-1 and hence it must be equal to zero, that is $a_1 = a_2 = a_3 = a_4$. Hence

$$P(x) = a_4(x^4+x^3+x^2+x) = a_4x\left(\frac{x^4-1}{x-1}\right)$$

and we are done. Moreover, it is easy to compute that

$$Q(x) = a_4(x^7+x^4+x^2+x).$$ ■

Second Solution. Let ω be a primitive 5-th root of unity, that is, $\omega^5 = 1$ but $\omega^k \neq 1$ for $k = 1,2,3,4$. Putting $x = \omega, \omega^2, \omega^3, \omega^4$, we find that

$$P(\omega^3) = P(\omega), \quad P(\omega^6) = P(\omega) = P(\omega^2),$$

$$P(\omega^9) = P(\omega^4) = P(\omega^3), \quad P(\omega^{12}) = P(\omega^2) = P(\omega^4).$$

Hence $P(\omega) = P(\omega^2) = P(\omega^3) = P(\omega^4)$. Then

$$\begin{aligned} P(x) &= P(\omega)+C(x-\omega)(x-\omega^2)(x-\omega^3)(x-\omega^4)\\ &= P(\omega)+C(1+x+x^2+x^3+x^4), \end{aligned}$$

for some real number C.
Since, $P(0) = 0$, we find that $P(\omega) = -C$, which gives

$$P(x) = C(x+x^2+x^3+x^4) = Cx(x+1)(x^2+1).$$

Hence the nonzero roots of P are -1 and $\pm i$, which are all on the unit circle. ■

Example 2.29. Find all positive integers $n \geq 4$ such that there are distinct complex numbers a, b, c such that

$$(a-b)^n+(b-c)^n+(c-a)^n = 0$$

and their images in the complex plane are vertices of an equilateral triangle.

Vlad Mihaly - Romanian Mathematical Olympiad 2020

Solution. Let $\omega = \frac{-1+i\sqrt{3}}{2}$ be a primitive cube root of unity. If z is any complex number, viewed as a point in the complex plane, then ωz is the result of rotating z by 120 degrees counterclockwise with center at the origin. If a, b, c is an equilateral triangle, then $a - b$ represents the vector from the vertex b to the vertex a. Since the sides of an equilateral triangle have equal length and the exterior angles are 120 degrees, it follows that $b - c$ and $c - a$ are $a - b$ rotated clockwise or counterclockwise by 120 degrees. Thus a, b, c are the vertices of an equilateral triangle if and only if

$$\{b - c, c - a\} = \{\omega(a - b), \omega^2(a - b)\}.$$

(A nice exercise is to show that this reduces to the fact that a, b, c are the vertices of an equilateral triangle if and only if $a+\omega^{\pm 1}b+\omega^{\pm 2}c = 0$ or equivalently if and only if

$$0 = (a + \omega b + \omega^2 c)(a + \omega^{-1} b + \omega^{-2} c) = a^2 + b^2 + c^2 - ab - bc - ca,$$

but we will not need this form here.) Dividing the given equation by $(a-b)^n$, we therefore get

$$1 + \omega^n + \omega^{2n} = 0.$$

If n is a multiple of 3, then $1 + \omega^n + \omega^{2n} = 3$ and this equation does not hold, but otherwise $\omega^n = \omega^{\pm 1}$ and this equation becomes $1 + \omega^{\pm 1} + \omega^{\pm 2} = 0$ which does hold. Thus the answer is all n which are not multiples of 3. ■

Example 2.30. Let $P(x) = (x^{2009} - 2009)(x^{2008} - 2008) \cdot \ldots \cdot (x - 1)$. Find all complex numbers a such that $P(x)$ is divisible by $(x - a)^2$.

Solution. We saw in Theorem 2.9 that the roots of the polynomial $x^k - k$ are k equally spaced points on a circle centered at the origin with the radius $\sqrt[k]{k}$. In particular, all the polynomials of the form $x^k - k$ have only simple roots. If the polynomial $P(x)$ is divisible by $(x - a)^2$, then it has a double root at a and it must be a root of two of these factors. Thus there exists m and n with $1 \leq m < n \leq 2009$ such that $x^m - m$ and $x^n - n$ have a common root. Hence the corresponding circles must agree, which gives $\sqrt[m]{m} = \sqrt[n]{n}$. The function

$f(x) = x^{\frac{1}{x}}$ is decreasing[2] on $(e, +\infty)$ and increasing at $(1, e)$, since

$$f'(x) = f(x) \cdot \frac{1 - \ln x}{x},$$

and thus we must have $m < e < n$. Thus $m = 1, 2$ and $n \geq 3$. We cannot have a solution for $m = 1$, since $\sqrt[n]{n} > 1$ for all $n > 1$. Thus we must have $m = 2$ which gives the solution $\sqrt{2} = \sqrt[4]{4}$, and since f is decreasing on (e, ∞) this is the only solution. This case gives the polynomials $x^2 - 2$ and $x^4 - 4$ which have common roots $\pm\sqrt{2}$, yielding $a = \pm\sqrt{2}$. ■

2.7 Using the modulus, real part, imaginary part, and argument of roots

The main reason why we separate this section is the explicit need for you to implement your knowledge about complex numbers and some extra techniques like extremal elements, etc..

Example 2.31. Let $P(x)$ be a nonconstant irreducible polynomial with integer coefficients over $\mathbb{Z}[x]$. Prove that for all integers $n \geq m \geq 0$ the polynomial

$$P(x + m + 1) \cdot \ldots \cdot P(x + n),$$

is not the square of any polynomial with rational coefficients.

Navid Safaei

Solution. Assume on the contrary that

$$P(x + m + 1) \cdot \ldots \cdot P(x + n) = Q(x)^2$$

for some polynomial $Q(x)$ with rational coefficients and some $n \geq m \geq 0$. This implies that all of the roots of the polynomial

$$P(x + m + 1) \cdot \ldots \cdot P(x + n) = Q(x)^2$$

[2] It is clear that we only need a discrete version of this statement. You can prove it either by induction or the AM-GM inequality.

are multiple roots. However, we will prove that there is at least one simple root for $Q(x)^2$. Let α be a root of $P(x)$ such that $\mathrm{Re}(\alpha)$ is minimal. Recall that α is a simple root of P. (Since P is irreducible, P is the minimal polynomial of α, but if α were a double root of P, then α would be a root of P', a polynomial of lower degree.) Hence $\alpha - n$ is a simple root of $P(x+n)$. However, $\alpha - n$ is not a root of any other polynomial

$$P(x+m+1), \ldots, P(x+n-1).$$

Otherwise, $\alpha - n + k$ would be a root of $P(x)$, for some $m+1 \leq k \leq n-1$. But $\mathrm{Re}(\alpha - n + k) < \mathrm{Re}(\alpha)$, contradicting the choice of α. Hence we have found at least one simple root and we are done. ■

In the two following examples, we need to use the concept of root and what we learned about the modulus.

Example 2.32. Let $a < 1$ and z be a root of the polynomial

$$(a-2)x^{2018} + aix^{2017} + aix + 2 - a.$$

Find the value of $|z|$.

High School Mathematics Journal 07/2018

Solution. Rearranging, we get $z^{2017}((a-2)z + ai) = (a-2) - aiz$. Hence

$$|z|^{2017} = \left|\frac{(a-2) - aiz}{(a-2)z + ai}\right|.$$

Now, let $z = x + iy$ for some real numbers x, y. Then

$$\left|\frac{(a-2) - aiz}{(a-2)z + ai}\right| = \left|\frac{(a-2) - ai(x+iy)}{(a-2)(x+iy) + ai}\right| = \left|\frac{a - 2 + ay - iax}{x(a-2) + i(a + y(a-2))}\right|.$$

Hence

$$\left|\frac{(a-2) - aiz}{(a-2)z + ai}\right|^2 = \frac{(a-2+ay)^2 + a^2x^2}{(a-2)^2x^2 + (a+y(a-2))^2}.$$

Thus

$$\left|\frac{(a-2) - aiz}{(a-2)z + ai}\right|^2 - 1 = \frac{(a-2+ay)^2 + a^2x^2}{(a-2)^2x^2 + (a+y(a-2))^2} - 1$$

$$= \frac{4(1-a)(1-(x^2+y^2))}{(a-2)^2x^2 + (a+y(a-2))^2} = \frac{4(1-a)(1-|z|^2)}{(a-2)^2x^2 + (a+y(a-2))^2}.$$

Thus

$$|z|^{4034} - 1 = \frac{4(1-a)(1-|z|^2)}{(a-2)^2x^2 + (a+y(a-2))^2}.$$

Since the denominator is positive and $a < 1$ we find that $|z|^{4034} - 1$ and $1 - |z|^2$ must have the same sign. This cannot happen unless $|z| = 1$. ■

2.8 Trigonometric representation of roots

This section needs some sophisticated trigonometric techniques. You may need to take a look at some books about trigonometry[3].

Example 2.33. Find the least positive integer n such that the polynomial

$$P(z) = \sqrt{3}z^{n+1} - z^n - 1$$

has a root on the unit circle.

Moldovan Mathematical Olympiad 2008

Solution. Assume that there is a root z for $P(z)$ with $|z| = 1$. Therefore $z^n\left(z\sqrt{3} - 1\right) = 1$. Hence $|z^n| \cdot |z\sqrt{3} - 1| = 1$. Since $|z| = 1$, we can find that $|z\sqrt{3} - 1| = 1$. Whence writing $z = \cos\theta + i\sin\theta$, we have

$$\left|z\sqrt{3} - 1\right| = \left|\sqrt{3}\cos\theta - 1 + i\sqrt{3}\sin\theta\right| = 1,$$

[3]For example, you can take a look at *T. Andreescu, Z. Feng - 103 Trigonometry Problems from the Training of the USA IMO Team* or *T. Andreescu, V. Crişan - 115 Trigonometry Problems from the AwesomeMath Summer Program.*

yielding

$$\left(\sqrt{3}\cos\theta - 1\right)^2 + 3\sin^2\theta = 1.$$

Thus $4 - 2\sqrt{3}\cos\theta = 1$. Hence $\cos\theta = \frac{\sqrt{3}}{2}$, which gives $\theta = \pm\frac{\pi}{6}$. Now, substituting this into the original equation, we find that

$$\sqrt{3}\left(\cos\left(\pm\frac{\pi}{6}\right) + i\sin\left(\pm\frac{\pi}{6}\right)\right)^{n+1} - \left(\cos\left(\pm\frac{\pi}{6}\right) + i\sin\left(\pm\frac{\pi}{6}\right)\right)^n - 1 = 0.$$

Therefore

$$\sqrt{3}\cos\left(\pm\frac{(n+1)\pi}{6}\right) - \cos\left(\pm\frac{n\pi}{6}\right) - 1 = 0,$$

and

$$\sqrt{3}\sin\left(\pm\frac{(n+1)\pi}{6}\right) - \sin\left(\pm\frac{n\pi}{6}\right) = 0.$$

The first equation can be rewritten as

$$\begin{aligned} 1 &= \sqrt{3}\left(\frac{\sqrt{3}}{2}\cos\left(\frac{n\pi}{6}\right) - \frac{1}{2}\sin\left(\frac{n\pi}{6}\right)\right) - \cos\left(\frac{n\pi}{6}\right) \\ &= \frac{1}{2}\cos\left(\frac{n\pi}{6}\right) - \frac{\sqrt{3}}{2}\sin\left(\frac{n\pi}{6}\right) = \cos\left(\frac{(n+2)\pi}{6}\right) \end{aligned}$$

and hence it holds for $n \equiv 10 \pmod{12}$. The second equation can be rewritten as

$$\begin{aligned} 0 &= \sqrt{3}\left(\frac{\sqrt{3}}{2}\sin\left(\frac{n\pi}{6}\right) + \frac{1}{2}\cos\left(\frac{n\pi}{6}\right)\right) - \sin\left(\frac{n\pi}{6}\right) \\ &= \frac{1}{2}\sin\left(\frac{n\pi}{6}\right) + \frac{\sqrt{3}}{2}\cos\left(\frac{n\pi}{6}\right) = \sin\left(\frac{(n+2)\pi}{6}\right) \end{aligned}$$

and hence holds for $n \equiv 4 \pmod{6}$. Thus the polynomial has a root on the unit circle if and only if $n \equiv 10 \pmod{12}$ and the answer is $n = 10$. ■

Example 2.34. Assume that $P(z) = z^{n+1} - z^n - 1$ has a root that lies on the unit circle. Prove that $n + 2$ is divisible by 6.

Solution. Assume that r is a root with $|r| = 1$. Hence

$$r^{n+1} - r^n = 1, \quad r^n(r-1) = 1.$$

Therefore $|r|^n|r-1| = 1$, and so $|r-1| = 1$. Now, we have

$$1 = |r-1|^2 = (r-1)(\overline{r}-1) = |r|^2 + 1 - 2\,\mathrm{Re}(r) = 2 - 2\,\mathrm{Re}(r).$$

Hence $\mathrm{Re}(r) = \frac{1}{2}$. Thus

$$\mathrm{Im}(r) = \pm\sqrt{1 - \frac{1}{4}} = \pm\frac{\sqrt{3}}{2}$$

and

$$r = \frac{1}{2} \pm i\frac{\sqrt{3}}{2} = \cos\left(\frac{\pi}{3}\right) \pm i\sin\left(\frac{\pi}{3}\right).$$

Therefore

$$\begin{aligned} r^{n+1} - r^n - 1 &= \cos\left(\frac{(n+1)\pi}{3}\right) \pm i\sin\left(\frac{(n+1)\pi}{3}\right) - \cos\left(\frac{n\pi}{3}\right) \mp i\sin\left(\frac{n\pi}{3}\right) - 1 \\ &= 0, \end{aligned}$$

implying that

$$\cos\left(\frac{(n+1)\pi}{3}\right) - \cos\left(\frac{n\pi}{3}\right) - 1 = 0, \quad \sin\left(\frac{(n+1)\pi}{3}\right) - \sin\left(\frac{n\pi}{3}\right) = 0.$$

Applying the sum-to-product rules these become

$$-2\sin\left(\frac{\pi}{6}\right)\sin\left(\frac{(2n+1)\pi}{6}\right) - 1 = 0, \quad 2\sin\left(\frac{\pi}{6}\right)\cos\left(\frac{(2n+1)\pi}{6}\right) = 0,$$

or after simplifying

$$\sin\left(\frac{(2n+1)\pi}{6}\right) = -1, \quad \cos\left(\frac{(2n+1)\pi}{6}\right) = 0.$$

These hold when $2n + 1 \equiv 9 \pmod{12}$, hence when $n \equiv 4 \pmod{6}$. Thus $n + 2$ is divisible by 6. ■

Example 2.35. Let a and b be real nonzero numbers and let $z_0 \in \mathbb{C} \setminus \mathbb{R}$ be a root to the equation $z^{n+1} + az + nb = 0$, where n is a positive integer. Prove that

$$|z_0| \geq \sqrt[n+1]{b}.$$

Mihály Bencze - Mathematical Reflections, Problem U296

Solution. Let $z_0 = |z_0|(\cos\alpha + i\sin\alpha)$, where $\sin\alpha \neq 0$. From the given equation we have

$$|z_0|^{n+1}\cos(n+1)\alpha + a|z_0|\cos\alpha + nb = 0$$

and

$$|z_0|^{n+1}\sin(n+1)\alpha + a|z_0|\sin\alpha = 0.$$

Multiplying the first equation by $\sin\alpha$, the second equation by $\cos\alpha$ and subtracting side by side, we get

$$|z_0|^{n+1}\sin n\alpha = nb\sin\alpha$$

and since $\sin\alpha \neq 0$ we get that $\sin n\alpha \neq 0$ and

$$|z_0|^{n+1} = \frac{nb\sin\alpha}{\sin n\alpha}. \tag{2.4}$$

We can prove by induction on n that $|\sin n\alpha| \leq n|\sin\alpha|$ and since $\sin\alpha \neq 0$, then $|\sin n\alpha| < n|\sin\alpha|$. From (2.4) we have

$$|z_0|^{n+1} = |b|\frac{n|\sin\alpha|}{|\sin n\alpha|} \geq |b|.$$

This gives us $|z_0| \geq \sqrt[n+1]{|b|} \geq \sqrt[n+1]{b}$ and we are done. ■

Example 2.36. Find all real roots of the polynomial

$$P_d(x) = \sum_{k=0}^{d} 2^k \binom{2d}{2k} x^k (x-1)^{d-k}.$$

Solution. Clearly, $P_d(x) > 0$ for all $x > 1$. Assume that $x < 0$. Putting $x = -t$, where $t > 0$, then

$$\begin{aligned} P_d(x) &= P_d(-t) = \sum_{k=0}^{d} 2^k \binom{2d}{2k} (-t)^k (-t-1)^{d-k} \\ &= (-1)^d \sum_{k=0}^{d} 2^k \binom{2d}{2k} t^k (t+1)^k. \end{aligned}$$

If d is even, then $P_d(x) > 0$ and if d is odd, then $P_d(x) < 0$. Thus $P_d(x)$ has no roots with $x < 0$. Thus all roots x have $x \in [0,1]$. Then we can easily write

$$P_d(x) = \sum_{k=0}^{d} \binom{2d}{2k} \left(\sqrt{2x}\right)^{2k} \left(i\sqrt{1-x}\right)^{2d-2k}.$$

If we define

$$Q_d(x) = \sum_{k=0}^{d} \binom{2d}{2k-1} \left(\sqrt{2x}\right)^{2k-1} \left(i\sqrt{1-x}\right)^{2d-2k+1},$$

then

$$P_d(x) + Q_d(x) = (\sqrt{2x} + i\sqrt{1-x})^{2d},$$

and

$$P_d(x) - Q_d(x) = (\sqrt{2x} - i\sqrt{1-x})^{2d}.$$

Hence

$$2P_d(x) = \left(\sqrt{2x} + i\sqrt{1-x}\right)^{2d} + \left(\sqrt{2x} - i\sqrt{1-x}\right)^{2d}.$$

Note that $\left|\sqrt{2x} + i\sqrt{1-x}\right| = \sqrt{1+x}$. Thus

$$\sqrt{\frac{2x}{1+x}} + i\sqrt{\frac{1-x}{1+x}}$$

is a point on the unit circle in the first quadrant of the complex plane. Thus we can find an angle $\alpha \in \left[0, \frac{\pi}{2}\right]$ such that

$$\cos\alpha = \sqrt{\frac{2x}{1+x}}, \quad \sin\alpha = \sqrt{\frac{1-x}{1+x}}.$$

Then

$$\left(\sqrt{\frac{2x}{1+x}}+i\sqrt{\frac{1-x}{1+x}}\right)^{2d}=\cos 2d\alpha+i\sin 2d\alpha$$

and

$$\left(\sqrt{\frac{2x}{1+x}}-i\sqrt{\frac{1-x}{1+x}}\right)^{2d}=\cos 2d\alpha-i\sin 2d\alpha.$$

Hence

$$P_d(x)=\frac{(\sqrt{1+x})^d}{2}\left(\left(\sqrt{\frac{2x}{1+x}}+i\sqrt{\frac{1-x}{1+x}}\right)^{2d}+\left(\sqrt{\frac{2x}{1+x}}-i\sqrt{\frac{1-x}{1+x}}\right)^{2d}\right),$$

$$=(\sqrt{1+x})^d\cos 2d\alpha.$$

Thus we find roots for P_d when $\cos 2d\alpha=0$, that is, when $2d\alpha=k\pi+\frac{\pi}{2}$ or equivalently $\alpha=\frac{(2k+1)\pi}{4d}$ for $k=0,\ldots,d-1$. The resulting roots are

$$x=\frac{\cos^2\alpha}{1+\sin^2\alpha}=\frac{\cos^2\frac{(2k+1)\pi}{4d}}{1+\sin^2\frac{(2k+1)\pi}{4d}}.$$

These are distinct since the function

$$f(t)=\frac{\cos^2 t}{1+\sin^2 t}$$

is decreasing for $t\in[0,\pi/2]$. Therefore we have found d distinct real roots in $[0,1]$ and since P_d has degree d these are the only roots. ∎

2.9 Triangle Inequality and polynomials

For the absolute value of real numbers, the triangle inequality says

$$|a+b|\leq|a|+|b|$$

with equality if and only if a and b have the same sign. Similarly, we can prove that for each two complex numbers z_1,z_2 the following inequality holds:

$$|z_1+z_2|\leq|z_1|+|z_2|.$$

One can give a geometric proof of this by noting that in the complex plane $|z-w|$ is the distance between the points z and w. Alternately, on can give a purely algebraic proof. If $z_2=0$, it reduces to $|z_1|\leq|z_1|$ and we are done. Thus we may assume $z_2\neq 0$. Dividing both sides by $|z_2|$ and putting $\frac{z_1}{z_2}=z_3$, we arrive at the following inequality:

$$|z_3+1|\leq|z_3|+1.$$

Now, notice that

$$|z_3+1|^2=(z_3+1)(\overline{z_3}+1)=|z_3|^2+2\,\mathrm{Re}(z_3)+1.$$

Since $\mathrm{Re}(z_3)\leq|z_3|$, we find that

$$|z_3+1|^2\leq|z_3|^2+2|z_3|+1=(|z_3|+1)^2.$$

Therefore $|z_3+1|\leq|z_3|+1$. Equality occurs whenever $\mathrm{Re}(z_3)=|z_3|$, that is, z_3 is a positive real number and this means that $\frac{z_1}{z_2}$ is a positive real number. Geometrically, this says that the images of z_1,z_2 in the complex plane lie on the same ray from the origin.
Combining this inequality and induction gives the following.

Corollary 2.14 (Triangle Inequality) *Let $z_1,z_2,\ldots,z_n$ be complex numbers. Then the following inequality holds:*

$$|z_1+z_2+\ldots+z_n|\leq|z_1|+\ldots+|z_n|.$$

The equality occurs whenever the images of $z_1,z_2,\ldots,z_n$ in the complex plane all lie on the same ray from the origin. Equivalently, equality occurs when $\frac{z_i}{z_j}$ is a positive real number for all i,j with $1\leq i,j\leq n$ and $z_j\neq 0$.

2.9.1 Some aspects of Triangle Inequality

In this section, we shall focus on some trigonometric and geometric aspects of triangle inequality.

Example 2.37. Let x, y, z be positive real numbers. Prove that

$$\frac{xy}{\sqrt{(x^2+xz+z^2)(y^2+yz+z^2)}}+\frac{xz}{\sqrt{(x^2+xy+y^2)(z^2+yz+y^2)}}$$
$$+\frac{zy}{\sqrt{(z^2+zx+x^2)(y^2+yx+x^2)}}\geq 1.$$

Solution. Let $\omega=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}=\frac{-1+i\sqrt{3}}{2}$ be a primitive cube root of unity and consider the three complex numbers $A=x$, $B=\omega y$, and $C=\omega^2 z$. Then $|A-B|=|x-y\omega|$, and we compute Note that

$$|A-B|=\sqrt{(x-y\omega)(x-y\overline{\omega})}=\sqrt{x^2+y^2-xy(\omega+\overline{\omega})}=\sqrt{x^2+xy+y^2}.$$

Analogously, $|A-C|=\sqrt{x^2+xz+z^2}$, $\quad |B-C|=\sqrt{y^2+yz+z^2}$.
Thus the original inequality reduces to

$$\frac{|A|\cdot|B|}{|A-C|\cdot|B-C|}+\frac{|A|\cdot|C|}{|A-B|\cdot|B-C|}+\frac{|B|\cdot|C|}{|A-B|\cdot|A-C|}\geq 1.$$

By the Triangle Inequality, we find that

$$\frac{|A|\cdot|B|}{|A-C|\cdot|B-C|}+\frac{|A|\cdot|C|}{|A-B|\cdot|B-C|}+\frac{|B|\cdot|C|}{|A-B|\cdot|A-C|}$$
$$\geq\left|\frac{AB}{(A-C)(B-C)}+\frac{BC}{(B-A)(C-A)}+\frac{AC}{(A-B)(C-B)}\right|=1. \quad \blacksquare$$

Example 2.38. Let $a\geq 2$ and $x_1,\ldots,x_n$ be real numbers. Prove that the numbers

$$A=\cos x_1+\frac{\cos x_2}{a}+\ldots+\frac{\cos x_n}{a^{n-1}},$$
$$B=\sin x_1+\frac{\sin x_2}{a}+\ldots+\frac{\sin x_n}{a^{n-1}}$$

cannot simultaneously be zero.

Gazeta Matematică

Solution. For $n=1$, we find that $A^2+B^2=1$. Let $n\geq 2$ and assume that $A=B=0$. Let $z_k=\cos x_k+i\sin x_k$ for $k=1,2,\ldots,n$. Then $A+iB=0$ implies that

$$z_1+\frac{z_2}{a}+\ldots+\frac{z_n}{a^{n-1}}=0.$$

Therefore

$$\begin{aligned}1=|z_1| &= \left|\frac{z_2}{a}+\ldots+\frac{z_n}{a^{n-1}}\right|\\ &\leq \frac{|z_2|}{a}+\ldots+\frac{|z_n|}{a^{n-1}}\\ &= \frac{1}{a}+\ldots+\frac{1}{a^{n-1}}\\ &= \frac{1}{a}\cdot\frac{1-\frac{1}{a^{n-1}}}{1-\frac{1}{a}}\\ &< \frac{1}{a}\cdot\frac{1}{1-\frac{1}{a}}\\ &= \frac{1}{a-1}\leq 1,\end{aligned}$$

contradiction. Thus A, B cannot simultaneously be zero. $\blacksquare$

2.9.2 Polynomials and Triangle Inequality

There is a standard technique for using the triangle inequality to bound the roots of a polynomial.
Let r be a root of polynomial $P(x)=a_dx^d+\ldots+a_0$. We choose one (or in rare cases more than one) term in the equality $P(r)=0$ and think of it as "large". We then isolate it on one side of the equality. For example if we picked the leading term a_dr^d as the large term, we would write

$$a_dr^d=-a_{d-1}r^{d-1}-\ldots-a_0.$$

Now we take the modulus of both sides and apply the triangle inequality to the side with a sum. For the example above we find

$$|a_dr^d|=|a_{d-1}r^{d-1}+\ldots+a_0|\leq|a_{d-1}||r^{d-1}|+\ldots+|a_0|.$$

We then use whatever other hypotheses we have to draw a conclusion. For example, from the inequality above if we assume $|r| \geq 1$, then we have

$$|r| \leq \frac{|a_{d-1}|}{|a_d|} + \frac{|a_{d-2}|}{|a_d|} \cdot \frac{1}{|r|} + \ldots + \frac{|a_0|}{|a_d|} \cdot \frac{1}{|r|^{d-1}} \leq \frac{|a_{d-1}| + |a_{d-2}| + \ldots + |a_0|}{|a_d|}.$$

Hence we conclude that any root r of $P(x)$ has

$$|r| \leq \max\left(1, \frac{|a_{d-1}| + |a_{d-2}| + \ldots + |a_0|}{|a_d|}\right).$$

Many problems involving roots of polynomials can be solved in this way and we will now turn to a few examples.

Example 2.39. Find all complex numbers z satisfying simultaneously the following equations:

$$z^{2015} + z^{2014} + |z| = 3,$$

$$3z^{2015} - |z|^{2014} - z = 1.$$

Solution. Note that $3 = |z^{2015} + z^{2014} + |z|| \leq |z|^{2015} + |z|^{2014} + |z|$. Thus $|z| \geq 1$. Otherwise, the right-hand side of the inequality must be less than 3, which is a contradiction. Furthermore, $3z^{2015} = |z|^{2014} + z + 1$. By Triangle Inequality

$$3|z|^{2015} = \left||z|^{2014} + z + 1\right| \leq |z|^{2014} + |z| + 1.$$

If $|z| > 1$, then $|z|^{2015} > |z|^{2014}$, $|z|^{2015} > |z|$ and $|z|^{2015} > 1$, which contradicts the above inequality. So $|z| = 1$. Hence the equality case of Triangle Inequality occurs, that is, $\frac{z^{2015}}{z^{2014}} = z$ must be a positive real number. Therefore $z = 1$, and one easily checks that this is a solution. ■

Example 2.40. Let a, b, c be three complex numbers such that all the roots of the equation $x^3 + ax^2 + bx + c = 0$ have modulus 1. Prove that all the roots of the equation $x^3 + |a|x^2 + |b|x + |c| = 0$ have also modulus 1.

Solution. Let z_1, z_2, z_3 be the roots of polynomial $x^3 + ax^2 + bx + c$ and let r_1, r_2, r_3 be the roots of polynomial $x^3 + |a|x^2 + |b|x + |c|$. By Vieta's formulas we find that $|c| = |z_1 z_2 z_3| = 1$,

$$|a| = |-a| = |z_1 + z_2 + z_3| \leq |z_1| + |z_2| + |z_3| = 3,$$

and finally

$$|b| = |z_1 z_2 + z_1 z_3 + z_3 z_2| = |z_1 z_2 z_3| \cdot \left|\frac{1}{z_1} + \frac{1}{z_2} + \frac{1}{z_3}\right| = |z_1 z_2 z_3| \cdot |\overline{z_1} + \overline{z_2} + \overline{z_3}|.$$

Since $|c| = 1$, this gives

$$|b| = |\overline{z_1} + \overline{z_2} + \overline{z_3}| = |\overline{z_1 + z_2 + z_3}| = |z_1 + z_2 + z_3| = |a|.$$

Hence

$$x^3 + |a|x^2 + |b|x + |c| = x^3 + |a|x^2 + |a|x + 1 = (x+1)(x^2 + (|a| - 1)x + 1).$$

The discriminant of polynomial $x^2 + (|a| - 1)x + 1$ is $(|a| + 1)(|a| - 3)$. Since $|a| \leq 3$, then $(|a| + 1)(|a| - 3) \leq 0$. If the discriminant is negative, then this quadratic polynomial has two non-real roots, say $r_3 = \overline{r_2}$, and we see that

$$|r_2|^2 = r_2 \cdot \overline{r_2} = r_3 r_2 = 1.$$

Thus $|r_2| = |r_3| = 1$. If the discriminant is zero, then $|a| = 3$. Hence it is

$$x^2 + (|a| - 1)x + 1 = x^2 + 2x + 1 = (x+1)^2,$$

which has a double root at $r = -1$. In both cases, all three roots of the polynomial are of modulus 1. ■

Example 2.41. Let $P(x)$ be a polynomial with integer coefficients such that the absolute values of its coefficients are less than or equal to 2018. If $P(2020)$ is a prime number, prove that $P(x)$ is irreducible over $\mathbb{Z}[x]$.

Solution. First, we prove the following lemma.

Lemma. All the roots of $P(x)$ have absolute value less that 2019.

Proof. Assume on the contrary, that there is a root r such that $|r| \geq 2019$. Writing $P(x) = a_d x^d + \ldots + a_0$, we have

$$|r|^d = |r^d| \leq |a_d r^d| = |a_{d-1} r^{d-1} + \ldots + a_0|.$$

By the Triangle Inequality,

$$|r|^d \leq |a_{d-1}||r|^{d-1} + \ldots + |a_0| \leq 2018(|r|^{d-1} + \ldots + 1)$$

$$= 2018\frac{|r|^d - 1}{|r| - 1} \leq 2018\frac{|r|^d - 1}{2018} = |r|^d - 1.$$

The above contradiction shows that our assumption was wrong and the conclusion follows. □

Back to our problem, we can write that $P(x) = a_d(x - r_1) \cdot \ldots \cdot (x - r_d)$. Assume now that $P(x) = Q(x)R(x)$ for some nonconstant polynomials $Q(x)$ and $R(x)$ with integer coefficients. Since $P(2020) = Q(2020)R(2020)$ is prime, either $|Q(2020)| = 1$ or $|R(2020)| = 1$. Assume the latter. Letting b be the leading coefficient of R and $s_1, \ldots, s_k$ be its roots, we can write

$$R(x) = b(x - s_1) \cdot \ldots \cdot (x - s_k).$$

Since each root s_i of R is also a root of P, the Lemma tells us that $|s_1|, \ldots, |s_k| < 2019$. Hence we conclude that

$$1 = |R(2020)| = |b||2020 - s_1| \cdot \ldots \cdot |2020 - s_k|$$

$$\geq 1 \cdot (2020 - |s_1|) \cdot \ldots \cdot (2020 - |s_k|) > 1.$$

This is a contradiction. ■

Example 2.42. Given that $a_1, \ldots, a_{101}$ are nonzero real numbers such that any of the polynomials $a_{i_1}x^{100} + a_{i_2}x^{99} + \ldots + a_{i_{101}}$ has an integer root, where $i_1, \ldots, i_{101}$ is a permutation of the numbers $1, 2, \ldots, 101$, find all possible values of $a_1 + \ldots + a_{101}$.

Nairi Sedrakyan

Solution. We will show that at least one of these polynomials has 1 as a root. If we show this, then it will follow that $a_1 + \ldots + a_{101} = 0$ (and hence that 1 is always a root).
Without loss of generality, assume that $|a_{101}| = \max(|a_1|, \ldots, |a_{101}|)$. Consider the polynomial

$$a_{101}x^{100} + a_{i_1}x^{99} + \ldots + a_{i_{100}},$$

where $i_1, \ldots, i_{100}$ is an arbitrary permutation of the numbers $1, 2, \ldots, 100$. If $|r| \geq 2$ is a root, then

$$a_{101}r^{100} = -a_{i_1}r^{99} - \ldots - a_{i_{100}}$$

or equivalently

$$a_{101} = -\frac{a_{i_1}}{r} - \ldots - \frac{a_{i_{100}}}{r^{100}}.$$

By Triangle Inequality,

$$\begin{aligned} |a_{101}| &\leq \frac{|a_{i_1}|}{|r|} + \ldots + \frac{|a_{i_{100}}|}{|r|^{100}} \leq |a_{101}| \cdot \left(\frac{1}{|r|} + \frac{1}{|r|^2} + \ldots + \frac{1}{|r|^{100}}\right) \\ &\leq |a_{101}| \cdot \left(\frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^{100}}\right) < |a_{101}|. \end{aligned}$$

But this is a contradiction. We also cannot have a root at zero since the a_i are nonzero. Thus all integer roots must be ± 1. Now we just need to show that -1 cannot always be a root. Suppose on the contrary that it always is. Look at the two polynomials

$$a_{101}x^{100} + a_{100}x^{99} + \ldots + a_2x + a_1$$

and

$$a_{101}x^{100} + a_1x^{99} + \ldots + a_{99}x + a_{100}.$$

If -1 is a root of both of these, then we get

$$a_{101} - a_{100} + a_{99} - \ldots - a_2 + a_1 = 0$$

and

$$a_{101} - a_1 + a_2 - \ldots + a_{99} - a_{100} = 0.$$

Adding these, we get $a_{101} = 0$, contrary to the hypotheses. Thus there must be at least one polynomial with 1 as a root and so $a_1 + \ldots + a_{101} = 0$. ■

In the following example we combine the Triangle Inequality with Vieta's formula.

Example 2.43. Let $P(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$, $a_n \neq 0$ be a polynomial with complex coefficients such that there is an m with $\left|\frac{a_m}{a_n}\right| > \binom{n}{m}$. Prove that P has at least one zero with absolute value less than 1.

Titu Andreescu - Mathematical Reflections, Problem O83

Solution. Let w_k for $k = 1, 2, \ldots, n$ be the roots of P and note that $w_k \neq 0$ because $a_n \neq 0$. The roots of the polynomial $Q(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$ are therefore $\{1/w_k, k = 1, \ldots, n\}$.
By Vieta's formula

$$\left|\frac{a_m}{a_n}\right| = \sum_{I \in \mathcal{I}_{n-m}} \prod_{k \in I} \frac{1}{|w_k|}$$

where $\mathcal{I}_{n-m}$ is the set of all subsets of $\{1, 2, \ldots, n\}$ such that $|\mathcal{I}_{n-m}| = n - m$. If all roots of P have absolute value greater than or equal to 1, then $1/|w_k| \leq 1$ and for any integer $m \in [0, n-1]$

$$\left|\frac{a_m}{a_n}\right| \leq \sum_{I \in \mathcal{I}_{n-m}} 1 = \binom{n}{n-m} = \binom{n}{m}$$

and this contradicts the hypothesis. ∎

Example 2.44. Let $1 < t < 2$ be a real number. Prove that for all sufficiently large positive integers d there is a monic polynomial $P(x)$ of degree d, such that all of its coefficients are either 1 or -1 and

$$|P(t) - 2019| \leq 1.$$

Navid Safaei - Iranian Team Selection Test 2019

Solution. First we shall prove the following lemma.

Lemma. Let (b_n) be a sequence of positive real numbers satisfying

$$b_k \leq 2b_0 + b_1 + \ldots + b_{k-1}$$

for all k. Then for each real number z such that $|z| \leq 2b_0 + b_1 + \ldots + b_n$ there are $a_0, \ldots, a_n \in \{1, -1\}$ such that

$$\left|z - \sum_{i=0}^{n} a_ib_i\right| \leq b_0.$$

Proof. We proceed by induction on n. The base case $n = 0$ is easy since if $0 \leq z \leq 2b_0$ we can take $a_0 = +1$ and if $-2b_0 \leq z < 0$, we can take $a_0 = -1$. For the inductive step, we write the inequality $|z| \leq 2b_0 + b_1 + \ldots + b_n$ in the form

$$|z - \mathrm{Sgn}(z)b_n| \leq 2b_0 + b_1 + \ldots + b_{n-1},$$

where $\mathrm{Sgn}(z) = 1$ if $z \geq 0$ and $\mathrm{Sgn}(z) = -1$ if $z < 0$. By the inductive hypothesis we have $a_0, \ldots, a_{n-1} \in \{1, -1\}$ such that

$$\left|z - \mathrm{Sgn}(z)b_n - \sum_{i=0}^{n-1} a_ib_i\right| \leq b_0,$$

and defining $a_n = \mathrm{Sgn}(z)$ gives

$$\left|z - \sum_{i=0}^{n} a_ib_i\right| \leq b_0.$$

This completes our proof. ❑

Returning to our problem, let us define $b_i = t^i$. It is easy to deduce that

$$b_k - b_0 = t^k - 1 = (1 + t + \ldots + t^{k-1})(t-1) \leq 1 + t + \ldots + t^{k-1} = b_0 + b_1 + \ldots + b_{k-1}.$$

Hence the sequence (b_n) satisfies the hypothesis of our Lemma. If we also choose d large enough that $t^d \geq 2019$, then

$$2019 \leq t^d \leq 2 + t + \ldots + t^d.$$

Hence by our lemma, there are $a_0, \ldots, a_d \in \{1, -1\}$ such that

$$\left| \sum_{i=0}^{d} a_i t^i - 2019 \right| \leq 1$$

and we are done. ■

2.9.3 A useful lemma

One clever addition to the triangle inequality techniques we saw in the previous section, is that we can apply them to an mulitple of $P(x)$, for example to $(x-1)P(x)$. If we find a bound for all the roots of $(x-1)P(x)$, of course we have a bound for the roots of $P(x)$.
Let us illustrate this with the following example.

Example 2.45. Let $a_0 \geq a_1 \geq \ldots \geq a_{d-1} > 0$. Then all the roots of the polynomial

$$P(x) = a_{d-1}x^{d-1} + \ldots + a_0$$

satisfy $|z| \geq 1$. If one of its roots lies on the unit circle, prove that there is an integer $m \geq 2$, $m \mid d$, such that

$$P(x) = \frac{x^m - 1}{x - 1} \sum_{i=0}^{\frac{d}{m}-1} a_{mi} x^{mi}.$$

R.E. Shafer - American Mathematical Monthly

Solution. Note that

$$(z-1)P(z) = a_{d-1}z^d + (a_{d-2} - a_{d-1})z^{d-1} + \ldots + (a_0 - a_1)z - a_0.$$

Let r be a root of $P(z)$ such that $|r| \leq 1$. Then

$$\begin{aligned} |a_0| &= |a_{d-1}r^d + (a_{d-2} - a_{d-1})r^{d-1} + \ldots + (a_0 - a_1)r| \\ &\leq |a_{d-1}r^d| + |(a_{d-2} - a_{d-1})r^{d-1}| + \ldots + |(a_0 - a_1)r| \\ &= a_{d-1} + a_{d-2} - a_{d-1} + \ldots + a_0 - a_1 = a_0. \end{aligned}$$

Hence the equality case occurs throughout. Thus we must have $|r| = 1$. Also because $a_0 > 0$ this means that the complex numbers

$$a_{d-1}r^d,\ (a_{d-2} - a_{d-1})r^{d-1}, \ldots, (a_0 - a_1)r$$

must all be non-negative real numbers. In particular, r^d is a non-negative real number satisfying $|r^d| = 1$, which means $r^d = 1$. Let m be the order of r. Then $m \mid d$, $d \geq 2$ (it is clear that $P(1) \neq 0$). Now, for all k not divisible by m we have $r^k \neq 1$, so $a_{k-1} - a_k = 0$. This shows that $P(x)$ is the linear combination of polynomials of the form

$$x^{im}(1 + x + x^2 + \ldots + x^{m-1}) = x^{im}\frac{x^m - 1}{x - 1}.$$

Thus

$$P(x) = \frac{x^m - 1}{x - 1} \sum_{i=0}^{\frac{d}{m}-1} a_{mi} x^{mi}.$$ ■

The first part of this problem is interesting enough that we restate it as a stand-alone result which is part (a) below. Applying part (a) to the reciprocal polynomial $Q(x)$ of $P(x)$, or adapting the argument above gives part (b).

Corollary 2.15 *(a) If the coefficients of the polynomial $P(x)$ are positive real numbers in ascending order, then all roots of $P(x)$ lie outside or on the unit circle.*
(b) If the coefficients of the polynomial $Q(x)$ are positive real numbers in descending order, then all of the roots of $Q(x)$ lie inside or on the unit circle.

Example 2.46. Let $d \geq 2$ be a positive integer and let z be a complex number such that $|z| < 1$. Prove that

$$P(z) = z^{d-1} + 2z^{d-2} + 3z^{d-3} + \ldots + d \neq 0.$$

Solution. Since the coefficients are in a strictly increasing order, then all the roots lie outside the unit circle. ■

2.10 A useful identity

As always, identities help us! Below is a useful identity for solving some problems concerning complex roots of polynomials.

Theorem 2.16 *For all complex numbers r, z,*

$$|r-z|^2 - |1-r\overline{z}|^2 = (|r|^2-1)(1-|z|^2).$$

Proof. Observe that

$$\begin{aligned} |r-z|^2 - |1-r\overline{z}|^2 &= (r-z)(\overline{r}-\overline{z}) - (1-r\overline{z})(1-\overline{r}z). \\ &= |r|^2 + |z|^2 - 1 - |r|^2 \cdot |z|^2 \\ &= (|r|^2-1)(1-|z|^2). \end{aligned}$$

□

This identity has an invaluable implication.

Corollary

If $|z|<1, |r|>1$, then $|r-z| > |1-r\overline{z}|$.

If $|z|<1, |r|<1$, then $|r-z| < |1-r\overline{z}|$.

We first illustrate this idea with an example from the Serbian Olympiads that needs the same logic as the above lemma.

Example 2.47. Let $Q(z) = P(z+i) - P(z-i)$. If all the roots of the polynomial $P(z)$ are real, prove that all the roots of the polynomial $Q(z)$ are real.

Serbian Mathematical Olympiad 2005

Solution. Let $P(x) = C(x-r_1)\cdot\ldots\cdot(x-r_d)$, where $r_1, \ldots, r_d$ are real numbers. If polynomial $Q(z)$ has a root z, then

$$P(z+i) = P(z-i),$$

which gives

$$(z+i-r_1)\cdot\ldots\cdot(z+i-r_d) = (z-i-r_1)\cdot\ldots\cdot(z-i-r_d).$$

Then by taking the moduli on both sides, we find that

$$|(z+i-r_1)|\cdot\ldots\cdot|(z+i-r_d)| = |(z-i-r_1)|\cdot\ldots\cdot|(z-i-r_d)|.$$

Now, we compare $|(z+i-r_j)|$ and $|(z-i-r_j)|$ for all j. Note that

$$|(z+i-r_j)|^2 = (z+i-r_j)(\overline{z}+\overline{i}-r_j) = 1+|z|^2+{r_j}^2+2\mathrm{Im}(z)-2r_j\cdot\mathrm{Re}(z).$$

Similarly,

$$|(z-i-r_j)|^2 = (z-i-r_j)(\overline{z}-\overline{i}-r_j) = 1+|z|^2+{r_j}^2-2\mathrm{Im}(z)-2r_j\cdot\mathrm{Re}(z).$$

If $\mathrm{Im}(z)>0$, then $|(z+i-r_j)| > |(z-i-r_j)|$. Hence

$$|(z+i-r_1)|\cdot\ldots\cdot|(z+i-r_d)| > |(z-i-r_1)|\cdot\ldots\cdot|(z-i-r_d)|.$$

Analogously, if $\mathrm{Im}(z)<0$, then $|(z+i-r_j)| < |(z-i-r_j)|$. Hence

$$|(z+i-r_1)|\cdot\ldots\cdot|(z+i-r_d)| < |(z-i-r_1)|\cdot\ldots\cdot|(z-i-r_d)|.$$

Thus equality occurs only when $\mathrm{Im}(z)=0$, which means that z must be real.■

Example 2.48. Let $P(x) = a_d x^d + \ldots + a_0$, $a_d a_0 \neq 0$, be a polynomial with complex coefficients such that all of its roots lie inside the unit circle. Let C be a complex number such that $|C|=1$. If

$$Q(x) = \sum_{k=0}^{d} (a_k + C\overline{a_{d-k}})x^k,$$

prove that all the roots of $Q(x)$ lie on the unit circle.

Solution. Let us denote the roots of $P(x)$ by $r_1, \ldots, r_d$ with $|r_1|, \ldots, |r_d| < 1$. Since $a_0 \neq 0$, we have $r_1, \ldots, r_d \neq 0$. Now, we can write

$$P(x) = a_d(x-r_1)\cdot\ldots\cdot(x-r_d).$$

It is easy to deduce that

$$Q(x) = a_d(x-r_1)\cdot\ldots\cdot(x-r_d) + C\overline{a_d}(1-x\overline{r_1})\cdot\ldots\cdot(1-x\overline{r_d}).$$

Now, assume that $Q(z)=0$ for some complex number z. Then

$$|(z-r_1)\cdot\ldots\cdot(z-r_d)| = |C|\cdot|(1-z\overline{r_1})\cdot\ldots\cdot(1-z\overline{r_d})|.$$

Since $|C|=1$, then

$$|(z-r_1)\cdot\ldots\cdot(z-r_d)| = |(1-z\overline{r_1})\cdot\ldots\cdot(1-z\overline{r_d})|.$$

From the identity

$$|z-r_i|^2 - |1-z\overline{r_i}|^2 = (|z|^2-1)(1-|r_i|^2),$$

since $1-|r_i|^2>0$, we get

$$|(z-r_1)\cdot\ldots\cdot(z-r_d)| > |(1-z\overline{r_1})\cdot\ldots\cdot(1-z\overline{r_d})|$$

whenever $|z|>1$ and $|(z-r_1)\cdot\ldots\cdot(z-r_d)| < |(1-z\overline{r_1})\cdot\ldots\cdot(1-z\overline{r_d})|$ whenever $|z|<1$. Hence we must have $|z|=1$. ■

Example 2.49. Let $P(z)=a_0+a_1z+\ldots+a_dz^d$ be a polynomial with complex coefficients. We define its "reverse" as

$$P^*(z) = \overline{a_0}z^d + \overline{a_1}z^{d-1} + \ldots + \overline{a_d}.$$

(i) Prove that $P^*(z) = z^d\overline{P\left(\frac{1}{\overline{z}}\right)}$.

(ii) Let all roots of the polynomial $q_{d-l}(z)$ of degree $d-l$ lie inside or on the unit circle ($l>0, l\in\mathbb{Z}$). Prove that all the roots of the polynomial

$$Q(z) = z^l q_{d-l}(z) + {q_{d-l}}^*(z)$$

lie on the unit circle.

Solution. **(i)** We have

$$\begin{aligned} z^d\overline{P\left(\frac{1}{\overline{z}}\right)} &= z^d\cdot\overline{a_0+\frac{a_1}{\overline{z}}+\ldots+\frac{a_d}{\overline{z}^d}} \\ &= z^d\left(\overline{a_0}+\frac{\overline{a_1}}{z}+\ldots+\frac{\overline{a_d}}{z^d}\right) \\ &= \overline{a_0}z^d+\overline{a_1}z^{d-1}+\ldots+\overline{a_d} \\ &= P^*(z). \end{aligned}$$

(ii) Let $q_{d-l}(z)=C(z-z_1)\cdot\ldots\cdot(z-z_{d-l})$ and $|z_i|\le 1$ for all $i=1,\ldots,d-l$. If s is a root of $P(z)$, then $\frac{1}{\overline{s}}$ must be a root of $P^*(z)$. This leads to

$${q_{d-l}}^*(z) = \overline{C}(1-z\overline{z_1})\cdot\ldots\cdot(1-z\overline{z_{d-l}}).$$

Assume that $Q(r)=0$ for some complex number r. Then

$$r^l q_{d-l}(r) + {q_{d-l}}^*(r) = 0.$$

Thus $r^l q_{d-l}(r) = -{q_{d-l}}^*(r)$ and then

$$|r^l q_{d-l}(r)| = |{q_{d-l}}^*(r)|.$$

Thus $|r^l|\cdot|q_{d-l}(r)| = |{q_{d-l}}^*(r)|$, or

$$|r^l|\cdot|(r-z_1)\cdot\ldots\cdot(r-z_{d-l})| = |(1-r\overline{z_1})\cdot\ldots\cdot(1-r\overline{z_{d-l}})|.$$

If $|z_i|=1$ for some i, then

$$|r-z_i| = |\overline{z_i}|\cdot|r-z_i| = |r\overline{z_i}-1| = |1-r\overline{z_i}|.$$

Thus without loss of generality, we can assume that $|z_i|<1$ for all i. Now according to the above corollary, if $|r|>1$ then

$$\begin{aligned} |r^l|\cdot|(r-z_1)\cdot\ldots\cdot(r-z_{d-l})| &> |r^l|\cdot|(1-r\overline{z_1})\cdot\ldots\cdot(1-r\overline{z_{d-l}})| \\ &> |(1-r\overline{z_1})\ldots(1-r\overline{z_{d-l}})|, \end{aligned}$$

contradiction.

Moreover, if $|r| < 1$ then

$$|r^l| \cdot |(r - z_1) \cdot \ldots \cdot (r - z_{d-l})| < |r^l| \cdot |(1 - r\overline{z_1}) \cdot \ldots \cdot (1 - r\overline{z_{d-l}})| < |(1 - r\overline{z_1}) \cdot \ldots \cdot (1 - r\overline{z_{d-l}})|$$

and we obtain again a contradiction. So $|r| = 1$. ■

2.11 Defining a polynomial with complex roots

In this section we provide some relatively innovative examples. To solve these problems, you must first choose the right variables and the right polynomial. Then you translate the statement of the problem to a new language using these definitions. Finally, you must use what you have so far learned from complex polynomials.
We start with some number theoretic problems.

Example 2.50. Find all positive integers n such that 37 divides

$$1\underbrace{0\ldots0}_{n-1}1\underbrace{0\ldots0}_{n-1}1.$$

Solution. First, we prove the following lemma.
Lemma. The polynomial $x^{2n} + x^n + 1$ is divisible by $x^2 + x + 1$ if and only if $n \not\equiv 0 \pmod 3$.

Proof. The roots of x^2+x+1 are $\omega, \overline{\omega}$, where $\omega = \frac{-1+i\sqrt{3}}{2}$ is a primitive cube root of unity. Hence x^2+x+1 divides a polynomial $P(x)$ with real coefficients if and only if $P(\omega) = 0$.
Suppose $n \not\equiv 0 \pmod 3$. Then $2n$ and n have different nonzero residues modulo 3. Hence

$$\omega^{2n} + \omega^n + 1 = \omega^2 + \omega + 1 = 0.$$

Thus $x^2 + x + 1$ divides $x^{2n} + x^n + 1$.

If $n \equiv 0 \pmod 3$, then $\omega^n = 1$ and

$$\omega^{2n} + \omega^n + 1 = 3.$$

Hence $x^{2n} + x^n + 1 \equiv 3 \pmod{x^2 + x + 1}$. ❑

Let $P(x) = x^{2n} + x^n + 1$. It is clear that

$$P(10) = 10^{2n} + 10^n + 1 = 1\underbrace{0\ldots0}_{n-1}1\underbrace{0\ldots0}_{n-1}1.$$

Moreover, $10^2+10+1 = 111 = 3\cdot37$. Hence if $n \not\equiv 0 \pmod 3$, then 37 divides $1\underbrace{0\ldots0}_{n-1}1\underbrace{0\ldots0}_{n-1}1$ and if $n \equiv 0 \pmod 3$, then the remainder when we divide by 37 is 3. ■

Example 2.51. Prove that for each $M > 0$ there are positive integers a, b, c such that $\gcd(a, b, c) = 1$ and

$$\gcd(a + b + c, a^2 + b^2 + c^2, a^{2014} + b^{2014} + c^{2014}) > M.$$

V.A. Senderov - Kvant

Solution. Let $P(x) = x^{4028} + x^{2014} + 1$ and $\omega^3 = 1$ with $\omega \neq 1$. Then

$$P(\omega) = \omega^{4028} + \omega^{2014} + 1 = \omega^2 + \omega + 1 = 0,$$

that is, $P(\overline{\omega}) = P(\omega) = 0$ implies that $P(x)$ is divisible by

$$(x - \omega)(x - \overline{\omega}) = x^2 + x + 1.$$

Now assume $a = x^2$, $b = x$, $c = 1$. Then

$$\gcd(a + b + c, a^2 + b^2 + c^2, a^{2014} + b^{2014} + c^{2014})$$
$$= \gcd(x^2 + x + 1, x^4 + x^2 + 1, x^{4028} + x^{2014} + 1).$$

It is clear that

$$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1),$$

hence

$$\gcd(x^2+x+1, x^4+x^2+1, x^{4028}+x^{2014}+1) = x^2+x+1.$$

Thus if we choose an x with $x^2+x+1 > M$ and define $a = x^2$, $b = x$, $c = 1$ (which are relatively prime since $c = 1$), then we will have

$$\begin{aligned}\gcd(a,b,c) &= \gcd(x^2+x+1, x^4+x^2+1, x^{4028}+x^{2014}+1)\\ &= x^2+x+1 > M.\end{aligned}$$

■

Example 2.52. Prove there are infinitely many 7-tuples $(x_1,\ldots,x_7)$ of natural numbers such that $\gcd(x_1,\ldots,x_7) = 1$ and for all $k = 2,3,4,5,6$, $x_1^k + x_2^k + \ldots + x_7^k$ is divisible by $x_1+\ldots+x_7$.

Gazeta Matematică

Solution. First, we prove the following lemma.

Lemma. Let $P_k(x) = 1+x^k+x^{2k}+\ldots+x^{6k}$ for some $k \in \{1,2,\ldots,6\}$. Then $P_k(x)$ is divisible by $P(x) = 1+x+\ldots+x^6$.

Proof. Since $(x-1)P(x) = x^7-1$, we see that the roots of $P(x)$ are the primitive 7-th roots of unity. Thus $P(x)$ divides a polynomial $P_k(x)$ if and only if $P_k(\omega) = 0$ for all six primitive 7-th roots of unity ω. Since

$$P_k(x) = \frac{x^{7k}-1}{x^k-1},$$

it is clear that $P_k(\omega) = 0$. Hence $P_k(x)$ is divisible by $P(x)$. ❑

Now, choose an integer $m \geq 2$ and let

$$x_1 = 1, \quad x_2 = m, \quad \ldots, \quad x_7 = m^6.$$

Thus

$$x_1+\ldots+x_7 = P(m), \quad x_1^k + x_2^k + \ldots + x_7^k = P_k(m).$$

Since by the Lemma $P(x)$ divides $P_k(x)$, there exists a polynomial $Q_k(x)$ with integer coefficients such that $P_k(x) = P(x)Q_k(x)$. Hence $P_k(m) = P(m)Q_k(m)$. Thus $P_k(m)$ is divisible by $P(m)$ for each $k \in \{2,3,4,5,6\}$. ■

Example 2.53. Let x, y be two positive rational numbers. Assume that for some positive integers m and n the number $x^{\frac{1}{n}} + y^{\frac{1}{m}}$ is rational. Prove that $x^{\frac{1}{n}}$ and $y^{\frac{1}{m}}$ are rational numbers.

Solution. Let $\alpha = x^{1/n}$, then α is certainly a root of the polynomial $t^n - x$, but there is no reason this has to be the minimal polynomial of α. For example, if $x = r^k$ for some rational number r and integer k which divides n, then $\alpha = r^{k/n}$ is a root of $t^{n/k} - r$. One might worry that α could be a root of an even lower degree polynomial not of this form. However this is not the case as the following lemma shows.

Lemma. Let x be a positive rational number and define $\alpha = x^{1/n}$. Then the minimal polynomial of α is $t^d - r$ for some positive integer d dividing n and some positive rational number r (and hence $x = r^{n/d}$).

Proof. Let $P(t)$ be the (monic) minimal polynomial of α and assume that it has degree d. Since α is a root of $t^n - x$, it follows that $P(t)$ divides $t^n - x$ and hence all roots of P are roots of $t^n - x$. But these roots are $\alpha\omega$ for ω some n-th root of unity. Since Vieta's formulas say that $(-1)^d P(0)$ is the product of these roots (and a product of n-th roots of unity is an n-th root of unity), it follows that $P(0) = (-1)^d\alpha^d\omega$ for some n-th root of unity ω. But since P has rational coefficients, $P(0)$ is a rational number. Hence ω is real and so $\omega = \pm 1$. Thus $P(0) = \pm\alpha^d$ is rational. Hence $\alpha^d = r$ is rational and α is a root of the polynomial $t^d - r$. Since this is a monic polynomial of the same degree as $P(t)$ with α as a root, it must in fact be $P(t)$. (If they are not equal, then $P(t) - (t^d - r)$ is a nonzero polynomial of lower degree with α as a root, a contradiction.) ❑

Returning to the problem, let $\alpha = x^{1/n}$ and $\beta = y^{1/m}$ and let $c = \alpha+\beta$, which by the hypotheses is a positive rational number. By the Lemma, the minimal polynomial of α is $t^d - r$ for some positive integer d and positive rational number r and the minimal polynomial of β is similarly $t^{d'} - r'$. Assume without loss of generality that $d' \geq d$. Since $\alpha = c - \beta$, we see that β is also a root of $(c-t)^d - r$ and hence of the monic polynomial $(t-c)^d + (-1)^{d+1}r$. This is a monic polynomial of degree at most d' with β as a root. Hence it

must be the minimal polynomial of β. Thus we conclude that $d = d'$ and that

$$t^d - r' = (t-c)^d + (-1)^{d+1}r.$$

If $d > 1$, then the coefficient of t^{d-1} on the left of this equality is zero and on the right is $-dc$ which is nonzero since c, d are positive. This would be a contradiction. Hence we must have $d = 1$ and hence α and β are both rational numbers. ∎

We end this section with a great problem from the Saint Petersburg Mathematical Olympiad. This problem needs great insight into polynomials. It also has noteworthy elements of combinatorial thinking.

Example 2.54. Consider a regular n-gon with the number 1 written on one of its vertices and number 0 is written on all the other vertices. Gabriel modifies the numbers by a sequence of steps. At the first step, Gabriel adds to the value at each vertex the value of its neighbor (in the clockwise direction). At the second step, he adds to the value at each vertex the number written on the vertex that is the neighbor of its neighbor (in the clockwise direction). He continues in this way adding values at vertices one more step clockwise until on the final step he adds the value of its neighbor (in counterclockwise direction). After the above-mentioned process, it turns out that $n-1$ of the resulting numbers are equal. Find all possible values for n.

M. Antipov

Solution. Label the vertices by $0, 1, \ldots, n-1$ so that the vertex which initially has the value 1 is vertex 0 and the clockwise neighbor has 1 lower index modulo n. If the numbers on the vertices are $a_0, \ldots, a_{n-1}$, then we associate to them the polynomial $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. Thus the polynomial corresponding to the starting state will be just the constant polynomial 1. Note that since the labels should be thought of as being cyclic modulo n, we should think of this polynomial as being defined modulo $x^n - 1$.
The step of adding the value at the neighbor k places clockwise is the same as multiplying by $1 + x^k$, and then taking the result modulo $x^n - 1$. Therefore our final polynomial will be the remainder of $(1+x)\cdot\ldots\cdot(1+x^{n-1})$ taken

modulo $x^n - 1$. Thus we have reduced the problem to a purely polynomial problem. If we ask that the $n-1$ equal values be b and the n-th value equals $a+b$ and is at vertex m, then the problem becomes the following: Find all integers n such that the remainder of $(1+x)\cdot\ldots\cdot(1+x^{n-1})$ modulo $x^n - 1$ is of the form

$$ax^m + b(1 + x + \ldots + x^{n-1})$$

for some a, b and $0 \le m \le n-1$. We can refine this a little more if we let $P(x) = 1 + x + \ldots + x^{n-1}$. Since $(x-1)P(x) = x^n - 1$, the desired condition is that $P(x)$ divides $(1+x)\cdot\ldots\cdot(1+x^{n-1}) - ax^m$ for some a, m.
Suppose that $(1+x)\cdot\ldots\cdot(1+x^{n-1}) - ax^m$ is a multiple of $P(x)$.
If n is even, then -1 is a root of $P(x)$. Thus

$$0 = (1-1)\cdot\ldots\cdot(1+(-1)^n) - a(-1)^m = (-1)^{m+1}a,$$

and hence $a = 0$. (This says that all n values are equal.) Plugging in $x = 1$, we find that $P(1) = n$ divides $(1+1)\cdot\ldots\cdot(1+1^{n-1}) = 2^{n-1}$. Hence n must be a power of 2. Conversely, if $n = 2^r$, then the factors of $(1+x)\cdot\ldots\cdot(1+x^{n-1})$ include

$$(1+x)(1+x^2)(1+x^4)\cdot\ldots\cdot(1+x^{2^{r-1}})$$

and the product of these is easily seen to be $P(x)$. (This follows by induction on r or by noting that it is the same as saying that any number in the range $0, 1, \ldots, 2^r - 1$ can be written uniquely as $\sum_{i=0}^{r-1} d_i 2^i$ for $d_i \in \{0, 1\}$.)
Now suppose n is odd. We first prove the following lemma.

Lemma. Let n be an odd number and let ω be a primitive n-th root of unity. Then

$$(1+\omega)\cdot\ldots\cdot(1+\omega^{n-1}) = 1.$$

Proof. Since the roots of $x^n - 1$ are the n-th roots of unity which we can write as $1, \omega, \ldots, \omega^{n-1}$, we have $x^n - 1 = (x-1)(x-\omega)(x-\omega^2)\cdot\ldots\cdot(x-\omega^{n-1})$. Putting $x = -1$ and using the fact that n is odd, we find that

$$-2 = -2(-1-\omega)\cdot\ldots\cdot(-1-\omega^{n-1}) = -2(1+\omega)\cdot\ldots\cdot(1+\omega^{n-1}).$$

The result follows. ❑

Returning to our problem, since ω is a root of $P(x)$, we find that

$$(1+\omega)\cdot\ldots\cdot(1+\omega^{n-1})-a\omega^m=0.$$

By the Lemma, we get $a\omega^m=1$. Thus ω^m must be a real number which is an n-th root of unity. Since n is odd, this forces $\omega^m=1$ and hence $m=0$. Hence we also conclude that $a=1$. (This says that the one different value is the one at vertex 0, which is one higher than all the rest.) Thus $(1+x)\cdot\ldots\cdot(1+x^{n-1})-1$ is a multiple of $P(x)$.
Now, assume that $n=pl$ for some odd prime p and for some integer l. Let α be a primitive p-th root of unity. Then the numbers $1,\alpha,\alpha^2,\ldots,\alpha^{n-1}$ cycle through the numbers $1,\alpha,\alpha^2,\ldots,\alpha^{p-1}$ taking each value l times. Thus the Lemma implies

$$2(1+\alpha)\cdot\ldots\cdot(1+\alpha^{n-1})=(2(1+\alpha)\cdot\ldots\cdot(1+\alpha^{p-1}))^l=2^l$$

and hence

$$(1+\alpha)\cdot\ldots\cdot(1+\alpha^{n-1})=2^{l-1}.$$

Since p divides n, α is also an n-th root of unity and hence a root of

$$\frac{x^n-1}{x-1}=P(x).$$

Hence plugging in α we get

$$0=(1+\alpha)\cdot\ldots\cdot(1+\alpha^{n-1})-1=2^{l-1}-1.$$

Whence $l=1$ and $n=p$ is a prime number.
Conversely, if n is an odd prime number, then all roots of $P(x)$ are primitive n-th roots of unity. So the Lemma says that all roots of $P(x)$ are roots of $(1+x)\cdot\ldots\cdot(1+x^{n-1})-1$. This implies that $P(x)$ divides $(1+x)\cdot\ldots\cdot(1+x^{n-1})-1$. Thus the possible n are odd prime numbers and powers of 2. ■

2.12 Miscellaneous problems

Example 2.55. Let $S=\{z\in\mathbb{C}\mid |z|=1\}$. Prove that there is no nonconstant polynomial $P(x)$ with real coefficients such that $P(S)\subseteq\mathbb{R}$.

Solution. Suppose that $P(x)=a_dx^d+\ldots+a_0$ with $a_d\neq 0$. Because $P(z)$ is real for each complex number z such that $|z|=1$, it is easy to deduce that

$$P(z)=\overline{P(z)}=P(\overline{z})=P\left(\frac{1}{z}\right).$$

Whence the equation $P(x)=P\left(\frac{1}{x}\right)$ has infinitely many solutions. Therefore

$$P(x)=P\left(\frac{1}{x}\right)$$

for all x, but in this case

$$\lim_{x\to\infty}P(x)=\lim_{x\to\infty}P\left(\frac{1}{x}\right)=P(0).$$

Hence $P(x)$ must be constant, contrary to the hypothesis. ■

Example 2.56. Find all polynomials $P(x)$ with real coefficients such that for each real number θ we have

$$P(\cos\theta+i\sin\theta)=|P(\cos\theta+i\sin\theta)|.$$

Solution. We can easily find that for each complex number z such that $|z|=1$ we have $P(z)=|P(z)|$. This implies that $P(z)$ is real for all $|z|=1$. Then by the above problem $P(z)=c$, where $c\geq 0$. ■

We end this chapter with two inequalities that require one to define a polynomial and use complex numbers.

Example 2.57. Let a,b,c,d be real numbers satisfying

$$a^2+b^2+c^2+d^2\leq 1.$$

Prove that $4abcd-\frac{3}{4}\leq ab+ac+bc+cd+da+db\leq 4abcd+\frac{5}{4}$.

Gabriel Dospinescu - Crux Mathematicorum

Solution. Define

$$\begin{aligned} S &= ab + ac + bc + cd + da + db, \\ P(x) &= (x-a)(x-b)(x-c)(x-d) \\ &= x^4 - (a+b+c+d)x^3 + Sx^2 - (abc + bcd + cda + dab)x + abcd. \end{aligned}$$

Then

$$|P(it)|^2 = |t^4 - St^2 + abcd + i((a+b+c+d)t^3 - (abc + bcd + cda + dab)t)|^2.$$

It is clear that $|x+iy| \geq |x|$. Thus $|P(it)|^2 \geq |t^4 - St^2 + abcd|^2$.
On the other hand,

$$\begin{aligned} |P(it)|^2 &= (a+it)(b+it)(c+it)(d+it)(a-it)(b-it)(c-it)(d-it) \\ &= (a^2+t^2)(b^2+t^2)(c^2+t^2)(d^2+t^2). \end{aligned}$$

Therefore we easily find that

$$(a^2+t^2)(b^2+t^2)(c^2+t^2)(d^2+t^2) \geq |t^4 - St^2 + abcd|^2.$$

Putting $t = \frac{1}{2}$, we have

$$\left(a^2+\frac{1}{4}\right)\left(b^2+\frac{1}{4}\right)\left(c^2+\frac{1}{4}\right)\left(d^2+\frac{1}{4}\right) \geq \left|\frac{1}{16} - \frac{S}{4} + abcd\right|^2.$$

Finally, by the AM-GM Inequality,

$$\left(a^2+\frac{1}{4}\right)\left(b^2+\frac{1}{4}\right)\left(c^2+\frac{1}{4}\right)\left(d^2+\frac{1}{4}\right) \leq \left(\frac{a^2+b^2+c^2+d^2+1}{4}\right)^4 = \frac{1}{16}.$$

Therefore

$$\left|\frac{1}{16} - \frac{S}{4} + abcd\right|^2 \leq \frac{1}{16}.$$

Hence

$$\left|\frac{1}{4} - S + 4abcd\right| \leq 1.$$

Thus

$$-\frac{3}{4} \leq S - 4abcd \leq \frac{5}{4}.$$

■

Example 2.58. Let $x_1, \ldots, x_n$ be real numbers. For $1 \leq k \leq n$, define

$$S_k = \sum_{1 \leq i_1 < \ldots < i_k \leq n} x_{i_1} \cdot \ldots \cdot x_{i_k},$$

and $S_0 = 1$. Prove that

$$\prod_{k=1}^{n}(1+x_k^2) \geq 2\left|\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor}(-1)^k S_{2k}\right| \cdot \left|\sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor}(-1)^k S_{2k+1}\right|.$$

High School Mathematics Journal 10/2018

Solution. Let $P(x) = (x+x_1)\cdot\ldots\cdot(x+x_n) = x^n + S_1 x^{n-1} + \ldots + S_n$. It is clear that

$$\prod_{k=1}^{n}(1+x_k^2) = \prod_{k=1}^{n}(x_k+i)\prod_{k=1}^{n}(x_k-i) = P(i)P(-i) = |P(i)|^2.$$

Since

$$P(i) = i^n + S_1 i^{n-1} + \ldots + S_n = i^n\left(\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor}(-1)^k S_{2k} - i\sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor}(-1)^k S_{2k+1}\right),$$

we get

$$|P(i)|^2 = \left(\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor}(-1)^k S_{2k}\right)^2 + \left(\sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor}(-1)^k S_{2k+1}\right)^2,$$

which is indeed greater than or equal to

$$2\left|\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor}(-1)^k S_{2k}\right| \cdot \left|\sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor}(-1)^k S_{2k+1}\right|$$

and we are done. ■

2.13 Proposed problems

Problem 2.1. Let $n \equiv 3 \pmod 8$ and let

$$(x^2+1)^n = a_{2n}x^{2n} + a_{2n-1}x^{2n-1} + \ldots + a_1x + a_0.$$

Find $a_0 + a_8 + \ldots + a_{2n-6}$.

Alessandro Ventullo

Problem 2.2. Let x_1, x_2, x_3, x_4 be the roots of the equation

$$x^4 - (m+2)x^3 + (m^2+m+1)x^2 + 2x - 2 = 0, \quad m \in \mathbb{R}.$$

(a) If $x_1 = 1+i$, find $m \in \mathbb{R}$ and solve the equation.

(b) Under conditions of point (a), evaluate $x_1^{2006} + x_2^{2006} + x_3^{2006} + x_4^{2006}$.

Trident Competition 2006

Problem 2.3. **(a)** Solve in $\mathbb{C}$ the equation

$$x^6 + 3x^5 + 12x^4 + 19x^3 + 15x^2 + 6x + 1 = 0.$$

(b) Evaluate $\sum_{k=1}^{6} \left|1 + \frac{1}{x_k}\right|$ and $\sum_{k=1}^{6} |x_k|^2$, where $x_1, x_2, x_3, x_4, x_5, x_6$ are the roots of the given equation.

Vasile Berghea - Gazeta Matematică B 9/2007 *Problem* C:3217

Problem 2.4. Let

$$P(x) = (x-r)(x-r^2)(x-r^3)(x-r^4)$$

be a polynomial with real coefficients. Find all possible values of r.

Problem 2.5. Let $r_1, \ldots, r_{10}$ be the nonreal roots of polynomial $x^{11}+11x+1$. Find the largest positive integer less than or equal to $\left|\sum_{j=1}^{10} r_j^{10}\right|$.

Korean Mathematical Olympiad, 2nd Round 2010

Problem 2.6. Let r_1, r_2, r_3 be the roots of polynomial $P(x) = x^3+111x^2+1$. Let $Q(x)$ be a polynomial of degree 3 such that

$$Q\left(r_i + \frac{1}{r_i}\right) = 0 \text{ for all } i = 1, 2, 3.$$

Find $\frac{Q(1)}{Q(-1)}$.

Problem 2.7. Find the product of the roots of the equation

$$\sum_{k=1}^{2017} \frac{1}{z - \varepsilon_k} = 0,$$

where ε_k are the roots of the polynomial $x^{2018} - 1$, other than 1.

Problem 2.8. Let x and y be complex number and let n be a positive integer. Prove that

$$x^{2n} - x^n y^n + y^{2n} = \prod_{\substack{1 \le k < 3n \\ \gcd(k,6)=1}} \left(x^2 - 2\cos\left(\frac{k\pi}{3n}\right)xy + y^2\right).$$

Roman Witula, Ddyta Hetmaniok, Damian Slota - The College Mathematics Journal, Problem 1876

Problem 2.9. Consider the polynomial

$$f(x) = x^n + 2x^{n-1} + 3x^{n-2} + \ldots + nx + n + 1$$

and let $\varepsilon = \cos\frac{2\pi}{n+2} + i\sin\frac{2\pi}{n+2}$. Prove that

$$f(\varepsilon)f(\varepsilon^2)\cdot\ldots\cdot f(\varepsilon^{n+1}) = (n+2)^n.$$

Mihai Piticari - Alexandru Myller Competition 2003

Problem 2.10. Let n be a positive integer and let $z_1, \ldots, z_n$ be the roots of $1 + z^n$. For each $a > 0$, prove that

$$\frac{1}{n}\sum_{k=1}^{n}\frac{1}{|z_k - a|^2} = \frac{1 + a^2 + \ldots + a^{2(n-1)}}{(1+a^n)^2}.$$

Gheorghe Stoica - American Mathematical Monthly, Problem 11947

Problem 2.11. Let $a \neq 0, b, c$ be real numbers. Prove that there is a polynomial $P(x)$ with real coefficients such that $aP(x)^2 + bP(x) + c$ is divisible by $x^2 + 1$.

Alexander Golovanov

Problem 2.12. Prove that if k, m, n are non-negative integers, then the polynomial

$$P(x) = x^{3k+2} + x^{3m+1} + x^{3n}$$

is divisible by $x^2 + x + 1$.

Polish Mathematical Olympiad 1966

Problem 2.13. Prove that for every positive integer k the polynomial

$$(x^4 - 1)(x^3 - x^2 + x - 1)^k + (x+1)x^{4k-1}$$

is divisible by $x^5 + 1$.

Polish Mathematical Olympiad 1986

Problem 2.14. Let $f(x)$ be a polynomial and let n be a positive integer. Prove that if $f(x^n)$ is divisible by $x - 1$, then it is also divisible by

$$x^{n-1} + x^{n-2} + \ldots + x + 1.$$

Polish Mathematical Olympiad 1988

Problem 2.15. Determine all pairs (n, r), where n is a positive integer and r is a real number for which the polynomial $(x+1)^n - r$ is divisible by the polynomial $2x^2 + 2x + 1$.

Polish Mathematical Olympiad 1996

Problem 2.16. Using a given sequence of positive real numbers $q_1, q_2, \ldots$, a sequence of polynomials is constructed in the following way:

$$\begin{aligned} f_0(x) &= 1 \\ f_1(x) &= x \\ f_{n+1}(x) &= (1+q_n)xf_n(x) - q_n f_{n-1}(x) \qquad \text{if } n \geq 1. \end{aligned}$$

Prove that all real roots of these polynomials belong to the interval $[-1, 1]$.

Moscow Mathematical Olympiad 1968

Problem 2.17. Find all complex numbers $a \neq 0$ and b such that for every complex root z of the equation $x^4 - ax^3 - bx - 1 = 0$, we have $|a - z| \geq |z|$.

Nikolai Nikolov - Bulgarian Mathematical Olympiad 2006

Problem 2.18. If a non-real number z_0 is a root of the polynomial $z^{n+1} - z^2 + az + 1$, where a is any real number and $n \geq 2$, prove that

$$|z_0| > \frac{1}{\sqrt[n]{n}}.$$

German Team Selection Test 2009

Problem 2.19. Prove that if the roots of the polynomial

$$P(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + (-1)^n \in \mathbb{C}[x]$$

have the same modulus, then $P(-1) \in \mathbb{R}$.

N. Micu - Romanian Mathematical Olympiad 1974

Problem 2.20. Let d be an odd positive integer and let

$$P(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0$$

be a polynomial with complex coefficients such that all of its roots lie on the unit circle and $a_0 \neq 1$. Prove that $\frac{a_{d-1}-a_1}{1-a_0}$ is a real number.

Problem 2.21. Let $a \neq 0$, $m > n$, $m \neq 2n$ and assume that the absolute values of all roots of polynomial $ax^m + bx^n + c$ are the same. Prove that $b = 0$.

Problem 2.22. Let $P(x) = a_dx^d + a_{d-1}x^{d-1} + \ldots + a_0$ be a polynomial with complex coefficients such that all of its roots lie inside the unit circle. Let

$$P^*(x) = x^d\overline{P}\left(\frac{1}{x}\right).$$

Prove that all the roots of $P(z) + P^*(z)$ lie on the unit circle.

Problem 2.23. Let $|a| \leq 1$ be a real number. Prove that all the roots of the equation $x^{n+1} - ax^n - ax + 1 = 0$ lie on the unit circle.

Problem 2.24. Let a, b, c, d be real numbers such that $b - d \geq 5$ and all roots x_1, x_2, x_3, and x_4 of the polynomial $P(x) = x^4 + ax^3 + bx^2 + cx + d$ are real. Find the smallest value the product

$$(x_1^2 + 1)(x_2^2 + 1)(x_3^2 + 1)(x_4^2 + 1)$$

can take.

Titu Andreescu - USA Mathematical Olympiad 2014

Chapter 3

Finding Polynomials. Part I

Many years ago, the most important topic in polynomials was finding some unknown polynomial(s) from one or more system of equations. Recently, we have seen fewer problems from this topic in mathematical competitions. The reason may partially be the lack of innovation or creativity in proposing such problems. Although finding polynomials is no longer a central topic in polynomials and mathematical competitions, there are plenty of problems that include some elements and ideas from this topic.
In this and the next two chapters, we deeply investigate finding polynomials.

3.1 Some basic properties

On many occasions, good substitutions are helpful. One technique is to find values for the variables that lead to some expression vanishing or at least simplifying.

Example 3.1. **(i)** Find all polynomials $P(x)$ such that

$$P(x + x^2) = x + x^2 + \ldots + x^{2017} + x^{2018}.$$

(ii) Find all polynomials $Q(x)$ such that

$$Q(x + x^2 + x^3) = x + x^2 + \ldots + x^{2017} + ax^{2018} + bx^{2019} + x^{2020},$$

for some real numbers a and b.

Solution. (i) Putting $x = 1$, we find that $P(2) = 2018$. Putting $x = -2$, we find that

$$P(2) = -2 + 4 - 8 + \ldots + (-2)^{2018} = \frac{2^{2019} - 1}{3} \neq 2018.$$

Thus there is no such polynomial.

(ii) Putting $x = -1$ and $x = i$ we find that

$$Q(-1) = a - b, \quad Q(-1) = (1 - a) + i(1 - b).$$

Therefore $b = 1$, $a - b = 1 - a$, which gives $(a, b) = (1, 1)$. But $x = 0$ and $x = \omega = \frac{-1+i\sqrt{3}}{2}$ give

$$Q(0) = 0, \quad Q(\omega) = (b - a) + \omega(2 - a).$$

and hence $(a, b) = (2, 2)$. Thus there is no solution. ■

Example 3.2. Find all polynomials $P(x)$ such that for any real numbers x, y we have

$$P(x + y) \geq P(x) + (x + 1)P(y).$$

First Solution. Putting $x = -1$, we find that $P(y - 1) \geq P(-1)$ for each y. This implies that $P(x)$ has even degree and positive leading coefficient. Furthermore, putting $x = y = 0$, we find that $P(0) \leq 0$. On the other hand, setting $x = -2$, $y = 0$, we get $P(0) \geq 0$. Thus $P(0) = 0$. Now, setting $y = -x$, we get

$$P(x) + (x + 1)P(-x) \leq 0.$$

The left-hand side is an odd degree polynomial with a positive leading coefficient. Thus the polynomial cannot be negative for all sufficiently large $x > 0$. It follows that $P(x)$ must be constant. Since $P(0) = 0$, we conclude that $P(x) = 0$. ■

Second Solution. Clearly $P(x) = 0$ is a solution. Suppose P is not the zero polynomial and let $d = \deg P \geq 0$. Substituting $y = x^2$ and rearranging, we get $P(x + x^2) - P(x) - (x + 1)P(x^2) \geq 0$. The left-hand side is a polynomial of degree $2d + 1$, hence this cannot hold for all x. Thus the only solution is the zero polynomial. ■

Example 3.3. Find all pairs of positive real numbers (a, b) such that the polynomial

$$P(x) = ax^2 + b$$

satisfies following inequality for all real numbers x, y:

$$P(xy) + P(x + y) \geq P(x)P(y).$$

Solution. By rewriting explicitly the original inequality, we get

$$(ax^2y^2 + b) + (a(x + y)^2 + b) \geq (ax^2 + b)(ay^2 + b).$$

Putting $y = 0$, we obtain

$$a(1 - b)x^2 + b(2 - b) \geq 0$$

for all real numbers x. Thus $1 - b \geq 0$, which gives $0 < b \leq 1$. Substituting $y = -x$, we find that

$$a(1 - a)x^4 - 2abx^2 + b(2 - b) \geq 0$$

for all real numbers x. Thus $a(1 - a) \geq 0$. Hence $0 < a \leq 1$. If $a = 1$, we get $-2bx^2 + b(2 - b) \geq 0$, that is, $-2x^2 + 2 - b \geq 0$. The latter inequality is absurd for all sufficiently large x, so $0 < a < 1$. Now, from

$$a(1 - a)x^4 - 2abx^2 + b(2 - b) \geq 0,$$

we get

$$(a(1 - a)x^2 - ab)^2 + ab(2 - 2a - b) \geq 0.$$

Hence $2-2a-b \geq 0$. In short, we find that $0 < a < 1, 0 < b \leq 1, 0 < 2a+b \leq 2$. Now, we prove that the preceding conditions are sufficient. That is, let

$$\begin{aligned} Q(x,y) &= (ax^2y^2+b)+(a(x+y)^2+b)-(ax^2+b)(ay^2+b) \\ &= (a-a^2)x^2y^2+a(1-b)(x^2+y^2)+2axy+b(2-b). \end{aligned}$$

Since $a(1-b) \geq 0$ and $x^2+y^2 \geq -2xy$, we can write

$$Q(x,y) \geq a(1-a)x^2y^2+2abxy+b(2-b).$$

Let $z = xy$. We must study the sign of $R(z) = a(1-a)z^2+2abz+b(2-b)$. By the same reasoning as before, we see that $R(z) \geq 0$ for all real numbers z whenever $0 < 2a+b \leq 2$ and we are done. ∎

Example 3.4. Let d be a positive integer. Show that if d is odd, then there are no polynomials $P(x)$, $Q(x)$ such that the only coefficients of these polynomials are 1, -1 and

$$\frac{P(x)}{Q(x)} = x^d - x^{d-1} + 1.$$

Solution. Let $\deg P(x) = p$ and $\deg Q(x) = q$. Since the given equation says $P(x) = (x^d - x^{d-1}+1)Q(x)$, we see that $p = q+d$. Since d is odd, this means that $p+q$ is odd. Plugging in $x = 1$, we get $P(1) = Q(1)$, hence $P(1)+Q(1)$ is even. However $P(1)$ is a sum of $p+1$ terms each equal to ± 1, that is, a sum of $p+1$ odd numbers and similarly for Q. Thus $(p+1)+(q+1)$ is even, hence $p+q$ is even, a contradiction. ∎

3.2 When two polynomials are identical?

When we are trying to find the polynomials that satisfy a given equation, it is usually the case that both sides of the equation are themselves polynomials. Thus we need to think about what equations we can extract from an equality of two polynomials. We saw one answer to this in the previous section, we can plug in values to extract equations. We also need to think about how we can prove two polynomials are identical.

The most direct way to answer this is probably to invoke the definition: two polynomials $P(x)$ and $Q(x)$ are equal exactly when all the corresponding coefficients of the polynomials are equal. In particular, this implies that $\deg P(x) = \deg Q(x)$. We will take this approach in the next section. Before we do this, it is natural to wonder if we can use the method of the previous section instead. That is, can we prove two polynomials are equal by just plugging in values?

Assume that $\deg P(x) = p \geq \deg Q(x) = q$. If we have $P(x) = Q(x)$, for at least $p+1$ different complex numbers, then the polynomial $P(x) - Q(x)$ has degree at most p, but has at least $p+1$ distinct complex roots. This means that $P(x) - Q(x)$ must be the zero polynomial. Therefore $P(x)$, $Q(x)$ are identical (and in particular $p = q$).

Identity Principle

If the equation $P(x) = Q(x)$ has at least $1 + \max\{\deg P(x), \deg Q(x)\}$ distinct roots, then $P(x)$ and $Q(x)$ are identical.
If the equation $P(x) = Q(x)$ has infinitely many roots, then $P(x)$ and $Q(x)$ are identical.

Example 3.5. Determine all polynomials $P(x)$ of the smallest possible degree with the following properties:

(i) the leading coefficient is 200;

(ii) the coefficient of the lowest power which is not equal to zero is 2;

(iii) the sum of all of its coefficients is 4;

(iv) $P(-1) = 0$;

(v) $P(2) = 6$;

(vi) $P(3) = 8$.

Solution. From condition (iii), we find that $P(1) = 4$. Defining

$$Q(x) = P(x) - (2x + 2),$$

we find that

$$Q(1) = Q(2) = Q(3) = Q(-1) = 0.$$

Thus we can write

$$Q(x) = P(x) - (2x + 2) = (x - 1)(x - 2)(x - 3)(x + 1)R(x)$$

and hence

$$P(x) = 2x + 2 + (x - 1)(x - 2)(x - 3)(x + 1)R(x)$$

for some polynomial $R(x)$. Since we see that the leading coefficient of P is the same as the leading coefficient of R, condition (i) tells us that the leading coefficient of R is 200. The constant coefficient of P is $P(0) = 2 - 6R(0)$. From condition (ii) we know that this is either 2 or 0. In the first case, we see that $R(0) = 0$ and hence setting $R = 200x$ gives a polynomial

$$P(x) = 2(x + 1) + 200x(x - 1)(x - 2)(x - 3)(x + 1)$$

of degree 5 that satisfies all the conditions of the problem. Thus we only need to look for other solutions of degree at most 5, and hence we may assume R is constant or linear. In the second case we see that $R(0) = \frac{1}{3}$. Since this is not the same as the leading coefficient of R, we see that R cannot be constant and the only linear possibility is $R(x) = 200x + \frac{1}{3}$. But it is easy to check that in this case the x coefficient of P is not equal to either 0 or 2. Hence the minimal degree is 5 and the only solution of degree 5 is

$$\begin{aligned} P(x) &= 200x(x - 1)(x - 2)(x - 3)(x + 1) + 2x + 2 \\ &= 200x^5 - 1000x^4 + 1000x^3 + 1000x^2 - 1198x + 2. \end{aligned}$$

■

Example 3.6. Let m and n be positive integers with $n > 1$ and let $a_1, \ldots, a_m$ be a nonconstant arithmetic progression. Find the largest value of m for which there is a polynomial $P(x)$ of degree n such that $P(a_1), \ldots, P(a_m)$ is a nonconstant arithmetic progression.

Solution. Let $a_2 - a_1 = d \neq 0$ and $P(a_2) - P(a_1) = D \neq 0$. Then

$$a_k = a_1 + (k - 1)d \quad \text{for } k = 1, \ldots, m$$

and $P(a_k) = P(a_1) + (k - 1)D$ for $k = 1, \ldots, m$. Let $r = \dfrac{D}{d} \neq 0$. Define

$$Q(x) = P(x) - r(x - a_1) - P(a_1).$$

Then

$$\begin{aligned} Q(a_k) &= P(a_k) - r(a_k - a_1) - P(a_1) \\ &= P(a_k) - (k - 1)D - P(a_1) \\ &= 0. \end{aligned}$$

Since $\deg Q(x) = \deg P(x) = n$ and $Q(x)$ has $a_1, \ldots, a_m$ as roots, we find that $n \geq m$. Now, we provide an example for $m = n$. That is,

$$P(x) = (x - a_1) \cdot \ldots \cdot (x - a_n) + x.$$

Then $P(a_k) = a_k$ and we are done. ■

We end this section with a synthetic problem concerning polynomial values that in some sense needs the above-mentioned knowledge.

Example 3.7. Can there be a sequence $(a_n)_{n>0}$ of positive integers and a polynomial P such that $a_n = P(n)$ for all sufficiently large positive integer n if:

(i) $a_n = 2^n$?

(ii) $a_n = \left\lfloor \dfrac{n^2 + n + 1}{3} \right\rfloor$?

Solution. **(i)** First, we shall prove the following lemma.

Lemma. Let $\deg P(x) = d$. Then for all sufficiently large x we have

$$P(x) < x^{d+1}.$$

Proof. Let $P(x) = a_d x^d + \ldots + a_0$, and $M = \max |a_i|$.

For each $x > M + 1$, we have

$$1 + x + \ldots + x^d = \frac{x^{d+1} - 1}{x - 1} < \frac{x^{d+1}}{M}.$$

Thus for $x > M + 1$

$$x^{d+1} > M(1 + x + \ldots + x^d) \geq \sum_{k=0}^{d} |a_k| x^k \geq \left| \sum_{k=0}^{d} a_k x^k \right| = |P(x)| \geq P(x),$$

and we are done. □

Now, let $\deg P(x) = d$ and suppose $P(n) = 2^n$ for all sufficiently large positive integers n. Then by the Lemma, for all sufficiently large positive integers n we have $2^n < n^{d+1}$. But in fact the reverse inequality holds for all sufficiently large n, so this is a contradiction.

(ii) Suppose $P(n)$ is a polynomial such that

$$P(n) = \left\lfloor \frac{n^2 + n + 1}{3} \right\rfloor$$

for all sufficiently large positive integers n. Define

$$Q(n) = \frac{n^2 + n + 1}{3}.$$

For all $n \equiv 1 \pmod 3$, we have

$$\left\lfloor \frac{n^2 + n + 1}{3} \right\rfloor = \frac{n^2 + n + 1}{3}.$$

Hence $P(n) = Q(n)$ for infinitely many n, thus P and Q are identical. But if $n = 3m$ is large enough, then we see that

$$P(3m) = \left\lfloor \frac{9m^2 + 3m + 1}{3} \right\rfloor = 3m^2 + m \neq Q(3m) = 3m^2 + m + \frac{1}{3}.$$ ■

3.3 Examining the coefficients

As we have already said, two polynomials are identical exactly when all the corresponding coefficients agree, and in particular the degrees are the same. This provides another strategy for finding the polynomials satisfying a given equation.

Strategy

(i) *Degree Condition* (DC): examine the degree of both sides of the polynomial identity.

(ii) *Examining Coefficients* (EC): examine the coefficients of identical monomials on both sides.

For examining the coefficients, you almost always use some algebraic techniques for finding the coefficient of x^d. You can see the first volume of the polynomial trilogy for this.

Example 3.8. If the polynomials

$$P(x) = a_2 x^2 + 3x + a_0, \quad Q(x) = b_3 x^3 - x^2 + b_1 x - 4$$

are identical, then $b_3 = 0$, $a_2 = -1$, $b_1 = 3$, $a_0 = -4$.

Example 3.9. Polynomials $P(x)$, $Q(x)$ have integer coefficients and satisfy the relation

$$P(Q(x+1)) = P(x^3)\,(Q(x+1))^5 \qquad \forall x.$$

(i) Prove that the degree of the polynomial $P(x)Q(x)$ is divisible by 8.

(ii) Find an example of monic polynomials satisfying the above equation.

(iii) Are there non-monic polynomials that satisfies the above equation?

Solution. (i) Let $\deg P(x) = p$ and $\deg Q(x) = q$. Then

$$\deg P(Q(x+1)) = pq,$$

$$\deg\left(P(x^3)\,(Q(x+1))^5\right) = \deg P(x^3) + \deg\,(Q(x+1))^5 = 3p + 5q.$$

Hence $pq = 3p + 5q$, which gives $(p-5)(q-3) = 15$. Then

$$(p,q) \in \{(6,18),(8,8),(10,6),(20,4)\}.$$

Since $\deg P(x)Q(x) = \deg P(x) + \deg Q(x) = p + q$, it is easy to check that this is divisible by 8 for all four cases.

(ii) It is easy to see that $P(x) = x^p$, $Q(x) = (x-1)^q$ satisfy the statement of our problem for all pairs $(p,q) \in \{(6,18),(8,8),(10,6),(20,4)\}$.

(iii) It is easy to see that if $P(x)$, $Q(x)$ satisfy the original equation, then $CP(x)$, $Q(x)$, where C is a constant, satisfy it too. Thus P need not be monic. If $a \neq 0$ is the leading coefficient of Q, then looking at the leading coefficient of both sides gives $a^p = a^5$, and since all four cases have p even, we see that $a = 1$. Thus Q must be monic. ■

Example 3.10. Find all polynomials $P(x)$ such that

$$P(2x) + 2P(-x) = 6P(x) \qquad \forall x.$$

Solution. Let $P(x) = a_d x^d + \ldots + a_0$. Examining the coefficient of x^k on both sides, for $0 \leq k \leq d$, we find that

$$(2^k + 2(-1)^k)a_k = 6a_k.$$

Hence either $a_k = 0$ or $2^k + 2(-1)^k = 6$, which implies $k \in \{2,3\}$. Thus

$$P(x) = a_3x^3 + a_2x^2.$$ ■

Example 3.11. Find all polynomials $P(x)$ with real coefficients such that

$$P(a+b-2c)+P(b+c-2a)+P(c+a-2b) = 3P(a-b)+3P(b-c)+3P(c-a)$$

for all real numbers a, b, c.

Benelux Mathematical Olympiad 2010

Solution. It is clear that if $P_1(x)$, $P_2(x)$ are solutions to the above equation, then $C_1P_1(x) + C_2P_2(x)$, where $C_1, C_2 \in \mathbb{R}$, is also a solution. Furthermore, setting $a = b = c$, we get $P(0) = 0$. If $b = c = 0$, then

$$P(-2a) = P(a) + 3P(-a).$$

Hence writing $P(x) = a_dx^d + \ldots + a_0$ and comparing the leading coefficients, we obtain

$$(-2)^d = 1 + 3(-1)^d.$$

Hence $d \in \{1,2\}$. It is easy to check that polynomials $P_1(x) = x^2$, $P_2(x) = x$ satisfy the statement of the problem. Hence all polynomials of the form $C_1x^2 + C_2x$ satisfy the condition of the problem. ■

Example 3.12. Let $\deg P(x) = d$. Find all polynomials $P(x)$ such that

$$P(x + P(x)) = P(P(x)) + P(x)^d + 1 \qquad \forall x.$$

Mongolian Mathematical Olympiad 2015

Solution. If $d = 1$, then $P(x) = ax + b$ with $a \neq 0$. Therefore

$$P(x + P(x)) = a(x + ax + b) + b = (a^2 + a)x + ab + b$$

and

$$P(P(x)) + P(x)^d + 1 = a(ax + b) + ax + 2b + 1 = (a^2 + a)x + ab + 2b + 1.$$

Hence $b = -1$ and $P(x) = ax - 1$.
If $d > 1$, examining the leading coefficients on both sides, we find that

$$a_d^{d+1} = a_d^{d+1} + a_d^d.$$

Hence $a_d^d = 0$, impossible. ■

Example 3.13. Find all polynomials $P(x) \neq 0$ with real coefficients such that for all $k = 0, 1, \ldots, (\deg P)^2$ we have

$$P(P(k)) = P(k)^2.$$

Swiss IMO Team Selection Test 2011

First Solution. Let $P(x) = a_d x^d + \ldots + a_0$. Then for $1 + d^2$ points, we have

$$P(P(x)) = P(x)^2.$$

The polynomial $Q(x) = P(P(x)) - P(x)^2$ has $1 + d^2$ distinct roots. Since $\deg Q(x) \leq d^2$, we conclude that $Q(x) = 0$, i.e., $P(P(x)) = P(x)^2$. The degree condition shows that $d \in \{0, 2\}$. If $d = 0$, then $P(x) = c$. Thus $c = c^2$, i.e., $c = 0$ or $c = 1$. Since $c \neq 0$, then $P(x) = 1$. If $d = 2$, then $P(x) = a_2 x^2 + a_1 x + a_0$. Thus

$$P(a_2 x^2 + a_1 x + a_0) = (a_2 x^2 + a_1 x + a_0)^2.$$

Since

$$P(a_2 x^2 + a_1 x + a_0) = a_2(a_2 x^2 + a_1 x + a_0)^2 + a_1(a_2 x^2 + a_1 x + a_0) + a_0,$$

examining the coefficients of x^4, we find that $a_2^3 = a_2^2$. Thus $a_2 = 1$ and

$$a_1(x^2 + a_1 x + a_0) + a_0 = 0.$$

Thus $a_1 = a_0 = 0$, which implies that $P(x) = x^2$ is the only nonconstant solution. ■

Second Solution. If $P(x) = c \neq 0$ is a constant polynomial, then the equation becomes $c = c^2$, and hence $c = 1$. If P is not constant, then we see that $P(t) = t^2$ for infinitely many values of t, namely for all t which are $P(x)$ for some x. Hence $P(x) = x^2$. ■

3.3.1 Using rewritings

In some cases, the facts we learn about a polynomial may allow us to rewrite the polynomial, and hence (hopefully) lead to a simpler equation. Two common cases of such rewriting are the following.

Strategy

(i) If $P(r) = 0$ for some r, we can write $P(x) = (x - r)^k Q(x)$ for some polynomial $Q(x)$ such that $Q(r) \neq 0$ and some positive integer k.

(ii) If $\deg P(x) = d$, we can write $P(x) = a_d x^d + Q(x)$ for some polynomial $Q(x)$ such that $\deg Q(x) < d$.

Example 3.14. Find all polynomials $P(x)$ with real coefficients such that

$$P(x^2) = x^2(1 + x^2)P(x) \qquad \forall x.$$

Solution. Clearly $P(x) = 0$ is a solution. Otherwise, let $\deg P(x) = d \geq 0$. After comparing the degree of both sides, we find that $2d = 4 + d$. Hence $d = 4$. Moreover, $P(0) = 0$. Writing $P(x) = x^r Q(x)$, where $1 \leq r \leq 4$ and $Q(0) \neq 0$, we find that $x^{2r} Q(x^2) = x^{r+2}(1 + x^2)Q(x)$.
Then $2r = r + 2$, which gives $r = 2$. Thus $Q(x^2) = (1 + x^2)Q(x)$ for some quadratic polynomial Q. Putting $x = i$, we get $Q(-1) = 0$, which implies that $Q(x) = (1 + x)R(x)$ for some linear polynomial $R(x)$. Then R satisfies

$$(1 + x^2)R(x^2) = (1 + x^2)(1 + x)R(x).$$

Hence $R(x^2) = (1 + x)R(x)$. Writing $R(x) = ax + b$, where $a \neq 0$, we have

$$ax^2 + b = (1 + x)(ax + b).$$

Hence $b = (a + b)x + b$, implying $a + b = 0$. That is, $R(x) = a(x - 1)$. Noting that the case $a = 0$ gives the zero polynomial, which we already saw was a solution, we have solutions

$$P(x) = ax^2(x^2 - 1), \qquad \forall a.$$ ■

Example 3.15. Let d be a positive integer. Determine all polynomials $P(x)$ with real coefficients such that

$$(1+x^d)P(x) = P(x^2) \qquad \forall x.$$

Solution. Note that $P(x) = 0$ is clearly a solution.
Otherwise, let $\deg P(x) = D \geq 0$. It is clear that

$$\deg(1+x^d)P(x) = d + D, \quad \deg P(x^2) = 2D.$$

Hence $D = d$. Now, set

$$P(x) = a(x^d - 1) + Q(x), \quad a \neq 0, \quad \deg Q(x) < d.$$

Then

$$(1+x^d)P(x) = (1+x^d)(a(x^d-1)+Q(x)) = a(x^{2d}-1) + (1+x^d)Q(x)$$

and

$$P(x^2) = a(x^{2d}-1) + Q(x^2).$$

Hence we arrive at

$$(1+x^d)Q(x) = Q(x^2).$$

If $\deg Q(x) = k \geq 0$, we get $d + k = 2k$, i.e., $k = d$, a contradiction. We conclude that $Q(x) = 0$. Since the zero polynomial gives the case $a = 0$, we have solutions

$$P(x) = a(x^d - 1), \qquad \forall a. \quad \blacksquare$$

Example 3.16. Find all polynomials $P(x)$ such that

$$P(P(x)) = (x^2 + x + 1)P(x) \qquad \forall x.$$

Solution. The zero polynomial is clearly a solution.
Otherwise let $\deg P(x) = d \geq 0$. Then

$$\deg P(P(x)) = d^2, \quad \deg(x^2+x+1)P(x) = 2 + d.$$

Hence $d^2 = 2 + d$, that is, $d = 2$. Let $P(x) = a_2x^2 + a_1x + a_0$, $a_2 \neq 0$. Then

$$a_2(a_2x^2 + a_1x + a_0)^2 + a_1(a_2x^2 + a_1x + a_0) + a_0 = (x^2+x+1)(a_2x^2 + a_1x + a_0).$$

Hence comparing the coefficient of x^4, we find that $a_2^2 = a_2$. Thus $a_2 = 1$. Therefore

$$(x^2 + a_1x + a_0)^2 + a_1(x^2 + a_1x + a_0) + a_0 = (x^2 + x + 1)(x^2 + a_1x + a_0).$$

Comparing the coefficient of x^3, we find that $2a_1 = a_1 + 1$, which gives $a_1 = 1$. Therefore

$$(x^2 + x + a_0)^2 + (x^2 + x + a_0) + a_0 = (x^2 + x + 1)(x^2 + x + a_0).$$

Comparing the coefficient of x, we find that $2a_0 + 1 = a_0 + 1$, which gives $a_0 = 0$, and so $P(x) = x^2 + x$. It is easy to check that this is a solution. Thus the solutions are $P(x) = 0$ or $P(x) = x^2 + x$. $\blacksquare$

Example 3.17. Find the minimal degree of a polynomial $Q(x)$ for which there is a polynomial $P(x)$ with real coefficients such that

$$P(P(x)) = P(x)^{40} + x^{80} + Q(x) \qquad \forall x.$$

Solution. If $P(x) = 0$, then $Q(x) = -x^{80}$ has degree 80. Otherwise, suppose $\deg P(x) = d \geq 0$ and write the given equation as

$$Q(x) = P(P(x)) - P(x)^{40} - x^{80}.$$

The three terms on the right have degrees d^2, $40d$, and 80, respectively. If no two of these are equal, then the leading term cannot cancel and hence $\deg Q(x) \geq \max(d^2, 40d, 80) \geq 80$. We cannot have $d^2 = 80$ since d is an integer. If $40d = 80$, so that $d = 2$, then the leading coefficients of the last two

terms are both negative and cannot cancel and again $\deg Q(x) = 80$. Thus we are left with the case $d^2 = 40d$ and the leading coefficients of the first two terms cancel. Write $P(x) = a_{40}x^{40} + R(x)$ with $a_{40} \neq 0$ and $\deg R(x) = k < 40$. Then we see that the cancellation of the leading coefficients means $a_{40}^{41} = a_{40}^{40}$, and hence $a_{40} = 1$. In this case, we find

$$Q(x) = R(x^{40} + R(x)) - x^{80}.$$

The first term on the right has degree $40k$ and again $Q(x)$ will have degree at least 80 unless the two terms have the same degree and the leading coefficients cancel. Hence we are reduced to the case $k = 2$ and $R(x) = x^2 + bx + c$ is monic. In this case, we find

$$Q(x) = 2(x^2 + bx + c)x^{40} + bx^{40} + (x^2 + bx + c)^2 + b(x^2 + bx + c) + c,$$

which is a polynomial of degree 42. Thus the minimum degree is 42. ■

Example 3.18. Find all polynomials $P(x)$ with real coefficients such that

$$P(x^2 - y^2) = P(x + y)P(x - y) \qquad \forall x, y.$$

First Solution. Clearly $P(x) = 0$ is a solution. Otherwise, let $\deg P(x) = d \geq 0$. Setting $y = 0$ gives $P(x^2) = P(x)^2$ for all x. Examining the leading coefficients, we see that $P(x)$ is monic, so we can write $P(x) = x^d + R(x)$ where $\deg R(x) < d$. Then

$$x^{2d} + R(x^2) = x^{2d} + R(x)^2 + 2x^d R(x).$$

Hence $R(x^2) = R(x)^2 + 2x^d R(x)$. Suppose $\deg R(x) = r \geq 0$. Then the degree of $R(x^2)$ is $2r$ and the degree of $R(x)^2 + 2x^d R(x)$ is $\max(2r, r + d) = r + d$. Since $r < d$, we get a contradiction. Thus the only possibility is $R(x) = 0$ and so $P(x) = x^d$. It is easy to check that this is a solution, hence the solutions are $P(x) = 0$ or $P(x) = x^d$ for $d \geq 0$. ■

Second Solution. If a polynomial $P(x) = cx^d$ is a solution, then we find $c = c^2$, hence $c = 0$ or 1. Thus the only solutions of this form are $P(x) = 0$ and $P(x) = x^d$ for $d \geq 0$. If we have any other solution, then it must have a complex root $r \neq 0$. Set $y = 0$. Then $P(x^2) = P(x)^2$ for all x. Iterating this (or using induction), we see that $P\left(x^{2^n}\right) = P(x)^{2^n}$ for all integers $n \geq 1$. Choose $m = 2^n > \deg P(x)$ and considering the complex solutions of the equation $x^m = r$, and denote them $r_1, \ldots, r_m$. (We saw in Theorem 2.9 that there are m distinct roots of this equation.) Plugging $x = r_i$, it follows that

$$P(r_i)^m = P\left(r_i^m\right) = P(r) = 0.$$

Hence $r_1, \ldots, r_m$ are distinct roots of $P(x)$. This is a contradiction since P can only have $\deg P(x)$ roots. Thus the only solutions are the ones we found earlier. ■

Third Solution. Assume that $P(x)$ has a root $r \neq 0$ and restrict to x, y with $x - y = r$. Then

$$x^2 - y^2 = r(x + y) = r(2x - r),$$

and hence the equation becomes $P(r(2x - r)) = 0$ for each x. Since $r \neq 0$, we can set $x = \frac{r^2+t}{2r}$ and then get $P(t) = 0$ for all t. Thus $P(x) = 0$. So if P has any nonzero root, then it is the zero polynomial. The only other possibility is $P(x) = cx^d$ for some $c \neq 0$ and $d \geq 0$. As in the previous solution, this gives solutions $P(x) = x^d$ for $d \geq 0$. ■

Example 3.19. Find all polynomials with real coefficients $P(x)$ and $Q(x)$ such that

$$P(x)^2 + Q(y)^2 = P(y^2) + Q(x^2) \qquad \forall x, y.$$

Vadym Radchenko - Ukrainian Mathematical Olympiad 2002

Solution. Assume that $P(x)$ and $Q(x)$ are nonconstant. Substituting $y = 0$, we get that $P(x)^2 - Q(x^2)$ is constant and so $P(x)$ and $Q(x)$ have the same degree. Let

$$P(x) = a_d x^d + \ldots + a_0, \quad Q(x) = b_d x^d + \ldots + b_0.$$

Then $a_d^2 = b_d$. Now, going back to the original equation, the coefficient of y^{2d} on the left-hand side is b_d^2 and on the right-hand side is a_d. Hence $b_d^2 = a_d^4 = a_d$,

which gives $a_d = 1$ and then $b_d = 1$. Writing

$$P(x) = x^d + P_1(x), \quad Q(x) = x^d + Q_1(x)$$

with $\deg P_1(x)$, $\deg Q_1(x) < d$, we obtain

$$P_1^2(x) + 2x^d P_1(x) + Q_1^2(y) + 2y^d Q_1(y) = P_1(y^2) + Q_1(x^2).$$

Let $\deg P_1(x) = m \geq 0$ and $\deg Q_1(x) = n \geq 0$, where $m, n < d$. Then the left-hand side contains terms of degree $d+m$ and $d+n$ in x, y, but the right-hand side contains only terms of degrees $2m$ and $2n$ in x, y. This shows that $P_1(x) = Q_1(x) = 0$ and so $P(x) = Q(x) = x^d$. ∎

Example 3.20. Find all polynomials $P(x)$ such that

$$P(x)^3 + 3P(x)^2 = P(x^3) - 3P(-x) \qquad \forall x.$$

Solution. If $P(x)$ is a constant polynomial, say $P(x) = c$, then we find

$$c^3 + 3c^2 + 2c = 0$$

and hence $P(x) = 0$, $P(x) = -1$, or $P(x) = -2$.
Otherwise, let $\deg P(x) = d > 0$. Writing $P(x) = a_d x^d + Q(x)$, where $\deg Q(x) = k \leq d - 1$ and comparing the coefficients of x^{3d} on both sides, we find that $a_d^3 = a_d$. Therefore $a_d = \pm 1$. Then the given equation becomes

$$(\pm x^d + Q(x))^3 + 3(\pm x^d + Q(x))^2 = \pm x^{3d} + Q(x^3) \mp 3(-1)^d x^d - 3Q(-x).$$

After expanding, we find that

$$3x^{2d}Q(x) \pm 3x^d Q(x)^2 + Q(x)^3 + 3x^{2d} \pm 6x^d Q(x) + 3Q(x)^2$$
$$= Q(x^3) \mp 3(-1)^d x^d - 3Q(-x).$$

Assume that $Q(x)$ is nonconstant so $d > 0$. Then the left-hand side has degree $2d + k$, while the right-hand side has degree $\max\{3k, d\}$, which is impossible. Thus $Q(x) = c$ is a constant polynomial, and we get

$$3cx^{2d} \pm 3c^2 x^d + c^3 + 3x^{2d} \pm 6cx^d + 3c^2 = c \mp 3(-1)^d x^d - 3c$$

or equivalently

$$(3c+3)x^{2d} \pm (3c^2 + 6c + 3(-1)^d)x^d + (c^3 + 3c^2 + 2c) = 0.$$

From the coefficient of x^{2d}, we see that $3c + 3 = 0$, which gives $c = -1$. This makes the constant term cancel, but the coefficient of x^d then gives $-3 + 3(-1)^d = 0$, that is, d must be even. Hence the nonconstant solutions are $P(x) = \pm x^d - 1$, where d is an even positive integer. ∎

Example 3.21. Find all real numbers a and rational functions $R(x)$ such that

$$R(x)^2 = R(x^2) + a.$$

Japanese Mathematical Olympiad 1995

Solution. If $R(x) = c$ is constant, then we get a trivial solution for $a = c^2 - c$. If $R(x)$ is a nonconstant polynomial, then let $\deg R(x) = r > 0$. We can write $R(x) = b_r x^r + S(x)$ where $b_r \neq 0$ and $\deg S(x) = s < r$. Then we find

$$b_r^2 x^{2r} + 2b_r x^r S(x) + S(x)^2 = b_r x^{2r} + S(x^2) + a.$$

From the coefficients of x^{2r} on both sides we get $b_r^2 = b_r$ and hence $b_r = 1$ and the equation cancels to

$$2x^r S(x) + S(x)^2 = S(x^2) + a.$$

If S is not the zero polynomial, then the left-hand side has degree $r+s$ and the right-hand side has degree $2s$, a contradiction. Thus we must have $S(x) \equiv 0$ and hence $a = 0$. Thus we get the solutions $R(x) = x^r$ and $a = 0$.
If $R(x)$ is a non-polynomial rational function, write $R(x) = \frac{P(x)}{Q(x)}$ for some coprime polynomials $P(x)$ and $Q(x)$ with $Q(x)$ nonconstant and monic. Then

$$\frac{P(x)^2}{Q(x)^2} = a + \frac{P(x^2)}{Q(x^2)}.$$

Hence

$$\frac{P(x)^2 - aQ(x)^2}{Q(x)^2} = \frac{P(x^2)}{Q(x^2)}.$$

Since both sides are irreducible rational functions with monic denominators, we find that

$$Q(x)^2 = Q(x^2), \quad P(x)^2 - aQ(x)^2 = P(x^2).$$

From the equality $Q(x)^2 = Q(x^2)$, we get $Q(x) = x^d$ with $d \geq 1$ (see the solutions to Example 3.18 for several proofs of this). Hence we have

$$P(x)^2 - ax^{2d} = P(x^2). \tag{3.1}$$

Write $P(x) = a_n x^n + \ldots + a_0$, with $a_n \neq 0$. Note that since Q is nonconstant, Q has a factor of x. Since P and Q are relatively prime, it follows that $a_0 = P(0) \neq 0$. Setting $x = 0$, we get $a_0^2 = a_0$, and hence $a_0 = 1$. Since P clearly cannot be a constant polynomial, there is some smallest positive index k such that $a_k \neq 0$. Hence $P(x) = a_n x^n + \ldots + a_k x^k + 1$. Then the lowest nonconstant nonzero term in $P(x)^2$ is $2a_k x^k$ and the lowest nonconstant nonzero term in $P(x^2)$ is $a_k x^{2k}$. Since $2k > k$ and the lowest nonconstant terms on the two sides of (3.1) must agree, we must have $k = 2d$ and $a = 2a_k$. Note that in particular, this implies $n \geq k = 2d > d$. Equating the coefficients of x^{2n} on both sides of (3.1), we get $a_n^2 = a_n$ and hence $a_n = 1$. Let the next most significant nonzero coefficient of $P(x)$ be the coefficient of x^m, so $P(x) = x^n + a_m x^m + \ldots + 1$. Then the next nonzero coefficient of $P(x)^2$ is $2a_m x^{m+n}$ and of $P(x^2)$ is $a_m x^{2m}$. Since $m + n > 2m$ and the next nonzero coefficients on the two sides of (3.1) must agree, we must have $n + m = 2d$. But we already saw that $n \geq k = 2d$, hence we must have $m = 0$, $n = k = 2d$, and $a = 2a_n = 2$. Thus we have

$$R(x) = \frac{x^{2d}+1}{x^d} = x^d + \frac{1}{x^d}, \quad a = 2, d \geq 1$$

and it is easy to check that these are solutions. ∎

Example 3.22. Find all polynomials $P(x)$ and $Q(x)$ such that

$$P(x + Q(y)) = Q(x + P(y)).$$

Solution. We clearly have trivial solutions with $P(x) = Q(x)$. Note that the only solutions with either P or Q a constant polynomial are of this trivial type. Thus we may assume $P \neq Q$ and that neither is a constant polynomial.

Putting $x = -P(y)$, we get $P(Q(y) - P(y)) = Q(0)$. Since P is not a constant polynomial this implies that $Q(y) - P(y)$ must be one of the finitely many roots of $P(z) = Q(0)$. However, since $Q(y) - P(y)$ is a continuous function of y, it cannot jump between the roots. Hence we must have $Q(y) - P(y) = C$ for some constant C, which is nonzero since we assumed $P \neq Q$. Then $Q(y) = P(y) + C$, so we compute

$$P(x + P(y) + C) = P(x + P(y)) + C.$$

Taking $y = 0$ and $x = z - P(0)$, we find that

$$P(z) + C = P(z + C).$$

Since this says $P(z + C) - P(z) = C$ is a constant polynomial, we deduce that $P(x)$ is linear. Writing $P(x) = ax + b$, we deduce that $aC = C$. Therefore $a = 1$ and $P(x) = x + b$. It follows that $Q(x) = x + b + C = x + c$ and it is easy to check that these are solutions. ∎

Example 3.23. Find all polynomials $P(x)$ such that $P(2014) = 1$ and

$$xP(x - c) = (x - 2014)P(x), \quad \text{for some integer } c.$$

Iberoamerican Mathematical Olympiad 2014

Solution. Let $P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0$. Then

$$x(a_d(x - c)^d + a_{d-1}(x - c)^{d-1} + \ldots + a_1(x - c) + a_0)$$

$$= (x - 2014)(a_d x^d + a_{d-1} x^{d-1} + \ldots a_1 x + a_0).$$

Examining the coefficient of x^d in the above identity, we find that

$$-dca_d + a_{d-1} = a_{d-1} - 2014a_d.$$

Therefore $dc = 2014$ and so

$$d \in \{1, 2, 19, 38, 53, 106, 1007, 2014\} \text{ and } c = \frac{2014}{d}.$$

Now, putting $x = cd = 2014$ into the original equation, we get

$$P((d-1)c) = 0.$$

Putting $x = (d-1)c$, we get $P((d-2)c) = 0$. Iterating this, we get

$$P((d-1)c) = \ldots = P(c) = P(0) = 0.$$

Since $\deg P(x) = d$ and we have found d distinct roots, we obtain

$$P(x) = a_d x(x-c)(x-2c)\cdot\ldots\cdot(x-(d-1)c).$$

Since $P(2014) = P(dc) = 1$, we find that

$$1 = a_d cd(cd-c)(cd-2c)\cdot\ldots\cdot(cd-(d-1)c) = a_d c^d d!.$$

Hence $a_d = \frac{1}{c^d d!}$ and then

$$P(x) = \frac{1}{c^d d!}x(x-c)(x-2c)\cdot\ldots\cdot(x-(d-1)c),$$

where $cd = 2014$, $d \in \{1, 2, 19, 38, 53, 106, 1007, 2014\}$. ■

3.4 Equations that hold for infinitely many values

There are many important facts about polynomials that, if you know them, make solving problems easier. One of these we have encountered before (If two polynomials agree at infinitely many points, then they are identical.), but is worth looking at in more detail.

One way this fact arises is in problems like: Find all polynomials $P(x)$ such that

$$P(Q(x)) = 2Q(x) + 1,$$

for some nonconstant polynomial $Q(x)$. To solve this, we can simply note that since $Q(x)$ is nonconstant, it assumes infinitely many values, thus the equation $P(x) = 2x + 1$ has infinitely many solutions. Therefore $P(x) = 2x + 1$.

We will see more elaborate uses of this fact below.

Example 3.24. Find all nonconstant polynomials $P(x)$ and $Q(x)$ with real coefficients such that

$$P(Q(x)^2) = P(x)Q(x)^2.$$

Solution. Let $\deg P(x) = m$ and $\deg Q(x) = n$. Then

$$\deg P(Q(x)^2) = 2nm, \quad \deg P(x)Q(x)^2 = m + 2n.$$

Therefore $2mn = m + 2n$, which gives $(m-1)(2n-1) = 1$. Since m and n are positive integers, we find that $m = 2$, $n = 1$. Writing

$$P(x) = ax^2 + bx + c, \quad a \neq 0,$$

we find that

$$aQ(x)^4 + bQ(x)^2 + c = P(x)Q(x)^2.$$

Hence c must be divisible by $Q(x)^2$. Since $Q(x)$ is nonconstant, this forces $c = 0$. So

$$aQ(x)^2 + b = P(x).$$

Substituting this into the original equation, we find that

$$aQ(Q(x)^2)^2 + b = aQ(x)^4 + bQ(x)^2.$$

Now, consider the equation

$$aQ(t)^2 + b = at^2 + bt.$$

This equation has $Q(x)^2$ as a root. Since $Q(x)$ is nonconstant, it can assume infinitely many real values. Hence the aforementioned equation has infinitely many roots. Thus for each real number x,

$$Q(x)^2 = x^2 + \frac{b}{a}x - \frac{b}{a}.$$

Whence $x^2 + \frac{b}{a}x - \frac{b}{a}$ must be the square of a polynomial, hence it has double root. Therefore its discriminant must be zero, implying that $\frac{b}{a} \in \{0, -4\}$. Hence either $Q(x)^2 = x^2$ or $Q(x)^2 = (x-2)^2$. In the first case, we get $Q(x) = \pm x$ and we find $P(x) = ax^2$. In the second we have $Q(x) = \pm(x-2)$ and we find $P(x) = a(x-2)^2 - 4a$. It is easy to check that these are solutions. ■

Example 3.25. Find all nonconstant polynomials $P(x)$ and $Q(x)$ with real coefficients such that $P(Q(x)) = P(x)Q(x) - P(x)$.

Solution. Let $\deg P(x) = m$ and $\deg Q(x) = n$. Then

$$\deg P(Q(x)) = mn, \quad \deg P(x)Q(x) - P(x) = m + n.$$

Hence $mn = m+n$, which gives $(m-1)(n-1) = 1$. Since m and n are positive integers, we get $m = n = 2$. Writing $P(x) = ax^2 + bx + c$, we get

$$aQ(x)^2 + bQ(x) = P(x)Q(x) - (P(x) + c),$$

implying that $P(x)+c$ is divisible by $Q(x)$. Since $P(x)$ and $Q(x)$ have the same degree, it follows that there is a real number d such that $P(x) + c = dQ(x)$. Hence $P(x) = dQ(x) - c$. Substituting this into the original equation, we get

$$\begin{aligned} dQ(Q(x)) - c &= (dQ(x) - c)Q(x) - (dQ(x) - c) \\ &= dQ(x)^2 - (d + c)Q(x) + c. \end{aligned}$$

Considering the equation $dQ(t) = dt^2 - (d + c)t + 2c$, we deduce that it has $Q(x)$ as a root. Since $Q(x)$ is nonconstant, it can assume infinitely many real values. Hence the aforementioned equation has infinitely many roots. Thus

$$Q(x) = x^2 - \left(1 + \frac{c}{d}\right)x + \frac{2c}{d}.$$

Since $P(x) = dQ(x) - c$, we conclude that

$$P(x) = dx^2 - (d + c)x + c. \qquad \blacksquare$$

Example 3.26. Find all monic polynomials P and Q, with real coefficients, such that

$$P(1) + P(2) + \ldots + P(n) = Q(1 + 2 + 3 + \ldots + n), \text{ for all } n \geq 1.$$

Ovidiu Furdui - Mathematical Reflections, Problem U95

Solution. Since $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$, we can write the equation as

$$P(1) + P(2) + \ldots + P(n) = Q\left(\frac{n(n+1)}{2}\right).$$

Subtracting the analogous equation for $n - 1$

$$P(1) + P(2) + \ldots + P(n-1) = Q\left(\frac{n(n-1)}{2}\right),$$

we get

$$P(n) = Q\left(\frac{n^2+n}{2}\right) - Q\left(\frac{n^2-n}{2}\right),$$

for each integer $n \geq 2$. This holds for infinitely many values, so we have the equality of polynomials

$$P(x) = Q\left(\frac{x^2+x}{2}\right) - Q\left(\frac{x^2-x}{2}\right).$$

Writing $Q(x) = x^d + \ldots + b_0$, we compute

$$Q\left(\frac{x^2+x}{2}\right) - Q\left(\frac{x^2-x}{2}\right)$$

$$= \left(\left(\frac{x^2+x}{2}\right)^d - \left(\frac{x^2-x}{2}\right)^d\right) + b_{d-1}\left(\left(\frac{x^2+x}{2}\right)^{d-1} - \left(\frac{x^2-x}{2}\right)^{d-1}\right) + \ldots.$$

If we apply the binomial theorem to expand the first term, the x^{2d} term cancels, but the x^{2d-1} terms combine to give $\frac{d}{2^{d-1}}x^{2d-1}$. Since all the other terms are degree $2(d-1)$ or less, we have

$$P(x) = Q\left(\frac{x^2+x}{2}\right) - Q\left(\frac{x^2-x}{2}\right) = \frac{d}{2^{d-1}}x^{2d-1} + \ldots$$

Since $P(x)$ is monic, we find that $d = 2^{d-1}$, which gives $d \in \{1, 2\}$. If $d = 1$, then writing $Q(x) = x + b$, we find

$$P(x) = Q\left(\frac{x^2+x}{2}\right) - Q\left(\frac{x^2-x}{2}\right) = x.$$

If $d = 2$, then writing $Q(x) = x^2 + ax + b$, we find

$$P(x) = Q\left(\frac{x^2+x}{2}\right) - Q\left(\frac{x^2-x}{2}\right) = x^3 + ax. \qquad \blacksquare$$

3.5 The only periodic polynomial is constant

Suppose that $P(x + c) = P(x)$ for some nonzero constant number c. This equation says that the function $P(x)$ is periodic with period c, or more tersely we say $P(x)$ is c-periodic. Applying this formula for $x = 0, c, 2c, \ldots$, we find that

$$P(0) = P(c) = P(2c) = \ldots P(2019c) = \ldots.$$

This says that the equation $P(x) = P(0)$ has infinitely many solutions, which implies that $P(x) = P(0)$ for all x, that is, $P(x)$ is a constant polynomial. Hence we deduce the following.

Theorem

The only periodic polynomial is the constant polynomial.

Example 3.27. Find all polynomials $P(x)$ such that

$$P((x+1)^2) = P(x^2) + 2x + 1 \qquad \forall x.$$

Solution. Since $2x + 1 = (x + 1)^2 - x^2$, we find that

$$P((x+1)^2) - (x+1)^2 = P(x^2) - x^2.$$

Defining $Q(x) = P(x^2) - x^2$, we obtain $Q(x) = Q(x + 1)$. Hence $Q(x)$ is 1-periodic and so it is constant. Thus $P(x^2) - x^2 = C$ for some constant C. This implies that $P(x) = x + C$ for all $x \geq 0$ and therefore for all x. $\blacksquare$

Example 3.28. Find all polynomials $P(x)$ such that

$$(x^2 - 6x + 8)P(x) = (x^2 + 2x)P(x - 2) \qquad \forall x.$$

Solution. Write the original equation as

$$(x - 2)(x - 4)P(x) = x(x + 2)P(x - 2).$$

Substituting $x = 0, -2, 4$, we find that $P(0) = P(-2) = P(2) = 0$. Hence we can write $P(x) = x(x+2)(x-2)Q(x)$ for some polynomial $Q(x)$. Substituting this into the original equation, we get $(x-2)Q(x) = xQ(x-2)$. Setting $x = 0$, we obtain $Q(0) = 0$. Hence we can write $Q(x) = xR(x)$ for some polynomial $R(x)$ and we find that $R(x) = R(x - 2)$. So $R(x)$ is 2-periodic and therefore it is constant. Thus

$$P(x) = x(x + 2)(x - 2)Q(x) = Cx^2(x^2 - 4). \qquad \blacksquare$$

Example 3.29. Find all polynomials $P(x)$ such that

$$(x - 2015)^k P(x) = (x - 2016)^k P(x + 1) \qquad \forall x$$

for some positive integer k.

Solution. It is clear that $(x - 2016)^k$ divides $P(x)$. Writing

$$P(x) = (x - 2016)^k Q(x)$$

for some polynomial $Q(x)$, we find that

$$(x-2015)^k P(x) = (x-2015)^k (x-2016)^k Q(x) = (x-2016)^k (x-2015)^k Q(x+1).$$

Therefore $Q(x) = Q(x + 1)$. Hence $Q(x)$ is 1-periodic and therefore it is constant. Thus $P(x) = C(x - 2016)^k$ for some constant C. $\blacksquare$

In the next problem, we shall provide a more general statement about periodicity, for rational functions.

Example 3.30. Find all polynomials $P(x)$ and $Q(x)$ such that

$$P(x)P(x + 1) \cdot \ldots \cdot P(x + n) = Q(x)Q(x + 1) \cdot \ldots \cdot Q(x + n)$$

for some positive integer n.

First Solution. Using the substitution $x \mapsto x+1$, we find that

$$P(x+1)P(x+2)\cdot\ldots\cdot P(x+n+1) = Q(x+1)Q(x+2)\cdot\ldots\cdot Q(x+n+1).$$

Comparing it with the original equation, we obtain

$$Q(x)P(x+n+1) = P(x)Q(x+n+1).$$

Now, we shall proceed our proof by introducing the greatest common divisor of $P(x)$ and $Q(x)$. Let

$$D(x) = \gcd(P(x), Q(x)).$$

Then

$$\gcd(P(x+n+1), Q(x+n+1)) = D(x+n+1).$$

Putting $P(x) = D(x)A(x)$ and $Q(x) = D(x)B(x)$, where $A(x)$ and $B(x)$ have no common factor, we find that

$$A(x+n+1)B(x) = A(x)B(x+n+1).$$

Since $A(x)$ divides the left-hand side and has no common factor with $B(x)$, $A(x)$ must divide $A(x+n+1)$. However, $A(x)$ and $A(x+n+1)$ are monic polynomials of the same degree, so this forces $A(x+n+1) = A(x)$. Hence

$$B(x+n+1) = B(x).$$

This implies that $A(x)$ and $B(x)$ are $(n+1)$-periodic, and hence $A(x)$ and $B(x)$ are constant. Hence $P(x)$ are $Q(x)$ are proportional, that is, there is a constant K such that $P(x) = KQ(x)$. Plugging this back into the original equation, we find that $K^{n+1} = 1$ and all such pairs satisfy the equation. ■

Second Solution. Rewrite the equation $Q(x)P(x+n+1) = P(x)Q(x+n+1)$ as

$$\frac{P(x)}{Q(x)} = \frac{P(x+n+1)}{Q(x+n+1)}.$$

Then the rational function

$$R(x) = \frac{P(x)}{Q(x)}$$

is periodic. Defining $K = R(0)$, we find that

$$K = R(0) = R(n+1) = R(2(n+1)) = \ldots.$$

Thus $R(x) = K$ infinitely many times. Hence the equation

$$\frac{P(x)}{Q(x)} = K \text{ or } P(x) - KQ(x) = 0$$

has infinitely many solutions. Since the left-hand side is a polynomial, we find that it must be equal to zero. Therefore

$$\frac{P(x)}{Q(x)} = K \quad \forall x,$$

that is, $R(x)$ must be constant. Again, plugging in we find $K^{n+1} = 1$. ■

Third Solution. We can also use limits at infinity of rational functions to finish the problem. Recall that if $R(x) = \frac{P(x)}{Q(x)}$ is a rational function, then

$$\lim_{x\to\infty} R(x) = \lim_{x\to\infty} \frac{P(x)}{Q(x)}$$

is infinity if $\deg P(x) > \deg Q(x)$, is 0 if $\deg P(x) < \deg Q(x)$, and is the ratio of the leading coefficients of $P(x)$ and $Q(x)$ if $\deg P(x) = \deg Q(x)$.
After finding that $\frac{P(x)}{Q(x)}$ is $(n+1)$-periodic, we choose an a with $Q(a) \neq 0$ and we conclude that

$$\frac{P(a)}{Q(a)} = \frac{P(a+m(n+1))}{Q(a+m(n+1))}$$

for all positive integer m. If we define $K = \frac{P(a)}{Q(a)}$, then letting m tend to infinity, we see that $a+m(n+1)$ tends to infinity, so

$$K = \lim_{m\to\infty} \frac{P(a+m(n+1))}{Q(a+m(n+1))} = \lim_{x\to\infty} \frac{P(x)}{Q(x)}.$$

But starting from any t, we also have

$$\frac{P(t)}{Q(t)} = \frac{P(t+m(n+1))}{Q(t+m(n+1))}$$

for all positive integer m. As m tends to infinity, $t + m(n+1)$ also tends to infinity, so we have

$$\frac{P(t)}{Q(t)} = \lim_{m\to\infty} \frac{P(t+m(n+1))}{Q(t+m(n+1))} = \lim_{x\to\infty} \frac{P(x)}{Q(x)} = K.$$

Therefore for each x we have

$$\frac{P(x)}{Q(x)} = K,$$

and we finish as before. ■

The three solutions of the previous problem are all really proving a stronger statement, which is worth emphasizing in its own right.

Example 3.31. Prove that if a rational function $R(x)$ is periodic, then it is constant.

First Solution. Assume that $R(x)$ is T-periodic, so that $R(x) = R(x+T)$ for some $T \neq 0$. Write $R(x) = \frac{P(x)}{Q(x)}$, where $P(x)$ and $Q(x)$ are relatively prime. Then, clearing denominators in the equation $R(x) = R(x+T)$, we find

$$P(x)Q(x+T) = Q(x)P(x+T).$$

Since $P(x)$ and $Q(x)$ are relatively prime, we must have $Q(x) \min Q(x+T)$. However, $Q(x)$ and $Q(x+T)$ are polynomials with the same degree and leading coefficient, so this implies $Q(x) = Q(x+T)$ and hence we conclude that $P(x) = P(x+T)$. Thus $P(x)$ and $Q(x)$ are both T-periodic, and hence are constant. Thus $R(x)$ is constant. ■

Second Solution. Assume $R(x)$ is T-periodic and write $R(x) = \frac{P(x)}{Q(x)}$. Then we see that $R(0) = R(T) = R(2T) = \ldots$.
Hence the equation $P(x) = R(0)Q(x)$ has infinitely many roots, so we conclude that $P(x) = R(0)Q(x)$ for all x and hence $R(x) = R(0)$ for all x. ■

Third Solution. Suppose $R(x)$ is T-periodic and choose any a with $R(a)$ finite. Then we find that $R(a) = R(a+mT)$ for all positive integers m. Since $a + mT$ tends to infinity as m tends to infinity, we have

$$R(a) = \lim_{m\to\infty} R(a+mT) = \lim_{x\to\infty} R(x).$$

Since we have $R(t) = R(t+mT)$ for all t, and $t + mT$ tends to infinity as m tends to infinity, we have

$$R(t) = \lim_{m\to\infty} R(t+mT) = \lim_{x\to\infty} R(x) = R(a).$$

Thus $R(x) = R(a)$ for all x. ■

Example 3.32. If $R(x)$ is a rational function and $R(x) = R(x^2)$, then $R(x)$ is constant.

First Solution. Let $R(x) = \frac{P(x)}{Q(x)}$ and choose a number $M > 1$ so that all roots r of $Q(x)$ have $|r| < M$. Then for any $t > M$, we see that $R(t)$ is defined. Iterating the equation, we find that

$$C = R(t) = R(t^2) = R(t^4) = \ldots = R(t^{2^n}) = \ldots.$$

Thus the equation $P(x) - CQ(x) = 0$ has infinitely many roots, so $P(x) = CQ(x)$ and $R(x) = C$ for all x. ■

Second Solution. Write $R(x) = \frac{P(x)}{Q(x)}$, where $P(x)$ and $Q(x)$ are relatively prime and $Q(x)$ is monic. Then $R(x) = R(x^2) = \frac{P(x^2)}{Q(x^2)}$. The polynomials $P(x^2)$ and $Q(x^2)$ are also relatively prime, since if they had any common root r, then r^2 would be a common root of $P(x)$ and $Q(x)$, a contradiction. Since $Q(x^2)$ is also monic, we must have $Q(x) = Q(x^2)$ and $P(x) = P(x^2)$. This implies $\deg Q(x) = 2 \deg Q(x)$ and hence $\deg Q(x) = 0$, so Q is constant, and the same argument applies to $P(x)$. ■

Example 3.33. Let $k \geq 2$ be an integer. Determine all polynomials $P(x)$ with real coefficients

$$P(x)\,P\left(2x^k - 1\right) = P\left(x^k\right) P(2x - 1).$$

Solution. Let $R(x) = \frac{P(2x-1)}{P(x)}$. Then the equation becomes $R(x) = R(x^k)$. Adapting either proof of the previous example, we see that $R = C$ is constant. Hence $P(2x-1) = CP(x)$ for some constant C.
Suppose $r \neq 1$ is a (complex) root of $P(x)$.
Then we find that $P(2r-1) = CP(r) = 0$, hence $2r-1$ is also a root of $P(x)$. Iterating this, we find that $4r-3, 8r-7, \ldots$ and hence $2^k(r-1)+1$ for all nonnegative integer k are roots of $P(x)$. Since $r \neq 1$, these are all distinct and we conclude that $P(x) = 0$.
Thus either $P(x) = 0$ or the only root of $P(x)$ is at 1. In the latter case we have $P(x) = A(x-1)^d$ for some constant A and integer $d \geq 0$. It is easy to check that these are solutions to the given equation. ∎

Example 3.34. Find all polynomials $P(x)$ and $Q(x)$ such that

$$P(x)Q(x+1) = P(x+2016)Q(x).$$

Solution. Define $R(x) = P(x)P(x+1)\cdot\ldots\cdot P(x+2015)$. Notice that

$$\frac{Q(x)}{R(x)} = \frac{Q(x+1)}{R(x+1)}.$$

Hence the rational function $\frac{Q(x)}{R(x)}$ is 1-periodic. This implies that $\frac{Q(x)}{R(x)}$ is constant, so

$$Q(x) = CR(x) = CP(x)P(x+1)\cdot\ldots\cdot P(x+2015).$$ ∎

3.6 The polynomial $P(x+1) - P(x)$

For a polynomial $P(x)$, the polynomial $P(x+1)-P(x)$ is a discrete version of the derivative of $P(x)$. As a result it has many uses and many lovely features. For example, if we are interested in whether the sequence $P(0), P(1), \ldots$ is increasing (or decreasing), then we can just look at whether $P(x+1) - P(x)$ is positive (or negative).

Let $P(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$ and assume that $a_d \neq 0$. Then

$$P(x+1)-P(x) = a_d\left((x+1)^d - x^d\right) + a_{d-1}\left((x+1)^{d-1} - x^{d-1}\right) + \ldots + a_0(1-1).$$

Expanding the first term using the binomial theorem, we see that the x^d term cancels and the x^{d-1} term is $da_d x^{d-1}$. Since the x^{d-1} in the second term also cancels, all other terms have degree at most $d-2$. Thus

$$P(x+1) - P(x) = da_d x^{d-1} + Q(x)$$

for some polynomial $Q(x)$ of degree at most $d-2$. If $d \geq 1$, then $da_d \neq 0$, we get that

$$\deg(P(x+1) - P(x)) = d-1.$$

More generally:

Theorem

Let t be a nonzero real number. If a polynomial $P(x)$ is of degree $d \geq 1$ with leading coefficient $a_d \neq 0$, then the polynomial $P(x+t) - P(x)$ is of degree $d-1$ with leading coefficient dta_d.

Note that we can iterate this result easily. If $P(x)$ is a polynomial of degree $d \geq 2$ with leading coefficient a_d, then

$$P(x+2) - 2P(x+1) + P(x) = (P(x+2) - P(x+1)) - (P(x+1) - P(x))$$

is a polynomial of degree $d-2$ with leading coefficient $d(d-1)a_d$. If $d < 2$, then $P(x+2)-2P(x+1)+P(x) = 0$. (It is sometimes more convenient to shift this to $P(x+1) - 2P(x) + P(x-1)$, which does not change the conclusions.) Similarly,

$$P(x+3) - 3P(x+2) + 3P(x+1) - P(x)$$

is a polynomial of degree $d-3$ with leading coefficient $d(d-1)(d-2)a_d$. Strictly speaking, this conclusion only follows if $d \geq 3$, but we can use it for $d < 3$ if we interpret the zero polynomial as having any negative degree and leading coefficient 0.

Now suppose $Q(x)$ is a fixed polynomial of degree d and consider the equation $P(x+1) - P(x) = Q(x)$. The theorem tells us that if $P(x)$ is a polynomial of degree $d+1$, then $P(x+1) - P(x)$ will be a polynomial of degree d. Thus we can hope to find a solution $P(x)$ which is a polynomial of degree $d+1$. In fact we can, and this follows by induction on d. If $Q(x) = C$ is constant, then we can take $P(x) = Cx$ (or more generally $P(x) = Cx + C'$). For the inductive step, suppose we can find a solution for all polynomials of degree less than d. Let a_d be the leading coefficient of $Q(x)$ and write $Q(x) = a_d x^d + R(x)$ where $\deg R(x) < d$. By the theorem, we know that if we take

$$P_0(x) = \frac{a_d}{d+1} x^{d+1},$$

then $P_0(x+1) - P_0(x) = a_d x^d + S(x)$ for some polynomial $S(x)$ of degree at most $d-1$. Since $R(x) - S(x)$ has degree at most $d-1$, the inductive hypothesis tells us that there is a polynomial $P_1(x)$ of degree at most d such that $P_1(x+1) - P_1(x) + R(x) - S(x)$. Hence if we define

$$P(x) = P_0(x) + P_1(x),$$

we will have

$$\begin{aligned} P(x+1) - P(x) &= P_0(x+1) - P_0(x) + P_1(x+1) - P_1(x) \\ &= a_d x^d + S(x) + R(x) - S(x) = Q(x). \end{aligned}$$

Note that if we have two solutions

$$P(x+1) - P(x) = Q(x) \quad \text{and} \quad T(x+1) - T(x) = Q(x),$$

then it follows that $P(x) - T(x)$ is 1-periodic and hence constant. Thus any two solutions differ by a constant and we have proven the following theorem.

Theorem

Let $Q(x)$ be a polynomial of degree d. Then there is a polynomial $P(x)$ of degree $d+1$ such that $P(x+1) - P(x) = Q(x)$. Any other polynomial that satisfies this equation differs from $P(x)$ by just adding a constant. If the leading coefficient of $Q(x)$ is a_d, then the leading coefficient of $P(x)$ is $\frac{a_d}{d+1}$.

The proof of the theorem does give an algorithm for finding $P(x)$, though it is not a great one. (Let $P(x) = x(x-1)\cdots(x-d)$ and compute $P(x+1) - P(x)$ and you may discover a better one.) But let us close by just remarking that this last theorem is related to sums. For example, if we take

$$P(x) = \frac{x(x-1)(2x-1)}{6},$$

then we compute that

$$P(x+1) - P(x) = \frac{x(x+1)(2x+1)}{6} - \frac{x(x-1)(2x-1)}{6} = x^2$$

and this is equivalent to the well-known summation formula

$$\sum_{k=0}^{n-1} k^2 = \frac{n(n-1)(2n-1)}{6}.$$

Example 3.35. Find all polynomials $P(x)$ with real coefficients such that

$$2(1 + P(x)) = P(x-1) + P(x+1),$$

$$P(0) = 8, \quad P(2) = 32.$$

Solution. Write the given equation as

$$P(x+1) - 2P(x) + P(x-1) = 2.$$

From the theorems above, we see that if $P(x)$ is a monic polynomial of degree 2, then $P(x+1) - 2P(x) + P(x-1)$ will be a constant polynomial with leading coefficient $2 \cdot 1 \cdot 1 = 2$. This just says it is a solution of the equation. If $P(x)$ has degree $d > 2$, then $P(x+1) - 2P(x) + P(x-1)$ will have degree $d-2$ and hence will not be constant. Thus these are the only solutions. Thus

$$P(x) = x^2 + bx + c.$$

Since $P(0) = 8$ and $P(2) = 32$, we obtain that $P(x) = x^2 + 10x + 8$. ■

Example 3.36. Let $P(x) = x^3 + ax^2 + bx + c$. Show that if $P(r) = 0$ for some complex number r, then

$$\frac{P(x)}{x-r} - 2\frac{P(x+1)}{x+1-r} + \frac{P(x+2)}{x+2-r} = 2$$

for all $x \neq r, r-1, r-2$.

Solution. Writing $P(x) = (x-r)Q(x)$ for some monic polynomial $Q(x)$ of degree 2, we find that

$$\frac{P(x)}{x-r} - 2\frac{P(x+1)}{x+1-r} + \frac{P(x+2)}{x+2-r} = Q(x+2) - 2Q(x+1) + Q(x).$$

Since $Q(x)$ is a monic polynomial of degree 2, it follows from the theorem that $R(x) = Q(x+1) - Q(x)$ is a linear polynomial with leading coefficient 2. Using the theorem again we see that $R(x+1) - R(x) = 2$. However

$$\begin{aligned} R(x+1) - R(x) &= (Q(x+2) - Q(x+1)) - (Q(x+1) - Q(x)) \\ &= Q(x+2) - 2Q(x+1) + Q(x). \end{aligned}$$

■

Example 3.37. Find all polynomials $P(x)$ such that

$$P(1+x^3) = P(x^3) + P(x^2).$$

Alexander Golovanov

Solution. Suppose $P(x)$ has degree d and leading coefficient $a_d \neq 0$. Then by the theorem, $P(1+t) - P(t)$ has degree $d-1$ and leading coefficient da_d. Therefore $P(1+x^3) - P(x^3)$ has degree $3(d-1)$ and leading coefficient da_d. Since

$$P(1+x^3) - P(x^3) = P(x^2),$$

comparing degrees we find that $3d - 3 = 2d$, which implies $d = 3$. However, comparing the leading coefficients, we get $da_d = a_d$, which forces $d = 1$, a contradiction. So there is no such a polynomial. ■

Example 3.38. Find all polynomials $P(x)$ with real coefficients such that for all real numbers x, y, z we have

$$P(x) + P(y) + P(z) + P(x+y+z) = P(x+y) + P(x+z) + P(y+z) + P(0).$$

Solution. Let $Q(x) = P(x+z) - P(x)$ and let $R(x) = Q(x+y) - Q(x)$. Then we see that

$$\begin{aligned} R(x) - R(0) &= Q(x+y) - Q(x) - Q(y) + Q(0) \\ &= P(x+y+z) - P(x+y) - P(x+z) - P(y+z) \\ &\quad + P(x) + P(y) + P(z) - P(0) = 0. \end{aligned}$$

Hence $R(x) = R(0)$, so $R(x)$ is a constant polynomial. But then by the theorem (with $t = y$), $Q(x)$ is a linear polynomial, and by the theorem (with $t = z$), $P(x)$ is a quadratic polynomial. ■

Remark. Suppose we drop from the hypotheses of this problem the condition that $P(x)$ be a polynomial. From the proof, the identity satisfied by $Q(x)$ can be written as $Q(x+y) - Q(0) = (Q(x) - Q(0)) + (Q(y) - Q(0))$. This says that $Q(x) - Q(0)$ is additive. Without assuming that Q is a polynomial, it follows after a little work that there is a constant a (and in fact $a = Q(1) - Q(0)$) such that $Q(r) = ar + Q(0)$ for all rational r. Hence if we just assume Q is continuous, we can still conclude that $Q(x)$ is a linear polynomial. This can be pushed through to prove that if $P(x)$ is continuous, it must be a quadratic polynomial.

Example 3.39. For each positive integer d, prove that there exists a unique monic polynomial $P(x)$ of degree d such that $P(1) \neq 0$ and $P(x)$ has the following property:
For any sequence of real numbers $a_1, a_2, \ldots$ that satisfies

$$P(n)a_1 + \ldots + P(1)a_n = 0,$$

for all $n > 1$, there exists a natural number N such that for each positive integer $m > N$ we have $a_m = 0$.

Iranian Team Selection Test 2015

Solution. Suppose that $P(x)$ is a monic polynomial of degree d satisfying the problem conditions. Setting $a_1 = 1$, then it is clear that we can inductively define a sequence $(a_n)_{n\geq 1}$ satisfying the given recursion. We simply set

$$a_2 = -\frac{P(2)a_1}{P(1)}, \quad a_3 = -\frac{P(2)a_2 + P(3)a_1}{P(1)}, \text{ etc..}$$

By hypothesis, this sequence must be eventually all zeros, so there is some largest M with $a_M \neq 0$ and $a_n = 0$ for all $n > M$. For each $k \geq M$, the recursion therefore says that

$$a_1P(k) + a_2P(k-1) + \ldots + a_MP(k-M+1) = 0. \tag{3.2}$$

The left-hand side is a polynomial, but it has infinitely many roots, which means that it is the zero polynomial.
Now, we prove the following lemma.

Lemma. For any polynomial $P(x)$ of degree $d \geq 1$, if there are real numbers $b_2, \ldots, b_M$ such that for each real number x we have

$$P(x) + b_2P(x-1) + \ldots + b_MP(x-M+1) = 0,$$

then $M \geq d+2$.

Proof. We prove this lemma by induction on d. For the base case $d = 1$, let $P(x) = cx + d$ with $c \neq 0$ is a linear polynomial, and suppose by way of a contradiction, that $M \leq 2$. Hence there is a constant b_2 such that

$$P(x) + b_2P(x-1) = (cx+d) + b_2(cx+d-c) = 0.$$

From the coefficient of x, we see that $b_2 = -1$. But then this equation reduces to $c = 0$, which is not true. Thus we must have $M \geq 3$.
For the inductive step, suppose the result is true for all polynomials of degree less than d. Suppose $P(x)$ has degree d and we have

$$P(x) + b_2P(x-1) + \ldots + b_MP(x-M+1) = 0.$$

Looking at the leading coefficient, we see that $1 + b_2 + \ldots + b_M = 0$. Hence we can write $b_M = -1 - b_2 - \ldots - b_{M-1}$ and rewrite this as

$$(P(x) - P(x-M+1)) + b_2(P(x-1) - P(x-M+1)) + \ldots$$
$$+b_{M-1}(P(x-M+2) - P(x-M+1)) = 0$$

and then as

$$(P(x) - P(x-1)) + (1+b_2)(P(x-1) - P(x-2)) + \ldots$$
$$+(1+b_2+\ldots+b_{M-1})(P(x-M+2) - P(x-M+1)) = 0.$$

(This last step is Abel's summation by parts. If you do not see it immediately, compare the coefficients of $P(x-k)$ on both sides.) But $Q(x) = P(x) - P(x-1)$ is a polynomial of degree $d-1$ and therefore the inductive hypothesis says that this sum must have at least $(d-1)+2 = d+1$ terms. This says $M-1 \geq d+1$ and hence $M \geq d+2$, completing the proof. ❑

Returning to our problem, we see from the Lemma that $M \geq d+2$. For $k = M-1$, the polynomial identity (3.2) gives

$$a_1P(M-1) + a_2P(M-2) + \ldots + a_{M-1}P(1) + a_MP(0) = 0$$

but the recursive definition of a_{M-1} gives

$$a_1P(M-1) + a_2P(M-2) + \ldots + a_{M-1}P(1) = 0.$$

Comparing these and recalling that $a_M \neq 0$, we get $P(0) = 0$. Similarly, comparing the polynomial identity (3.2) for $k = M-2$ and the recursive definition of a_{M-2}, we conclude that $P(-1) = 0$. Continuing in this way for $k = M-1, M-2, \ldots, 2$, we conclude that

$$P(0) = P(-1) = \ldots = P(3-M) = 0.$$

This gives us $M-2 \geq d$ roots of $P(x)$. Since $P(1) \neq 0$, it follows that $M = d+2$, and since $P(x)$ is monic, we have

$$P(x) = x(x+1)\cdot\ldots\cdot(x+d-1).$$

Thus we have shown that this is the only polynomial of degree d that could possibly satisfy the conditions of the problem. It remains only to show that this polynomial does actually satisfy the conditions of the problem. It suffices to prove it for the sequence beginning with $a_1 = 1$ (since any other sequence satisfying the given recursion is just a multiple of this one). In this case, we claim that the resulting sequence will be

$$a_k = (-1)^{k-1}\binom{d+1}{k-1},$$

which will be zero for $k > d+2$. One can prove this directly using binomial coefficient identities, but an easier argument is just to back up through the proof above. For this choice of a_k, the identity (3.2), which we want to hold, becomes

$$\binom{d+1}{0}P(x) - \binom{d+1}{1}P(x-1) + \ldots + (-1)^{d+1}\binom{d+1}{d+1}P(x-d-1) = 0.$$

This does hold. To see this, note that the left-hand side is the result of applying the map $P(x) \mapsto P(x) - P(x-1)$ a total of $d+1$ times. Since we start with a polynomial $P(x)$ of degree d and since each step lowers the degree by 1, it follows that the result will have negative degee, and hence will be the zero polynomial. Thus for this choice of $a_1, \ldots, a_{d+2}$, we will have

$$a_1P(x) + a_2P(x-1) + \ldots + a_{d+2}P(x-d-1) = 0$$

for all x. The chosen $P(x)$ has $P(0) = P(-1) = \ldots = P(3-M) = 0$, so this identity for $x = 2$ reduces to $a_1P(2) + a_2P(1) = 0$, and similarly for each $x = 3, \ldots, d+2$, it reduces to the recursion after we drop the vanishing terms with $P(k)$ for $k \leq 0$. For $n = d+3, d+4, \ldots$, the recursion reduces to this identity since $a_n = 0$ for $n > d+2$. ■

3.7 Divisibility and the greatest common divisor of two polynomials

We know that if $ab = cd$ for some positive integers a, b, c, d and $\gcd(a, c) = 1$, then $a \mid d$ and $c \mid b$. If we write $d = ak$ for some positive integer k, then we also have $b = ck$. Analogously, we have following theorem in polynomials.

Theorem

If $P(x)Q(x) = R(x)S(x)$, and $\gcd(P(x),\ R(x)) = 1$, then $P(x) \mid S(x)$ and $R(x) \mid Q(x)$. Furthermore, there is a polynomial $T(x)$ such that $S(x) = P(x)T(x)$ and $Q(x) = R(x)T(x)$.

We also have the following properties.

Theorem

(i) If $\gcd(P(x), Q(x)) = D(x)$, then

$$\gcd(P(x+r),\ Q(x+r)) = D(x+r).$$

(ii) If $\gcd(P(x), Q(x)) = 1$, then for each complex number c,

$$\gcd(P(x+c), Q(x+c)) = 1.$$

Example 3.40. Let $P(x)(x+1) = Q(x)(x^2 - x + 1)$. Since

$$\gcd(x+1, x^2 - x + 1) = 1,$$

the above Theorem implies that there is a polynomial $T(x)$ such that

$$Q(x) = (x+1)T(x) \quad \text{and} \quad P(x) = (x^2 - x + 1)T(x).$$

Example 3.41. Find all pairs of polynomials $P(x)$ and $Q(x)$ with real coefficients for which

$$P(x)Q(x+1) - P(x+1)Q(x) = 1.$$

Putnam Competition 2010

First Solution. We will show that the only such polynomials are of the form $P(x) = ax + b$ and $Q(x) = cx + d$ where $ad - bc = -1$.

It is easy to see that

$$P(x)Q(x+1) - P(x+1)Q(x) = 1, \quad P(x-1)Q(x) - P(x)Q(x-1) = 1.$$

Therefore

$$P(x)(Q(x+1) + Q(x-1)) = Q(x)(P(x-1) + P(x+1)).$$

Observe that $P(x)$ and $Q(x)$ have no common nonconstant factor, otherwise this common factor would divide $P(x)Q(x+1) - P(x+1)Q(x) = 1$, a contradiction. Hence $P(x)$ divides $P(x-1) + P(x+1)$ and $Q(x)$ divides $Q(x+1) + Q(x-1)$. But $P(x)$ and $P(x-1) + P(x+1)$ are polynomials of the same degree and similarly for $Q(x)$, so this means there is a constant C such that

$$P(x-1) + P(x+1) = CP(x), \quad Q(x+1) + Q(x-1) = CQ(x).$$

Comparing the leading coefficients, we get $C = 2$, that is,

$$P(x-1) + P(x+1) = 2P(x), \quad Q(x+1) + Q(x-1) = 2Q(x).$$

We obtain that $P(x+1) - P(x) = P(x) - P(x-1)$. Hence $P(x+1) - P(x)$ is periodic, hence constant, and thus $P(x)$ is linear (or constant). The same argument applies to $Q(x)$. Writing $P(x) = ax + b$ and $Q(x) = cx + d$, we compute that

$$\begin{aligned} P(x)Q(x+1) - P(x+1)Q(x) &= (ax+b)(cx+c+d) - (ax+a+b)(cx+d) \\ &= bc - ad. \end{aligned}$$

Thus we have a solution exactly when $ad - bc = -1$. ■

Second Solution. Let $\deg P(x) = m$ and $\deg Q(x) = n$. Assume that $\max\{m, n\} \geq 2$. Then we can write

$$P(x) = a_m x^m + \ldots + a_0 \quad \text{and} \quad Q(x) = b_n x^n + \ldots + b_0,$$

where a_m and b_n are nonzero. Then we compute

$$P(x)Q(x+1) - P(x+1)Q(x) = a_m b_n (x^m(x+1)^n - (x+1)^m x^n) + \ldots = 1.$$

We see that the x^{m+n} term cancels and hence all the unwritten terms are of degree at most $m + n - 2$. Thus the coefficient of x^{m+n-1} on the left-hand side is $(n-m)a_m b_n$. The coefficient of x^{m+n-1} on the right-hand side is zero. So $m = n \geq 2$.

Now, if the pair $(P(x), Q(x))$ satisfies the given identity, then so does the pair $(P(x), Q(x) - tP(x))$ for any real number t. Since $P(x)$ and $Q(x)$ have the same degree, call it $n \geq 2$, then we can choose t so that $\deg(Q(x) - tP(x)) < n$. But then we have a solution with two polynomials of different degree, so we obtain a contradiction. We conclude that $P(x)$ and $Q(x)$ are both linear (or constant) and we finish as in the previous solution. ■

Example 3.42. Let $n \geq 2$ be an integer and $a \neq 0, \pm 1$ be a real number. Find all polynomials $P(x)$ such that

$$(1 + a^2x^2)P(ax) = (1 + a^{2n+2}x^2)P(x).$$

Marcel Chiriţă - Mathematics Magazine 1981

Solution. Define a sequence of polynomials $Q_m(x) = 1 + a^{2m}x^2$ and note that this gives $Q_m(ax) = Q_{m+1}(x)$. Then we can write

$$Q_1(x)P(ax) = Q_{n+1}(x)P(x).$$

Since $Q_i(x)$ is a quadratic polynomial and it has no real roots, it is irreducible over $\mathbb{R}[x]$. We have the following.

Lemma. For each $i \neq j$, $\gcd(Q_i(x), Q_j(x)) = 1$.

Proof. If $Q_i(x)$ and $Q_j(x)$ have a common factor, then it must divide

$$a^{2j}Q_i(x) - a^{2i}Q_j(x) = a^{2j} - a^{2i} = a^{2i}(a^{2j-2i} - 1).$$

However since $a \neq 0, \pm 1$, the right-hand side is a nonzero constant. Thus the gcd is 1. ❑

From the Lemma, $Q_1(x)$ divides $P(x)$, and so $Q_1(ax) = Q_2(x)$ divides $P(ax)$, and therefore by the Lemma again it divides $P(x)$. Continuing in this way, we obtain that $R(x) = Q_1(x)Q_2(x) \cdot \ldots \cdot Q_n(x)$ divides $P(x)$.

Writing $P(x) = R(x)S(x)$, we find that

$$Q_1(x)R(ax)S(ax) = Q_{n+1}(x)R(x)S(x).$$

Since

$$\begin{aligned} Q_1(x)R(ax) &= Q_1(x)Q_1(ax)Q_2(ax)\cdot\ldots\cdot Q_n(ax) \\ &= Q_1(x)Q_2(x)\cdot\ldots\cdot Q_{n+1}(x) \\ &= Q_{n+1}(x)R(x), \end{aligned}$$

we find that $S(ax) = S(x)$. Comparing leading coefficients in $S(ax) = S(x)$, we find that $a^d = 1$, which forces $d = 0$, and so $S(x) = C$ is a constant polynomial. Hence $P(x) = CR(x)$.
It is easy to check that this is a solution. ■

Example 3.43. Find all polynomials $P(x)$ and $Q(x)$ such that

$$P(x)^3 - Q(x)^2 = ax + b$$

for some nonzero complex numbers a and b.

Kürschák Competition 2017

Solution. Let $x = -\frac{z^2+b}{a}$. Then

$$P\left(-\frac{z^2+b}{a}\right)^3 - Q\left(-\frac{z^2+b}{a}\right)^2 = -z^2.$$

Since $P\left(-\frac{z^2+b}{a}\right)$ and $Q\left(-\frac{z^2+b}{a}\right)$ are polynomials in z^2, we can write

$$P\left(-\frac{z^2+b}{a}\right) = f(z^2), \quad Q\left(-\frac{z^2+b}{a}\right) = g(z^2),$$

which gives $f(z^2)^3 - g(z^2)^2 = -z^2$. Hence

$$(g(z^2) - z)(g(z^2) + z) = f(z^2)^3.$$

Let

$$D(z) = \gcd(g(z^2) - z, g(z^2) + z).$$

Then $D(z)$ must divide $(g(z^2)+z)-(g(z^2)-z) = 2z$. Hence either $D(z) = 1$ or $D(z) = z$. Assuming the latter, we get that z divides $g(z^2)$, and so z^2 divides $g(z^2)^2$. Thus z^2 divides $g(z^2)^2 + z^2 = f(z^2)^3$, that is, $f(z^2)^3$ is divisible by z^6. Hence the left-hand side of $f(z^2)^3 - g(z^2)^2 = z^2$ is divisible by z^4 but the right-hand side is not, a contradiction. Thus the former case occurs, that is, $D(z) = 1$.
Thus there are polynomials $A(z)$ and $B(z)$ such that

$$g(z^2) - z = A(z)^3, \quad g(z^2) + z = B(z)^3.$$

Therefore

$$2z = B(z)^3 - A(z)^3 = (B(z) - A(z))(B(z)^2 + A(z)B(z) + A(z)^2).$$

This implies that $\deg(B(z)^2 + A(z)B(z) + A(z)^2) \le 1$. It is clear that

$$\deg A(z) = \deg B(z) = d \ge 1.$$

Denote the leading coefficients of $A(z)$ and $B(z)$ by a and b, respectively. The leading coefficient of $B(z)^2 + A(z)B(z) + A(z)^2$, is $a^2 + ab + b^2 \neq 0$. Hence

$$\deg(B(z)^2 + A(z)B(z) + A(z)^2) = 2d \ge 2,$$

contradiction. So there are no polynomials P and Q satisfying the required conditions ■

Remark. A general result of Mason states that if f, g, h are polynomials with complex coefficients such that $f + g = h$, then

$$\max(\deg f, \deg g, \deg h) \le \deg(\mathrm{rad}(fgh)) - 1,$$

where if $P(x) = C(x - r_1)^{\alpha_1}\cdot\ldots\cdot(x - r_t)^{\alpha_t}$, where $r_1, \ldots, r_t$ are distinct complex numbers, then

$$\mathrm{rad}(P(x)) = (x - r_1)\cdot\ldots\cdot(x - r_t).$$

To see that this general result solves the problem, note that if we have a solution, then comparing degrees shows that $\deg P(x) = 2d$ and $\deg Q(x) = 3d$ for some $d \geq 1$. Thus

$$6d = \max(\deg P(x)^3, \deg Q(x)^2, 1) \leq \deg(\mathrm{rad}(P(x)^3 \cdot Q(x)^2 \cdot (ax+b)) - 1.$$

Note that

$$\deg(\mathrm{rad}(P(x)^3 \cdot Q(x)^2 \cdot (ax+b)) = \deg(\mathrm{rad}(P(x)Q(x)(ax+b)) \leq 5d+1.$$

Therefore $6d \leq 5d$, impossible.

3.8 Using odd and even polynomials

3.8.1 Substituting $-x$ instead of x

Don't underestimate the simple substitution $x \mapsto -x$. It solves many problems. Let us show some examples.

Example 3.44. Find all pairs of polynomials P, Q with real coefficients such that

$$P(x^2+1) = (Q(x))^2 + 2x, \qquad Q(x^2+1) = (P(x))^2$$

for any real number x.

Polish Mathematical Olympiad 2016

Solution. We have

$$2x + (Q(x))^2 = P(x^2+1) = P\left((-x)^2+1\right) = (Q(-x))^2 - 2x,$$

so

$$\begin{aligned} 4x &= (Q(-x))^2 - (Q(x))^2 \\ &= (Q(-x) - Q(x))(Q(-x) + Q(x)) \\ &= F(x)G(x), \end{aligned}$$

where $F(x) = Q(-x) - Q(x)$ and $G(x) = Q(-x) + Q(x)$. From the last equality, we see that one of the polynomials $F(x)$, $G(x)$ is of degree 0 and the other is of degree 1. Since $G(x)$ is an even polynomial, it follows that $G(x)$ has even degree, so it must have degree 0, i.e., $G(x)$ is constant (and nonzero). Therefore the polynomial $F(x)$ is of degree 1. As $F(0) = 0$, there exist $a, c \in \mathbb{R}$, $a, c \neq 0$, such that $G(x) = 2c$ and $F(x) = 2ax$ for all $x \in \mathbb{R}$. So

$$Q(x) = \frac{1}{2}(G(x) - F(x)) = -ax + c \qquad \forall x \in \mathbb{R}.$$

From the relation $Q(x^2+1) = (P(x))^2$ it follows that the degree of the polynomial P is equal to 1, so there are $\alpha, \beta \in \mathbb{R}$, $\alpha \neq 0$, such that $P(x) = \alpha x + \beta$. Hence

$$-a(x^2+1) + c = \alpha^2 x^2 + 2\alpha\beta x + \beta^2.$$

It follows that $-a = \alpha^2$, $2\alpha\beta = 0$, $c - a = \beta^2$. Since $\alpha \neq 0$, we get $\beta = 0$ and $a = c = -\alpha^2$, i.e., $P(x) = \alpha x$ and $Q(x) = \alpha^2(x-1)$. From the relation $P(x^2+1) = (Q(x))^2 + 2x$ we obtain

$$\alpha(x^2+1) = \alpha^4(x-1)^2 + 2x.$$

If $x = 1$, we get $2\alpha = 2$, i.e., $\alpha = 1$. We have proved that there is at most one pair of such polynomials: $P(x) = x$ and $Q(x) = x - 1$. It's easy to see that these polynomials satisfy the two given conditions and so this is the only solution to the problem. ■

Example 3.45. Find all polynomials $P(x)$ with real coefficients which satisfy the following equality for all real numbers x:

$$P(x^2) + x\,(3P(x) + P(-x)) = (P(x))^2 + 2x^2.$$

Vietnamese Mathematical Olympiad 2006

Solution. Clearly, $\deg P > 0$. If $\deg P = 1$, then $P(x) = ax + b$, where $a, b \in \mathbb{R}$, $a \neq 0$. Substituting this into the given equation, we have

$$(a^2 - 3a + 2)x^2 + 2b(a-2)x + b^2 - b = 0 \qquad \forall x \in \mathbb{R},$$

which gives

$$a^2 - 3a + 2 = b(a-2) = b^2 - b = 0.$$

Solving this system of equations, we get $(a,b) \in \{(1,0),(2,0),(2,1)\}$. Therefore $P(x) = x$, $P(x) = 2x$, or $P(x) = 2x+1$.

Now, let $\deg P = n \geq 2$ and let $P(x) = ax^n + Q(x)$, where $a \neq 0$ and $Q(x)$ is a polynomial with real coefficients with $\deg Q = k < n$. Substituting this into the equation we get

$$\begin{aligned} & (a^2-a)x^{2n} + (Q(x))^2 - Q(x^2) + 2ax^nQ(x) \\ = \; & (3+(-1)^n)\,ax^{n+1} + (3Q(x) + Q(-x))\,x - 2x^2 \qquad \forall x \in \mathbb{R}. \end{aligned}$$

Observe that the degree of the right-hand side polynomial is $n+1$ and $n+1 < 2n$, so $a^2 - a = 0$, which gives $a = 1$. Hence

$$\begin{aligned} & 2x^nQ(x) + (Q(x))^2 - Q(x^2) \\ = \; & (3+(-1)^n)\,x^{n+1} + (3Q(x) + Q(-x))\,x - 2x^2 \qquad \forall x \in \mathbb{R}. \end{aligned}$$

Observe that the degree of the left-hand side polynomial is $n+k$, while the degree of the right-hand side polynomial is $n+1$, so $k = 1$. Moreover, if $x = 0$, we get $(Q(0))^2 - Q(0) = 0$, which gives $Q(0) = 0$ or $Q(0) = 1$. Thus $Q(x) = bx$ or $Q(x) = bx + 1$.

(i) If $Q(x) = bx$, then

$$(3+(-1)^n - 2b)\,x^{n+1} - (b^2 - 3b + 2)x^2 = 0 \qquad \forall x \in \mathbb{R}.$$

It follows that $3 + (-1)^n - 2b = 0$ and $b^2 - 3b + 2 = 0$, which gives $b = 1$ and n is odd or $b = 2$ and n is even. Therefore $P(x) = x^{2n+1} + x$ or $P(x) = x^{2n} + 2x$, where $n \in \mathbb{N}^*$. An easy check shows that both polynomials satisfy the given equation (even if $n = 0$, in which case we recover two of the linear solutions we found earlier).

(ii) If $Q(x) = bx + 1$, then

$$(3+(-1)^n - 2b)\,x^{n+1} - 2x^n - (b^2 - 3b + 2)x^2 - 2(b-2)x = 0 \qquad \forall x \in \mathbb{R},$$

which is impossible (the coefficient of x^n is nonzero).

In conclusion, all the desired polynomials are $P(x) = x$, $P(x) = x^{2n} + 2x$, $P(x) = x^{2n+1} + x$, where $n \in \mathbb{N}$. ■

3.8.2 More advanced techniques

We say a polynomial $P(x)$ (or more generally a function) is even if it satisfies $P(-x) = P(x)$ and odd if it satisfies $P(-x) = -P(x)$. One of the reasons the substitution $x \mapsto -x$ works is that it allows us to split a polynomial equation into its even and odd parts. Sometimes it helps to do this even more explicitly.

Strategy

(i) A polynomial $P(x)$ is even if and only if there exists a polynomial $Q(x)$ such that $P(x) = Q(x^2)$.

(ii) A polynomial $P(x)$ is odd if and only if there exists a polynomial $R(x)$ such that $P(x) = xR(x^2)$.

(iii) Each polynomial $P(x)$ can be expressed in the form $Q(x^2) + xR(x^2)$ for some polynomials $R(x)$ and $Q(x)$, hence $P(x)$ is expressed as a sum of its even and odd parts.

Example 3.46. If $R(x)$ is a rational function and $R(x) = R(-x)$, prove that $R(x) = S(x^2)$ for some rational function $S(x)$.

Solution. Write $R(x) = \frac{P(x)}{Q(x)}$ where $P(x)$ and $Q(x)$ are relatively prime. Then

$$\frac{P(x)}{Q(x)} = R(x) = R(-x) = \frac{P(-x)}{Q(-x)},$$

hence $P(x)Q(-x) = Q(x)P(-x)$. Since $\gcd(P(x), Q(x)) = 1$, we conclude that $Q(x) \mid Q(-x)$ and $P(x) \mid P(-x)$. But these are polynomials of the same degree so there is a constant C such that $Q(-x) = CQ(x)$ and $P(-x) = CP(x)$ and comparing leading coefficients, we see that $C = \pm 1$. If $C = 1$, then and $P(x) = P(-x)$ and $Q(x) = Q(-x)$ are both even, and hence can be written as polynomials in x^2. Hence $R(x) = S(x^2)$. If $C = -1$, then $P(-x) = P(x)$ and $Q(-x) = -Q(x)$, which implies $P(0) = Q(0) = 0$, contradicting the fact that $P(x)$ and $Q(x)$ are relatively prime. ■

So we get the following.

Corollary 3.1 *If $R(x)$ is a rational function and $R(x) = R(1-x)$, then $R(x) = S\left(x^2 - x\right)$ for some rational function $S(x)$.*

Example 3.47. Prove that for each positive integer d there exists a polynomial $P(x)$ with real coefficients of degree d such that the polynomial $xP(x)^2 - (P(x)-1)^2$ is an odd polynomial.

Nikolai Nikolov - Bulgarian Mathematical Olympiad 2010

Solution. Write $P(x) = Q(x^2) + xR(x^2)$ for some polynomials $Q(x)$ and $R(x)$. Then

$$xP(x)^2 - (P(x)-1)^2 = x\left(Q(x^2) + xR(x^2)\right)^2 - \left(Q(x^2) - 1 + xR(x^2)\right)^2.$$

The above expression is equal to

$$2x^2Q(x^2)R(x^2) - (Q(x^2)-1)^2 - x^2R^2(x^2)$$

$$+x(x^2R^2(x^2) + Q^2(x^2) - 2Q(x^2)R(x^2) + 2R(x^2)).$$

Since we need an odd polynomial, we must have

$$2x^2Q(x^2)R(x^2) - (Q(x^2)-1)^2 - x^2R^2(x^2) = 0,$$

that is,

$$(Q(x)-1)^2 - 2xQ(x)R(x) + xR^2(x) = 0. \tag{3.3}$$

Thus we want to generate pairs of polynomials $(Q(x), R(x))$ that are solutions to (3.3). To do this, we invoke a famous recursive trick for generating solutions to a quadratic equation in two variables. It is easy to find the trivial solution $Q_0(x) = 1$, $R_{-1}(x) = 0$. (The unusual choice of the subscript here will make more sense later.) Suppose we fix $Q(x) = Q_0(x)$ and think of (3.3) as a quadratic equation in $R(x)$. Since it is a quadratic it has two roots, one of which is $R_{-1}(x)$, and Vieta's formula tells us that the sum of the two roots

is $2Q_0(x)$. Therefore the second root must be $R_0(x) = 2Q_0(x) - R_{-1}(x) = 2$. (It would be easy to check this, but thanks to Vieta we do not need to do so.) Hence we have found a second solution $Q_0(x) = 1$, $R_0(x) = 2$ to (3.3). Now we turn it around and think of $R(x) = R_0(x)$ as fixed and view (3.3) as a quadratic equation in $Q(x)$. One root is $Q_0(x)$ and Vieta says the sum of the roots is $2 + 2xR_0(x)$. Hence the other root is $Q_1(x) = 2 + 2xR_0(x) - Q_0(x) = 4x + 1$. Thus we have a third solution $(Q_1(x), R_0(x))$, and we can clearly continue in this way indefinitely. Define $R_{-1}(x) = 0$, $Q_0(x) = 1$, $R_0(x) = 2$ and define

$$Q_k(x) = 2 + 2xR_{k-1}(x) - Q_{k-1}(x)$$

and

$$R_k(x) = 2Q_k(x) - R_{k-1}(x)$$

for $k \geq 1$. Then it follows by induction on k that $R_k(x)$ and $Q_k(x)$ are polynomials of degree k and that the pairs $(Q_k(x), R_k(x))$ and $(Q_{k+1}(x), R_k(x))$ are both solutions to (3.3).

Returning to $P(x)$ and the original problem, if we take the solution $(Q_k(x), R_k(x))$, then $P(x) = Q_k(x^2) + xR_k(x^2)$ is a solution to the original problem, and it is easy to see that $\deg P(x) = 2k+1$. If we take the solution $(Q_{k+1}(x), R_k(x))$, then $P(x) = Q_{k+1}(x^2) + xR_k(x^2)$ is a solution to the original problem with $\deg P(x) = 2k+2$. Thus we have produced solutions of all positive degrees. ■

3.9 Defining a new polynomial

You should be well aware that in algebra problems or inequalities, a clever change of variables can make the problem easier or even solve it completely. For problems where we want to find polynomial solutions, the analogous technique is to define a new polynomial and to rewrite our equation in terms of this new polynomial.

Example 3.48. Find all nonconstant polynomials $P(x)$ such that

$$P(x)^2 = P(x^2) - 2P(x) \quad \forall x.$$

Solution. Rewriting the equality as $P(x)^2+2P(x)=P(x^2)$ and adding 1 to both sides, we get

$$(P(x)+1)^2=P(x^2)+1.$$

Defining $Q(x)=P(x)+1$, we get $Q(x)^2=Q(x^2)$. We saw this equation in the solutions to Example 3.18, and in particular we showed that the nonconstant solutions are $Q(x)=x^d$, where d is a positive integer. So $P(x)=x^d-1$. ■

In the next example, we introduce you to a more sophisticated argument, that is, if $P(0)=b$, we can write $P(x)=b+x^kQ(x)$ for some positive integer k and some polynomial $Q(x)$ such that $Q(0)\neq 0$.

Example 3.49. Find all polynomials $P(x)$ with real coefficients such that

$$P(x)P(2x^2)=P(2x^3+x^2)\quad\forall x.$$

Mathematics and Youth

Solution. Putting $x=0$, we find that $P(0)=0$ or $P(0)=1$. First assume that $P(0)=0$. Writing $P(x)=x^kQ(x)$ where $k\geq 1$ and $Q(0)\neq 0$, we get

$$2^kx^{3k}Q(x)Q(2x^2)=(2x^3+x^2)^kQ(2x^3+x^2).$$

Thus

$$2^kx^kQ(x)Q(2x^2)=(2x+1)^kQ(2x^3+x^2).$$

Putting $x=0$, we find that $Q(0)=0$, a contradiction.
Now assume that $P(0)=1$. Writing $P(x)=1+x^kQ(x)$ where $k\geq 1$ and $Q(0)\neq 0$, we find that

$$(1+x^kQ(x))(1+2^kx^{2k}Q(2x^2))=1+(2x^3+x^2)^kQ(2x^3+x^2).$$

Therefore

$$2^kx^{3k}Q(x)Q(2x^2)+x^kQ(x)+2^kx^{2k}Q(2x^2)=(2x^3+x^2)^kQ(2x^3+x^2).$$

Thus

$$2^kx^{2k}Q(x)Q(2x^2)+Q(x)+2^kx^kQ(2x^2)=x^k(2x+1)^kQ(2x^3+x^2).$$

Putting $x=0$, we get $Q(0)=0$, a contradiction. ■

Example 3.50. Let k be a real number such that there exists a nonconstant polynomial $P(x)$ with real coefficients satisfying

$$P(k+x^2)=P(x)^2\qquad\forall x.$$

Prove that $k=0$.

Nikolai Nikolov

Solution. Since $P(x)^2=P(k+x^2)=P(k+(-x)^2)=P(-x)^2$, one of the two equations $P(-x)=\pm P(x)$ must have infinitely many solutions, hence must hold for all x. Thus we find that $P(x)$ is either even or odd.
First assume that $P(x)$ is even. Then $P(x)=R(x^2)$ for some polynomial $R(x)$. In terms of R the equation reads $R((x^2+k)^2)=R(x^2)^2$, which since x^2 takes on infinitely many values, implies $R(x)^2=R((x+k)^2)$. Further writing $S(x)=R(x-k)$, we see that $S(x)$ satisfies $S(x^2+k)=(S(x))^2$. That is, $S(x)$ satisfies the same equation as $P(x)$, but $S(x)$ has lower degree since $\deg P=2\deg S$. Thus if we assume $P(x)$ is a solution of minimal degree, then it follows that $P(x)$ is an odd polynomial.
Now assume that $P(x)$ is an odd polynomial and $k\neq 0$. Write $P(x)=xS(x^2)$ for some polynomial $S(x)$. Hence

$$P(x^2+k)=P(x)^2=x^2S(x^2)^2,$$

and again since x^2 takes on infinitely many values, this implies

$$P(x+k)=xS(x)^2.$$

Since $P(0)=0$, it follows that $S(-k)=0$.
Hence we can write $S(x-k)=x^rT(x)$ for some polynomial $T(x)$ with $T(0)\neq 0$ and some $r>0$. Then we get

$$P(x)=(x-k)\,(S(x-k))^2=(x-k)x^{2r}T(x)^2.$$

Since $P(x)$ is an odd polynomial, it has no monomial of even degree. Therefore the coefficient of x^{2r} on the left-hand side is 0. However, the coefficient of x^{2r} on the right-hand side is $-kT(0)^2$, which is nonzero since k and $T(0)$ are nonzero. This is a contradiction, so we must have $k=0$. ■

Second Solution. Looking at leading coefficients, we see that $P(x)$ must be monic, hence we can write

$$P(x) = (x - r_1)(x - r_2) \cdot \ldots \cdot (x - r_d),$$

where $r_1, r_2, \ldots, r_d$ are the roots of $P(x)$ taken with multiplicity. Then

$$P(k + x^2) = (x^2 + k - r_1)(x^2 + k - r_2) \cdot \ldots \cdot (x^2 + k - r_d).$$

The factors in this product with distinct r_i are relatively prime (since any common factor of $x^2 + k - r_i$ and $x^2 + k - r_j$ with $r_i \neq r_j$ would have to divide $(x^2 + k - r_j) - (x^2 + k - r_i) = r_i - r_j$, a nonzero constant).
Now from the equation we have

$$(x^2 + k - r_1)(x^2 + k - r_2) \cdot \ldots \cdot (x^2 + k - r_d) = (x - r_1)^2 (x - r_2)^2 \cdot \ldots \cdot (x - r_d)^2.$$

Look at a root r of $P(x)$ of maximum multiplicity, say multiplicity m. Then r is a root of the right-hand side with multiplicity $2m$. But by the above, r can be a root of only one type of factor $x^2 + k - r_i$ on the left, this factor occurs at most m times (since r has maximum multiplicity), and this factor is quadratic so r can be at most a double root. Thus the multiplicity of r as a root of the left-hand side is at most $2m$. Thus we must have equality throughout. This means that $r' = r^2 + k$ is also a root of $P(x)$ with multiplicity m and that r is a double root of $x^2 + k - r' = 0$. The latter can only occur if $k = r'$ and $r = 0$. Thus the only possible root of maximum multiplicity is $r = 0$, and since r' also has this multiplicity, we must have $r = r' = 0$ and hence $k = r' - r^2 = 0$. ■

Example 3.51. Find all polynomials P with real coefficients having the following property: if $x + y$ is a rational number, then also $P(x) + P(y)$ is a rational number.

Polish Mathematical Olympiad 2003

Solution. First observe that the conditions of the problem are satisfied by every polynomial of the form $P(x) = ax + b$, where a and b are rational numbers. We will prove that these are the only polynomials with the given property.

Let P be a polynomial satisfying the given conditions. For an integer n, we consider the polynomial $Q(x) = P(n + x) + P(n - x)$. The polynomial Q assumes rational values for all real numbers x, so it is a constant polynomial (by the Intermediate Value Theorem) and $Q(0) = 2P(n)$. Hence $Q(x) = 2P(n)$ for all x. In particular taking $x = 1$ we see that for any integer n we have $P(n - 1) + P(n + 1) = 2P(n)$. Since we can write this as

$$P(n) - P(n - 1) = P(n + 1) - P(n),$$

we see that $P(n) - P(n - 1) = a$ is constant for integer n. Hence an easy induction gives $P(n) = an + b$, where $b = P(0)$, for all positive integer n. This is infinitely many agreements, hence $P(x) = ax + b$ for all x. ■

3.9.1 Using symmetry

If $P(a - x) = P(x)$, by making the substitution $x \mapsto \frac{a}{2} + x$, we have

$$P\left(\frac{a}{2} + x\right) = P\left(\frac{a}{2} - x\right).$$

That is, the polynomial $P\left(\frac{a}{2} + x\right)$ is even, and therefore

$$P\left(\frac{a}{2} + x\right) = Q(x^2),$$

for some polynomial $Q(x)$. Thus

$$P(x) = Q\left(x^2 - ax + \frac{a^2}{4}\right).$$

We can write this more simply as $P(x) = R(x^2 - ax)$ for some polynomial $R(x)$.
Analogously, if $P(a - x) = -P(x)$, we find that $P\left(\frac{a}{2} + x\right)$ is an odd polynomial. Hence

$$P\left(\frac{a}{2} + x\right) = xQ(x^2),$$

for some polynomial $Q(x)$. Thus

$$P(x) = \left(x - \frac{a}{2}\right) Q\left(x^2 - ax + \frac{a^2}{4}\right)$$

or in a simpler form

$$P(x) = \left(x - \frac{a}{2}\right) R(x^2 - ax).$$

Thus we have shown:

Theorem

(i) If $P(a-x) = P(x)$, then $P(x) = R(x^2 - ax)$.

(ii) If $P(a-x) + P(x) = 0$, then $P(x) = \left(x - \frac{a}{2}\right) R(x^2 - ax)$.

(iii) $\gcd(P(x), P(-x)) = D(x^2)$ for some polynomial $D(x)$ and hence $\gcd(P(x), P(a-x)) = D(x^2 - ax)$ for some polynomial $D(x)$.

Example 3.52. Prove that the graph of the polynomial $P(x)$ is symmetric with respect to the point $A(a, b)$ if and only if there exists a polynomial $Q(x)$ such that

$$P(x) = b + (x-a)Q\left((x-a)^2\right).$$

Spanish Mathematical Olympiad 2001

Solution. The reflection of the point $(a+h, b+k)$ through the point (a, b) is the point $(a-h, b-k)$. Therefore the graph of $y = P(x)$ is symmetric with respect to the point (a, b) if and only if for each h there is a k with $P(a+h) = b+k$ and $P(a-h) = b-k$. Since we can define $k = P(a+h) - b$, we find that this reduces to just $P(a-h) + P(a+h) = 2b$ for all h. If we define $R(x) = P(a+x) - b$, we see that this is equivalent to $R(x) + R(-x) = 0$. Hence it holds if and only if $R(x) = xQ(x^2)$ for some polynomial $Q(x)$ and this translates into $P(x) = b + (x-a)Q((x-a)^2)$, as desired. ■

Example 3.53. Find all polynomials $P(x)$ and $Q(x)$ such that

$$P(x^2) = P(x)Q(1-x) + Q(x)P(1-x) \qquad \forall x.$$

Belarusian Mathematical Olympiad 2015

Solution. Using the substitution $x \mapsto 1 - x$, we get

$$P(x^2) = P((1-x)^2) = P((x-1)^2).$$

Hence the polynomial $P(x^2)$ is 1-periodic, which means that $P(x) = C$ for some constant C. Thus

$$C = CQ(1-x) + CQ(x).$$

If $C = 0$, we are done. If $C \neq 0$, then $Q(x) + Q(1-x) = 1$. Hence by using the substitution $x \mapsto \frac{1}{2} + x$, we find that

$$Q\left(\frac{1}{2} + x\right) - \frac{1}{2} + Q\left(\frac{1}{2} - x\right) - \frac{1}{2} = 0.$$

Hence the polynomial

$$R(x) = Q\left(\frac{1}{2} + x\right) - \frac{1}{2}$$

is odd. Therefore

$$Q\left(\frac{1}{2} + x\right) - \frac{1}{2} = xS(x^2)$$

for some polynomial $S(x)$. Thus

$$Q(x) = \left(x - \frac{1}{2}\right) S\left(\left(x - \frac{1}{2}\right)^2\right) + \frac{1}{2}.$$ ■

Example 3.54. Let $m \geq 2$, be an integer. Find all polynomials $P(x)$ such that if $x_1^m + x_2^m = 1$, then $P(x_1) + P(x_2) = 1$.

Solution. Let ω be a primitive m-th root of unity. It is clear that

$$1 = x_1^m + x_2^m = x_1^m + \omega^m x_2^m.$$

Hence $P(x_1) + P(x_2) = 1 = P(x_1) + P(\omega x_2)$. Thus $P(x_2) = P(\omega x_2)$ for infinitely many x_2. Therefore $P(x) = P(\omega x)$ for each x. Write

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0.$$

Then equating coefficients of x^k in $P(x) = P(\omega x)$, we get $a_k\omega^k = a_k$, which implies that either $a_k = 0$ or m divides k. Thus

$$P(x) = a_0 + a_m x^m + \ldots + a_d (x^m)^{\frac{d}{m}} = Q(x^m).$$

Hence for $x_1^m + x_2^m = 1$, we have $Q(x_1^m) + Q(x_2^m) = 1$. This implies that

$$Q(z) + Q(1-z) = 1$$

for infinitely many z and hence for all z. Thus

$$Q\left(\frac{1}{2}+z\right) - \frac{1}{2} + Q\left(\frac{1}{2}-z\right) - \frac{1}{2} = 0.$$

Therefore $Q\left(\frac{1}{2}+z\right) - \frac{1}{2}$ is an odd polynomial, that is,

$$Q\left(\frac{1}{2}+z\right) - \frac{1}{2} = zR(z^2)$$

for some polynomial $R(z)$. Hence

$$Q(z) = \frac{1}{2} + \left(z - \frac{1}{2}\right) R\left(\left(z-\frac{1}{2}\right)^2\right).$$

Therefore

$$P(x) = Q(x^m) = \frac{1}{2} + \left(x^m - \frac{1}{2}\right) R\left(\left(x^m - \frac{1}{2}\right)^2\right). \quad \blacksquare$$

Remark. A similar problem posed in the Tuymaada Olympiad 2001 was the following:
"Find all polynomials $P(x)$ such that $P(\sin x) + P(\cos x) = 1$ for all real numbers x."

3.10 Miscellaneous problems

Example 3.55. Find all polynomials $P(x)$ such that, for any real numbers x, y, z such that $x + y + z = 0$, the points $(x, P(x))$, $(y, P(y))$ and $(z, P(z))$ are collinear in the coordinate plane.

Mongolian Mathematical Olympiad 2018

Solution. A little geometry shows that the points $(x, P(x))$, $(y, P(y))$ and $(z, P(z))$ are collinear if and only if

$$(x-y)P(z) + (y-z)P(x) + (z-x)P(y) = 0.$$

Thus we want to find all polynomials $P(x)$ such that this holds whenever $x + y + z = 0$.
Now, if $P_1(x)$ and $P_2(x)$ satisfy this condition, it is easy to deduce that $a_1P_1(x) + a_2P_2(x)$ satisfies this condition for any constants a_1, a_2. It is clear that $P(x) = 1$ and $P(x) = x$ satisfy the condition, and from the identity

$$z^3(x-y) + x^3(y-z) + y^3(z-x) = -(x+y+z)(x-y)(y-z)(z-x),$$

we find that the polynomial $P(x) = x^3$ also satisfies the condition. Thus all polynomials of the form

$$P(x) = a_3x^3 + a_1x + a_0$$

are solutions to the problem.
Now, put $(x, y, z) = (x, 2x, -3x)$. Since this satisfies $x + y + z = 0$, we find that

$$-xP(-3x) + 5xP(x) - 4xP(2x) = 0.$$

Write $P(x) = a_dx^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0$. Then equating coefficients of x^{k+1} we get that

$$a_k((-3)^k + 2^{k+2} - 5) = 0$$

for all k. If $k \geq 2$ is even, then $(-3)^k + 2^{k+2} - 5 \equiv 2 \pmod 3$. Therefore $(-3)^k + 2^{k+2} - 5 \neq 0$, and hence $a_k = 0$, for even $k \geq 2$. Now, if k is an odd

number and $a_k \neq 0$, we must have $2^{k+2} - 3^k = 5$. This is true for $k = 1, 3$. But for $k \geq 5$ we have

$$\left(\frac{3}{2}\right)^k \geq \left(\frac{3}{2}\right)^5 > 4,$$

hence $3^k > 2^{k+2} - 5$. Thus for all odd $k \geq 5$, we also have $a_k = 0$. It follows that for all $k \neq 0, 1, 3$, we have $a_k = 0$. Thus $P(x) = a_3x^3 + a_1x + a_0$ are the only solutions. ∎

Example 3.56. Prove that there exists an infinite set of points $\ldots, P_{-2}, P_{-1}, P_0, P_1, \ldots$ in the plane with the following property: For any three distinct integers a, b and c, points P_a, P_b, P_c are collinear if and only if $a + b + c = 2014$.

Sam Vandervelde - USA Mathematical Olympiad 2014

Solution. By using the substitution $a \mapsto a-671$, $b \mapsto b-671$ and $c \mapsto c-671$, we can replace the condition $a + b + c = 2014$ with the simpler condition $a + b + c = 1$. Thus we will do so.

We will look for an infinite family of points of the form $P_n = (n, Q(n))$ for some polynomial $Q(x)$. This is not fully general, but it is the simplest possible construction and we will see below that it is general enough to provide a solution. As remarked in the preceding solution, the statement that the points $(a, Q(a))$, $(b, Q(b))$, and $(c, Q(c))$ are collinear is equivalent to

$$(b - c)Q(a) + (c - a)Q(b) + (a - b)Q(c) = 0.$$

Since $Q(x)$ is a polynomial, the left-hand side of this equality is a polynomial in a, b, c. To solve the problem, we want it to vanish whenever $a + b + c = 1$, and it will obviously vanish if any two of a, b, c are equal (geometrically, this is just the fact that if there are only two distinct points, then they lie on a line). Hence

$$(b - c)Q(a) + (c - a)Q(b) + (a - b)Q(c)$$

must be divisible by $(1 - a - b - c)(a - b)(b - c)(c - a)$, and we can write

$$(b-c)Q(a)+(c-a)Q(b)+(a-b)Q(c) = (1-a-b-c)(a-b)(b-c)(c-a)R(a,b,c)$$

for some polynomial $R(x, y, z)$.

We also want these to be the only cases where the three points are collinear. Therefore we need an extra hypothesis that any integer solution to $R(a, b, c) = 0$ has either $a+b+c = 1$ or two of a, b, c equal. The easiest way to arrange this is just to assume $R(x, y, z) = 1$ so that $R = 0$ has no solutions at all. Again, this is not fully general, but we will see that it is good enough to provide a solution.

Thus we are reduced to looking for a polynomial $Q(x)$ such that

$$(b-c)Q(a)+(c-a)Q(b)+(a-b)Q(c) = (1-a-b-c)(a-b)(b-c)(c-a).$$

The highest exponent of a occurring on the right-hand side is a^3 and the a^3 term is $(b - c)a^3$. Comparing this to the left-hand side, we see that if there is a solution, then $Q(x)$ must be a monic cubic polynomial. Write $Q(x) = x^3 + R(x)$, where $R(x)$ has degree at most 2. From the identity

$$(b - c)a^3 + (c - a)b^3 + (a - b)c^3 = -(a + b + c)(a - b)(b - c)(c - a),$$

we get

$$(b - c)R(a) + (c - a)R(b) + (a - b)R(c) = (a - b)(b - c)(c - a).$$

The highest degree term in a on the right-hand side is $(c - b)a^2$, hence comparing to the left-hand side we see that $R(x)$ is a quadratic polynomial with leading coefficient -1, and since

$$(b - c)a^2 + (c - a)b^2 + (a - b)c^2 = -(a - b)(b - c)(c - a)$$

we find that $R(x) = -x^2$ is a solution. (It should be clear from the geometry of the problem that the linear and constant coefficients of $Q(x)$ can be changed without changing whether we have a solution.) Thus we have found a solution

$$Q(x) = x^3 - x^2.$$

Undoing our earlier change of coordinates, we find that a solution to the original problem is the points

$$P_n = (n + 671, Q(n)) = (n + 671, n^3 - n^2).$$ ∎

We end this chapter with a relatively hard problem from the Canadian Olympiad 2018 that needs great concentration on what you have learned.

Example 3.57. Find all polynomials $P(x)$ with real coefficients that have the following property: there exists a polynomial $Q(x)$ with real coefficients such that

$$P(1) + P(2) + \ldots + P(n) = P(n)Q(n)$$

for all positive integer n.

Canadian Mathematical Olympiad 2018

Solution. Let $\deg P(x) = d$ and write $P(x) = a_d x^d + \ldots + a_0$ where $a_d \neq 0$. Writing the original equation for $n+1$ and cancelling, we get and equation without an n-long sum,

$$P(n)Q(n) + P(n+1) = P(n+1)Q(n+1).$$

Since the above equality is true for each positive integer n, we find that

$$P(x)Q(x) + P(x+1) = P(x+1)Q(x+1),$$

or equivalently

$$P(x)Q(x) = P(x+1)(Q(x+1) - 1) \tag{3.4}$$

for each x. Recall from Section 3.6 that there is a polynomial $R(x)$ of degree $d+1$ with leading coefficient $\frac{a_d}{d+1}$, such that

$$R(x) - R(x-1) = P(x).$$

Summing this for $x = 1, \ldots, n$, we find that

$$P(1) + P(2) + \ldots + P(n) = R(n) - R(0).$$

Thus we have $P(n)Q(n) = R(n) - R(0)$ for all positive integer n, and hence $P(x)Q(x) = R(x) - R(0)$ for all x. Since $P(x)$ has degree d and leading coefficient a_d and $R(x)$ has degree $d+1$ and leading coefficient $\frac{a_d}{d+1}$, we conclude that $Q(x)$ is linear and has leading coefficient $\frac{1}{d+1}$, that is,

$$Q(x) = \frac{1}{d+1}(x+b)$$

for some real number b. Plugging this into (3.4), we find

$$\frac{1}{d+1}(x+b)P(x) = \frac{1}{d+1}P(x+1)(x+b+1-d-1).$$

Hence

$$(x+b)P(x) = P(x+1)(x+b-d).$$

Now, substituting $x = -b$, we get $P(1-b) = 0$. Substituting $x = 1-b$, we get $P(2-b) = 0$. Continuing in this way for $x = -b, 1-b, \ldots, d-1-b$, we find

$$P(1-b) = P(2-b) = \ldots = P(d-b) = 0.$$

Since $\deg P(x) = d$, and we have found d roots, we conclude that

$$P(x) = a_d(x+b-1)(x+b-2)\cdot\ldots\cdot(x+b-d).$$

There is one additional constraint which we have not yet imposed, namely that $P(0)Q(0) = R(0) - R(0) = 0$. Since

$$P(x)Q(x) = \frac{a_d}{d+1}(x+b)(x+b-1)(x+b-2)\cdot\ldots\cdot(x+b-d),$$

this condition forces

$$0 = P(0)Q(0) = \frac{a_d}{d+1}b(b-1)(b-2)\cdot\ldots\cdot(b-d),$$

hence we must have $b \in \{0, 1, \ldots, d\}$. Thus the final answer is that

$$P(x) = a_d(x+b-1)(x+b-2)\cdot\ldots\cdot(x+b-d)$$

for some $d \geq 0$, $a_d \neq 0$, and some $b \in \{0, 1, \ldots, d\}$. ■

3.11 Proposed problems

Problem 3.1. Let $P(x) = x^2 + a$, $(a \neq 0)$ and $Q(x) = x^3 + bx + c$.
If $Q(P(x)) = P(Q(x))$ for all real numbers x, find the value of $Q(10)$.

Problem 3.2. Find all polynomials $P(x)$ of degree d such that

$$P(1) + P(x) + \ldots + P(x^d) = (1 + x + \ldots + x^d)P(x).$$

Problem 3.3. Find all polynomials $P(x)$ such that

$$P(2x) = 8P(x) + (x-2)^2 \qquad \forall x \in \mathbb{R}.$$

P. Černek - Czech-Slovak Mathematical Olympiad 2001

Problem 3.4. Let

$$3P(x^2) + 2122x^2 = 2(x^2+2)P(x) + x^4 + 4024x^3 + 8048x + 1959.$$

Find $P(2013)$.

Problem 3.5. Find all polynomials $P(x)$ with real coefficients such that for all nonzero real numbers x we have

$$P(x)P\left(\frac{1}{x}\right) = 1.$$

Problem 3.6. Find all polynomials $P(x)$ and $Q(x)$ such that

$$(x+1)P(x-1) - x^2Q(x+1) = x^2 - x - 1,$$

$$P(x+1) - (x+2)Q(x+3) = -1.$$

Problem 3.7. Find all polynomials $P(x)$ and $Q(x)$ with rational coefficients such that

$$2x + 1 + (3x+1)P(x) = Q(x)^2.$$

Problem 3.8. Find all polynomials $P(x)$ and $Q(x)$ with real coefficients such that

$$P(Q(x)+1) = 1 + Q(P(x)),$$
$$Q(P(x)+1) = 1 + P(Q(x)),$$
$$P(0) = Q(0) = 0.$$

Problem 3.9. Find all polynomials $P(x)$ with real coefficients such that

$$P(x)P(y) = P\left(\frac{x+y}{2}\right)^2 - P\left(\frac{x-y}{2}\right)^2.$$

Problem 3.10. Find all polynomials $P(x)$ with complex coefficients such that $P(0) = 0$ and for all integers $n > 2$ and for all real numbers $a_1, a_2, \ldots, a_n$ with $a_1 + a_2 \ldots + a_n \neq 0$,

$$P\left(\frac{a_1}{a_1 + a_2 + \ldots + a_n}\right) + \ldots + P\left(\frac{a_n}{a_1 + a_2 + \ldots + a_n}\right) = 0.$$

Problem 3.11. Let $P(x)$ be a nonzero polynomial such that

$$P(x)(x-1)^{20} = (x^2 + ax + 1)^{30} + (x^2 + bx + c)^{10}$$

for some real numbers a, b, c. Evaluate $P(1) + a^2 + b^2 + c^2$.

Problem 3.12. Find all monic polynomials $P(x)$ with real coefficients such that for each real number x

$$P(x + P(x)) = x^2 + P(P(x)).$$

Problem 3.13. Find all monic polynomials $P(x)$ with real coefficients such that for each real number x

$$P(x + P(x)) = 2x^3 + x^2 + P(P(x)).$$

Problem 3.14. (a) Determine the set of all polynomials $P(x)$ with real coefficients such that $(x-4)P(x+1) - xP(x) + 20 = 0$, $\forall x \in \mathbb{R}$.

(b) From the set determined in point (a), find the polynomial satisfying $P(0) = 29$.

I. V. Maftei - Romanian Mathematical Olympiad 1971

Problem 3.15. Let $P(x)$ be a polynomial with integer coefficients such that $P(a) = 1$, $P(b) = 2$, $P(17) = 3$ for some integers $a < b < 17$.

(i) Prove that the equation $P(x) = 5$ has at most one integer solution.

(ii) Find all polynomials $P(x)$ for which the equation $P(x) = 5$ has exactly one integer solution.

Problem 3.16. Anna is playing a mathematical computer game. The computer is hiding a polynomial $P(x)$. The degree and coefficients of $P(x)$ are unknown to Anna, but she knows that the coefficients are strictly positive real numbers. At each move, Anna inputs a real number a and the computer outputs $P(a)$. This is repeated until Anna can determine what $P(x)$ must be. For a strategy S used by Anna, denote by $S(P)$ the number of moves she needs to determine $P(x)$. Call a strategy S *optimal* if $S(P) \leq S'(P)$ for all possible strategies S' and all polynomials P with strictly positive coefficients. Does there exist an optimal strategy?

Problem 3.17. Find all polynomials P and Q such that for all real numbers x,

$$Q(x^2) = (x+1)^4 - x\,(P(x))^2\,.$$

P. Černek - Czech-Slovak Mathematical Olympiad 2001

Problem 3.18. Find all polynomials $P(x)$ with real coefficients such that

$$P\left(x^2\right) P\left(x^3\right) = (P(x))^5 \qquad \forall x \in \mathbb{R}.$$

Polish Mathematical Olympiad 2008

Problem 3.19. Determine all pairs of polynomials $P(x)$ and $Q(x)$ with real coefficients such that $x^3 Q(x) = P(Q(x))$ for all real numbers x.

Problem 3.20. Find all polynomials $P(x)$ such that

$$\frac{1}{\frac{1}{P(x)} - \frac{1}{P(P(x))}}$$

is also a polynomial.

Adapted from Oleg Mushkarov

Problem 3.21. Find all polynomials $P(x)$ satisfying

$$P(P(x)) + x = P(x + P(x)).$$

Problem 3.22. Find all polynomials $P(x)$ such that

$$\begin{aligned} P(x) + \binom{2018}{2} P(x+2) + \ldots + \binom{2018}{2016} P(x+2016) + P(x+2018) \\ = \binom{2018}{1} P(x+1) + \binom{2018}{3} P(x+3) + \ldots + \binom{2018}{2015} P(x+2015) \\ + \binom{2018}{2017} P(x+2017). \end{aligned}$$

Nordic Mathematical Contest 2018

Problem 3.23. Given a positive integer k, find all polynomials $P(x)$ with real coefficients such that $P(P(x)) = (P(x))^k$.

Canadian Mathematical Olympiad 1975

Problem 3.24. Let $n \geq 3$ be an integer.
Find all polynomials $f_1(x), \ldots, f_n(x)$ such that for all $1 \leq k \leq n$

$$f_k(x) f_{k+1}(x) = f_{k+1}(f_{k+2}(x)),$$

where $f_{n+1}(x) = f_1(x)$, $f_{n+2}(x) = f_2(x)$.

Oleg Mushkarov - Bulgarian Mathematical Olympiad 2012

Problem 3.25. Find all polynomials $P(x)$ with real coefficients such that

$$P(x)^2 - P(x-1)P(x+1) = 2P(x).$$

Problem 3.26. Find all polynomials $P(x)$ with real coefficients such that

$$P(x-1)P(x+1) > P(x)^2 - 1$$

for all real numbers x.

Nikolai Nikolov

Problem 3.27. Determine all polynomials $P(x)$ with real coefficients such that

$$(x+1)P(x-1) - (x-1)P(x)$$

is a constant polynomial.

Canadian Mathematical Olympiad 2013

Problem 3.28. Find all polynomials $P(x)$ with real coefficients such that for all real numbers x,

$$(x+1)P(x-1) + (x-1)P(x+1) = 2xP(x).$$

E. Kováč - Czech-Slovak Mathematical Olympiad 2002

Problem 3.29. Find all polynomials $P(x)$ with real coefficients such that

$$(x-1)P(x+1) - (x+1)P(x-1) = 4P(x).$$

Belarusian Mathematical Olympiad 2013

Problem 3.30. Let a, b be real numbers with $a \neq 0$. Find all polynomials $P(x)$ such that

$$xP(x-a) = (x-b)P(x) \qquad \forall x.$$

Vietnamese Mathematical Olympiad 1984

Problem 3.31. Find all polynomials $P(x)$ with real coefficients which satisfy

$$(x^3 + 3x^2 + 3x + 2)P(x-1) = (x^3 - 3x^2 + 3x - 2)P(x)$$

for all real numbers x.

Vietnamese Mathematical Olympiad 2003

Problem 3.32. Give an example of a polynomial $P(x)$ of degree 2001 for which the identity

$$P(x) + P(1-x) = 1$$

holds.

V. Senderov - Moscow Mathematical Olympiad 2001

Problem 3.33. Does there exist a positive integer d and a polynomial $P(x)$ with integer coefficients such that $x^d + x + 2 = P(P(x))$?

Chapter 4

Finding Polynomials. Part II: Uniqueness Lemmas

4.1 First Uniqueness Lemma

In one common group of problems concerning finding a polynomial, we have fixed polynomials $P(x)$, $Q(x)$, and $R(x)$ and we are asked to find all polynomials $f(x)$ such that

$$f(P(x))f(Q(x)) = f(R(x)).$$

For example, we could be asked to find all f with

$$f(x)f(x+1) = f(x^2), \quad f(x)f(x+1) = f(x^2+x+1).$$

In this section we provide a very powerful approach to deal with such problems.

Example 4.1. Let P, Q, R be three polynomials such that $\deg P \neq \deg Q > 0$. Prove that for all $k > 0$ there is at most one monic polynomial f of degree k such that

$$f(P(x))f(Q(x)) = f(R(x)).$$

M. Troinikov and V.A. Senderov - Kvant, Problem M1465

Solution. Letting $\deg P = a$, $\deg Q = b$ and assume without loss that $a > b > 0$. Looking at the degrees of both sides, we find that there cannot be any solutions unless $\deg R = a + b$.

Assume the contrary, i.e., assume that there are at least two monic polynomials f and g of degree k satisfying the condition. Then polynomial $f - g$ is of degree $m < k$. Hence we can write

$$f(R) - g(R) = f(P)(f(Q) - g(Q)) + g(Q)(f(P) - g(P)).$$

The degree of the left-hand side of the above equality is $m(a + b)$ and the degree of the right-hand side is $ka + mb$ (note that the second term has degree $kb + ma < ka + mb$, since $k > m$ and $a > b$). These cannot be equal since $m(a + b) < ka + mb$, a contradiction. ∎

Remark. We have reproduced this problem exactly as it was originally posed, but it should be clear that one can pull a lot more out of the proof. First note that the condition that f is monic is only used to guarantee that the the leading coefficients of f and g agree, so that $f - g$ has lower degree. If we let the leading coefficients of f, $P(x)$, $Q(x)$, and $R(x)$ be a, p, q, and r, respectively, then comparing leading coefficients we find

$$a^2 p^k q^k = ar^k.$$

Thus the leading coefficient of f must be $a = \left(\frac{r}{pq}\right)^k$. Thus the leading coefficient of f is completely determined by $P(x)$, $Q(x)$, $R(x)$ and k, and hence the leading coefficients of f and g must cancel. Thus we may drop the hypothesis that f is monic. (This does not really add any greater generality, because we could define

$$h(x) = f\left(\frac{pqx}{r}\right)$$

and we would have $h(x)$ monic and

$$h\left(\frac{r}{pq}P(x)\right) h\left(\frac{r}{pq}Q(x)\right) = h\left(\frac{r}{pq}R(x)\right).$$

Thus we could apply the result as originally stated to a slightly different choice of polynomials $P(x)$, $Q(x)$, and $R(x)$.)

More significantly, the condition that $\deg P \neq \deg Q$ can be substanitally weakened. The only place we used this condition was to argue that the two polynomials $f(P)(f(Q)-g(Q))$ and $g(Q)(f(P)-g(P))$ have difference degrees, and hence the degree of the sum is the larger degree. If $\deg P(x) = \deg Q(x)$, then these two terms have the same degree and one might worry that the leading coefficients could cancel. Using the notation from the previous discussion, and letting the leading coefficient of $f(x) - g(x)$ be b, we see that the leading coefficients of these polynomials are $abp^k q^m$ and $abq^k p^m$, respectively. Thus the only way there can be cancellation is if

$$\left(\frac{p}{q}\right)^{k-m} = -1.$$

Thus it would be enough to assume ratio of the leading coefficients of P and Q is not a root of -1. Since we are usually interested in cases where $P(x)$ and $Q(x)$ are real-valued, it would be enough to assume they are real-valued and

$$\deg(P(x) + Q(x)) = \max(\deg P(x), \deg Q(x)).$$

There is one other clever addition we can make to this result. Suppose $pq = r$, so that all solutions are monic. (This makes the argument cleaner, but as we have already seen we can always reduce to this case.) Suppose $f(x)$ is a solution of minimal degree, and let $\deg f(x) = d$. Then it is clear that the polynomial $f(x)^m$ is a solution of degree dm. Now suppose $g(x)$ is a solution of degree k. Then $f(x)^k$ and $g(x)^d$ are both solutions of degree dk, hence they must be equal, that is, $f(x)^k = g(x)^d$. Thus $f(x)$ and $g(x)$ are both powers of a third polynomial $h(x)$, which is also monic and of degree $\gcd(k, d)$. Further, by Bezout's identity, we can write $h(x) = f(x)^r g(x)^s$ for some integers r, s (possibly negative), and hence $h(x)$ is also a solution. Since we assumed d was minimal, it follows that $h(x) = f(x)$, k is a multiple of d, and $g(x) = f(x)^{k/d}$. Thus it suffices to find one solution $f(x)$ to the equation. If $f(x)$ is not a power of lower degree polynomial, then it is the solution of minimal degree. (If it is a power, then taking the correct root of $f(x)$ will give the solution of minimal degree.) Once we have found this minimal solution, all other solutions are simply powers of it.

Thus we have more generally,

First Uniqueness Lemma

Let $P(x)$, $Q(x)$, $R(x)$ be polynomials with real coefficients such that $\deg(P(x)+Q(x)) = \max(\deg P(x), \deg Q(x))$. For each positive integer d, there is at most one polynomial $f(x)$ of degree d satisfying

$$f(P(x))f(Q(x)) = f(R(x)).$$

If $f(x)$ is a solution of minimal degree, then all other solutions are powers of $f(x)$.

In the rest of this section, we provide you some examples that may be solved with the above lemma.

Example 4.2. Find all nonconstant polynomials $P(x)$ such that

$$P(x)P(x+1) = P(x^2+2).$$

Solution. We claim that $P(x) = x^2-x+2$ is one solution. This is equivalent to the identity

$$(x^2-x+2)((x+1)^2-(x+1)+2) = (x^2+2)^2-(x^2+2)+2,$$

which is easily checked. The roots of $P(x)$ are distinct, so $P(x)$ is not the square of a linear polynomial. Hence it is the minimal solution and by the Lemma, the solutions are $P(x) = (x^2-x+2)^n$ for all $n > 0$. ■

Remark. In this case there are no solutions for odd degree, as we proved using the Lemma. One could also prove it directly. If $P(x)$ is a solution of odd degree, then $P(x)$ has at least one real root. Let α be the largest real root. Plugging $x = \alpha$ into the equation, we see that α^2+2 is also a real root. But $\alpha^2+2 > \alpha$, contradicting the assumption of maximality.

Example 4.3. Find all nonconstant polynomials $P(x)$ such that

$$P(x^2) + P(x)P(x+1) = 0.$$

Solution. Let $f(x) = -P(x)$. Then $f(x)$ satisfies the equation

$$f(x^2) = f(x)f(x+1).$$

Hence the Lemma applies. From the easily checked identity

$$(x^2-x)((x+1)^2-(x+1)) = x^2(x-1)(x+1) = x^4-x^2,$$

we see that $f(x) = x^2-x$ is a solution with distinct roots, hence the minimal solution. Thus the solutions are $f(x) = (x^2-x)^m$ and hence $P(x) = -(x^2-x)^m$ for all $m > 0$. ■

Example 4.4. Find all nonconstant polynomials $P(x)$ such that

$$P(x^2+x+1) = P(x)P(x+1).$$

Solution. The identity

$$(x^2+1)((x+1)^2+1) = (x^2+x+1)^2+1$$

shows that $P(x) = x^2+1$ is one solution, and since it has distinct roots, it is minimal. Thus by the Lemma, the solutions are $(x^2+1)^n$ for all $n > 0$. ■

Example 4.5. Find all nonconstant polynomials $P(x)$ such that

$$P(x^2) = P(x)P(x-1).$$

Solution. From the identity

$$(x^2+x+1)((x-1)^2+(x-1)+1) = (x^2+x+1)(x^2-x+1) = x^4+x^2+1$$

we see that $P(x) = x^2+x+1$ is the minimal solution. Thus by the Lemma the solutions are $(x^2+x+1)^n$ for all $n > 0$. ■

Example 4.6. Find all nonconstant polynomials $P(x)$ such that

$$P(x^3+1) = P(x+1)P(x^2-x+1).$$

Solution. Since $x^3+1=(x+1)(x^2-x+1)$, we see that $P(x)=x$ is the minimal solution. So by the Lemma the solutions are x^n for each integer $n>0$. ■

Example 4.7. Find all nonconstant polynomials $f(x)$ with only real roots such that

$$f(-x^2)=f(x)f(-x).$$

Solution. Note that in this case the Lemma does not apply since $P(x)=x$ and $Q(x)=-x$ so $P(x)+Q(x)=0$ and $\deg P(x)+Q(x)<\deg P(x), \deg Q(x)$. Comparing leading coefficients will see that $f(x)$ must be monic. Suppose $f(x)$ has a real root r. Then plugging in $x=r$ we see that $-r^2$ is also a real root. If $|r|>1$, then we can define a sequence $(x_n)_{n\geq 0}$ of roots by $x_0=r$, $x_1=-r^2$, and $x_{n+1}=-x_n^2$ for $n\geq 1$. Since $|x_0|<|x_1|<|x_2|<\cdots$, we see that $f(x)$ has infinitely many roots and hence $f(x)=0$. Similarly, if $f(x)$ has a root r with $0<|r|<1$, then we get an infinite sequence of roots with decreasing absolute value. Thus every root of f must be in $\{0,1,-1\}$ and hence $f(x)=x^r(x-1)^s(x+1)^t$ for some $r,s,t\geq 0$. This gives

$$f(x)f(-x)=(-1)^{r+s+t}x^{2r}(x^2-1)^{s+t}$$

and

$$f(-x^2)=(-1)^{r+s+t}x^{2r}(x^2+1)^s(x^2-1)^t,$$

hence we conclude that $s=0$ and all nonconstant solutions are

$$f(x)=x^r(x+1)^t,$$

for some integers r,t with $r+t>0$. ■

Remark. This last example shows that at least some condition on the leading coefficients of $P(x)$ and $Q(x)$ is required in our Lemma, since we found multiple solutions of the same degree. There even more solutions if we drop the condition that $f(x)$ have only real roots. The argument in the solution implies that all roots of $f(x)$ must be 0 or lie on unit circle. However, it is easy to check that

$$f(x)=\frac{x^{2m+1}+1}{x+1}$$

is a solution for all m, and products of these give a whole zoo of solutions.

Example 4.8. Find all polynomials $P(x)$ such that

$$P(x)P(2x^2)=P(2x^3+x).$$

International Mathematical Olympiad Shortlist

Solution. From the identity

$$(x^2+1)(4x^4+1)=(2x^3+x)^2+1$$

we see that $P(x)=x^2+1$ is the minimal solution. Hence by the Lemma, the nonconstant solutions are $(x^2+1)^n$ for $n>0$. The constant solutions are easily checked to be $P(x)=0$ or 1. ■

Example 4.9. Find all nonconstant polynomials $P(x)$ such that

$$P(2x^2+3x-3)=P(2x)P(2x+1).$$

Solution. Let $P(x)=\frac{(x-2)(x+1)(x+4)}{8}$. From the factorizations

$$(2x^2+3x-3)-2=(x-1)(2x+5),$$

$$(2x^2+3x-3)+1=(x+2)(2x-1),$$

and

$$(2x^2+3x-3)+4=(x+1)(2x+1),$$

we find that

$$\begin{aligned} P(2x^2+3x-3) &= \frac{(2x-2)(2x+1)(2x+4)}{8}\cdot\frac{(2x-1)(2x+2)(2x+5)}{8} \\ &= P(2x)P(2x+1). \end{aligned}$$

The roots of $P(x)$ are distinct, so it is the minimal solution and hence by the Lemma, the nonconstant solutions are $\left(\frac{(x-2)(x+1)(x+4)}{8}\right)^n$ for all $n>0$. ■

Example 4.10. Find all nonconstant polynomials $P(x)$ such that

$$P(x^2+1) = P(x)P(x+4).$$

Solution. In this case the Lemma does apply, but we will prove that in fact there are no solutions, so the Lemma while applicable is unhelpful.
Suppose $P(x)$ is a nonconstant solution and let α be a complex root. Since the triangle inequality implies

$$|\alpha| + |\alpha - 4| \geq 4$$

we can choose β to be one of α and $\alpha - 4$ and to have $|\beta| \geq 2$. Plugging in $x = \beta$, we find that

$$P(\beta^2+1) = P(\beta)P(\beta+4) = 0.$$

Thus $P(x) = 0$ has a root $x_0 = \beta^2 + 1$ with $|x_0| \geq |\beta|^2 - 1 \geq 3$. Define the sequence $(x_n)_{n\geq 0}$ by $x_{n+1} = x_n^2 + 1$ for $n \geq 0$. Then by induction we find $P(x_n) = 0$ and $|x_{n+1}| > |x_n| \geq 3$. For the latter, we use the triangle inequality

$$|x_{n+1}| \geq |x_n|^2 - 1 \geq 3|x_n| - 1 > |x_n| \geq 3.$$

Thus the sequence $(x_n)_{n\geq 0}$ are all distinct roots of $P(x)$ and hence $P(x)$ has infinitely many roots, making it the zero polynomial. This is a contradiction, so there are no nonconstant solutions. ■

As the previous example shows if we pick the three inner polynomials carelessly, then there will not be any solutions to our equation. Indeed looking back at the examples above, you should see that they all rely on fairly specific polynomial identities. However there are some infinite families of examples for which solutions exist. The following example is one such.

Example 4.11. Let a and b be real numbers. Find all polynomials P such that

$$P(x^2+ax+b) = P(x)P(x+1).$$

Solution. Let $Q(x) = x^2 + (a-1)x + b$ so that $x^2 + ax + b = x + Q(x)$. Then since $Q(x)$ divides $Q(x+Q(x)) - Q(x)$, we conclude that $Q(x)$ divides $Q(x+Q(x))$. By explicit calculation, we can find the quotient:

$$\begin{aligned} Q(x+Q(x)) &= (x+Q(x))^2 + (a-1)(x+Q(x)) + b \\ &= x^2 + 2xQ(x) + Q(x)^2 + (a-1)x + (a-1)Q(x) + b \\ &= Q(x)(Q(x) + 2x + a) = Q(x)Q(x+1). \end{aligned}$$

Thus we see that $Q(x)$ is one solution. The discriminant of $Q(x)$ is $(a-1)^2 - 4b$. So if $(a-1)^2 \neq 4b$, then the roots of $Q(x)$ are distinct and it is the minimal solution. Hence by the Lemma, all nonconstant solutions are $(x^2+(a-1)x+b)^n$ for $n > 0$. The constant solutions add the case $n = 0$ and the zero solution. If $(a-1)^2 = 4b$, then

$$Q(x) = \left(x - \frac{a-1}{2}\right)^2$$

and hence $x - \frac{a-1}{2}$ is the minimal solution. In this case the nonzero solutions are $\left(x - \frac{a-1}{2}\right)^n$ for all $n \geq 0$. ■

The solution to the preceding problem proved a very pretty identity for monic quadratic polynomials. If $Q(x)$ is a monic polynomial of degree 2, then

$$Q(x+Q(x)) = Q(x)Q(x+1).$$

We will use this identity in the next example.

Example 4.12. Let b and c be integers and let $P(x) = x^2 + bx + c$. If $m \geq 2$ is a positive integer, prove that there are positive integers $x_1, \ldots, x_{m+1}$ such that

$$P(x_1)P(x_2)\cdot \ldots \cdot P(x_m) = P(x_{m+1}).$$

Solution. As in the previous solution we compute that

$$P(n+P(n)) = P(n)P(n+1)$$

for any n. We will use this identity and induction on m to solve the problem. For $m = 2$ choose $x_1 = n$, $x_2 = n+1$, $x_3 = n + P(n)$. Assume that the

statement of the problem is true for $k = m - 1$, that is, there are positive integers $z_1, \ldots, z_m$ such that

$$P(z_1)P(z_2) \cdot \ldots \cdot P(z_{m-1}) = P(z_m).$$

Since

$$P(z_m)P(1 + z_m) = P(P(z_m) + z_m),$$

we can multiply both sides by $P(1 + z_m)$ and then

$$P(z_1)P(z_2) \cdot \ldots \cdot P(z_{m-1})P(1 + z_m) = P(P(z_m) + z_m).$$

Now, putting

$$x_1 = z_1, \ldots, x_{m-1} = z_{m-1},\ x_m = 1 + z_m,\ x_{m+1} = P(z_m) + z_m$$

we are done. ∎

4.2 Second Uniqueness Lemma: induction and uniqueness

Another interesting type of problem is to find, given a fixed polynomial $Q(x)$, all polynomials $P(x)$ that satisfy $P(Q(x)) = Q(P(x))$. A pair of polynomials satisfying this condition are called permutable. Similarly to the previous section, if we have solutions $P_1(x)$ and $P_2(x)$ to this equation, then we can build more solutions. In this case, $P_1(P_2(x))$ will be a solution. Since setting $P(x)$ to be $Q(x)$ always provides one solution, we can always define a whole chain of solutions

$$Q(x), Q(Q(x)), Q(Q(Q(x))), \ldots.$$

It is convenient to have a notation for this, so we denote $Q^{(1)}(x) = Q(x)$ and inductively define $Q^{(n+1)}(x) = Q(Q^{(n)}(x))$. Also, by convention, we set $Q^{(0)}(x) = x$. Note that this fits with the recursive definition of $Q^{(n)}(x)$ in the sense that $Q^{(m+n)}(x) = Q^{(m)}(Q^{(n)}(x))$ for any $m, n \geq 0$. Also notice that $P(x) = x$ is also always a solution to our equation. Hence we can state that $Q^{(n)}(x)$ for $n \geq 0$ are always solutions.

There are differences between this problem and the one in the previous section. First, in that section when we found a solution $f(x)$ of degree d, we automatically got solutions of degree dm for any $m \geq 0$. For the current problem, from a solution of degree d, we get solutions of degrees d^m for $m \geq 0$. Thus we get a much sparser set of solutions. Second, pairs of permutable polynomials are much rarer (though proving this is beyond the scope of this book). For "most" choices of $Q(x)$, the only solutions are the ones we have already found, $Q^{(n)}(x)$.

Still there are also similarities between the two problems. In particular, we will see that this problem has a similar uniqueness result: If $Q(x)$ is nonlinear, then given a fixed degree and leading coefficient, there is at most one polynomial $P(x)$ with that degree and leading coefficient such that $P(Q(x)) = Q(P(x))$. The interesting case for permutable polynomials is where $Q(x)$ is non-linear, but as a warm-up, we will first deal with the cases where $Q(x)$ is constant and linear.

Example 4.13. If $Q(x) = C$ is a constant polynomial, then the only polynomials $P(x)$ which are permutable with $Q(x)$ are the ones that have C as a fixed point, that is, those with $P(C) = C$.

Solution. Just plug in $Q(x) = C$. ∎

Example 4.14. Suppose $Q(x) = ax + b$ with $a \neq 0$ is a linear polynomial. Find all polynomials $P(x)$ that are permutable with $Q(x)$.

Solution. First suppose $a \neq 1$. Then the equation $Q(r) = r$ has a unique solution $r = \frac{b}{1-a}$ and we can write $Q(x) = a(x - r) + r$. Letting

$$R(x) = P(x + r) - r,$$

we see that the equation

$$P(a(x - r) + r) = a(P(x) - r) + r$$

becomes $R(a(x-r)) = aR(x-r)$, which we can rewrite as just $R(ax) = aR(x)$. Writing $R(x) = c_d x^d + c_{d-1}x^{d-1} + \ldots + c_0$ and looking at the coefficient of x^k

in this equality, we see that $(a^k - a)c_k = 0$. Thus, if a is not a root of unity, the only nonzero coefficient is c_1. Thus we find that $R(x) = cx$ for some constant c and hence $P(x) = c(x - r) + r$. If m is the order of a, so $a^m = 1$ and $m > 0$ is minimal, then we see that the nonzero coefficients of $R(x)$ are those with $k \equiv 1 \pmod{m}$. Hence we can write $R(x) = xS(x^m)$ for some polynomial $S(x)$ and hence $P(x) = xS((x - r)^m) + r$.

Now suppose $a = 1$ and $b \neq 0$. Then we have $P(x + b) = P(x) + b$, or equivalently $P(x + b) - P(x) = b$. The right hand side is a polynomial of degree 0 and leading coefficient b, so by the results of Section 3.6, we see that $P(x)$ is linear with leading coefficient 1. Thus we find $P(x) = x + c$ for some constant c.

Finally, if $a = 1$ and $b = 0$, that is, if $Q(x) = x$, then we have already seen that every polynomial $P(x)$ is a solution. ■

Now we turn to some more interesting examples where $Q(x)$ is nonlinear.

Example 4.15. Find all nonconstant polynomials $P(x)$ such that

$$P(x^2 + 1) = (P(x))^2 + 1.$$

Serbian Mathematical Olympiad 2015

Solution. Let $Q(x) = x^2 + 1$. Then the problem is asking for polynomials $P(x)$ which are permutable with $Q(x)$, that is, with $P(Q(x)) = Q(P(x))$.

We will prove by induction on the degree of the polynomial $P(x)$ that the only nonconstant polynomials of this type are the ones we have already found

$$x, Q(x), Q(Q(x)), \ldots.$$

The base case follows from the previous example, or an easy computation. If $P(x) = ax + b$ is linear, then we want $(ax + b)^2 + 1 = a(x^2 + 1) + b$. From the leading coefficient we get $a^2 = a$, hence $a = 1$, and from the coefficient of x we get $2ab = 0$, hence $b = 0$. Thus the only solution is $P(x) = x$.

Now suppose we have a solution $P(x)$ of degree $d \geq 2$ and suppose that all solutions of lower degree are in the sequence above. Observe that

$$(P(-x))^2 = P(x^2 + 1) - 1 = (P(x))^2,$$

so $P(x) = \pm P(-x)$. If the positive sign occurs, then there is a polynomial $R(x)$ such that $P(x) = R(x^2)$. Let $S(x) = R(x - 1)$. Then

$$P(x) = S(x^2 + 1) = S(Q(x)).$$

So

$$Q(S(Q(x))) = Q(P(x)) = P(Q(x)) = S(Q(Q(x))).$$

Since $Q(x)$ takes on infinitely many values, this implies that

$$Q(S(x)) = S(Q(x)).$$

Since

$$\deg S(x) = \frac{1}{2} \deg P(x) < \deg P(x),$$

the induction hypothesis implies that $S(x) = Q^{(n)}(x)$ for some n and hence

$$P(x) = Q^{(n+1)}(x).$$

Now suppose $P(x) = -P(-x)$. We will show that there is an increasing sequence of real numbers (x_n) such that $P(x_n) = x_n$. We define it as follows:

$$x_0 = 0, \quad x_{n+1} = x_n^2 + 1 \qquad \forall n \geq 1.$$

Clearly $P(0) = 0$ since $P(x)$ is odd. Inductively, we see that if $P(x_n) = x_n$, then

$$P(x_{n+1}) = P(x_n^2 + 1) = (P(x_n))^2 + 1 = x_n^2 + 1 = x_{n+1}.$$

Hence $P(x_n) = x_n$ for all n. Also notice that since $Q(x)$ is an increasing function of x for $x \geq 0$ and since $x_0 < x_1$, we have $x_1 = Q(x_0) < Q(x_1) = x_2$. Iterating this we find that x_n is an increasing sequence and hence its terms are distinct. Thus the equation $P(x) = x$ has infinitely many roots, whence $P(x) = x$. ■

Remark. Note that most of the solution above would be unchanged if we replace $Q(x)$ by $Q(x) = x^2 + t$ for a constant t. In particular, the proof that a linear $P(x)$ must be just x did not look at the constant term, so it is unchanged. The argument that $P(x) = \pm P(x)$ only used the fact that

$Q(x)$ is even, which is true for all t. The argument in the case where $P(x)$ is even only needs to be modified slightly to define $S(x) = R(x - t)$, so that $P(x) = S(Q(x))$. The only place where t was used was in the argument for the case where $P(x)$ is odd. We needed to know that $x_1 = Q(x_0) > x_0 = 0$ to conclude that the sequence (x_n) is increasing and hence has distinct terms. Thus the argument above, with only minor changes, applies for all $t > 0$.

Example 4.16. Find all nonconstant polynomials $P(x)$ such that

$$P(x^2 - 1) = (P(x))^2 - 1 \qquad \forall x \in \mathbb{R}.$$

Polish Mathematical Olympiad (Modified) 2000

Solution. As above, set $Q(x) = x^2 - 1$. Then we want all polynomials $P(x)$ that are permutable with $Q(x)$ so that $P(Q(x)) = Q(P(x))$.
We will again prove by induction on the degree of $P(x)$ that the only nonconstant polynomials of this type are

$$x, Q(x), Q(Q(x)), \ldots.$$

As we remarked, most of the previous solution goes through without any major changes. We still have

$$(P(-x))^2 = P(x^2 - 1) + 1 = (P(x))^2,$$

so $P(x) = \pm P(-x)$. If the positive sign occurs so $P(x)$ is even, then we write $P(x) = R(x^2)$ and define $S(x) = R(x+1)$. Then $P(x) = S(x^2-1) = S(Q(x))$, so the inductive argument is unchanged.
The only difference is in the argument when $P(x)$ is odd.
We still have $P(0) = 0$, hence $P(-1) = P(Q(0)) = Q(P(0)) = Q(0) = -1$.
However if we try to iterate this argument, we will only get that $P(0) = 0$ again.
Instead, we note that since $P(x)$ is odd, we also have $P(1) = -P(-1) = 1$.
Now, notice that if $x \geq -1$, we can set $x = y^2 - 1$. Then

$$P(x) = P(y^2 - 1) = (P(y))^2 - 1 \geq -1.$$

So for all $x \geq -1$ we have $P(x) \geq -1$. Now, we define a sequence of real numbers (a_n) by $a_1 = 1$ and $a_{n+1} = \sqrt{1 + a_n}$ for all $n \geq 1$. Note that since the function $f(x) = \sqrt{1 + x}$ is increasing for $x \geq -1$ and $1 = a_1 < a_2 = \sqrt{2}$, we have $a_2 = f(a_1) < f(a_2) = a_3$. Iterating this we see that the sequence (a_n) is increasing. Hence its terms are distinct and $a_n > 1$ for $n > 1$. We can also prove by induction on n that $P(a_n) = a_n$ for all $n \geq 1$. The base case $n = 1$ is obvious. Assume that $P(a_n) = a_n$. Then

$$(P(a_{n+1}))^2 = P(a_{n+1}^2 - 1) + 1 = P(a_n) + 1 = a_n + 1 = a_{n+1}^2,$$

which gives $P(a_{n+1}) = \pm a_{n+1}$. However since $P(a_{n+1}) \geq -1 > -a_{n+1}$, we must have the plus sign. So $P(a_{n+1}) = a_{n+1}$ and the induction step is proven. Thus $P(x) = x$ has infinitely many roots, and we conclude that $P(x) = x$. ■

Remark. The argument in the previous solution actually applies for

$$Q(x) = x^2 - t$$

for any $t \in (0, 2)$. The only thing that needs checked is the final argument in the case where $P(x)$ is odd. We find $P(-t) = -t$ and since $P(x)$ is odd, $P(t) = t$. We then define the sequence a_n by $a_1 = t$ and $a_{n+1} = \sqrt{t + a_n}$. Since $0 < t < 2$, we have $a_2 = \sqrt{2t} > t = a_1$, and hence the sequence (a_n) is still increasing. In particular $a_n > t$ for $n > 1$. We again compute that $P(a_{n+1}) = \pm a_{n+1}$ and that $P(a_{n+1}) \geq -t > -a_{n+1}$ so that the plus sign must hold. Hence $P(a_n) = a_n$ for all n and $P(x) = x$.
The two previous cases leave one block of polynomials $Q(x) = x^2 + t$ unsolved, so let's take care of them.

Example 4.17. Suppose $t > 2$. Find all nonconstant polynomials $P(x)$ such that

$$P(x^2 - t) = (P(x))^2 - t \qquad \forall x \in \mathbb{R}.$$

Solution. Set $Q(x) = x^2 - 1$, so we want all polynomials $P(x)$ that are permutable with $Q(x)$ so that $P(Q(x)) = Q(P(x))$.
In this case the solution for the first example $Q(x) = x^2 + 1$, works with only minor changes.

We again define a sequence x_n by $x_0 = 0$ and $x_{n+1} = x_n^2 - t = Q(x_n)$. The sequence (x_n) is not quite increasing because $x_1 = -t < x_0$. However we compute that

$$x_2 = t^2 - t > 2t - t > t = |x_1|.$$

Hence

$$x_2 = Q(x_1) = Q(|x_1|) < Q(x_2) = x_3.$$

Thus iterating this, we see that the sequence (x_n) is increasing for $n \geq 2$. (Alternately, we could borrow a trick from the preceding solution and start the sequence at t using the fact that $P(t) = -P(-t) = t$ and get an increasing sequence.) Thus again we have $P(x_n) = x_n$ for all n and hence $P(x) = x$. ■

The last three example combine to cover almost every polynomial of the form $Q(x) = x^2 + t$. The only two missing cases are $t = 0$ and $t = -2$. The attentive reader may recall that we have already solved the case $t = 0$ in the solutions to Example 3.18, but we will give a different proof using the following uniqueness lemma for permutable polynomials.

Second Uniqueness Lemma

Let $Q(x)$ be a nonlinear polynomial. Then for any $d \geq 1$ and any nonzero real number a, there is at most one polynomial $P(x)$ of degree d with leading coefficient a such that $P(Q(x)) = Q(P(x))$.

Proof. Suppose $Q(x)$ is a polynomial of degree $m \geq 2$ and write

$$Q(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0$$

with $b_m \neq 0$. Suppose on the contrary that $P_1(x)$ and $P_2(x)$ are distinct polynomials of degree d with leading coefficient a such that $P_i(Q(x)) = Q(P_i(x))$. Then $R(x) = P_1(x) - P_2(x)$ is a nonzero polynomial of some degree $k < d$. Note that

$$\begin{aligned} R(Q(x)) &= P_1(Q(x)) - P_2(Q(x)) = Q(P_1(x)) - Q(P_2(x)) \\ &= Q(P_2(x) + R(x)) - Q(P_2(x)). \end{aligned}$$

The left-hand side of this equality is a polynomial of degree km. Since we can write

$$Q(P_2 + R) = b_m((P_2 + R)^m - P_2^m) + b_{m-1}((P_2 + R)^{m-1} - P_2^{m-1}) + \ldots$$

and

$$(P_2 + R)^j - P_2^j = \sum_{i=0}^{j-1} \binom{j}{i} P_2^i R^{j-i}$$

is a polynomial of degree $(j-1)d + k$, we see that the right-hand side is a polynomial of degree $(m-1)d + k > mk$. This is a contradiction, hence we have proved uniqueness. ❑

This Lemma has limited uses since for most polynomials $Q(x)$ solutions only exist for a small number of degrees. But for the last two quadratic cases it is spectacularly helpful. We will start with the case we have already seen, and then do the harder case.

Example 4.18. Find all nonconstant polynomials $P(x)$ such that

$$P(x^2) = (P(x))^2 \qquad \forall x \in \mathbb{R}.$$

Solution. Note that the polynomial $P(x) = x^d$ has $P(x^2) = x^{2d} = (P(x))^2$. Hence it is a solution which is monic of degree d. Let $P(x) = a_d x^d + \ldots$, with $a_d \neq 0$, be any solution of degree d. Then looking at the leading coefficients of $P(x^2) = (P(x))^2$, we get $a_d = a_d^2$ and hence $a_d = 1$. Thus $P(x)$ must be monic and hence by the Lemma $P(x) = x^d$. ■

Example 4.19. Find all nonconstant polynomials $P(x)$ such that

$$P(x^2) - 2 = (P(x))^2 - 2 \qquad \forall x \in \mathbb{R}.$$

Solution. Recall that in the first solution to Example 1.7 we defined a family of polynomials $T_k(x)$ by $T_0(x) = 2$, $T_1(x) = x$, and

$$T_{k+1}(x) = xT_k(x) - T_{k-1}(x).$$

We saw that $T_k(x)$ is a monic polynomial of degree k such that

$$T_k\left(x+\frac{1}{x}\right) = x^k + \frac{1}{x^k}.$$

Though we did not say so at the time, these polynomials are closely related to the Chebyshev polynomials, which are arguably the most remarkable family of polynomials.

In particular, note that $T_2(x) = x^2 - 2$. Hence we are looking for polynomials that are permutable with T_2. Since we compute that

$$\begin{aligned} T_k\left(T_m\left(x+\frac{1}{x}\right)\right) &= T_k\left(x^m + \frac{1}{x^m}\right) = x^{km} + \frac{1}{x^{km}} \\ &= T_m\left(x^k + \frac{1}{x^k}\right) = T_m\left(T_k\left(x+\frac{1}{x}\right)\right) \end{aligned}$$

and since $x + \frac{1}{x}$ takes on infinitely many values, we conclude that the polynomials T_k and T_m are permutable for all k, m. In particular, $T_d(x)$ is a monic polynomial of degree d that is permutable with $T_2(x)$.

Now we finish exactly as in the previous solution. Let $P(x) = a_d x^d + \ldots$, with $a_d \neq 0$, be degree d that is permutable with $T_2(x)$. Then looking at the leading coefficients of $P(T_2(x)) = T_2(P(x))$, we get $a_d = a_d^2$ and hence $a_d = 1$. Thus $P(x)$ must be monic and hence by the Lemma $P(x) = T_d(x)$. ■

Example 4.20. Let $a \neq 0$ and b, c be real numbers. Find all polynomials $P(x)$ such that

$$P(ax^2 + bx + c) = aP(x)^2 + bP(x) + c.$$

Solution. Define a linear function $\ell(x) = ax + \frac{b}{2}$ and let $t = ac + \frac{b}{2} - \frac{b^2}{4}$. Then we compute that

$$\ell(ax^2 + bx + c) = a^2x^2 + abx + ac + \frac{b}{2} = a^2x^2 + abx + \frac{b^2}{4} + t = (\ell(x))^2 + t.$$

Also define a new polynomial $R(x)$ by

$$R(x) = aP\left(\frac{x - b/2}{a}\right) + \frac{b}{2}$$

and note that this means

$$R(\ell(x)) = aP\left(\frac{(ax + b/2) - b/2}{a}\right) + \frac{b}{2} = aP(x) + \frac{b}{2} = \ell(P(x)).$$

Then we compute that

$$\begin{aligned} R\left((\ell(x))^2 + t\right) &= R(\ell(ax^2 + bx + c)) = \ell(P(ax^2 + bx + c)) \\ &= \ell(aP(x)^2 + bP(x) + c) = (\ell(P(x)))^2 + t \\ &= (R(\ell(x)))^2 + t. \end{aligned}$$

Thus $R(x^2 + t) = (R(x))^2 + t$. Thus we have found that $P(x)$ is permutable with $ax^2 + bx + c$ if and only if $R(x)$ is permutable with $x^2 + t$. Since the five preceding examples combined to find all such polynomials, we are in principle done.

More explicitly, the answer is as follows. Let $Q(x) = ax^2 + bx + c$ and compute the constant $t = ac + \frac{b}{2} - \frac{b^2}{4}$. If $t \neq 0, -2$, then the only possibilities for $P(x)$ are $Q^{(n)}(x)$ for $n \geq 0$. If $t = 0$, then we have

$$Q(x) = \frac{1}{a}\left(\left(ax + \frac{b}{2}\right)^2 - \frac{b}{2}\right).$$

In this case, the possible $P(x)$ are

$$P(x) = \frac{1}{a}\left(\left(ax + \frac{b}{2}\right)^n - \frac{b}{2}\right)$$

for $n \geq 1$. If $t = -2$, then we have

$$Q(x) = \frac{1}{a}\left(\left(ax + \frac{b}{2}\right)^2 - 2 - \frac{b}{2}\right).$$

In this case, the possible $P(x)$ are

$$P(x) = \frac{1}{a}\left(T_n\left(ax + \frac{b}{2}\right) - \frac{b}{2}\right),$$

where $T_n(x)$ are the polynomials discussed in the previous solution. ■

Remark. The previous solution gives another piece of the general answer. Suppose $P(x)$ and $Q(x)$ are permutable polynomials and let $\ell(x)$ be any linear function. Then we can always define new polynomials $R(x)$ and $S(x)$ so that $R(\ell(x)) = \ell(P(x))$ and $S(\ell(x)) = \ell(Q(x))$. Then $R(x)$ and $S(x)$ will be permutable polynomials.

With this final piece, we can now describe all pairs of permutable polynomials. This description was proven by J. F. Ritt (and in fact he gave all pairs of permutable rational functions), but the proof is far too involved and sophisticated to give here. We can build permutable functions in four basic ways:

- Let $Q(x)$ be an arbitrary polynomial. Then the polynomials $Q^{(m)}(x)$ and $Q^{(n)}(x)$ are permutable for all $m, n \geq 0$.
- Let $Q(x) = xR(x^m)$ for some polynomial $R(x)$. Then the polynomials $\omega Q^{(m)}(x)$ and $\omega' Q^{(n)}(x)$ are permutable for all $m, n \geq 0$ and any m-th roots of unity ω and ω'.
- The polynomials ωx^m and $\omega' x^n$ are permutable if ω is an $(n-1)$-st root of unity and ω' is an $(m-1)$-st root of unity.
- The polynomials $\omega T_m(x)$ and $\omega' T_n(x)$ are permutable, where $\omega = 1$ if n is even and $\omega = \pm 1$ if n is odd and $\omega' = 1$ if m is even and $\omega' = \pm 1$ if m is odd.

From any of the last three basic examples, we can construct additional examples by using linear functions $\ell(x)$ as described above. (For solutions built from the first example using ℓ just gives a solution corresponding to a different $Q(x)$.)

We now turn to some higher degree examples, which can be solved without invoking the general result above.

Example 4.21. Find all nonconstant polynomials P such that

$$P(x^3 - 2) = (P(x))^3 - 2.$$

Solution. If we define $Q(x) = x^3 - 2$, we see that the problem is asking for polynomials $P(x)$ that are permutable with $Q(x)$. Since the same proof works, we will actually consider the more general case $Q(x) = x^m - t$ where $m \geq 3$ is odd and $t > 0$.

We will prove by induction on the degree of $P(x)$ that the only nonconstant polynomials of this type are $Q^{(n)}(x)$ for $n \geq 0$.

The base case follows from the linear case above or by noting that if

$$P(x) = ax + b,$$

then we get

$$a(x^m - t) + b = (ax + b)^m - t$$

so the coefficient of x^{m-1} gives $ma^{m-1}b = 0$, hence $b = 0$, and then the constant term gives $-at = -t$, so $a = 1$.

For the induction step, suppose $P(x)$ has degree d and that all solutions of lower degree are of the form $Q^{(n)}(x)$ for some n. Let ω be a primitive m-th root of unity. Note that

$$(P(\omega x))^m = P\left((\omega x)^m - t\right) + 2 = P(x^m - t) + 2 = (P(x))^m.$$

Hence for every x there is an r (which we may assume satisfies $0 \leq r < m$) such that $P(\omega x) = \omega^r P(x)$. One of the m possible values of r must occur infinitely often. Hence for that r, we have $P(\omega x) = \omega^r P(x)$ for all x. From this equation, we see that all monomials in $P(x)$ (with nonzero coefficient) have exponents congruent to r modulo m. Thus $P(x) = x^r R(x^m)$ for some polynomial $R(x)$.

If $r = 0$, we set $S(x) = R(x + t)$ so that $P(x) = S(Q(x))$, then

$$Q(S(Q(x))) = Q(P(x)) = P(Q(x)) = S(Q(Q(x))),$$

and we conclude that $Q(S(x)) = S(Q(x))$. Since

$$\deg S(x) = \frac{1}{m} \deg P(x) < \deg P(x),$$

we have $S(x) = Q^{(n)}(x)$ for some n, and hence $P(x) = Q^{(n+1)}(x)$.

If $r \neq 0$ then $P(0) = 0$. Define a sequence of real numbers (x_n) by

$$x_0 = 0, \quad x_{n+1} = x_n^m - t \quad \forall n \geq 1.$$

Since $f(x) = x^m - t$ is an increasing function of x (this is where we are using the fact that m is odd) and $x_0 = 0 > x_1 = -t$, we conclude that $x_1 = f(x_0) > f(x_1) = x_2$. Iterating this, we see that (x_n) is decreasing, hence it has distinct terms. Since $P(x_0) = x_0$, we see by induction on n, that

$$P(x_{n+1}) = P(x_n^m - t) = P(x_n)^m - t = x_n^m - t = x_{n+1}$$

holds for all n. Thus $P(x) = x$ has infinitely many roots and hence holds for all x. ∎

Remark. Note that either applying this result to $-P(-x)$ or modifying the solution slightly solves the case $Q(x) = x^m + t$ for any $t > 0$.

Example 4.22. Find all nonconstant polynomials $P(x)$ such that

$$P((x+1)^3) = (P(x)+1)^3.$$

Solution. Let $Q(x) = (x+1)^3$. We will prove by induction on the degree of $P(x)$ that $P(x) = Q^{(n)}(x)$ for some $n \geq 0$.
Write

$$P(x) = Cx^k(x - r_1)(x - r_2)\cdots(x - r_m),$$

where C is the leading coefficient of $P(x)$ and $r_1, \ldots, r_m$ are the nonzero complex roots of $P(x)$. Then the roots of $P((x+1)^3)$ are -1 with multiplicity $3k$ and the three roots of $(x+1)^3 = r_j$ for each j. Note that if $r_j \neq r_k$, then the roots of $(x+1)^3 = r_j$ and $(x+1)^3 = r_k$ have no overlap (since a common root would divide $r_j - r_k \neq 0$). However since $P((x+1)^3) = (P(x)+1)^3$, we see that every root of $P((x+1)^3)$ must have multiplicity a multiple of 3. Thus each r_j occurs a multiple of 3 times. Also note that looking at the leading coefficient of $P((x+1)^3) = (P(x)+1)^3$, we see that $C = C^3$, hence $C = \pm 1$. Thus we can write $P(x) = x^k R(x)^3$ for some polynomial $R(x)$ with leading coefficient C.

If $k \neq 0$, then $P(0) = 0$. Define a sequence of real numbers (x_n) by

$$x_0 = 0, \quad x_{n+1} = (x_n + 1)^3 \quad \forall n \geq 1.$$

Since $f(x) = (x+1)^3$ is an increasing function of x and $x_0 = 0 < x_1 = 1$, we compute that $x_1 = f(x_0) < f(x_1) = x_2$ and iterating this we see that x_n is increasing. Further from the formula

$$P(x_{n+1}) = P((x_n+1)^3) = (P(x_n)+1)^3 = (x_n+1)^3 = x_{n+1}$$

it follows by induction on n that $P(x_n) = x_n$ for all n. Thus $P(x) = x$ has infinitely many roots and hence $P(x) = x$. Note that in particular, this proves the base case of the induction since if $\deg P(x) < 3$, then we must have $k > 0$. If $k = 0$, then $P(x) = R(x)^3$ and we see that

$$(R((x+1)^3))^3 = (R(x)^3 + 1)^3.$$

Since R has leading coefficient $C = \pm 1$, it follows that

$$R((x+1)^3) = R(x)^3 + 1.$$

Thus if we define $S(x) = R(x) - 1$ so that $P(x) = S(x)^3 + 1 = Q(S(x))$ we find that

$$S((x+1)^3) = (S(x)+1)^3.$$

Thus $S(x)$ is also permutable with $Q(x)$ and has lower degree than $P(x)$, hence by the induction hypothesis

$$S(x) = Q^{(n)}(x)$$

and hence $P(x) = Q(S(x)) = Q^{(n+1)}(x)$. ∎

Example 4.23. Let $n \geq 1$. Find all polynomials f with complex coefficients such that

$$1 + f(x^n + 1) = f(x)^n.$$

Vlad Matei - Romanian Team Selection Test 2013

Solution. If n is odd, then defining $g(x) = -f(x)$, we see that

$$g(x)^n + 1 = g(x^n + 1).$$

Thus $g(x)$ is permutable with $Q(x) = x^n + 1$ and by the solution to Example 4.21, we see that $g(x) = Q^{(n)}(x)$ and hence $f(x) = -Q^{(n)}(x)$ for some $n \geq 0$. Thus we may assume n is even. In this case, we will show there is no such polynomial f. Assume on the contrary that there is such an $f(x)$ and assume we have chosen the example with minimal degree.
Let ω be a primitive n-th root of unity. We find that

$$f(\omega x)^n = 1 + f((\omega x)^n + 1) = 1 + f(x^n + 1) = f(x)^n.$$

Hence $\frac{f(\omega x)}{f(x)}$ is always an n-th root of unity. Since it is continuous except at finitely many points in the complex plane, it follows that $f(\omega x) = \omega^m f(x)$ for some integer m, which we may assume satisfies $0 \leq m \leq n-1$. Comparing coefficients of both sides we find that $f(x) = x^m g(x^n)$ for some polynomial $g(x)$.
If $m = 0$, then we can define $h(x) = g(x-1)$ so that $f(x) = h(Q(x))$. Then we have

$$h(Q(x))^n = f(x)^n = 1 + f(Q(x)) = 1 + h(Q(Q(x))),$$

so $h(x)^n = 1 + h(Q(x))$. Thus $h(x)$ is an example with lower degree than $f(x)$, contrary to our assumption of minimality.
Thus we must have $m > 0$, so that $f(0) = 0$, then define a sequence by

$$x_0 = 0, \quad x_{k+1} = x_k^n + 1 \quad \forall n \geq 1.$$

Since $Q(x)$ is increasing and $x_0 < x_1$, we see that this sequence is increasing, hence it has distinct terms. We also see that $f(x_{k+1}) = f(x_k)^n - 1$. Since $f(x_0) = 0$, an easy induction argument shows that

$$f(x_{2k}) = 0, \quad f(x_{2k+1}) = -1$$

for all k. But then both $f(x) = 0$ and $f(x) = -1$ have infinitely many roots, a contradiction. Thus there is no such f. ■

Example 4.24. The degree of the polynomials P and Q with real coefficients do not exceed n. These polynomials satisfy the identity

$$P(x)\,x^{n+1} + Q(x)\,(x+1)^{n+1} = 1.$$

Determine all possible values of $Q(-\frac{1}{2})$.

K. Dilcher and M. Ulas - Tuymaada Competition 2020

First Solution. We first prove that there are unique polynomials $P(x), Q(x)$ of degree at most n satisfying the above identity. Assume on the contrary, that there are two pairs of polynomials, $(P_1(x), Q_1(x))$ and $(P_2(x), Q_2(x))$ such that

$$P_1(x)\,x^{n+1} + Q_1(x)\,(x+1)^{n+1} = 1 = P_2(x)\,x^{n+1} + Q_2(x)\,(x+1)^{n+1}.$$

Then

$$(P_1(x) - P_2(x))\,x^{n+1} + (Q_1(x) - Q_2(x))(x+1)^{n+1} = 0.$$

Since the polynomials $x^{n+1}, (x+1)^{n+1}$ are coprime, it follows that $(x+1)^{n+1}$ divides $P_1(x) - P_2(x)$ and x^{n+1} divides $Q_1(x) - Q_2(x)$. This, together with the degree condition, implies that $P_1(x) = P_2(x)$ and $Q_1(x) = Q_2(x)$.
Setting $x = -1 - y$, we get

$$Q(-1-y)(-1)^{n+1}y^{n+1} + P(-1-y)(-1)^{n+1}(y+1)^n = 1.$$

The uniqueness argument implies that

$$P(x) = (-1)^{n+1}Q(-1-x)$$

and

$$Q(x) = (-1)^{n+1}P(-1-x).$$

Plugging $x = -\frac{1}{2}$, we obtain

$$P\left(-\frac{1}{2}\right) = (-1)^{n+1}Q\left(-\frac{1}{2}\right),$$

and

$$P\left(-\frac{1}{2}\right)\left(-\frac{1}{2}\right)^{n+1} + Q\left(-\frac{1}{2}\right)\left(\frac{1}{2}\right)^{n+1} = 1.$$

It follows that $Q\left(-\frac{1}{2}\right) = 2^n$. ■

Second Solution. Begin as in the preceding solution, but after concluding that the pair $(P(x), Q(x))$, not that

$$1 = ((x+1)-x)^{2n+1} = \sum_{k=0}^{2n+1}(-1)^k\binom{2n+1}{k}(x+1)^{2n+1-k}x^k$$
$$= (x+1)^{n+1}\sum_{k=0}^{n}(-1)^k\binom{2n+1}{k}(x+1)^{n-k}x^k$$
$$+ x^n\sum_{k=n+1}^{2n+1}(-1)^k\binom{2n+1}{k}(x+1)^{2n+1-k}x^{k-n-1}.$$

Thus by uniqueness we must have

$$Q(x) = \sum_{k=0}^{n}(-1)^k\binom{2n+1}{k}(x+1)^{n-k}x^k,$$

and hence we compute

$$Q\left(-\frac{1}{2}\right) = \frac{1}{2^n}\sum_{k=0}^{n}\binom{2n+1}{k} = \frac{2^{2n}}{2^n} = 2^n. \quad \blacksquare$$

Third Solution. This solution is the same, in essence, as the above solution. Let us denote by $R(x)$ the polynomial $P(x)x^{n+1} + Q(x)(x+1)^{n+1}$. Since the coefficients of x, x^2, ..., x^n in $R(x)$ are zero and the coefficients of 1, x, x^2, ..., x^n in $P(x)x^{n+1}$ are zero, we find that the constant term of $Q(x)$ is 1 and the coefficients of x, ..., x^n in $Q(x)(x+1)^{n+1}$ are zero. Now, let $Q(x) = a_0 + \ldots + a_d x^d$, $d \le n$. We will prove by induction that $a_0, \ldots, a_d$ are uniquely be determined. The base is true for a_0. Assume that a_0, ..., a_t are uniquely determined. Write $(x+1)^{n+1} = 1 + b_1 x + \ldots + x^{n+1}$. Then the coefficient of x^{t+1} is $a_{t+1} + \underbrace{b_1 a_t + \ldots + b_{t+1}}_{\text{unique}}$. Since $t = d-1 \le n-1$, it follows that a_{t+1} is uniquely determined. This completes our proof.
According to the above fact, the polynomial $P(x)$ is also unique. Hence we can continue our proof as in either of the preceding solutions. $\blacksquare$

Fourth Solution. We first prove following lemma.

Lemma. If $\deg P(x) = d$, $k \ge d$, and $(x-1)^\alpha \mid P(x)$, then $(x-1)^\alpha \mid x^k P\left(\frac{1}{x}\right)$.

Proof. Write $P(x) = (x-1)^\alpha R(x)$. Then

$$x^k P\left(\frac{1}{x}\right) = x^k\left(\frac{1}{x}-1\right)^\alpha R\left(\frac{1}{x}\right) = x^{k-d}(1-x)^\alpha\left(x^{d-\alpha}R\left(\frac{1}{x}\right)\right).$$

This completes our proof. $\square$

By using the substitution $x \mapsto x-1$, we obtain

$$P(x-1)(x-1)^{n+1} + Q(x-1)x^{n+1} = 1.$$

Set $Q(x-1) = T(x)$.
It follows that $(x-1)^{n+1}$ divides $x^{n+1}Q(x-1) - 1 = x^{n+1}T(x) - 1$. Since this polynomial has degree at most $2n+1$, we can put $k = 2n+1$ in the lemma to obtain that $(x-1)^{n+1}$ divides $x^n T\left(\frac{1}{x}\right) - x^{2n+1}$. Setting $S(x) = x^n T\left(\frac{1}{x}\right)$, we see that

$$\deg S(x) \le n, \quad Q\left(-\frac{1}{2}\right) = T\left(\frac{1}{2}\right) = 2^{-n}S(2),$$

and $(x-1)^{n+1}$ divides $S(x) - x^{2n+1}$. Thus x^{n+1} divides $S(x+1) - (x+1)^{2n+1}$. Letting $A(x) = S(x+1)$, it follows that x^{n+1} divides $A(x) - (x+1)^{2n+1}$. Since $\deg A(x) \le n$, it follows that $A(x)$ is the remainder upon the division of $(x+1)^{2n+1}$ by x^{n+1}. Thus

$$A(x) = \sum_{i=0}^{n}\binom{2n+1}{i}x^i.$$

Thus

$$A(1) = S(2) = \sum_{i=0}^{n}\binom{2n+1}{i} = 2^{2n}.$$

Whence

$$Q\left(-\frac{1}{2}\right) = T\left(\frac{1}{2}\right) = 2^{-n}S(2) = 2^n.$$

4.3 Proposed problems

Problem 4.1. Let $R(t)$ be a polynomial of degree 2017. Prove that there exist infinitely many polynomials $P(x)$ such that

$$P((R^{2017}(t)+R(t)+1)^2-2)=P(R^{2017}(t)+R(t)+1)^2-2.$$

Find a relation between those polynomials $P(x)$.

Problem 4.2. Find all polynomials $P(x)$ with real coefficients such that

$$P(x)P(x+1)=P(x^2-x+3).$$

Taiwanese Team Selection Test 2014

Problem 4.3. Prove that if the polynomial f is nonzero and for every real number x,

$$f(x)f(x+3)=f(x^2+x+3),$$

then f has no real roots.

Polish Mathematical Olympiad 1986

Problem 4.4. Find all linear and quadratic polynomials $P(x)$ such that

$$P(x)P(2-x)=P(2+2x-x^2).$$

Problem 4.5. Find all nonconstant polynomials $P(x)$ such that

$$P(x)P(2x^2-2)=P(2x^3-5x).$$

Problem 4.6. Find all nonconstant polynomials $P(x)$ such that

$$P(x)P(x+2)=P(x^2+1).$$

Problem 4.7. Find all nonconstant polynomials $P(x)$ such that

$$P(x^3-3x)=P(x)^3-3P(x).$$

Chapter 5

Finding Polynomials. Part III: Using Roots

5.1 Basic facts

As you may have seen in the first volume of the polynomial trilogy, decomposing a polynomial into products of its factors is a fruitful strategy. As you may remember, each polynomial can be represented in the following form.

Theorem

Each monic polynomial $P(x)$ with real coefficients can be expressed as a product of the following form:

$$(x-r_1)^{\alpha_1}\cdot\ldots\cdot(x-r_t)^{\alpha_t}(x^2-2\mathrm{Re}(z_1)x+|z_1|^2)^{\beta_1}\cdot\ldots\cdot(x^2-2\mathrm{Re}(z_s)x+|z_s|^2)^{\beta_s},$$

for some real numbers $r_1,\ldots,r_t$ and non-real numbers $z_1,\ldots,z_s$.
Note that $\deg P(x)=\alpha_1+\ldots+\alpha_t+2(\beta_1+\ldots+\beta_s)$.

The above formulation can be very helpful in many cases. However, sometimes we restrict ourselves to some simplified cases, for example when a polynomial has only real roots.

Example 5.1. Find all nonconstant monic polynomials $P(x)$ and $Q(x)$ of degree d with d nonnegative integer roots such that

$$P(x) - Q(x) = 1.$$

Centro-American Mathematical Olympiad 2014

First Solution. Let

$$P(x) = (x - a_1) \cdot \ldots \cdot (x - a_d) \quad \text{and} \quad Q(x) = (x - b_1) \cdot \ldots \cdot (x - b_d)$$

with $0 \le a_1 \le \ldots \le a_d$, $0 \le b_1 \le \ldots \le b_d$ and a_i, b_i are integers for all $i = 1, 2, \ldots, d$. Then

$$(x - a_1) \cdot \ldots \cdot (x - a_d) - (x - b_1) \cdot \ldots \cdot (x - b_d) = 1.$$

Putting $x = b_1$, we find that $(b_1 - a_1) \cdot \ldots \cdot (b_1 - a_d) = 1$.
Therefore $|b_1 - a_i| = 1$, which gives $a_i \in \{b_1 - 1, b_1 + 1\}$.
Analogously, $b_i \in \{a_1 - 1, a_1 + 1\}$. Therefore each of $P(x)$ and $Q(x)$ has at most two distinct integer roots. We next prove that one of them has exactly one integer root. Assume that both $b_1 - 1$ and $b_1 + 1$ are roots of $P(x)$. Then using $b_1 - 1$, we find that any root of $Q(x)$ is in $\{b_1 - 2, b_1\}$ and using $b_1 + 1$ we find that any root of $Q(x)$ is in $\{b_1, b_1 + 2\}$. Hence b_1 is the only root of $Q(x)$. Now, we have two different cases.

(i) Suppose $Q(x)$ has only one real root. Then as we saw above, we can write

$$P(x) = (x - (b-1))^c (x - (b+1))^e,$$

for some $e, c \ge 0$ with $e + c = d$, and $Q(x) = (x - b)^d$. Then

$$(x - (b-1))^c (x - (b+1))^e = (x - b)^d + 1.$$

Putting $x = b + 1$, we get $0 = 2$, a contradiction. So it must be true that $e = 0$ and hence $c = d$. Thus $(x - (b-1))^d = (x - b)^d + 1$.

If $d = 1$, this holds and we have found the example $P(x) = x - b + 1$, $Q(x) = x - b$. Otherwise, checking the coefficient of x^{d-1} on both sides we find that $d(b-1) = db$, contradiction. So $d = 1$, $P(x) = x - b + 1$, $Q(x) = x - b$, where $b \ge 1$ is an integer, is the only example in this case.

(ii) Suppose $Q(x)$ has two real roots. In this case we can write

$$Q(x) = (x - (a-1))^c (x - (a+1))^e,$$

for some $e, c \ge 1$ with $e + c = d$, and $P(x) = (x - a)^d$. Examining the coefficient of x^{d-1} in the identity

$$(x - (a-1))^c (x - (a+1))^e = (x - a)^d - 1,$$

we find that

$$da = c(a-1) + e(a+1) = (c+e)a + e - c = da + e - c.$$

Therefore $e = c$. Rewriting the above identity as

$$(x - (a-1))^c (x - (a+1))^c = (x - a)^{2c} - 1$$

and putting $x = a + 2$, we get $3^c + 1 = 4^c$. So $c = 1$. Hence

$$Q(x) = (x - a + 1)(x - a - 1), \quad P(x) = (x - a)^2,$$

and it is easy to check that this is a solution. ■

Second Solution. From the first solution, we find that either $P(x)$ or $Q(x)$ is of the form $(x - b)^d$. Thus we find that either $P(x) = (x - b)^d + 1$ or $Q(x) = (x - b)^d - 1$. Thus the polynomial $(x - b)^d + 1$ or $(x - b)^d - 1$ must only have integer roots. Putting $y = x - b$, then we must find all d such that the polynomial $y^d + 1$ or $y^d - 1$ has only integer roots. It is clear that the only possible integer roots are $y = \pm 1$. For $y^d + 1$, we see that d must be odd and $y = -1$ is the only possible integer root. However, we can write

$$y^d + 1 = (y + 1)(y^{d-1} - y^{d-2} + \ldots - y + 1),$$

and $y = -1$ is not a root of $y^{d-1} - y^{d-2} + \ldots - y + 1$. Therefore $d = 1$.
For $y^d - 1$ and d odd, we see that only $y = 1$ is the only possible integer root. Since we can write

$$y^d - 1 = (y - 1)(y^{d-1} + y^{d-2} + \ldots + y + 1)$$

and $y = 1$ is not a root of the second factor, we must have $d = 1$. For $y^d - 1$ and d even, we can write

$$y^d - 1 = (y-1)(y+1)(y^{d-2} + y^{d-4} + \ldots + y^2 + 1)$$

and neither of $y = \pm 1$ is a root of the second factor. Thus $d = 2$
Working back, these give the same two examples as the previous solution. ∎

Example 5.2. Let $\deg P(x) = 2$, $\deg Q(x) = 4$. For all real number x we have

$$P(x)Q(x+4) = P(x+8)Q(x).$$

If $P(x)$ and $Q(x)$ have two and four real roots respectively, and the absolute value of the difference between the roots of $P(x)$ is greater than the sum of roots of $Q(x)$ by 8, find the minimum value of the sum of the squares of the roots of $Q(x)$.

Solution. Since we may cancel off any common constant factor, we may assume $P(x)$ and $Q(x)$ are monic. Then we can write

$$P(x) = (x-r)(x-s), \qquad Q(x) = (x-a)(x-b)(x-c)(x-d),$$

where $r > s$ and $a > b > c > d$. The condition $P(x)Q(x+4) = P(x+8)Q(x)$ says that the roots of the left-hand side, which are

$$S = \{r, s, a-4, b-4, c-4, d-4\},$$

are the same roots of the right-hand side, which are

$$T = \{r-8, s-8, a, b, c, d\}.$$

The added condition is that $r - s = a + b + c + d + 8$.
The largest element of S must be either r or $a-4$ and the largest element of T must be either $r-8$ or a. However these two sets are really the same, so this largest element must be common to them. It cannot be $r-8$ (since r is larger) or $a-4$ (since a is larger). Thus we must have $r = a$. Similarly the smallest element must be one of s and $d-4$, and one of $s-8$ and d. But it

cannot be d or s (since $s-8$ and $d-4$ are smaller). Thus $s-8 = d-4$, which gives $s = d+4$. Cancelling off these common elements, we find

$$\{a-4, b-4, c-4, d+4\} = \{a-8, b, c, d\}.$$

The largest remaining element must be either $a-4$ or $d+4$ (from the left), and must be either $a-8$ or b (from the right). However it cannot be $a-8$ (since $a-4$ is larger). Thus it must be b and either $b = a-4$ or $b = d+4$. Similarly, the smallest remaining element must be either $c-4$ or $d+4$ (from the left) and must be either $a-8$ or d (from the right). However it cannot be $d+4$ (since d is smaller). Thus it must be $c-4$ and either $c-4 = a-8$ or $c-4 = d$. Hence $c = a-4$ or $c = d+4$. Thus in one order or another, we see that b and c are $a-4$ and $d+4$. Hence we have $a > d+4$ and

$$P(x) = (x-a)(x-d-4), \qquad Q(x) = (x-a)(x-a+4)(x-d-4)(x-d).$$

In this case we have

$$S = T = \{a, a-4, a-8, d+4, d, d-4\},$$

so these always satisfy the polynomial condition.
Now the added condition reads $a - (d+4) = a + (a-4) + (d+4) + d$, which simplifies to $a + 3d + 12 = 0$. Note that the condition $a > d+4$ means that $d < -4$, but otherwise d is arbitrary. Writing $d = -4 - t$ and hence $a = 3t$ for some $t > 0$, we get

$$P(x) = (x-3t)(x+t), \qquad Q(x) = (x-3t)(x-3t+4)(x+t)(x+t+4).$$

The sum of the squares of roots of $Q(x)$ is therefore

$$(3t)^2 + (3t-4)^2 + (-t)^2 + (-t-4)^2 = 20t^2 - 16t + 32 = 20\left(t - \frac{2}{5}\right)^2 + \frac{144}{5}.$$

Hence the minimum is $\frac{144}{5}$, attained for $t = \frac{2}{5}$. ∎

5.2 Constructing an infinite sequence of roots

The most fundamental property of the roots of a nonzero polynomial $P(x)$ is that there are only finitely many of them. There are many ways we can exploit this property, but in this section we focus on one of them. We will try to use the hypotheses of the problem to construct a sequence (x_n) of distinct roots of $P(x)$. If we can, then $P(x)$ has infinitely many roots, and hence it is the zero polynomial. We saw this technique several times in earlier chapters, and the reader may notice that several of the examples below could be done more easily using the results of Chapter 4.

Example 5.3. Let $P(x)$ be a polynomial $P(x)$ with only real roots and no multiple roots. Suppose that whenever a and b are roots of $P(x)$, $a+b+ab$ is also a root of $P(x)$. Find all such polynomials.

Thailand Mathematical Olympiad 2013

Solution. From the special case where $a = b$, we see that if a is a root of $P(x)$, then $a^2 + 2a$ is also a root of the polynomial $P(x)$. Thus given a root a, we can build a sequence of roots

$$a, a^2 + 2a, (a^2 + 2a)^2 + (a^2 + 2a), \ldots.$$

We need to decide whether this sequence has infinitely many distinct values. For that, consider the following cases:

(i) If $a > 0$, then $a^2 + 2a > a$. Hence iterating this fact, we see that $0 < a < a^2 + 2a < (a^2 + 2a)^2 + 2(a^2 + 2a) < \ldots$. Thus the sequence is increasing and has infinitely many values.

(ii) If $-1 < a < 0$, then $0 > a > a^2 + 2a > -1$. Hence iterating this fact we see that $0 > a > a^2 + 2a > \ldots > -1$. Thus the sequence is decreasing and has infinitely many values.

(iii) If $-2 < a < -1$, then $0 > a^2 + 2a > -1$. Hence if we use the root $b = a^2 + 2a$ instead of a, then we are in case (ii).

(iv) If $a < -2$, then $a^2 + 2a > 0$. Hence if we use the root $b = a^2 + 2a$ instead of a, then we are in case (i).

The remaining cases are $a = 0, -1, -2$. If $a = 0$ and $b \in \{0, -1, -2\}$, then we see that $a + b + ab = b$, so the hypotheses of the problem give no new root. If $a = -1$ and $b \in \{0, -1, -2\}$, then we see that $a + b + ab = -1$, so again the hypotheses of the problem give no new root. If $a = -2$ and $b \in \{0, -1, -2\}$, then we see that $a + b + ab = -2 - b$. Checking the three cases, we see that we get a new root only when $a = b = -2$, when we get that 0 is also a root. Thus the possible roots are the subsets of $\{0, -1, -2\}$, which if they contain -2 also contain 0. Letting C be the leading coefficient of $P(x)$, we get the polynomials

$$C, \quad Cx, \quad C(x+1), \quad Cx(x+1), \quad Cx(x+2), \quad Cx(x+1)(x+2). \qquad \blacksquare$$

Example 5.4. Find all polynomials $P(x)$ and $Q(x)$ with real coefficients such that $P(2) = 2$, $Q(x)$ has only positive real roots, and

$$(x-2)P(x^2-1)Q(x+1) = P(x)Q(x^2) + Q(x+1).$$

Bulgarian Festival of Young Mathematicians 2015

Solution. Setting $x = 2$, we get $2Q(4) + Q(3) = 0$. Thus $Q(x)$ has a root in the interval $[3, 4]$. Let a be one such root. For any root b of $Q(x)$ with $b \geq 3$, setting $x = b - 1$, we find that

$$P(b-1)Q((b-1)^2) = 0.$$

Thus either $b-1$ is a root of $P(x)$ or $(b-1)^2$ is a root of $Q(x)$. If $P(b-1) = 0$, set $x = -\sqrt{b}$ and we see that $Q(1 - \sqrt{b}) = 0$. This is a contradiction since it gives a negative real root of $Q(x)$. Thus we must always have the second case, that $Q((b-1)^2) = 0$. But $(b-1)^2 > b$, since $b \geq 3$. Hence we can find an increasing sequence (x_n) of roots of $Q(x)$ by

$$x_1 = a, \quad x_{n+1} = (x_n - 1)^2.$$

This gives infinitely many distinct roots of $Q(x)$. Hence $Q(x) = 0$ and $P(x)$ can be any polynomial such that $P(2) = 2$. $\blacksquare$

Example 5.5. Find all polynomials $P(x)$ with only real roots such that

$$P(x^3+1) = P(x+1)P(x^2-x+1).$$

Solution. It is easy to see that $P(x) = 0$ is a solution. Assume that $P(x)$ is nonzero and suppose $P(\alpha) = 0$ for some complex number $\alpha \neq 1$. Setting $x = \alpha - 1$, we find that $P((\alpha-1)^3+1) = 0$.
Thus if we define a sequence (x_n) by $x_1 = \alpha$ and $x_n = (x_{n-1}-1)^3+1$ for $n \geq 1$, an easy induction shows that $P(x_n) = 0$ for all n. Note that the function $f(x) = (x-1)^3+1$ is an increasing function of x. Thus if $x_2 = (\alpha-1)^3+1 > x_1$, we have $x_3 = f(x_2) > f(x_1) = x_2$, and hence iterating this, we see that the sequence (x_n) is increasing. Conversely, if $x_2 < x_1$, then we have $x_3 = f(x_2) < f(x_1) = x_2$ and iterating this, we see that the sequence is decreasing. Hence we get infinitely many roots of $P(x)$, and hence a contradiction, unless $x_2 = x_1$. This means

$$0 = (\alpha-1)^3+1-\alpha = \alpha(\alpha-1)(\alpha-2).$$

So $\alpha \in \{0,1,2\}$ and we can write the possible polynomials as

$$P(x) = ax^n(x-1)^m(x-2)^t.$$

By checking this, we get $a = 1$, $m = t = 0$. Thus we have shown that either $P(x) = 0$ or $P(x) = x^n$ for some $n \geq 0$. ■

Example 5.6. Find all polynomials such that

$$P(x^2+x) = P(x)P(x+1).$$

Solution. Clearly $P(x) = 0$ is a solution. Assume $P(x)$ is nonzero. Then we can choose a root α of $P(x)$ with maximum modulus. Setting $x = \alpha$ and $x = \alpha - 1$, we get $P(\alpha^2+\alpha) = P(\alpha^2-\alpha) = 0$.
The triangle inequality gives $|\alpha^2+\alpha| + |\alpha^2-\alpha| \geq 2|\alpha|$, and hence

$$\max(|\alpha^2+\alpha|, |\alpha^2-\alpha|) \geq |\alpha|.$$

Since maximality of $|\alpha|$ gives the reverse inequality, we must have equality throughout. Equality in the triangle inequality occurs when

$$r = \frac{\alpha+\alpha^2}{\alpha-\alpha^2} = \frac{1+\alpha}{1-\alpha}$$

is a positive real number. Equality in taking the maximum forces $r = 1$. Thus $\alpha = \frac{1-r}{1+r} = 0$. Thus the only possible root of $P(x)$ is 0 and so $P(x) = ax^n$ for some $n \geq 0$. Since it is easy to check that $P(x)$ must be monic, we find that either $P(x) = 0$ or $P(x) = x^n$ for some $n \geq 0$. ■

Example 5.7. Find all polynomials $P(x)$ such that

$$P(x)P(x+1) = P(x^2+x+1).$$

Solution. Clearly $P(x) = 0$ is a solution. Assume $P(x)$ is nonzero. Then we can choose a root α of $P(x)$ with maximum modulus. Setting $x = \alpha$ and $x = \alpha - 1$, we get

$$P(\alpha^2+\alpha+1) = P(\alpha^2-\alpha+1) = 0.$$

By the triangle inequality, we find that

$$|\alpha^2+\alpha+1| + |\alpha^2-\alpha+1| \geq 2|\alpha|,$$

and hence

$$\max(|\alpha^2+\alpha+1|, |\alpha^2-\alpha+1|) \geq |\alpha|.$$

Since maximality of $|\alpha|$ gives the reverse inequality, we must have equality throughout. As in the previous solution, we must have

$$\frac{-\alpha^2+\alpha-1}{\alpha^2+\alpha+1} = 1,$$

since equality in the triangle inequality forces the ratio to be a positive real number, and then equality in the maximum forces it to be 1. This simplifies to $\alpha^2+1 = 0$, and hence $\alpha = \pm i$. Thus every root α of $P(x)$ has $|\alpha| \leq 1$, and if we have equality, then $\alpha = \pm i$.

Now we notice that looking at the leading coefficient of the equation, we see that $P(x)$ must be monic. Since 1 is not a root of $P(x)$, plugging in $x = 0$, we find that $P(0) = 1$. Thus from Vieta's formula, we see that the product of the roots of $P(x)$ is ± 1. Hence if $P(x)$ has any root with modulus less than 1, it must also have a root with modulus greater than 1. It follows that all roots of $P(x)$ have modulus 1, and hence are at $\pm i$. Thus since $P(x)$ is monic, $P(x) = (x-i)^m(x+i)^n$. Plugging this in we find that $m = n$, hence the solutions are $P(x) = 0$ and $P(x) = (x^2+1)^d$ for some $d \geq 0$. ∎

Example 5.8. Find all polynomials $P(x)$ with real coefficients such that

$$P(2019) = 2018, \quad (1 + P(x))^2 = P(1 + x^2).$$

Solution. Define $Q(x) = 1 + P(x)$. Thus

$$Q(2019) = 2019, \quad Q(1 + x^2) = 1 + Q(x)^2.$$

Let us define a sequence x_n with $x_0 = 2019$ and $x_{n+1} = 1 + x_n^2$ for all $n \geq 0$. We can inductively prove that $Q(x_n) = x_n$ for each n, with the induction step being the computation

$$Q(x_{n+1}) = Q(1 + x_n^2) = 1 + Q(x_n)^2 = 1 + x_n^2 = x_{n+1}.$$

Since $x_{n+1} - x_n = x_n^2 - x_n + 1 > 0$, we find that the sequence is strictly increasing. Therefore the equation $Q(x) = x$ has infinitely many solutions, which means that $Q(x) = x$. Thus $P(x) = x - 1$. ∎

Example 5.9. Find all polynomials with real coefficients $P(x)$ with $P(0) = 6$ and

$$P(x) = \sqrt{P(x^2+1) - 7} + 6$$

for all $x \geq 0$.

Solution. Rewrite the original equation as

$$P(x^2+1) = 7 + (P(x) - 6))^2.$$

Now, define the sequence $x_0 = 0$, $x_{n+1} = x_n^2 + 1$ for all $n \geq 0$. We can prove by induction that $P(x_n) = 6 + x_n$, with the induction step being the computation

$$P(x_{n+1}) = P(x_n^2 + 1) = 7 + (P(x_n) - 6))^2 = 7 + x_n^2 = 6 + x_{n+1}.$$

Since $x_{n+1} - x_n = x_n^2 - x_n + 1 > 0$, the sequence is strictly increasing, and we deduce that $P(x) = 6 + x$. ∎

Variant:
Find all polynomials with real coefficients $P(x)$ such that $P(2014) = 2024$ and

$$P(x) - 10 = \sqrt{P(x^2+3) - 13}$$

for all $x \geq 0$.

Example 5.10. Find all polynomials $P(x)$ with real coefficients of odd degree such that

$$P(0) = 0, \quad P(x^2 - x + 1) = P(x)^2 - P(x) + 1.$$

Solution. Using the substitution $x \mapsto 1 - x$ gives

$$P(x^2 - x + 1) = P(1-x)^2 - P(1-x) + 1.$$

Thus

$$P(1-x)^2 - P(1-x) = P(x)^2 - P(x).$$

This implies that either $P(x) = P(1-x)$ or $P(x) + P(1-x) = 1$. Since plugging in $x = 0$ into the original equation gives $P(1) = 1$, we find that $P(x) + P(1-x) = 1$. Putting $x = \frac{1}{2}$, we get

$$P\left(\frac{1}{2}\right) = \frac{1}{2}.$$

Now define a sequence (x_n) by $x_1 = \frac{1}{2}$, and $x_{n+1} = x_n^2 - x_n + 1$ for all $n \geq 1$. An easy induction, using the inductive step

$$0 < x_n < x_n + (x_n - 1)^2 = x_{n+1} = 1 - x_n(1 - x_n) < 1,$$

shows that $x_i \in (0,1)$ for each i and that the sequence is increasing. A second easy induction shows that $P(x_n) = x_n$, with the inductive step being

$$P(x_{n+1}) = P(x_n^2 - x_n + 1) = P(x_n)^2 - P(x_n) + 1 = x_n^2 - x_n + 1 = x_{n+1}.$$

Hence the equation $P(x) = x$ has infinitely many solutions in $(0,1)$ and therefore $P(x) = x$. ∎

Example 5.11. Find all polynomials $P(x)$ such that

$$P(x^2) = P(x)P(x+1).$$

Solution. Clearly the zero polynomial is a solution, so assume $P(x)$ is not the zero polynomial. If α is a root of $P(x)$, plugging in $x = \alpha$ we find that $P(\alpha^2) = 0$, and iterating this we get $P(\alpha^{2^n}) = 0$ for all $n \geq 0$. Since $P(x)$ has only finitely many roots, these must repeat, that is, there are two indices $i < j$ such that $\alpha^{2^i} = \alpha^{2^j}$. Hence either $\alpha = 0$ or $\alpha^{2^j - 2^i} = 1$. In the second, case taking the modulus, we find that $|\alpha| = 1$.
If α is a root, we can also take $x = \alpha - 1$ and we conclude that $P((\alpha-1)^2) = 0$. Thus by our previous result, either $\alpha = 1$ or $|\alpha - 1| = 1$. Putting these together we find that $\alpha = 0$ or 1, or α satisfies $|\alpha| = |\alpha - 1| = 1$. In the last case, we write $\alpha = x + iy$ and we find that $x^2 + y^2 = (x-1)^2 + y^2 = 1$. So $x = \frac{1}{2}$, $y = \frac{\pm\sqrt{3}}{2}$. Thus there are only four possible roots: $\alpha = 0, 1$, or $\frac{1 \pm i\sqrt{3}}{2}$. The last two cases cannot actually occur, since if $\alpha = \frac{1 \pm i\sqrt{3}}{2}$ is a root, then $\alpha^2 = \frac{-1 \pm i\sqrt{3}}{2}$ is also a root. However, this is not on our list of four possible roots. Thus we must have $\alpha = 0$ or 1.
Therefore we can write $P(x) = ax^m(x-1)^n$. By checking these, we find that $a = 1$ and $m = n$. Thus the polynomials are $P(x) = 0$ or $P(x) = x^m(x-1)^m$ for $m \geq 0$. ∎

Example 5.12. Find all monic polynomials $P(x)$ such that $P(x)^2 - 1$ is divisible by $P(x+1)$.

Solution. Let $d = \deg P(x)$ and let $r_1, \ldots, r_d$ be the roots of $P(x)$, which we assume are sorted so that

$$\mathrm{Re}(r_1) \leq \mathrm{Re}(r_2) \leq \ldots \leq \mathrm{Re}(r_d).$$

Since $P(x)^2 - 1$ is divisible by $P(x+1)$, we can write

$$P(x)^2 - 1 = P(x+1)Q(x)$$

for some polynomial $Q(x)$. In particular, plugging in $x = r_1 - 1$, we find that $P(r_1 - 1)^2 - 1 = 0$, hence $P(r_1 - 1) = \pm 1$. Since

$$P(x) = (x - r_1) \cdot \ldots \cdot (x - r_d),$$

we have

$$\pm 1 = P(r_1 - 1) = -(r_1 - r_2 - 1)(r_1 - r_3 - 1) \cdot \ldots \cdot (r_1 - r_d - 1).$$

However $\mathrm{Re}(r_1 - r_k - 1) \leq -1$, which implies that $|r_1 - r_k - 1| \geq 1$. Thus when we take moduli, we get

$$1 = |P(r_1 - 1)| \geq 1 \cdot 1 \cdot \ldots \cdot 1 = 1.$$

Thus we must have equality throughout. But this says $\mathrm{Re}(r_1 - r_k - 1) = -1$ and $|r_1 - r_k - 1| = 1$, hence $r_1 - r_k - 1 = -1$ and thus $r_k = r_1$. Hence all the roots of $P(x)$ agree and we can write $P(x) = (x - r)^d$. In this case, we need

$$P(x+1) = (x - r + 1)^d$$

to divide

$$\begin{aligned} P(x)^2 - 1 &= (x-r)^{2d} - 1 \\ &= (x - r + 1)((x-r)^{2d-1} - (x-r)^{2d-2} + \ldots + (x-r) - 1). \end{aligned}$$

Since we see that $r - 1$ is not a root of the second factor (it evaluates to $-2d$ at $x = r - 1$), we see that only $d = 1$ gives a solution. Thus $P(x) = x - r$ for any r are the solutions. ∎

5.3 Comparing the sets of roots of polynomials on both sides

If $P(x) = Q(x)$, then the sets of roots on both sides are equal and have the same multiplicity. What you need is succinctly enlisted here.

Strategy

(i) If $Q(r) = 0$, then $P(r) = 0$.

(ii) If the multiplicity of r in $P(x)$ is n, then the multiplicity of r in $Q(x)$ must be n, too.

(iii) Order the roots of $P(x)$ and $Q(x)$ to arrive at some result.

Example 5.13. Vlatka wrote down a finite set of distinct real numbers (possibly just one number). He then squared them all, and then subtracted one from each number. He got the same list of numbers he started with, in some order. What could the set of numbers have been?

Nikolai Nikolov

Solution. Let Vlatka's original set be $A = \{a_1, \ldots, a_d\}$. Then after his rewritings he had $\{a_1^2 - 1, a_2^2 - 1, \ldots, a_d^2 - 1\}$ which must again be A.
Thus each $a \in A$ must be of the form $a = b^2 - 1$ for some $b \in A$. In particular, this means that $a \geq -1$. Let a be the largest element of A. Since $a^2 - 1$ must also be in A, we have $a^2 - 1 \leq a$. Denote by $x_1 = \frac{1+\sqrt{5}}{2}$ and $x_2 = \frac{1-\sqrt{5}}{2}$ the roots of the polynomial $x^2 - x - 1$. Then this says that $a \leq x_1$.
Suppose there is some $a \in A$ with $0 < a < x_1$. Then $a = b^2 - 1$ for some $b \in A$, and we find $b = \pm\sqrt{1+a}$. However, since $b \geq -1 > -\sqrt{1+a}$, we must therefore have $b = \sqrt{1+a}$. For $0 < a < x_1$, we have $0 < a < \sqrt{1+a} < x_1$. Therefore the sequence (c_n) defined by $c_1 = a$ and $c_{i+1} = \sqrt{1+c_i}$ for $i \geq 1$ is increasing, contained in $(0, x_1)$, and all its elements are in A. This is a contradiction since A is finite. Thus A has no such element.

Next suppose there is an $a \in A$ with $a \leq 0$. Again we must have $a = b^2 - 1$ for some $b \in A$, hence $b = \pm\sqrt{1+a}$. However, we cannot have the plus sign since we saw in the previous paragraph that x_1 is the only possible positive element of A (and $\sqrt{1+a} < 1 < x_1$). Thus $b = -\sqrt{1+a}$. Define a sequence (c_n) by $c_1 = a$ and $c_{i+1} = -\sqrt{1+c_i}$ for $i \geq 1$. An easy induction shows that the elements c_i are all in $[-1, 0]$ and in A. The function $f(x) = -\sqrt{1+x}$ is a decreasing function of x for $x \in [-1, 0]$. Hence $f(f(x)) = -\sqrt{1-\sqrt{1+x}}$ is an increasing function. If we have $c_3 > c_1$, then it follows that

$$c_5 = f(f(c_3)) > f(f(c_1)) = c_3$$

and hence iterating this, we find $c_1 < c_3 < c_5 < \cdots$. However this would give infinitely many elements of A. Similarly if $c_3 < c_1$, then we have

$$c_5 = f(f(c_3)) < f(f(c_1)) = c_3$$

and iterating gives $c_1 > c_3 > c_5 > \cdots$ and infinitely many elements of A. Thus we must have $c_3 = c_1 = a$. But working back from $c_3 = a$, we find $c_2 = a^2 - 1$ and $c_1 = (a^2-1)^2 - 1 = a^4 - 2a^2 = a$. Thus any a must be a root of

$$a^4 - 2a^2 - a = a(a+1)(a^2 - a - 1).$$

Thus the possible elements of A are $0, 1, x_1$, and x_2. We see that $x_1 = x_1^2 - 1$ and $x_2 = x_2^1 - 1$ map to themselves when Vlatka rewrites and $0 = (-1)^2 - 1$ and $-1 = 0^2 - 1$ are interchanged. Thus if Vlatka has either 0 or -1 he must have both. Hence

$$A = \{x_1\}, \{x_2\}, \{x_1, x_2\}, \{0, -1\}, \{0, -1, x_1\}, \{0, -1, x_2\}, \{0, -1, x_1, x_2\}. \quad \blacksquare$$

Example 5.14. Find all polynomials $P(x)$ having only real roots and such that

$$P(x)P(-x) = P(x^2 - 1).$$

Solution. Clearly the zero polynomial is a solution. Assume $P(x)$ is a nonzero solution, say with degree d and leading coefficient a_d. Then looking at the

leading coefficients of both sides of the equation, we get $(-1)^d a_d^2 = a_d$ and hence $a_d = (-1)^d$. Thus we can write

$$P(x) = (r_1 - x)(r_2 - x) \cdot \ldots \cdot (r_d - x),$$

where r_i are the roots of $P(x)$. From this we get

$$P(x)P(-x) = (r_1^2 - x^2)(r_2^2 - x^2) \cdot \ldots \cdot (r_d^2 - x^2)$$

and

$$P(x^2 - 1) = (r_1 + 1 - x^2)(r_2 + 1 - x^2) \cdot \ldots \cdot (r_d + 1 - x^2).$$

Comparing these two formulas, we see that the lists of numbers $r_1, r_2, \ldots, r_d$ and $r_1^2 - 1, r_2^2 - 1, \ldots, r_d^2 - 1$ must be the same numbers, but possible in a different order.

Thus we are in the same situation as the preceding problem, except that our set A has been replaced with a list that may have repeated elements. The solution to that example still applies and we conclude that the only possible numbers on our list are $0, -1, x_1$, and x_2 and that 0 and -1 must occur the same number of times. Conversely it is easy to see that these conditions suffice. Hence either $P(x) = 0$ or $P(x) = (x(x+1))^a (x_1 - x)^b (x_2 - x)^c$ for some nonnegative integers a, b, c. ■

5.4 The form $P(Q(x))$

Many problems about finding polynomials involve compositions of polynomials. Because of the increasingly importance of this topic, we allot one section to compositions.

5.4.1 Some basic properties

Example 5.15. Do there exist polynomials $P(x)$, $Q(x)$, $R(x)$ of degree at least 2 such that

$$P(Q(x)) = Q(P(x)),\ Q(R(x)) = R(Q(x)) \text{ but } P(R(x)) \neq R(P(x))?$$

Volodymyr Barayman

Solution. The answer is yes. Setting

$$P(x) = x^2, \quad Q(x) = x^3, \quad R(x) = -x^2,$$

then

$$P(Q(x)) = Q(P(x)) = x^6, \quad Q(R(x)) = R(Q(x)) = -x^6.$$

But $P(R(x)) = x^4 \neq R(P(x)) = -x^4$. ■

Example 5.16. Find all nonconstant polynomials $P(x)$ and $Q(x)$ such that for all positive integer n we have

$$\underbrace{P(P(\ldots P(1)\ldots)}_{n} = Q(n).$$

Solution. Let $P^{(k)}(x)$ denote the nested composition of k copies of P. Then the hypothesis says that $P^{(n)}(1) = Q(n)$. Hence we compute

$$Q(n+1) = P^{(n+1)}(1) = P(P^{(n)}(1)) = P(Q(n)).$$

Therefore $P(Q(x)) = Q(x+1)$ holds for infinitely many x, hence it holds for all real numbers x. If $P(x)$ has degree $d \geq 1$ and leading coefficient $a_d \neq 0$ and $Q(x)$ has degree $m \geq 1$ and leading coefficient $b_m \neq 0$, then we see that $P(Q(x))$ has degree dm and leading coefficient $a_d b_m^d$ and $Q(x+1)$ has degree m and leading coefficient b_m. Since these agree, we conclude that $d = 1$ and $a_d = 1$, that is, $P(x)$ is linear and monic. If we write $P(x) = x + c$, then we compute $P^{(n)}(x) = x + nc$ and hence $Q(n) = P^{(n)}(1) = nc + 1$. Thus the solutions are $P(x) = x + c$ and $Q(x) = nc + 1$ for some constant c. ■

Example 5.17. Initially the polynomial $x^2 + 1$ is written on a blackboard. Each day Vlatka removes the polynomial $P(x)$ and write either $P(x^2 + 1)$ or $P(x)^2 + 1$. Prove that, a year after, the constant term of the resulting polynomial will be greater than $2^{2^{333}}$.

Arsenii Nikolaev

Solution. Denote by $P_k(x)$ the polynomial that is on the board at the start of day k. At the end of the year the polynomial will be $P_{366}(x)$ (or $P_{367}(x)$ for a leap year). Let $Q(x) = x^2 + 1$ and let $Q^{(k)}(x)$ denote the k-fold composition of the polynomial $Q(x)$. Vlatka starts with $P_1(x) = Q(x)$ written on the blackboard, and on day one she replaces it with either $P_2(x) = Q(x^2 + 1)$ or $P_2(x) = Q(x)^2 + 1$. However, both of these are just $Q(Q(x)) = Q^{(2)}(x)$. Thus $P_2(x) = Q^{(2)}(x)$ regardless of Vlatka's choice.
An easy induction shows that regardless of which rewriting she does, Vlatka starts day k with $P_k(x) = Q^{(k)}(x)$ written on the board. Indeed, if she starts day k with $P_k(x) = Q^{(k)}(x)$, then she either produces

$$Q^{(k)}(x^2 + 1) = Q^{(k)}(Q(x)) = Q^{(k+1)}(x)$$

or

$$(Q^{(k)}(x))^2 + 1 = Q(Q^{(k)}(x)) = Q^{(k+1)}(x).$$

Thus she gets $P_{k+1}(x) = Q^{(k+1)}(x)$ either way.
Hence at the end of one year Vlatka will have $Q^{(366)}(x)$ (or $Q^{(367)}(x)$) written on the board. Let $b_k = Q^{(k)}(1)$. Then $b_1 = 2 = 2^{2^0}$ and an easy induction using the calculation

$$b_{k+1} = b_k^2 + 1 \geq (2^{2^{k-1}})^2 + 1 = 2^{2^k} + 1 > 2^{2^k}$$

as the inductive step, shows that $b_k \geq 2^{2^{(k-1)}}$ for $k \geq 1$.
Hence $b_{366} \geq 2^{2^{365}} > 2^{2^{333}}$. ■

Example 5.18. Let $P(x)$ be a polynomial with real coefficients such that the polynomials $P(P(x))$, $P(P(P(x)))$ are strictly monotone on the real axis. Prove that $P(x)$ is strictly monotone on the real axis.

Kirill Suhov - Russian Mathematical Olympiad 2010

First Solution. Since a polynomial function $Q(x)$ is always continuous, the intermediate value property shows that if $Q(x)$ is not strictly monotone, then there are $a < b$ with $Q(a) = Q(b)$. Assume $P(x)$ is not strictly monotone, then there are $a < b$ such that $P(a) = P(b)$. However, we then compute

that $P(P(a)) = P(P(b))$, but this contradicts the hypothesis that $P(P(x))$ is strictly monotone. Hence $P(x)$ is strictly monotone. ■

Second Solution. A strictly monotone polynomial must have odd degree, and hence must be surjective. Thus $P(P(x))$ has odd degree and is surjective. If we write $P(x) = a_d x^d + \ldots + a_0$ with $a_d \neq 0$, then $P(P(x))$ has degree d^2, hence we see that d is odd. Further, the leading coefficient of $P(P(x))$ is a_d^{d+1}, which is positive since d is odd. Hence $P(P(x))$ must be strictly increasing. Now, choose $a > b$. Since $P(P(x))$ is surjective, there are real numbers x_a and x_b such that $P(P(x_a)) = a$ and $P(P(x_b)) = b$. Further, since $P(P(x))$ is strictly increasing, we get $x_a > x_b$. If $P(P(P(x)))$ is strictly increasing, we find that

$$P(a) = P(P(P(x_a))) > P(P(P(x_b))) = P(b).$$

Thus $P(a) > P(b)$. This implies that $P(x)$ is strictly increasing. On the other hand, if $P(P(P(x)))$ is strictly decreasing, then

$$P(a) = P(P(P(x_a))) < P(P(P(x_b))) = P(b).$$

Thus $P(a) < P(b)$. This implies that $P(x)$ is strictly decreasing. ■

5.4.2 Roots of $P(Q(x))$ and roots of $P(x)$

Since understanding the roots of a polynomial is always helpful, it will help if we understand the roots of a composition $P(Q(x))$. Suppose we factor $P(x)$ as $P(x) = C(x - r_1) \cdot \ldots \cdot (x - r_d)$, where $r_1, \ldots, r_d$ are the (complex) roots of $P(x)$, taken with multiplicity. Then

$$P(Q(x)) = (Q(x) - r_1) \cdot \ldots \cdot (Q(x) - r_d).$$

Thus the roots of $P(Q(x))$ are the union of the roots of the equations

$$Q(x) = r_1, \ldots, Q(x) = r_d.$$

Notice that the roots of $Q(x) = r$ and the roots of $Q(x) = r'$ are either exactly the same (if $r = r'$) or are completely disjoint (if $r \neq r'$).

Theorem

Let $r_1, \ldots, r_d$ be the roots of $P(x)$. The set of roots of polynomial $P(Q(x))$ can be partitioned into the union of the set of roots of polynomials $Q(x) - r_1, Q(x) - r_2, \ldots, Q(x) - r_d$.

Example 5.19. Are there two polynomials $P(x)$ and $Q(x)$ of degree 2013 with real coefficients such that the roots of $P(Q(x))$ are $2, 2^2, \ldots, 2^{2013^2}$?

Solution. Suppose there is such a pair of polynomials and let $r_1, \ldots, r_{2013}$ be the roots of $P(x)$. Then for each r_i some 2013 of the numbers 2^k, for $1 \leq k \leq 2013^2$, must be roots of $Q(x) - r_i$. Conversely, each $Q(2^k)$ in this range must be a root of $P(x)$. If we write $Q(x) = a_{2013}x^{2013} + a_{2012}x^{2012} + \cdots$, then we see by Vieta's formula that the roots of $Q(x) - r_i$ sum to $-\frac{a_{2012}}{a_{2013}}$, regardless of the value of r_i. Thus we have partitioned the numbers $2, 2^2, \ldots, 2^{2013^2}$ up into 2013 disjoint sets each of size 2013 and with the same sum. But one of these sets must contain 2^{2013^2}, which alone is larger than the sum of all the others, so this is a contradiction. Thus there are no such polynomials. ■

Example 5.20. Are there two polynomials $P(x)$ and $Q(x)$ of degree n with real coefficients such that roots of $P(Q(x))$ form an nonconstant arithmetic progression of length n^2?

Solution. If $n = 1$, then any arithmetic progression of length 1 is constant, so there are no examples. If $n = 2$, then it is easy to build examples, such as $P(x) = (x-1)(x-9)$ and $Q(x) = x^2$ for which the roots of $P(Q(x))$ are $-3, -1, 1, 3$.

Now assume $n > 2$. With a suitable shift and rescaling, we can assume that the roots of $P(Q(x))$ are $0, 1, \ldots, n^2 - 1$. Let $c_1, c_2, \ldots, c_n$ be roots of $P(x)$. Then the roots of $P(Q(x))$ are the union of the sets of roots of the equations $Q(x) = c_i$. Each such equation has at most n roots and $P(Q(x))$ has n^2 real roots. Hence each such equation must have n real roots, and hence each c_i must be real.

Thus $P(x)$ also has n real roots, and we may further assume $c_1 < c_2 < \ldots < c_n$. Now draw the graph of $y = Q(x)$. The roots of $Q(x) = c_i$ are the x-coordinates of the points where the horizontal line $y = c_i$ crosses this graph. Hence the roots of $P(Q(x))$ are the x-coordinates of the points where n different horizontal lines cross the graph $y = Q(x)$. Since the graph of $y = Q(x)$ has at most $n - 1$ local extrema, it must cross through all n horizontal lines, turn, cross back through all n, turn, and repeat this until it has crossed through all n lines a total of n times.

Thus the first horizontal line it crosses, which it will cross at $x = 0$, must be crossed at the x-coordinates

$$\{0, 2n-1, 2n, 4n-1, \ldots\},$$

and the second, which it will cross at $x = 1$, must be crossed at

$$\{1, 2n-2, 2n+1, 4n-2, \ldots\},$$

and similarly for the other horizontal lines.

Each of these sets will be the roots of one of the equations $Q(x) = c_i$. If we write

$$Q(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots,$$

then Vieta's formulas show that the sum of the roots of $Q(x) = c_i$ is $-\frac{a_{n-1}}{a_n}$ and the sum of the squares is $\left(\frac{a_{n-1}}{a_n}\right)^2 - 2\frac{a_{n-2}}{a_n}$, independent of c_i. Note that this is where we are using $n > 2$.

For the sets above, the first two terms sum to $2n - 1$, the next two sum to $6n - 1$, etc. Hence the sums will be equal if and only if n is even. However it is easy to check that

$$0^2 + (2n-1)^2 > 1^2 + (2n-2)^2, \quad (2n)^2 + (4n-1)^2 > (2n+1)^2 + (4n-1)^2,$$

and similarly each pair of squares in the first list has larger sum that the corresponding pair in the second list. Hence for n even, we have

$$0^2 + (2n-1)^2 + (2n)^2 + (4n-1)^2 + \ldots > 1^2 + (2n-2)^2 + (2n+1)^2 + (4n-2)^2 + \ldots.$$

This is a contradiction. Thus there are no such polynomials for $n > 2$. ■

Example 5.21. Find all polynomials $P(x)$ and $Q(x)$ such that

$$P(Q(x)) = P(x)^r$$

for some positive integer r.

Rafael Rafaelov

Solution. Comparing degrees we see that we must have $\deg Q(x) = r$. If $r = 1$, then $Q(x)$ is linear. We have already seen that in this case either $Q(x) = x$ or $Q(x) = c - x$ for some c, and in this second case $P(x) = P(c-x)$ so $P(x)$ has an axis of symmetry.
Now assume $r > 1$. Let the distinct roots of $P(x)$ be $z_1, \ldots, z_k$, which are therefore the roots of $P(x)^r$. The roots of $P(Q(x))$ are the union of the sets of roots of $Q(x) = z_i$. These sets are disjoint and each has at least one element, hence we get at least k roots. But since the two sides are equal, we get exactly k roots and in fact each equation $Q(x) = z_i$ has only one root. Thus there must be a permutation σ such that $Q(x) = z_i$ has only $z_{\sigma(i)}$ as a root. Hence $Q(x) = a(x - z_{\sigma(i)})^r + z_i$, where $a \neq 0$ is the leading coefficient of $Q(x)$. Since $\deg Q(x) = r > 1$, we see that the coefficient of x^{r-1} in $Q(x)$ is $-raz_{\sigma(i)}$. Hence all the $z_{\sigma(i)}$ must be equal. Since by construction the z_i are distinct, we see that we must have $k = 1$. Hence $P(x) = b(x - z)^l$ for some $b \neq 0, z$, and $l \geq 0$. Further, $Q(x) = z$ must have an r-fold root at $x = z$, so we must have $Q(x) = a(x-z)^r + z$ for some $a \neq 0$. Plugging these formulas in, we find that $b^r = ba^l$, hence $a^l = b^{r-1}$. ■

Example 5.22. Let p be a prime. Find all polynomials f and g with integer coefficients such that

$$f(g(x)) = 1 + x + \ldots + x^{p-1}.$$

Cezar Lupu and Vlad Matei - Romanian Team Selection Test 2014

Solution. Comparing leading coefficients, we see that the leading coefficients of $f(x)$ and $g(x)$ must both be ± 1. If $f(x)$ is linear, then we get solutions

$$f(x) = \pm x + c, \quad g(x) = \pm(x^{p-1} + x^{p-2} + \cdots + x + 1 - c).$$

If $g(x)$ is linear, then we get solutions

$$g(x) = \pm x + c, \quad f(x) = (\pm(x - c))^{p-1} + (\pm(x - c))^{p-2} + \cdots + 1.$$

Now suppose both $f(x)$ and $g(x)$ are nonlinear. Then we can write

$$f(x) = a_m x^m + P(x),$$

where $\deg P(x) \leq m - 1$ and $g = \sum_{i=0}^{n} b_i x^i$, where $m, n \geq 2$, and a_m and b_n are nonzero. Thus

$$f(g(x)) = a_m \left(b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0\right)^m + P(g(x)).$$

Comparing degrees, we see that $mn = p - 1$. The term $P(g(x))$ has degree at most $(m-1)n = mn - n = p - 1 - n \leq p - 3$, hence from the coefficient of x^{p-2}, we get $ma_m b_n^{m-1} b_{n-1} = 1$. However, this says that m divides 1, which cannot occur since was assumed $m \geq 2$. Thus the only solutions are the ones we found above with either $f(x)$ or $g(x)$ linear. ■

Example 5.23. Let $f(x)$ and $h(x)$ be quadratic polynomials with real coefficients, and let $g(x)$ be a nonconstant polynomial such that

$$f(g(h(x))) = h(g(f(x))).$$

Prove that if there exists a real number c such that $f(c) = h(c)$, then for all real numbers x we have $f(x) = h(x)$.

Solution. Write $f(x) = a(x-b)^2 + e$, $h(x) = A(x-B)^2 + E$, and assume that $g(x)$ has degree $d \geq 1$ and leading coefficient $K \neq 0$. Then equating leading coefficients, we find $aK^2A^{2d} = AK^2a^{2d}$, hence $a^{2d-1} = A^{2d-1}$. Since a and A are real, this implies $a = A$.
Since $f(x) = f(2b - x)$ and $h(x) = h(2B - x)$, we compute that

$$f(g(h(2B-x))) = f(g(h(x))) = h(g(f(x))) = h(g(f(2b-x))) = f(g(h(2b-x))).$$

Therefore the polynomial $R(x) = f(g(h(x)))$ satisfies $R(2B - x) = R(2b - x)$, or after the substitution $x \mapsto 2B - x$, $R(x) = R(x + 2b - 2B)$.

If $b \neq B$, then this says the polynomial $R(x)$ is periodic, hence constant, a contradiction. Thus we must have $b = B$.
Finally, plugging in $x = c$ and using that $a = A$ and $b = B$, we find that $e = E$. Hence $f(x) = h(x)$. ∎

5.5 Long-Run Behavior Lemma

Let $P(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ be a polynomial with real coefficients. Then for large x, the behavior of $P(x)$ will be dominated by the leading term. There are a number of ways to state this more formally and a number of useful facts we can extract from this. This section is devoted to a few of these.
The simplest version of this is probably the following. Suppose that $a_d > 0$. Since

$$\lim_{x\to\infty} \frac{P(x)}{x^d} = a_d > 0,$$

$P(x)$ will be positive for all sufficiently large x. More concretely, if α is the largest real root of $P(x)$, then $P(x)$ will be positive for $x > \alpha$.
If we use a little calculus, and apply this observation to the derivative of $P(x)$, we get a more powerful fact. If the leading coefficient of a polynomial $P(x)$ is positive, then after we pass the last local minimum of the graph of $P(x)$, the polynomial is strictly increasing.

Theorem

Let $P(x) = a_d x^d + \ldots + a_0$ with $a_d > 0$. Then for all sufficiently large x, the polynomial $P(x)$ is increasing.

Example 5.24. Find all real polynomials $P(x)$ such that there exists a natural number n satisfying the following equation:

$$\sum_{k=1}^{2n+1} (-1)^k \left\lfloor \frac{k}{2} \right\rfloor P(x+k) = 0.$$

Austrian-Polish Mathematical Competition

Solution. Clearly the zero polynomial is a solution. Otherwise, without loss of generality, we can assume that $P(x)$ is monic. Then by the Theorem, there exists a real number x_0 such that for all $x \geq x_0$, $P(x)$ is strictly increasing. Now notice that the $k = 1$ term in the given sum vanishes and group the remaining terms in pairs to rewrite the equation as

$$\sum_{m=1}^{n} m(P(x+2m) - P(x+2m+1)) = 0.$$

For $x \geq x_0$, we have $x + 2m + 1 > x + 2m > x_0$ for all m, hence by our choice of x_0, we have $P(x+2m+1) > P(x+2m)$. Thus every term in the sum on the left-hand side is negative, a contradiction. It follows that the zero polynomial is the only solution to the problem. ∎

Example 5.25. Let $P(x)$ and $Q(x)$ be nonlinear polynomials with real coefficients such that $P(P(x)) = Q(Q(x))$. Prove that either $P(x) = Q(x)$ or there is a constant C such that $P(x) + Q(x) = C$.

First Solution. Comparing degrees we see that $(\deg P(x))^2 = (\deg Q(x))^2$. Hence the degrees of $P(x)$ and $Q(x)$ are equal.
Let $\deg P(x) = \deg Q(x) = d \geq 2$, and write

$$P(x) = a_d x^d + \ldots + a_0, \quad Q(x) = b_d x^d + \ldots + b_0.$$

Considering the coefficient of x^{d^2}, we find that $a_d^{d+1} = b_d^{d+1}$. Therefore we can write $a_d = \varepsilon b_d$, where $\varepsilon \in \{-1, 1\}$ satisfies $\varepsilon^{d+1} = 1$. Now note that

$$P(P(x)) = a_d P(x)^d + a_{d-1}P(x)^{d-1} + \ldots + a_0,$$

$$Q(Q(x)) = b_d Q(x)^d + b_{d-1}Q(x)^{d-1} + \ldots + b_0.$$

For $k > 0$, look at the coefficient of $x^{d(d-1)+k}$ on both sides. The terms $P(x)^{d-1}$, $Q(x)^{d-1}$, and lower, have degree at most $d(d-1)$. Hence these coefficients come entirely from $a_d P(x)^d$ and $b_d Q(x)^d$. Thus we have

$$a_d \sum_{i_1+\ldots+i_d=d(d-1)+k} a_{i_1}a_{i_2}\cdot\ldots\cdot a_{i_d} = b_d \sum_{i_1+\ldots+i_d=d(d-1)+k} b_{i_1}b_{i_2}\cdot\ldots\cdot b_{i_d}.$$

We want to prove from these equations that $a_k = \varepsilon b_k$ for each $1 \le k \le d$. We will do so by downward induction on k. The base case $k = d$ is just our definition of ε. Suppose we have proved that $a_s = \varepsilon b_s$ for $k+1 \le s \le d$. Since every term in the sum has

$$d(d-1) + k = i_1 + \ldots + i_d \le i_1 + d(d-1),$$

we see that we must have $i_1 \ge k$ with equality if and only if $i_2 = \cdots = i_d = d$. Similarly, each index is at least k with equality if and only if all the other indices equal d. These d terms will contribute $da_k a_d^d$ to the left sum and $db_k b_d^d$ to the right sum. Now consider a term where all the indices are strictly greater than k, that is, $i_1, \ldots, i_d > k$. Such a term is

$$a_d a_{i_1} a_{i_2} \ldots a_{i_d} = \varepsilon^{d+1} b_d b_{i_1} b_{i_2} \ldots b_{i_d} = b_d b_{i_1} b_{i_2} \ldots b_{i_d}.$$

Thus these terms cancel. After cancelling off all these terms, we have already shown that we will be left with $da_d^d a_k = db_d^d b_k = d\varepsilon^d a_d^d b_k$. Therefore we conclude that $a_k = \varepsilon b_k$, completing the induction step.

If $\varepsilon = -1$, then we are done, since we have shown that every term of $P(x) + Q(x)$, except possibly the constant term, cancels. Suppose $\varepsilon = 1$, and that we try to extend the argument above to the coefficient of $x^{d(d-1)}$. The above argument shows that the contributions of $a_d P(x)^d$ and $b_d Q(x)^d$ will cancel except for the terms $da_0 a_d^d$ and $db_0 b_d^d$. The only change is that we will now get extra terms from the leading coefficients of $a_{d-1}P(x)^{d-1}$ and $b_{d-1}Q(x)^{d-1}$ (and only from these). Hence we get

$$da_d^d a_0 + a_{d-1} a_d^{d-1} = db_d^d b_0 + b_{d-1} b_d^{d-1}.$$

Since $\varepsilon = 1$, the extra terms cancel, and we conclude that $a_0 = b_0$. Thus in this case $P(x) = Q(x)$. ■

Second Solution. Follow the first solution to write

$$P(x) = a_d x^d + \ldots + a_0, \quad Q(x) = b_d x^d + \ldots + b_0,$$

where $a_d = \pm b_d$.

First, assume that $a_d = b_d$. Then

$$a_d(P(x) - Q(x))(P(x)^{d-1} + \ldots + Q(x)^{d-1})$$
$$= a_{d-1}P(x)^{d-1} + \ldots + a_0 - b_{d-1}Q(x)^{d-1} - \ldots - b_0.$$

If $d \ge 1$, note that the leading coefficient of

$$P(x)^{d-1} + \ldots + Q(x)^{d-1}$$

is a polynomial of degree $d(d-1)$ with leading coefficient $da_d^{d-1} \ne 0$. Since the right-hand side has degree at most $d(d-1)$, it follows that $P(x) - Q(x) = C$ is constant. Therefore

$$P(P(x)) = Q(Q(x)) = C + P(C + P(x)),$$

and since $P(x)$ takes on infinitely many values, we conclude that

$$P(x) = C + P(x + C).$$

However if $C \ne 0$, we know that $P(x+C) - P(x)$ has degree $d - 1 > 0$. Thus we find that $C = 0$ and $P(x) = Q(x)$.

Now assume that $a_d = -b_d$. Recall that in this case, d must be odd. Rewrite the original equation as

$$a_d(P(x) + Q(x))(P(x)^{d-1} - \ldots + Q(x)^{d-1})$$
$$= a_{d-1}P(x)^{d-1} + \ldots + a_0 - b_{d-1}Q(x)^{d-1} - \ldots - b_0.$$

Again, $P(x)^{d-1} - \ldots + Q(x)^{d-1}$ is of degree $d(d-1)$, hence the same argument above shows that $P(x) + Q(x)$ is constant. ■

Third Solution. First we prove the following lemma (which we will see later is very useful).

Long-run Behavior Lemma

Let $P(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$ be a polynomial with real coefficients, and define $a = \sqrt[d]{|a_d|}$ and $b = \frac{a_{d-1}}{da_d}$.

Then $\lim_{|x|\to\infty} \left(\sqrt[d]{|P(x)|} - a \cdot |x + b| \right) = 0.$

Remark. The absolute values are only needed to avoid taking even roots of negative numbers, so we could drop them if either d is odd or $a_d > 0$. We could also try to avoid them by working over the complex numbers, but this requires carefully specifying conventions.

Proof. Since we can replace $P(x)$ by $-P(x)$ if necessary, we can assume $a_d > 0$ and drop the absolute values. Then we have

$$\sqrt[d]{P(x)} - \sqrt[d]{a_d}x = \frac{P(x) - a_d x^d}{\sqrt[d]{P(x)^{d-1}} + \ldots + \sqrt[d]{a_d^{d-1}}x^{d-1}}$$
$$= \frac{a_{d-1}x^{d-1} + \ldots + a_0}{\sqrt[d]{P(x)^{d-1}} + \ldots + \sqrt[d]{a_d^{d-1}}x^{d-1}}.$$

Therefore

$$\lim_{|x|\to\infty}\left(\sqrt[d]{P(x)} - \sqrt[d]{a_d}x\right) = \lim_{|x|\to\infty} \frac{a_{d-1}x^{d-1} + \ldots + a_0}{\sqrt[d]{P(x)^{d-1}} + \ldots + \sqrt[d]{a_d^{d-1}}x^{d-1}}$$
$$= \frac{a_{d-1}}{d\sqrt[d]{a_d^{d-1}}}.$$

This completes our proof. ❑

Applying this Lemma to our problem, using the notation of the first solution, we find that

$$\lim_{|x|\to\infty}\left(\sqrt[d]{|P(P(x))|} - \sqrt[d]{|a_d|}\cdot\left|P(x) + \frac{a_{d-1}}{da_d}\right|\right) = 0$$

and

$$\lim_{|x|\to\infty}\left(\sqrt[d]{|Q(Q(x))|} - \sqrt[d]{|b_d|}\cdot\left|Q(x) + \frac{b_{d-1}}{db_d}\right|\right) = 0.$$

Since $P(P(x)) = Q(Q(x))$ and $|a_d| = |b_d|$, subtracting we get

$$\lim_{|x|\to\infty}\left(\left|P(x) + \frac{a_{d-1}}{da_d}\right| - \left|Q(x) + \frac{b_{d-1}}{db_d}\right|\right) = 0.$$

If $a_d = b_d$, then $P(x)$ and $Q(x)$ have the same sign for large x, and we get that

$$\lim_{|x|\to\infty}(P(x) - Q(x)) = \frac{b_{d-1} - a_{d-1}}{da_d}.$$

This implies that $P(x) - Q(x)$ is constant. We can either finish as in the first solution, or we can note that since $d \geq 2$, the fact that $P(x) - Q(x)$ is constant implies that $a_{d-1} = b_{d-1}$ and hence we find that $P(x) - Q(x) = 0$. If $a_d = -b_d$, then $P(x)$ and $Q(x)$ have opposite signs for large x, and so we get

$$\lim_{|x|\to\infty}(P(x) + Q(x)) + C) = 0.$$

Thus $P(x) + Q(x)$ is constant. ■

Remark 1. The assumption that $P(x)$ and $Q(x)$ are nonlinear is necessary, since if $P(x) = b - x$, then we compute that $P(P(x)) = x$, independently of b.

Remark 2. It was not require in the preceding solutions, but in the case where $P(x) + Q(x) = C$, we can describe $P(x)$ and $Q(x)$ more explicitly. In this case, we have

$$P(P(x)) = Q(Q(x)) = C - P(C - P(x)),$$

and since $P(x)$ takes on infinitely many values, this implies

$$P(x) + P(C - x) = C.$$

Therefore the polynomial $P\left(\frac{C}{2} + x\right) - \frac{C}{2}$ is an odd polynomial and so

$$P\left(\frac{C}{2} + x\right) - \frac{C}{2} = xR(x^2),$$

for some polynomial $R(x)$. Thus we can write

$$P(x) = \frac{C}{2} + \left(x - \frac{C}{2}\right)R\left(\left(x - \frac{C}{2}\right)^2\right) = \frac{C}{2} + \left(x - \frac{C}{2}\right)T(x^2 - Cx)$$

and we find that

$$Q(x) = \frac{C}{2} - \left(x - \frac{C}{2}\right)T(x^2 - Cx).$$

Example 5.26. If $P(x)$ and $Q(x)$ are two polynomials with real coefficients such that $P(P(P(x))) = Q(Q(Q(x)))$, prove that $P(x) = Q(x)$.

Navid Safaei

Solution. If $P(x)$ has degree d and leading coefficient a_d, then we see that $P(P(P(x)))$ has degree d^3 and leading coefficient $a_d^{1+d+d^2}$. Since $Q(x)$ gives an analogous formula, it follows that $Q(x)$ also has degree d and since $1+d+d^2$ is odd, it follows that the leading coefficients agree. (Note that this solves the constant case, so we may assume $d \geq 1$ below.)
It is easy to check that if $P(x) = ax + b$, then

$$P(P(P(x))) = a^3x + b(a^2 + a + 1),$$

so $P(P(P(x)))$ determines a and b, and hence $P(x)$.
Thus we may assume $d \geq 2$.
By the long-run behavior lemma, we find that

$$\lim_{|x|\to\infty} \left(\sqrt[d]{|P(P(P(x)))|} - a|P(P(x)) + b| \right) = 0$$

and

$$\lim_{|x|\to\infty} \left(\sqrt[d]{|Q(Q(Q(x)))|} - a|Q(Q(x)) + b'| \right) = 0,$$

hence

$$\lim_{|x|\to\infty} \left(|P(P(x)) + b| - |Q(Q(x)) + b'| \right) = 0.$$

Since $P(P(x))$ and $Q(Q(x))$ have the same leading coefficient, they have the same sign for large x, and hence it follows that $P(P(x)) - Q(Q(x)) = b' - b$ is constant.
Since $d \geq 2$, it follows that the coefficient of x^{d^2-1} in $P(P(x)) - Q(Q(x))$ vanishes. An easy calculation shows that this means the coefficients of x^{d-1} in $P(x)$ and $Q(x)$ agree. From this, we find that in the calculation above $b' = b$, and hence we conclude that $P(P(x)) = Q(Q(x))$. Repeating this argument (which is the third solution to the previous problem), we find that $P(x) - Q(x) = 0$. ∎

Remark. In Tournament of Towns 2004, the following problem was proposed: Let $P(x)$, $Q(x)$ be two real polynomials such that

$$P(P(x)) = Q(Q(x)) \text{ and } P(P(P(x))) = Q(Q(Q(x))).$$

Is it necessary that $P = Q$?
This was of course meant to be an easier question
(We have $P(P(P(x))) = Q(Q(Q(x))) = Q(P(P(x)))$. If $P(x)$ is nonconstant, then $P(P(x))$ takes on infinitely values and we conclude that $P(x) = Q(x)$.), but it is amusing to note that we could have solved the problem ignoring the first hypothesis.

Example 5.27. Let P, Q, R be real polynomials such that the polynomial $P(Q(x)) + P(R(x))$ is a constant polynomial.
Prove that either $P(x)$ or $Q(x) + R(x)$ is constant.

Zhautykov Competition 2012

First Solution. Assume that $P(x)$ is not constant. Without loss of generality, we can assume that $P(x)$ is monic. Thus we may write

$$P(x) = x^k + c_{k-1}x^{k-1} \ldots + c_0.$$

Since $P(Q(x))$ and $P(R(x))$ have the same degree, we see that $R(x)$ and $Q(x)$ have the same degree. If we write

$$R(x) = a_dx^d + \ldots + a_0, \quad Q(x) = b_dx^d + \ldots + b_0,$$

then examining the leading term, we find that $a_d^k + b_d^k = 0$. Thus k is odd and $a_d + b_d = 0$. After rewriting the original equation, we find that

$$(R(x)+Q(x))(R(x)^{k-1}-\ldots+Q(x)^{k-1}) = -c_{k-1}(R(x)^{k-1}+\ldots+Q(x)^{k-1})+\ldots.$$

The right-hand side has degree at most $d(k-1)$ and as in the previous solutions $R(x)^{k-1}-\ldots+Q(x)^{k-1}$ has degree $d(k-1)$ and leading coefficient ka_d^{k-1}. Thus we find that $R(x) + Q(x)$ must be constant. ∎

Second Solution. As in the first solution, we assume that $P(x)$ is nonconstant and we find $\deg P(x) = k$ is odd and the leading coefficients of $Q(x)$ and $R(x)$ have opposite signs.
By the long-run behavior lemma, we find that

$$\lim_{|x|\to\infty} \left(\sqrt[k]{|P(Q(x))|} - a|Q(x) + b| \right) = 0$$

and

$$\lim_{|x|\to\infty} \left(\sqrt[k]{|P(R(x))|} - a|R(x) + b| \right) = 0,$$

hence

$$\lim_{|x|\to\infty} (|Q(x) + b| - |R(x) + b|) = 0.$$

Since the leading coefficients of $Q(x)$ and $R(x)$ have opposite signs, we conclude that

$$\lim_{|x|\to\infty} (Q(x) + R(x)) = \pm 2b,$$

and hence $Q(x) + R(x)$ is constant. ■

Remark. You make recognize that the two solutions above are adapted from the last two solutions to Example 5.25. The first solution can also be adapted to solve this problem. In this solution, we use a backward induction to prove that for

$$R(x) = a_d x^d + \ldots + a_0, \quad Q(x) = b_d x^d + \ldots + b_0,$$

we have $a_k = -b_k$ whenever $k = d, \ldots, 1$.

Example 5.28. Let $Q(x)$ be a nonlinear polynomial. If $Q(Q(x))$ is an odd function, prove that $Q(x)$ is an odd function. If $Q(Q(x))$ is an even function, prove that $Q(x)$ is an even function.

Solution. For the first statement, we find that $Q(Q(x)) + Q(Q(-x)) = 0$. Then by the previous problem, we get that $Q(x) + Q(-x) = C$ is constant. In this case we get $Q(Q(x)) = -Q(Q(-x)) = -Q(C - Q(x))$, which implies that $Q(x) = -Q(C - x)$. Hence $Q(x) = -Q(C - x) = Q(x - C) - C$.

But if $C \neq 0$, this implies that $Q(x)$ is linear, contrary to the hypotheses. Thus we must have $C = 0$ and $Q(x)$ is odd.
For the second statement, $Q(Q(x)) = Q(Q(-x))$. This implies that $Q(Q(x))$ has even degree, and hence $Q(x)$ also has even degree. Since we can replace $Q(x)$ by $-Q(-x)$, we can also assume the leading coefficient of $Q(x)$ is positive. Thus by the Theorem, there is a constant C such that for all $x > C$, $Q(x)$ is strictly increasing.
Choose x large enough that $Q(x), Q(-x) > C$. If $Q(x) > Q(-x)$, then $Q(Q(x)) > Q(Q(-x))$ and if $Q(x) < Q(-x)$, then $Q(Q(x)) < Q(Q(-x))$. These are not allowed, so we must have $Q(x) = Q(-x)$ for all large x, and hence $Q(x) = Q(-x)$ for all x. ■

Example 5.29. Find all polynomials $P(x)$ and $Q(x)$ such that

$$P(P(P(P(x)))) = Q(Q(Q(Q(x)))).$$

Taiwanese Team Selection Test 2012

Solution. Define $P(P(x)) = f(x)$ and $Q(Q(x)) = g(x)$. Then

$$f(f(x)) = g(g(x)).$$

Hence by Example 5.25 either $f(x) = g(x)$ or $f(x) + g(x) = C$ for some constant C.
Assuming the former, we get $P(P(x)) = Q(Q(x))$. Hence by Example 5.25 we get that either $P(x) = Q(x)$ or $P(x) + Q(x) = D$ for some constant D. In the second case, by the remark after that example, we get that there is a polynomial $T(x)$ such that

$$P(x) = \frac{D}{2} + \left(x - \frac{D}{2} \right) T(x^2 - Dx),$$

$$Q(x) = \frac{D}{2} - \left(x - \frac{D}{2} \right) T(x^2 - Dx).$$

Assuming the latter, we have $P(P(x)) + Q(Q(x)) = C$. From the discussion after Example 5.25, we see that

$$P(P(x)) = \frac{C}{2} + \left(x - \frac{C}{2} \right) T(x^2 - Cx),$$

for some polynomial $T(x)$. In particular $P(P(x))$ has odd degree, and hence $P(x)$ has odd degree. But if $P(x)$ has odd degree d and leading coefficient a_d, then we compute that the leading coefficient of $P(P(x))$ is a_d^{d+1}, which is an even power and hence positive. Since a similar argument shows that $Q(Q(x))$ has positive leading coefficient, we cannot have $P(P(x))+Q(Q(x)) = C$. Thus there are no solutions in this case. ■

5.6 Miscellaneous problems

In this section we provide some examples for which you need to combine ideas from these three chapters about finding polynomials.

Example 5.30. Let n be a positive integer. Find all real polynomials f and g such that

$$(x^2+x+1)^n f(x^2-x+1) = (x^2-x+1)^n g(x^2+x+1),$$

for all real numbers x.

Marcel Chiriţă - Mathematical Reflections, Problem U337

First Solution. We first claim that x^n divides $f(x)$. If not, then we can write $f(x) = x^k P(x)$ where $k < n$ and $P(0) \neq 0$. Plugging this into the equation and cancelling, we find that

$$(x^2+x+1)^n P(x^2-x+1) = (x^2-x+1)^{n-k} g(x^2+x+1).$$

Now let ε be a primitive cube root of -1, so that ε satisfies $\varepsilon^2 - \varepsilon + 1 = 0$, and taking $x = \varepsilon$, we get

$$(2\varepsilon)^n P(0) = 0,$$

and hence a contradiction. Similarly, we find that x^n divides $g(x)$. Writing $f(x) = x^n P(x)$ and $g(x) = x^n Q(x)$, we find that

$$P(x^2-x+1) = Q(x^2+x+1).$$

Setting $R(x) = P(x^2-x+1) = Q(x^2+x+1)$, we compute that

$$\begin{aligned} R(1-x) &= P((1-x)^2-(1-x)+1) = P(x^2-x+1) = R(x) \\ &= Q(x^2+x+1) = Q((-x-1)^2+(-x-1)+1) = R(-x-1), \end{aligned}$$

hence after substituting $x \mapsto 1-x$, we get $R(x) = R(x-2)$. Thus $R(x)$ is a periodic polynomial, and hence constant. Thus $P(x) = Q(x) = C$ is constant and $f(x) = g(x) = Cx^n$ for some $n \geq 0$. ■

Second Solution. Let $R(x) = \frac{f(x)}{x^n}$, $S(x) = \frac{g(x)}{x^n}$. Then

$$R(x^2-x+1) = S(x^2+x+1).$$

The computation given in the previous solution shows that

$$T(x) = R(x^2-x+1) = S(x^2+x+1)$$

is a periodic rational function, hence constant. Thus $R(x) = S(x) = C$ is constant, and $f(x) = g(x) = Cx^n$. ■

Example 5.31. Find all polynomials $P(x)$ with real coefficients such that

$$P(x^2-2x) = P(x-2)^2.$$

First Solution. Clearly the constant polynomials $P(x) = 0$ and $P(x) = 1$ are solutions. Assume we have a solution $P(x)$ of degree $d \geq 1$. Let $x-1 = z$ and $Q(x) = P(x-1)$. Then

$$Q(z^2) = P(x^2-2x) = P(x-2)^2 = Q(z)^2.$$

Iterating this we find that $Q(x^{2^n}) = Q(x)^{2^n}$ for all n. In particular, we can choose n large enough that $2^n > d$. Now suppose r is any nonzero root of $Q(x)$. Then setting x to be any 2^n-th root of r, we find that all 2^n-th roots of r are roots of $Q(x)$. But this would give us more than d distinct roots of a degree d polynomial, a contradiction. Thus the only root of $Q(x)$ is zero and hence $Q(x) = ax^n$ for some n. Plugging in we find that $Q(x) = x^n$. Thus $P(x) = 0$ or $P(x) = (x+1)^n$ for some $n \geq 0$. ■

Second Solution. It is easy to check that $P(x) = x+1$ is a solution. Hence by the uniqueness lemma, the nonconstant solutions are $P(x) = (x+1)^n$ for $n > 0$.
Allowing constant solutions adds the case $n = 0$ and the zero solution. ∎

Example 5.32. Find all polynomials $P(x)$ with nonnegative integer coefficients such that for all positive integers n, $n^{P(n)} \leq P(n)^n$.

Solution. It is easy to check that $3^m > m^3$ for $m = 1, 2$ and $3^m = m^3$ for $m = 3$. Since for $m \geq 3$, we have

$$\frac{(m+1)^3}{m^3} = 1 + \frac{3}{m} + \frac{3}{m^2} + \frac{1}{m^3} < 3,$$

an easy induction shows that $3^m \geq m^3$ for all positive integers m with equality only for $m = 3$. Now, putting $m = P(3)$, we get $3^{P(3)} \leq P(3)^3$. Thus $P(3) = 3$. Let $\deg P(x) = d$. Then $3 = P(3) \geq 3^d$. Hence $d \in \{0, 1\}$. If $d = 1$, we find that $P(x) = x + a$ with $a \geq 0$. Since $P(3) = 3$, we get $a = 0$ and $P(x) = x$. If $d = 0$, then $P(x)$ is constant so $P(x) = P(3) = 3$. Thus $P(x) = x$ or $P(x) = 3$. ∎

Example 5.33. Consider the identity

$$1 + 2 + \ldots + n = \frac{1}{2}n(n+1).$$

If we set $P_1(x) = \frac{1}{2}x(x+1)$, then it is the unique polynomial such that for each positive integer n,

$$P_1(n) = 1 + 2 + \ldots + n.$$

In general, for each positive integer k, there is a unique polynomial $P_k(x)$ such that

$$P_k(n) = 1^k + \ldots + n^k, \quad n = 1, 2, \ldots.$$

Find the value of $P_{2010}\left(-\frac{1}{2}\right)$.

Singaporean Mathematical Olympiad 2010

Solution. For even k, let us define $Q(x) = P_k(x) - P_k(x-1)$. Then $Q(n) = n^k$ for each integer $n \geq 2$. Thus $Q(x) = x^k$. Therefore

$$P_k(-n+1) - P_k(-n) = (1-n)^k = (n-1)^k,$$

$$P_k(-n+2) - P_k(-n+1) = (n-2)^k, \ldots, P_k(0) - P_k(-1) = 0,$$

$$P_k(1) - P_k(0) = 1.$$

Summing these we get

$$P_k(1) - P_k(-n) = 1^k + 0 + 1^k + \ldots + (n-1)^k = 1 + P_k(n-1).$$

That is, for all integers $n \geq 2$, we have $P_k(n-1) + P_k(-n) = 0$. Hence for all x, we have $P_k(x-1) + P_k(-x) = 0$. Setting $x = \frac{1}{2}$, we get $P_k\left(-\frac{1}{2}\right) = 0$. ∎

Example 5.34. Find all polynomials $P(x)$ with complex coefficients such that

$$P(x^n + P(x)) = (2^n - 1)x^{n^2} + P(x^n).$$

Solution. Let $P(x) = a_d x^d + \ldots + a_0$. Then

$$P(x^n + P(x)) - P(x^n) = a_d((x^n + P(x))^d - x^{nd}) + \ldots + a_1(P(x)) = (2^n - 1)x^{n^2}.$$

The left-hand side of the above equality is divisible by $P(x)$. Hence $P(x)$ divides x^{n^2}. Therefore $P(x) = a_d x^d$. Thus

$$P(x^n + P(x)) = a_d(x^n + a_d x^d)^d = a_d x^{nd} + (2^n - 1)x^{n^2}.$$

If $n > d$, then the left-hand side has degree dn and the right-hand side has degree $n^2 > dn$. If $n < d$, then the left-hand side has degree d^2 and the right-hand side has degree $dn < d^2$. Thus these lead to contradictions, and hence $d = n$. In this case the equation becomes

$$a_n(1 + a_n)^n x^{n^2} = (a_n + (2^n - 1))x^{n^2},$$

and hence we see that a_n must be a root of $a_n(1+a_n)^n = a_n + 2^n - 1$. So the solutions are $P(x) = a_n x^n$, where a_n is the root of the above equation. ∎

Example 5.35. Find all polynomials $P(x)$ with real coefficients such that for each positive integer n, we have

$$P(P(n)) = \lfloor P(n)^2 \rfloor .$$

Solution. If $P(x) = C$ is constant, then $C = \lfloor C^2 \rfloor$, so C is a nonnegative integer satisfying $C \leq C^2 < C + 1$. It is easy to see that this gives $P(x) = 0$ or $P(x) = 1$. Now assume $P(x)$ is nonconstant. Since $x - 1 < \lfloor x \rfloor \leq x$, we have $P(n)^2 - 1 < \lfloor P(n)^2 \rfloor \leq P(n)^2$, which implies that

$$-1 < P(P(n)) - P(n)^2 \leq 0$$

for each positive integer n. Since $P(x)$, is nonconstant $|P(n)|$ tends to infinity as n tends to infinity. Hence we find that there are arbitrarily large values of x such that

$$-1 < P(x) - x^2 \leq 0.$$

A nonconstant polynomial must tend to $\pm\infty$ as x tends to $\pm\infty$, so this forces $P(x) - x^2$ to be a constant polynomial. Hence we can write $P(x) = x^2 + C$ for some constant C with $-1 < C \leq 0$. Hence we compute that

$$P(P(n)) = (n^2 + C)^2 + C = n^4 + 2Cn^2 + C^2 + C.$$

From the given equation this must be an integer for all positive integer n. In particular, for $n = 1$, we see that C^2+3C+1 is an integer and for $n = 2$ we see that $C^2+5C+16$ is an integer. Subtracting, we see that $2C$ must be an integer. Thus $C = 0$ or $C = -1/2$. However for $C = -1/2$, $P(P(1)) = C^2 + 3C + 1$ is not an integer. Thus only $C = 0$ is possible, and it is easy to see that this works. Therefore $P(x) \in \{x^2, 0, 1\}$. ∎

5.7 Proposed problems

Problem 5.1. Find all monic polynomials with only simple real roots such that $P(x^2) = \pm P(x)P(-x)$.

Problem 5.2. Let $P(x) \in \mathbb{Z}[x]$ be an irreducible polynomial having a root with absolute value greater than $\frac{3}{2}$. Prove that if $P(\alpha) = 0$, then $P(1+\alpha^3) \neq 0$.

Problem 5.3. Find all polynomials $P(x)$ with complex coefficients such that $P(x^3 - 1)$ is divisible by $P(x^2 + x + 1)$.

Gazeta Matematică

Problem 5.4. Find all polynomials $P(x)$ such that

$$P(x^2) = P\left(x + \frac{1}{2}\right) P\left(x - \frac{1}{2}\right).$$

Problem 5.5. Find the largest $c \in \mathbb{R}$ for which there exists a nonconstant polynomial $P(x)$ such that

$$P(x^2) = P(x - c)P(x + c).$$

Brazilian Training Camp

Problem 5.6. Find all polynomials $P(x) = x^3 + ax^2 + bx + c$ such that

$$P(x^2 - 2) = -P(x)P(-x).$$

John Murray - Irish Mathematical Olympiad 2012

Problem 5.7. Let $P(x)$, $Q(x)$ be quadratic trinomials such that the numbers $-22, 7, 13$ are three roots of the equation $P(Q(x)) = 0$. Find the fourth root of this equation.

P. Černek - Czech-Slovak Mathematical Olympiad 2000

Problem 5.8. Let $P(x)$ and $Q(x)$ be polynomials with complex coefficients such that $P(x)$ and $P(Q(x))$ are monic, $P(X)$ is nonconstant, and $Q(x)$ is nonlinear. Let

$$A = \{x \in \mathbb{C} : P(x) = 0\}, \quad B = \{x \in \mathbb{C} : P(Q(x)) = 0\}.$$

Prove that the following statements are equivalent:

(i) $A = B$;

(ii) there is a complex number r such that

$$P(x) = (x-r)^n, \quad Q(x) = \omega(x-r)^m + r,$$

where $n > 0$, $m > 1$ are integers and ω is an $n-$ th root of unity.

Problem 5.9. Let $f \in \mathbb{Z}[x]$ be a monic polynomial and let $(a_n)_{n\geq 1}$ be an arithmetic progression of natural numbers. Prove that if there exists $k \in \mathbb{Z}$ with $a_1 = f(k)$, then the set

$$\{a_n \mid n \geq 1\} \cap \{f(n) \mid n \in \mathbb{Z}\}$$

is infinite.

Gazeta Matematică B 11/2011, *Problem* 26536

Chapter 6

Lagrange's Interpolation Formula (L.I.F.)

6.1 The formula

We saw in Section 3.2 that two polynomials of degree d that agree at $d+1$ points are in fact the same polynomial. In geometric terms, this says that if we choose any $d+1$ points in the plane (with distinct x-coordinates), then there is at most one polynomial of degree d whose graph goes through them. This is a uniqueness result, but we are missing the corresponding existence result. We would like to fill in this gap, so we have the following question:

Suppose we are given $d+1$ points in the plane (with distinct x-coordinates), is there a polynomial of degree d whose graph goes through all of them?

If we are given a collection of points, then a function whose graph passes through those points is said to interpolate between them. Thus we can phrase this as asking for a polynomial of degree d that interpolates between $d+1$ points.

Before giving Lagrange's very pretty answer to this question, let's think about this problem a little. If we write down an arbitrary polynomial $P(x)$ of degree d in the usual way as $P(x) = a_d x^d + \cdots + a_0$, then we have $d+1$ unknowns, namely the coefficients $a_d, a_{d-1}, \ldots, a_0$. If we ask that this polynomial pass

through the point (x_1, y_1), then this says $P(x_1) = y_1$ and hence

$$a_d x_1^d + a_{d-1} x_1^{d-1} + \cdots + a_0 = y_1.$$

Since we know x_1 and y_1, this gives us a linear equation in our $d+1$ unknowns. If we want to interpolate between $d+1$ points, then we will get $d+1$ linear equations of this form in our $d+1$ unknowns. This is a nice situation: $d+1$ equations in $d+1$ unknowns. The fact that there should be a unique solution seems reasonable, but it is certainly possible to write down systems of linear equations without solutions. For example, if we have two points with the same x-coordinate, but different y-coordinates, it will clearly be impossible to find a polynomial that interpolates through both. Still, we have reason for optimism and we could study these linear equations to answer our question.

Lagrange resolved this in a very elegant way avoiding any tedious linear algebra. Assume that we have $d+1$ distinct complex numbers $r_0, r_1, \ldots, r_d$ and we have $d+1$ matching values $s_0, s_1, \ldots, s_d$. We want to find a polynomial $P(x)$ of degree at most d, such that $P(r_0) = s_0, \ldots, P(r_d) = s_d$. Look at the polynomial

$$Q_0(x) = (x - r_1)(x - r_2) \cdot \ldots \cdot (x - r_d).$$

This polynomial is very simple to understand at $x = r_1, \ldots, r_d$, it is zero. It is a little trickier to understand at $x = r_0$, since its value will be a long product, but we can fix this by looking at

$$\frac{Q_0(x)}{Q_0(r_0)} = \frac{(x - r_1)(x - r_2) \cdot \ldots \cdot (x - r_d)}{(r_0 - r_1)(r_0 - r_2) \cdot \ldots \cdot (r_0 - r_d)}.$$

This is still zero at $x = r_1, \ldots, r_d$, but now its value at r_0 is also easy, it is just 1. It should be clear that we can do the same thing for each r_i. Specifically, we define

$$Q(x) = (x - r_0)(x - r_1) \cdot \ldots \cdot (x - r_d)$$

and

$$Q_i(x) = \frac{Q(x)}{x - r_i}.$$

This is a formal way of saying that $Q_i(x)$ is the product of all of $x - r_0, \ldots$ $x - r_d$, except we omit $x - r_i$. Then the polynomial

$$\frac{Q_i(x)}{Q_i(r_i)} = \frac{(x - r_0) \cdot \ldots \cdot (x - r_{i-1})(x - r_{i+1}) \cdot \ldots \cdot (x - r_d)}{(r_i - r_0) \cdot \ldots \cdot (r_i - r_{i-1})(r_i - r_{i+1}) \cdot \ldots \cdot (r_i - r_d)}$$

will be 0 at $x = r_0, \ldots, r_{i-1}, r_{i+1}, \ldots, r_d$ and 1 at $x = r_i$.

Now it is easy to see what will happen if we combine these polynomials. Look at the polynomial

$$P(x) = \frac{Q_0(x)}{Q_0(r_0)} s_0 + \frac{Q_1(x)}{Q_1(r_1)} s_1 + \cdots + \frac{Q_d(x)}{Q_d(r_d)} s_d.$$

If we evaluate it at $x = r_i$, then all terms except the $Q_i(x)$ term are obviously zero, and the $Q_i(x)$ term is just $1 \cdot s_i$. Thus $P(r_i) = s_i$ for $i = 0, \ldots, d$. This answers our question, you can interpolate a polynomial of degree d through any $d+1$ points. The really impressive thing is that Lagrange not only proved this, but also gave a fairly simple formula for the unique polynomial that interpolates between them.

The aforementioned formula is called the *Lagrange's Interpolation Formula* (or L.I.F. for short).

Lagrange's Interpolation Formula

Let $(r_0, s_0), \ldots, (r_d, s_d)$ be any points in the Cartesian plane with distinct x-coordinates. Then there exists exactly one polynomial of degree at most 2 whose graph passes through these $d+1$ points. Furthermore, this polynomial is given by the following formula: Define

$$Q(x) = (x - r_0)(x - r_1) \cdot \ldots \cdot (x - r_d)$$

and

$$Q_i(x) = \frac{Q(x)}{x - r_i},$$

then

$$P(x) = \frac{Q_0(x)}{Q_0(r_0)} s_0 + \frac{Q_1(x)}{Q_1(r_1)} s_1 + \cdots + \frac{Q_d(x)}{Q_d(r_d)} s_d.$$

One can turn this around slightly. Instead of imagining being given $d+1$ points and asking for $P(x)$, we could start with a polynomial of degree at most d. In this case the L.I.F. becomes a polynomial identity:

Lagrange's Interpolation Formula - Alternative Formulation

Let $P(x)$ be any polynomial of degree at most d and $r_0, r_1, \ldots, r_d$ any $d+1$ distinct complex numbers. Then

$$P(x) = \frac{Q_0(x)}{Q_0(r_0)}P(r_0) + \ldots + \frac{Q_d(x)}{Q_d(r_d)}P(r_d).$$

Example 6.1. Consider the three points $(1,4)$, $(-1,0)$, $(0,2)$. According to the L.I.F., there exists only one polynomial of degree at most d satisfying $P(1)=4$, $P(-1)=0$, $P(0)=2$, and it is

$$\frac{x(x+1)}{2}\cdot 4 + \frac{x(x-1)}{8}\cdot 0 + \frac{(x-1)(x+1)}{-1}\cdot 2 = 2x+2.$$

Example 6.2. Let $P(x)$ be a polynomial of degree 5. When $P(x)$ is divided by $x-1$, $x-2$, $x-3$, $x-4$ and x^2-x-1, $P(x)$ leaves a remainder of 3, 1, 7, 36 and $x-1$, respectively. Find the square of the remainder when $P(x)$ is divided by $x+1$.

Singaporean Mathematical Olympiad 2010

Solution. We have $P(1)=3$, $P(2)=1$, $P(3)=7$, $P(4)=36$ and

$$P(x) = (x^2-x-1)Q(x) + x - 1,$$

where $Q(x)$ is a polynomial of degree 3. Hence

$$Q(1)=-3, \quad Q(2)=0, \quad Q(3)=1, \quad Q(4)=3.$$

Now, by the L.I.F., the polynomial $Q(x)$ is uniquely determined and we have

$$Q(x) = -3\cdot\frac{(x-2)(x-3)(x-4)}{(-1)(-2)(-3)} + 1\cdot\frac{(x-1)(x-2)(x-4)}{(2)(1)(-1)} + 3\cdot\frac{(x-1)(x-2)(x-3)}{(3)(2)(1)}.$$

Hence $Q(-1)=-27$. Therefore $P(-1)=-29$ and so $P(-1)^2=841$. ■

Example 6.3. Let $a \neq 0$ such that $|3ax^2+2bx+c| \leq 1$ for all $0 \leq x \leq 1$. Find the maximum value of a.

Solution. Write the L.I.F. for $P(x)=3ax^2+2bx+c$ and the x-coordinates $0, \frac{1}{2}, 1$. This says

$$3ax^2+2bx+c = \frac{(x-\frac{1}{2})(x-1)}{\frac{1}{2}}P(0) - \frac{(x-0)(x-1)}{\frac{1}{4}}P\left(\frac{1}{2}\right) + \frac{(x-\frac{1}{2})(x-0)}{\frac{1}{2}}P(1).$$

Comparing the leading coefficients, we find that

$$3a = 2P(0) - 4P(\tfrac{1}{2}) + 2P(1).$$

Since $|P(0)|$, $\left|P\left(\frac{1}{2}\right)\right|$, $|P(1)| \leq 1$, we get

$$3a = 2P(0) - 4P\left(\frac{1}{2}\right) + 2P(1) \leq 2+4+2 = 8.$$

Thus $a \leq \frac{8}{3}$. The equality case occurs when

$$P(0) = P(1) = 1, \quad P\left(\frac{1}{2}\right) = -1.$$

That is,

$$\begin{aligned} P(x) &= 2\left(x-\frac{1}{2}\right)(x-1)P(0) - 4(x-0)(x-1)P\left(\frac{1}{2}\right) \\ &\quad +2\left(x-\frac{1}{2}\right)(x-0)P(1) \\ &= (2x-1)(x-1) + 4x(x-1) + (2x-1)x \\ &= 8x^2-8x+1. \end{aligned}$$

Since for $0 \leq x \leq 1$, we have $0 \leq x(1-x) \leq \frac{1}{4}$, it is easy to see that $|P(x)| \leq 1$. Thus we are done. ■

Remark. The solution to the previous example is logically sound, but there is still something circular about it. The reason the solution worked is because we cleverly chose to apply the L.I.F. at the correct points $0, \frac{1}{2}, 1$. From this we got the upper bound on a, and analyzing the equality case we found our polynomial $P(x)$ and indeed the points where $P(x) = \pm 1$ are exactly $0, \frac{1}{2}, 1$. That justified our original choice. If we had chosen three different points, we would have gotten a different (weaker) upper bound on a, and we would have gotten a polynomial that was ± 1 at our chosen points, but it would not satisfy the condition that $|P(x)| \leq 1$ for all $0 \leq x \leq 1$.
For the quadratic case one could use symmetry or the knowledge that $0 \leq x(1-x) \leq \frac{1}{4}$ to reason that $0, \frac{1}{2}, 1$ are the correct points to take. However, to generalize this example to higher degree polynomials, one needs a deep understanding of a certain type of polynomials called the *Chebyshev polynomials*. We shall discuss this topic in our last (i.e., third) volume about polynomials.

Example 6.4. Maxim and Vlatka play the following game:
Maxim secretly chooses numbers $a_1, a_3, \ldots, a_{2017}$ lying in $[-1, 1]$. Vlatka secretly chooses numbers $a_2, a_4, \ldots, a_{2018}$ lying in $[-1, 1]$. Then they construct a polynomial of minimal degree such that $P(i) = a_i$ for all $1 \leq i \leq 2018$ and calculate $P(2019)$. Maxim wants $P(2019)$ to be as large as possible and Vlatka wants the value as small as possible. What can the value of $P(2019)$ be if both players use their best strategies?

Volodymyr Baravman

Solution. Note that the polynomial of minimal degree such that $P(i) = a_i$ for all $1 \leq i \leq 2018$ is the polynomial of degree at most 2017 obtained from the L.I.F., since this is the only polynomial of degree at most 2017 with the required values. Letting

$$L_i(x) = \frac{Q_i(x)}{Q_i(i)} = \frac{(x-1)\cdot\ldots\cdot(x-(i-1))(x-(i+1))\cdot\ldots\cdot(x-2018)}{(i-1)\cdot\ldots\cdot(i-(i-1))(i-(i+1))\cdot\ldots\cdot(i-2018)}$$

be the polynomials for the L.I.F., we will have

$$P(x) = a_1 L_1(x) + \ldots + a_{2018} L_{2018}(x),$$

Hence $P(2019) = a_1 L_1(2019) + \ldots + a_{2018} L_{2018}(2019)$.
From this the optimal strategies are clear. Maxim will set $a_{2i-1} = 1$ if $L_{2i-1}(2019)$ is positive and $a_{2i-1} = -1$ if it is negative. Vlatka, on the other hand, will set $a_{2i} = -1$ if $L_{2i}(2019)$ is positive and $a_{2i} = 1$ if it is negative.
Notice that both the numerator and denominator of $L_i(2019)$ are products of 2017 factors. Every factor in the numerator is of the form $2019 - j > 0$. Hence the numerator is positive. The denominator has $i-1$ positive factors ($i - j$ for $1 \leq j < i$) and $2018 - i$ negative factors ($i - j$ for $i < j \leq 2018$). Thus the sign of the denominator will be $(-1)^{2018-i} = (-1)^i$. Thus Maxim will look only at $L_{2i-1}(2019) < 0$ and will set all the $a_{2i-1} = -1$. Vlatka will look at all the $L_{2i}(2019) > 0$ and will set all the $a_{2i} = -1$. Since Maxim and Vlatka both will choose $a_i = -1$, we find that $P(x) = -1$ for all x, and hence $P(2019) = -1$. ■

Example 6.5. Let $a_0, \ldots, a_d$ be real numbers and let $r_0, \ldots, r_d$ be distinct rational numbers such that $P(x) = a_0 + \ldots + a_d x^d$ has an irrational leading coefficient. Prove that at least one of $P(r_0), \ldots, P(r_d)$ is irrational.

Solution. Let us write L.I.F. for $P(x)$ and $r_0, \ldots, r_d$. That is,

$$P(x) = \frac{(x-r_1)\cdot\ldots\cdot(x-r_d)}{(r_0-r_1)\cdot\ldots\cdot(r_0-r_d)}P(r_0) + \ldots + \frac{(x-r_0)\cdot\ldots\cdot(x-r_{d-1})}{(r_d-r_0)\cdot\ldots\cdot(r_d-r_{d-1})}P(r_d).$$

Now assume on the contrary, that $P(r_0), \ldots, P(r_d)$ are all rational numbers. Then the right-hand side produces a polynomial with rational coefficients that is identical to $P(x)$, contradicting the fact that $P(x)$ has an irrational leading coefficient. ■

The preceding example strikes at the very heart of the topic of rational-valued polynomials at rational points. We succinctly provide an implication of the before-mentioned example.

Corollary

If a polynomial $P(x)$ of degree d assumes rational values at any $d+1$ rational points, then all of its coefficients are rational.

Example 6.6. If $P(x)$ is a polynomial and $P(\mathbb{Z}) \subseteq \mathbb{Z}$, then $P(x) \in \mathbb{Q}[x]$.

6.2 Constructing identities

In the first volume of the polynomial trilogy we worked with identities. We have already seen that you can interpret the L.I.F. as a polynomial identity, but what you may not appreciate yet is the vast number of identities that are either special cases of the L.I.F. or follow easily from it. Even a very simple case of the L.I.F. can give a surprising identity. For example, consider the polynomial $P(x) = x^2$, and choose any three distinct numbers a, b, c. Then according to L.I.F. we have

$$x^2 = \frac{(x-a)(x-b)}{(c-a)(c-b)}c^2 + \frac{(x-a)(x-c)}{(b-a)(b-c)}b^2 + \frac{(x-c)(x-b)}{(a-c)(a-b)}a^2.$$

Example 6.7. Let x, y, z be distinct real numbers. Prove that:

(i) $$\frac{x^2}{(x-y)(x-z)} + \frac{y^2}{(y-z)(y-x)} + \frac{z^2}{(z-x)(z-y)} = 1;$$

(ii) $$\frac{x^2yz}{(x-y)(x-z)} + \frac{y^2xz}{(y-z)(y-x)} + \frac{z^2xy}{(z-x)(z-y)} = 0;$$

(iii) $$\frac{x^2(y+z)}{(x-y)(x-z)} + \frac{y^2(x+z)}{(y-z)(y-x)} + \frac{z^2(x+y)}{(z-x)(z-y)} = 0.$$

Solution. Let $P(t) = t^2$. Write the L.I.F. for the polynomial $P(t)$ and the real numbers x, y, z. This reads

$$t^2 = \frac{x^2(t-z)(t-y)}{(x-y)(x-z)} + \frac{y^2(t-z)(t-x)}{(y-z)(y-x)} + \frac{z^2(t-y)(t-x)}{(z-x)(z-y)}.$$

Examining the coefficient of t^2 on both sides, we have that

$$1 = \frac{x^2}{(x-y)(x-z)} + \frac{y^2}{(y-z)(y-x)} + \frac{z^2}{(z-x)(z-y)}.$$

Furthermore, for part (ii), examining the constant term on both sides of our main identity, we find that

$$0 = \frac{x^2yz}{(x-y)(x-z)} + \frac{y^2xz}{(y-z)(y-x)} + \frac{z^2xy}{(z-x)(z-y)}.$$

Finally, examining the coefficient of t on both sides, we get

$$0 = \frac{x^2(y+z)}{(x-y)(x-z)} + \frac{y^2(x+z)}{(y-z)(y-x)} + \frac{z^2(x+y)}{(z-x)(z-y)}.$$ ■

Example 6.8. Find all distinct positive integers x, y, z such that

$$\frac{x^2(x+y)(x+z)}{(x-y)(x-z)} + \frac{y^2(z+y)(x+y)}{(y-z)(y-x)} + \frac{z^2(z+x)(z+y)}{(z-x)(z-y)} = 2160 + (x+y-z)^2.$$

Solution. First, we write $(x+y)(x+z)$ as $x(x+y+z)+yz$. Therefore the left-hand side of the equation is equal to

$$\frac{x^3(x+y+z)}{(x-y)(x-z)} + \frac{y^3(x+y+z)}{(y-z)(y-x)} + \frac{z^3(x+y+z)}{(z-x)(z-y)}$$

$$+ \frac{x^2yz}{(x-y)(x-z)} + \frac{y^2xz}{(y-z)(y-x)} + \frac{z^2xy}{(z-x)(z-y)}.$$

Since

$$\frac{x^2yz}{(x-y)(x-z)} + \frac{y^2xz}{(y-z)(y-x)} + \frac{z^2xy}{(z-x)(z-y)} = 0,$$

the problem is reduced to computing the following expression:

$$\frac{x^3(x+y+z)}{(x-y)(x-z)} + \frac{y^3(x+y+z)}{(y-z)(y-x)} + \frac{z^3(x+y+z)}{(z-x)(z-y)}.$$

For this reason, we shall find

$$\frac{x^3}{(x-y)(x-z)} + \frac{y^3}{(y-z)(y-x)} + \frac{z^3}{(z-x)(z-y)}.$$

Note that

$$\frac{x^3}{(x-y)(x-z)}+\frac{y^3}{(y-z)(y-x)}+\frac{z^3}{(z-x)(z-y)}$$

$$=(x+y+z)\left(\frac{x^2}{(x-y)(x-z)}+\frac{y^2}{(y-z)(y-x)}+\frac{z^2}{(z-x)(z-y)}\right)$$

$$-\left(\frac{x^2(y+z)}{(x-y)(x-z)}+\frac{y^2(x+z)}{(y-z)(y-x)}+\frac{z^2(x+y)}{(z-x)(z-y)}\right).$$

Since

$$\frac{x^2}{(x-y)(x-z)}+\frac{y^2}{(y-z)(y-x)}+\frac{z^2}{(z-x)(z-y)}=1,$$

$$\frac{x^2(y+z)}{(x-y)(x-z)}+\frac{y^2(x+z)}{(y-z)(y-x)}+\frac{z^2(x+y)}{(z-x)(z-y)}=0,$$

we get

$$\frac{x^3}{(x-y)(x-z)}+\frac{y^3}{(y-z)(y-x)}+\frac{z^3}{(z-x)(z-y)}=x+y+z.$$

Therefore

$$\frac{x^3(x+y+z)}{(x-y)(x-z)}+\frac{y^3(x+y+z)}{(y-z)(y-x)}+\frac{z^3(x+y+z)}{(z-x)(z-y)}=(x+y+z)^2.$$

Hence we must solve the equation

$$(x+y+z)^2=2160+(x+y-z)^2.$$

Thus

$$4z(x+y)=2160.$$

Hence $z(x+y)=540=2^2\cdot 3^3\cdot 5$. Now it is easy to solve the above system in positive integers (though the number of solutions is quite large). ■

6.3 Comparing leading coefficients

After writing the L.I.F. for an arbitrary polynomial

$$P(x)=a_dx^d+\ldots+a_0$$

we can compare the corresponding coefficients to get more identities. This extra step disguises the L.I.F. and can lead to even more surprising identities. For example, by examining the leading coefficients, we find the following result.

Theorem

$$a_d=\frac{P(x_0)}{(x_0-x_1)\cdot\ldots\cdot(x_0-x_d)}+\ldots+\frac{P(x_d)}{(x_d-x_0)\cdot\ldots\cdot(x_d-x_{d-1})}.$$

Don't underestimate the above identity, you will see how it is applicable in a variety of occasions.

Example 6.9. Compute the value of the following expression:

$$\frac{(a+b-c)^2}{(a-c)(b-c)}+\frac{(c+b-a)^2}{(b-a)(c-a)}+\frac{(c+a-b)^2}{(a-b)(c-b)}.$$

Solution. Consider the polynomial $P(x)=(a+b+c-2x)^2$. Then

$$P(a)=(c+b-a)^2,\quad P(b)=(c+a-b)^2,\quad P(c)=(a+b-c)^2.$$

Therefore the leading coefficient formula leads to the following identity:

$$\begin{aligned}4&=\frac{P(a)}{(a-b)(a-c)}+\frac{P(b)}{(b-a)(b-c)}+\frac{P(c)}{(c-a)(c-b)}\\&=\frac{(a+b-c)^2}{(a-c)(b-c)}+\frac{(c+b-a)^2}{(b-a)(c-a)}+\frac{(c+a-b)^2}{(a-b)(c-b)}.\end{aligned}$$

■

Example 6.10. Let p be a prime number. For a polynomial $f(x)$ with integer coefficients, there is a permutation $a_1,\ldots,a_p$ of the set $\{0,1,\ldots,p-1\}$ such that $f(a_i)\equiv 2^{p-i} \pmod p$. Prove that $\deg f\geq p-1$.

Solution. Assume on the contrary, that $\deg f(x) < p-1$. We write the L.I.F. for the polynomial $f(x)$ and the points $0, \ldots, p-1$, which reads

$$f(x) = \frac{Q_0(x)}{Q_0(0)} f(0) + \ldots + \frac{Q_{p-1}(x)}{Q_{p-1}(p-1)} f(p-1).$$

Considering the leading coefficients, we find that the coefficient of x^{p-1} on the right-hand side must be zero. That is,

$$\frac{f(0)}{Q_0(0)} + \ldots + \frac{f(p-1)}{Q_{p-1}(p-1)} = 0.$$

From the definition, we see that

$$\begin{aligned} Q_k(k) &= (k-0)(k-1)\cdot\ldots\cdot(k-(k-1))(k-(k+1))\cdot\ldots\cdot(k-(p-1)) \\ &= (-1)^{p-1-k}(p-k-1)!k!. \end{aligned}$$

Hence multiplying the above identity by $(-1)^{p-1}(p-1)!$, we get

$$\binom{p-1}{0} f(0) - \binom{p-1}{1} f(1) + \cdots + (-1)^{p-1}\binom{p-1}{p-1} f(p-1) = 0.$$

Since it is a well-known fact that

$$\binom{p-1}{k} = (-1)^k \pmod{p},$$

we find that

$$f(0) + \ldots + f(p-1) \equiv 0 \pmod{p}.$$

But, on the other hand, the hypothesis says that the numbers $f(0), \ldots, f(p-1)$, in some order, are congruent to 2^{p-i} modulo p. Hence

$$f(0) + \ldots + f(p-1) \equiv 1 + 2 + \ldots + 2^{p-1} = 2^p - 1 \equiv 1 \pmod{p},$$

a contradiction. ■

Example 6.11. Let $Q(x) = (x-x_1)\cdot\ldots\cdot(x-x_d)$ and $Q_i(x) = \dfrac{Q(x)}{x-x_i}$. Prove that

$$\sum_{i=1}^{d} \frac{x_i^d}{Q_i(x_i)} = \sum_{i=1}^{d} x_i.$$

Solution. Consider the polynomial

$$P(x) = x^d - Q(x) = x^d - (x-x_1)\cdot\ldots\cdot(x-x_d).$$

Then $\deg P(x) \le d-1$ and $P(x_i) = x_i^d$. Writing the L.I.F. for $P(x)$ and $x_1, \ldots, x_d$, we find that

$$P(x) = \sum_{i=1}^{d} \frac{Q_i(x)}{Q_i(x_i)} x_i^d.$$

Examining the coefficients of x^{d-1} on both sides, we get

$$\sum_{i=1}^{d} x_i = \sum_{i=1}^{d} \frac{x_i^d}{Q_i(x_i)}.$$ ■

Remark. We can go one step farther with the above solution. Examining the coefficients of x^{d-1} on both sides, we find that

$$\sum_{1\le i<j\le d} x_i x_j = \sum_{i=1}^{d} \frac{S-x_i}{Q_i(x_i)} x_i^d,$$

where $S = \sum_{i=1}^{d} x_i$. From this and the problem above, we find that

$$\sum_{i=1}^{d} \frac{x_i^{d+1}}{Q_i(x_i)} = S^2 - \sum_{1\le i<j\le d} x_i x_j = \sum_{i=1}^{d} x_i^2 + \sum_{1\le i<j\le d} x_i x_j.$$

Example 6.12. Let k be positive integer and

$$b_i = (a_i - a_1)\cdot\ldots\cdot(a_i - a_{i-1})(a_i - a_{i+1})\cdot\ldots\cdot(a_i - a_n),$$

where $a_1, \ldots, a_n$ are distinct integers. Prove that $\sum_{i=1}^{n} \frac{a_i^k}{b_i}$ is an integer.

Solution. Define $Q(x) = (x - a_1) \cdot \ldots \cdot (x - a_n)$ and $Q_i(x) = \frac{Q(x)}{x - a_i}$. Notice that $b_i = Q_i(a_i)$. Since $Q(x)$ is monic, we can do long division by $Q(x)$ to write

$$x^k = Q(x)S(x) + T(x),$$

where $S(x)$ and $T(x)$ are polynomials with integer coefficients and

$$\deg T(x) < n.$$

(If $k < n$, then we will of course have $S(x) = 0$ and $T(x) = x^k$.) Putting $x = a_1, \ldots, a_n$ in the above equality, we find that

$$T(a_i) = a_i^k, \quad i = 1, \ldots, n.$$

Now, we write the L.I.F. for $T(x)$ and $a_1, \ldots, a_n$, which gives

$$T(x) = \sum_{i=1}^{n} \frac{Q_i(x)}{Q_i(a_i)} a_i^k.$$

Taking the coefficient of x^{n-1}, we see that

$$\sum_{i=1}^{n} \frac{a_i^k}{Q_i(a_i)} = \sum_{i=1}^{n} \frac{a_i^k}{b_i}$$

is equal to the x^{n-1} coefficient of $T(x)$ and is therefore an integer. ■

Example 6.13. Let $a_0, \ldots, a_d$ be pairwise distinct complex numbers. Find all $z_1, \ldots, z_d$ satisfying

$$\sum_{j=0}^{d} z_j a_j^k = \begin{cases} 0, & \text{if } k = 0, 1, \ldots, d-1, \\ 1, & \text{if } k = d. \end{cases}$$

Solution. Let

$$Q_0(x) = (x - a_1) \cdot \ldots \cdot (x - a_d) = x^d - s_{d-1}x^{d-1} + \ldots + (-1)^d s_0.$$

Multiply the first equation (i.e., $\sum_{j=0}^{d} z_j = 0$) by $(-1)^d s_0$, the second by $(-1)^{d-1} s_1$, and the last one by 1. Then adding all of them, we find that

$$z_0 Q_0(a_0) + z_1 Q_0(a_1) + \ldots + z_d Q_0(a_d) = 1.$$

Since $Q_0(a_1) = \ldots = Q_0(a_d) = 0$, we get

$$z_0 = \frac{1}{Q_0(a_0)} = \frac{1}{(a_0 - a_1) \cdot \ldots \cdot (a_0 - a_d)}.$$

Analogously, if we define $Q(x) = (x - a_0) \cdot \ldots \cdot (x - a_d)$ and $Q_i(x) = \frac{Q(x)}{x - a_i}$, we have

$$z_k = \frac{1}{Q_k(a_k)} = \frac{1}{(a_k - a_0) \cdot \ldots \cdot (a_k - a_d)}.$$

On the other hand, writing L.I.F. for the polynomial x^k, $0 \le k \le d$ and numbers $a_0, \ldots, a_d$, we get the following equality:

$$x^k = \sum_{i=0}^{d} \frac{Q_i(x)}{Q_i(a_i)} a_i^k.$$

By checking the coefficient of x^d in x^k (which is zero for $0 \le k \le d-1$ and is 1 for $k = d$), we find that

$$\sum_{i=0}^{d} \frac{a_i^k}{Q_i(a_i)} = \begin{cases} 0, & \text{if } k = 0, 1, \ldots, d-1, \\ 1, & \text{if } k = d. \end{cases}$$ ■

Example 6.14. Let $n \ge 2$ and $z_1, \ldots, z_n$ be distinct nonzero complex numbers. Prove that

$$\sum \frac{1}{z_1(z_1 - z_2) \cdot \ldots \cdot (z_1 - z_n)} = \frac{(-1)^{n-1}}{z_1 \cdot \ldots \cdot z_n}.$$

Solution. Write the L. I. F for the polynomial $P(x) = 1$ at points $z_1, \ldots, z_n$. It follows that

$$1 = \sum \frac{(x - z_2) \cdot \ldots \cdot (x - z_n)}{(z_1 - z_2) \cdot \ldots \cdot (z_1 - z_n)}.$$

Examining the constant terms on both sides, we find that

$$1 = \sum \frac{(-1)^{n-1} z_2 \cdot \ldots \cdot z_n}{(z_1 - z_2) \cdot \ldots \cdot (z_1 - z_n)}.$$

Hence after dividing both sides by $(-1)^{n-1} z_1 \cdot \ldots \cdot z_n$ the result follows. ■

Example 6.15. Let $R(x) = a_0 + \ldots + a_{p-1}x^{p-1}$ be a polynomial with integer coefficients, where p is an odd prime number. We know that p doesn't divide $R(a) - R(b)$ whenever p doesn't divide $a - b$. Prove that a_{p-1} is divisible by p.

Solution. The hypothesis that p doesn't divide $R(a) - R(b)$ whenever p doesn't divide $a - b$, means that the numbers $R(0), R(1), \ldots, R(p-1)$ are all in different congruence classes modulo p. Since there are p of these, there must be exactly one in each congruence class. (In this case, one says that $\{R(0), \ldots, R(p-1)\}$ forms a complete residue system mod p.) In particular, this means that

$$\sum_{i=0}^{p-1} R(i) \equiv 0 + 1 + \ldots + p - 1 = \frac{p(p-1)}{2} \equiv 0 \pmod{p}.$$

Note that, if we write the L.I.F. for $R(x)$ and $0, 1, \ldots, p-1$, we get

$$R(x) = \sum_{i=0}^{p-1} \frac{Q_i(x)}{Q_i(i)} R(i).$$

Therefore comparing the leading coefficients, we find that

$$a_{p-1} = \sum_{i=0}^{p-1} \frac{R(i)}{Q_i(i)}.$$

Since $Q_i(i) = (-1)^i i!(p-1-i)!$, this implies

$$(p-1)! a_{p-1} = \sum_{i=0}^{p-1} (-1)^i \binom{p-1}{i} R(i).$$

Since $\binom{p-1}{i} \equiv (-1)^i \pmod{p}$, we find that

$$(p-1)! a_{p-1} \equiv \sum_{i=0}^{p-1} R(i) \pmod{p}.$$

Since Wilson's theorem says that $(p-1)! \equiv -1 \pmod{p}$, we get

$$a_{p-1} \equiv -\sum_{i=0}^{p-1} R(i) \pmod{p}.$$

Therefore $a_{p-1} \equiv 0 \pmod{p}$. ■

Remark 1. The proof of the preceding example proves a very interesting result, so it is worth highlighting it. The proof shows that if $R(x)$ is any polynomial of degree at most $p-1$ with integer coefficients and a_{p-1} is the x^{p-1} coefficient of $R(x)$, then

$$\sum_{i=0}^{p-1} R(i) \equiv -a_{p-1} \pmod{p}.$$

For the special cases of the polynomials $R(x) = 1, x, \ldots, x^{p-1}$, we get

$$\sum_{i=0}^{p-1} i^k \equiv \begin{cases} 0, & \text{if } k = 0, \ldots, p-2 \\ -1, & \text{if } k = p-1 \end{cases} \pmod{p}.$$

Conversely, since any polynomial of degree at most $p-1$ is a linear combination these polynomials, this special case implies the general formula.
This result (and an extension to higher powers) can be easily proved using primitive roots, and we will give another proof in the next chapter using Newton's Identities.

Remark 2. Part of what is going on here is that there the L.I.F. modulo p for polynomials of degree $p-1$ and the points $0, 1, \ldots, p-1$ is a very special case. Recall that the key step in our proof of the L.I.F. was to build a polynomial $\frac{Q_i(x)}{Q_i(r_i)}$ of degree d which vanished the d points not equal to r_i and was equal to 1 at r_i. Working modulo p and with the points $0, 1, \ldots, p-1$, Fermat's Little Theorem gives us a novel way to find such a polynomial. Specifically, if we look at $x - i$, then this is equal to 0 if $x = i$ and otherwise it is relatively prime to p. Hence by Fermat's Little Theorem we have

$$(x-i)^{p-1} \equiv \begin{cases} 0, & x = i \\ 1, & x = 0, 1, \ldots, i-1, i+1, \ldots, p-1 \end{cases} \pmod{p}.$$

Thus the polynomial $1-(x-i)^{p-1}$ is congruent to 1 at $x = i$ and is congruent to 0 at the other points. Thus

$$P(x) = \sum_{i=0}^{p-1} a_i (1 - (x-i)^{p-1})$$

is a polynomial of degree at most $p-1$ with integer coefficients, such that $P(i) \equiv a_i \pmod{p}$, for $i = 0, \ldots, p-1$.

To illustrate the first Remark, here is a nice Chinese Mathematical Olympiad problem, which follows quickly from it.

Example 6.16. Let p be an odd prime number and $a_1, \ldots, a_p$ be integers. Prove that if there exists a polynomial $P(x)$ with integer coefficients of degree at most $\frac{p-1}{2}$ such that $P(i) \equiv a_i \pmod{p}$ for all $1 \leq i \leq p$, then for any $d \leq \frac{p-1}{2}$ we have

$$\sum_{i=1}^{p} (a_{i+d} - a_i)^2 \equiv 0 \pmod{p},$$

where the indices are taken modulo p.

Chinese Mathematical Olympiad 2016

Solution. Since $P(x)$ is a polynomial with integer coefficients, $P(i+p) \equiv P(i) \pmod{p}$. Therefore instead of interpreting the indices as cyclic in the above formula, we can just look at the sum

$$\sum_{i=1}^{p} (P(i+d) - P(i))^2 \equiv \sum_{i=1}^{p} (a_{i+d} - a_i)^2 \pmod{p}.$$

Let $Q(x) = P(x+d+1) - P(x+1)$. Then $Q(x)$ is a polynomial of degree at most $\frac{p-3}{2}$ with integer coefficients. Hence we can write

$$Q(x)^2 = a_{p-3}x^{p-3} + a_{p-4}x^{p-4} + \cdots + a_0,$$

for some integers a_k. Summing over x and using Remark 1 above, we find that

$$\sum_{i=1}^{p} (P(i+d) - P(i))^2 = \sum_{i=0}^{p-1} Q(i)^2 = \sum_{k=0}^{p-3} a_k \sum_{i=0}^{p-1} i^k \equiv 0 \pmod{p}.$$

Remark. One can prove that the converse to this result. That is, if for any $d \leq \frac{p-1}{2}$ we have

$$\sum_{i=1}^{p} (a_{i+d} - a_i)^2 \equiv 0 \pmod{p},$$

then there exists a polynomial $P(x)$ with integer coefficients of degree at most $\frac{p-1}{2}$ such that $P(i) \equiv a_i \pmod{p}$ for all $1 \leq i \leq p$. We will prove this in the next volume of the polynomial book.

We continue this section with a good example that has strong implications for the irreducibility of polynomials with integer coefficients.[1]

Example 6.17. Let $Q(x)$ be a monic polynomial of degree d and let $x_0, \ldots, x_d$ be distinct integers. Prove that

$$\max_{0 \leq i \leq d} |Q(x_i)| \geq \frac{d!}{2^d}.$$

G. Polya

[1] See for example, *Problems from the book*, Chapter 21, practice problem 16, pp. 515.

Solution. Assume without loss that $x_0 < x_1 < \cdots < x_d$. Writing the L.I.F. for the polynomial $Q(x)$ and the points $x_0, \ldots, x_d$, and comparing leading coefficients on both sides, we get

$$1 = \frac{Q(x_0)}{(x_0 - x_1) \cdot \ldots \cdot (x_0 - x_d)} + \ldots + \frac{Q(x_d)}{(x_d - x_0) \cdot \ldots \cdot (x_d - x_{d-1})}.$$

Taking the modulus on both sides and using the triangle inequality, it follows that

$$1 \leq \frac{|Q(x_0)|}{|(x_0 - x_1) \cdot \ldots \cdot (x_0 - x_d)|} + \ldots + \frac{|Q(x_d)|}{|(x_d - x_0) \cdot \ldots \cdot (x_d - x_{d-1})|}$$

$$\leq \max_{0 \leq i \leq d} |Q(x_i)| \left(\frac{1}{|(x_0 - x_1) \cdot \ldots \cdot (x_0 - x_d)|} + \ldots + \frac{1}{|(x_d - x_0) \cdot \ldots \cdot (x_d - x_{d-1})|} \right).$$

Since $|(x_i - x_1) \cdot \ldots \cdot (x_i - x_d)| \geq i!(d-i)!$, s gives

$$1 \leq \max_{0 \leq i \leq d} |Q(x_i)| \left(\frac{1}{0!d!} + \frac{1}{1!(d-1)!} + \ldots + \frac{1}{d!0!} \right).$$

That is,

$$d! \leq \max_{0 \leq i \leq d} |Q(x_i)| \left(\frac{d!}{0!d!} + \frac{d!}{1!(d-1)!} + \ldots + \frac{d!}{d!0!} \right)$$

$$= \max_{0 \leq i \leq d} |Q(x_i)| \left(\binom{d}{0} + \ldots + \binom{d}{d} \right) = 2^d \cdot \max_{0 \leq i \leq d} |Q(x_i)|.$$

Whence

$$\max_{0 \leq i \leq d} |Q(x_i)| \geq \frac{d!}{2^d}.$$

■

We end this section with two number theoretic problems that would be difficult to solved without the L.I.F.

Example 6.18. Let $k \geq 2$. Find the largest number of divisors of $\binom{n}{k}$ that may be among the numbers $n - k + 1, \ldots, n$.

Romanian Team Selection Test 2015

Solution. If we let $n = k!$, then we see that

$$\binom{k!}{k} = (k! - 1)(k! - 2) \cdot \ldots \cdot (k! - (k-1)).$$

Hence $n - 1, \ldots, n - k + 1$ all divide $\binom{n}{k}$. Thus we can have $k - 1$ divisors among the k numbers listed. The tricky part of this problem is proving that we cannot have all k being divisors, which we will do with a clever use of the L.I.F..
Let

$$Q(x) = x(x-1) \cdot \ldots \cdot (x-k+1), \quad Q_j(x) = \frac{Q(x)}{x - j}, \quad j = 0, 1 \ldots, k-1.$$

The L.I.F. for the constant polynomial $P(x) = 1$ at the points $0, \ldots, k-1$, reads

$$1 = \sum_{j=0}^{k-1} \frac{Q_j(x)}{Q_j(j)}.$$

We compute $Q_j(j) = (-1)^{k-j-1} j!(k-j-1)!$ and

$$Q_j(n) = \frac{n(n-1) \cdot \ldots \cdot (n-k+1)}{n-j} = \frac{k!}{n-j} \binom{n}{k}.$$

Therefore this formula gives

$$\frac{1}{k} = \frac{1}{k} \sum_{j=0}^{k-1} \frac{Q_j(n)}{Q_j(j)} = \sum_{j=0}^{k-1} (-1)^{k-j-1} \binom{k-1}{j} \cdot \frac{1}{n-j} \binom{n}{k}.$$

The left-hand side is not an integer, therefore at least one of $\frac{1}{n-j}\binom{n}{k}$ is not an integer. Therefore the number of divisors is at most $k - 1$. ■

Example 6.19. Let $d > 1$ be an integer and let $a_1, \ldots, a_{d+1}$ be distinct positive integers. Does there exist a polynomial $P(x)$ with integer coefficients of degree at most d that satisfies the following conditions?

(i) For all $1 \leq i < j \leq d+1$, $\gcd(P(a_i), P(a_j)) > 1$.

(ii) For all $1 \leq i < j < k \leq d+1$, $\gcd(P(a_i), P(a_j), P(a_k)) = 1$.

Mojtaba Zare - Iranian Team Selection Test 2018

Solution. Let $b_{i,j}$ for $1 \leq i, j \leq d+1$ be positive integers such that for every i, j, k, l with $\{i, j\} \neq \{k, l\}$ we have $\gcd(b_{i,j}, b_{k,l}) = 1$ and $b_{i,j} = b_{j,i}$. According to the L.I.F., there is a polynomial $P(x)$ with rational coefficients of degree at most d such that

$$P(a_i) = \prod_{j=1}^{d+1} b_{i,j}.$$

For each $1 \leq i \leq d+1$, we have

$$\gcd(P(a_i), P(a_j)) = b_{i,j} > 1,$$

$$\gcd(P(a_i), P(a_j), P(a_k)) = \gcd(b_{i,j}, P(a_k)) = 1.$$

Hence it suffices to prove that the above-mentioned polynomial can be chosen to have integer coefficients. To do so we will impose one more condition on the numbers $b_{i,j}$. Note that

$$P(x) = \sum_{i=1}^{d+!} \frac{Q_i(x)}{Q_i(a_i)} P(a_i).$$

Define $c = Q_1(a_1) \ldots Q_{d+1}(a_d)$, and further assume that $b_{i,j} \equiv 1 \pmod{c}$, for each i, j. Then $P(a_i) \equiv 1 \pmod{c}$, so we can write $P(a_i) = 1 + cd_i$ for some integer d_i. Note that

$$P(x) = \sum_{i=1}^{d+!} \frac{Q_i(x)}{Q_i(a_i)} P(a_i) = \sum_{i=1}^{d+!} \frac{Q_i(x)}{Q_i(a_i)} (1 + cd_i) = \sum_{i=1}^{d+!} \frac{Q_i(x)}{Q_i(a_i)} + c \sum_{i=1}^{d+!} \frac{Q_i(x)}{Q_i(a_i)} d_i$$

Since $c = Q_1(a_1) \cdot \ldots \cdot Q_{d+1}(a_d)$, we find that $c \sum_{i=1}^{d+!} \frac{Q_i(x)}{Q_i(a_i)} d_i$ has integer coefficients. Furthermore, $\sum_{i=1}^{d+!} \frac{Q_i(x)}{Q_i(a_i)}$ is the L.I.F. for the polynomial 1. Therefore

$$\sum_{i=1}^{d+!} \frac{Q_i(x)}{Q_i(a_i)} = 1.$$

Hence the polynomial

$$P(x) = 1 + c \sum_{i=1}^{d+!} \frac{Q_i(x)}{Q_i(a_i)} d_i$$

has integer coefficients and satisfies the desired conditions. ∎

6.4 A useful special case

Part of the power of the Lagrnage Interpolation Formula is that it applies for any set of points, but there is one particular case that arise more often than all the others and it is worth writing down this special case in some detail. Suppose $P(x) = a_d x^d + \ldots + a_0$ is a polynomial of degree at most d. When we write the L.I.F. for the points $0, 1, \ldots, d$, we get

$$P(x) = \sum_{i=0}^{d} \frac{Q_i(x)}{Q_i(i)} P(i),$$

where $Q(x) = x(x-1) \cdot \ldots \cdot (x-d)$ and $Q_i(x) = \frac{Q(x)}{x-i}$ for $i = 0, \ldots d$. In this case we compute

$$Q_i(i) = i \cdot (i-1) \cdot \ldots \cdot (i-(i-1)) \cdot (i-(i+1)) \cdot \ldots \cdot (i-d) = (-1)^{d-i} i!(d-i)!.$$

Hence the formula simplifies to

$$P(x) = \sum_{i=0}^{d} (-1)^{d-i} \binom{d}{i} P(i) \cdot \frac{x(x-1) \cdot \ldots \cdot (x-d)}{d!(x-i)}.$$

If we further restrict to (large) positive integer values for x, we can write this even more succinctly as

$$P(n) = \sum_{i=0}^{d} \frac{(-1)^{d-i}}{n-i} \binom{d}{i} \binom{n}{d} P(i).$$

Special case of the L.I.F.

For each polynomial $P(x)$ of degree at most d, we have

$$P(x) = \sum_{i=0}^{d} (-1)^{d-i} \binom{d}{i} P(i) \cdot \frac{x(x-1)\cdot\ldots\cdot(x-d)}{d!(x-i)}$$

and hence for positive integer $n > d$,

$$P(n) = \sum_{i=0}^{d} \frac{(-1)^{d-i}}{n-i} \binom{d}{i} \binom{n}{d} P(i).$$

A truly remarkable identity arises if we assume $P(x)$ has degree at most $d-1$ and taking the x^d coefficients of both sides

Lemma

For each polynomial $P(x)$ of degree at most $d-1$, we have

$$\sum_{i=0}^{d} (-1)^i \binom{d}{i} P(i) = 0.$$

This identity is very useful, since it shows that many very complicated looking sums actually vanish. We will see some examples of this below.
We saw this identity before in Section 3.6, but the L.I.F. has the nice feature of deriving it in one step rather than inductively. Because of the similarity between this easiest case of the L.I.F. and Section 3.6, we will see that many of the results below can also be proved using induction and the methods of that section.

Example 6.20. Let $a \geq 3$ and let $P(x)$ be a polynomial with real coefficients of degree d. Prove that

$$\max_{0\leq i\leq d+1} |a^i - P(i)| \geq \left(\frac{a-1}{2}\right)^d.$$

First Solution. Assume on the contrary, that

$$|a^i - P(i)| < \left(\frac{a-1}{2}\right)^d$$

for each $i = 0, 1, \ldots, d+1$. This means that

$$a^i - \left(\frac{a-1}{2}\right)^d < P(i) < a^i + \left(\frac{a-1}{2}\right)^d$$

for each $i = 0, 1, \ldots, d+1$. Note that we can rewrite this inequality as

$$(-1)^i a^i - \left(\frac{a-1}{2}\right)^d < (-1)^i P(i) < (-1)^i a^i + \left(\frac{a-1}{2}\right)^d.$$

Hence summing we get

$$\sum_{i=0}^{d+1} \binom{d+1}{i} \left[(-1)^i a^i - \left(\frac{a-1}{2}\right)^d\right] < \sum_{i=0}^{d+1} (-1)^i \binom{d+1}{i} P(i)$$
$$< \sum_{i=0}^{d+1} \binom{d+1}{i} \left[(-1)^i a^i + \left(\frac{a-1}{2}\right)^d\right].$$

From the Lemma above, we have

$$\sum_{i=0}^{d+1} (-1)^i \binom{d+1}{i} P(i) = 0,$$

and the sums on the ends can be done using the binomial theorem, so we get

$$(1-a)^{d+1} - 2^{d+1}\left(\frac{a-1}{2}\right)^d < 0 < (1-a)^{d+1} + 2^{d+1}\left(\frac{a-1}{2}\right)^d.$$

However, we can rewrite this as

$$(a-1)^{d+1} = |1-a|^{d+1} < 2(a-1)^d,$$

But, $a - 1 \geq 2$, so this is a contradiction. ■

Second Solution. There is a nice and interesting approach, based Section 3.6. We argue by induction on the degree d of $P(x)$. If $d = 0$, the result follows from the triangle inequality, since for $P(x) = c$ constant, we get

$$\max\{|1-c|, |a-c|\} \geq \frac{a-c+c-1}{2} = \frac{a-1}{2}.$$

Now, suppose the statement of problem holds true for all polynomials of degree at most $d-1$. Define

$$Q(x) = \frac{P(x+1) - P(x)}{a-1}.$$

We know that $\deg Q(x)$ is equal to $d-1$, so by the inductive hypothesis

$$|a^i - Q(x)| \geq \left(\frac{a-1}{2}\right)^{d-1}$$

for some $i, 0 \leq i \leq d$. If we substitute $Q(x)$ we can see that

$$|(P(i+1) - a^{i+1}) - (P(i) - a^i)| \geq \left(\frac{a-1}{2}\right)^{d-1} \cdot (a-1) = 2\left(\frac{a-1}{2}\right)^d.$$

Hence

$$\max\{|P(i+1) - a^{i+1}|, |P(i) - a^i|\} \geq \left(\frac{a-1}{2}\right)^d,$$

and we are done. ■

The first solution to the following example uses the Lemma above, and the second solution is another nice application of induction and Section 3.6. We would like that the reader learns these techniques thoroughly. However, we shall prove a slightly stronger result using some knowledge about Chebyshev polynomials in our third book.

Example 6.21. Let $P(x)$ be a polynomial of degree d for which $|P(x)| \leq 1$ for all $0 \leq x \leq 1$. Prove that

$$P\left(-\frac{1}{d}\right) \leq 2^{d+1} - 1.$$

First Solution. Let

$$R(x) = P\left(\frac{d-x}{d}\right).$$

Then for each $x \in [0, d]$ we have $|R(x)| \leq 1$ and we want to prove that

$$R(d+1) \leq 2^{d+1} - 1.$$

Since $R(x)$ has degree d, applying the Lemma for $d+1$ gives

$$\sum_{k=0}^{d+1} (-1)^{d+1-k} \binom{d+1}{k} R(k) = 0,$$

which we can rearrange to read

$$R(d+1) = \sum_{k=0}^{d} (-1)^{d-k} \binom{d+1}{k} R(k).$$

Hence

$$\begin{aligned} |R(d+1)| &= \left|\sum_{k=0}^{d} (-1)^{d-k} \binom{d+1}{k} R(k)\right| \\ &\leq \sum_{k=0}^{d} \binom{d+1}{k} |R(k)| \\ &\leq \sum_{k=0}^{d} \binom{d+1}{k} = 2^{d+1} - 1. \end{aligned}$$

■

Second Solution. Define $R(x)$ as in the first solution. We will prove the desired bound by induction on d. The case $d = 0$ is trivial. Assume that the inequality is true for all polynomials of degree less than or equal to $d-1$. Let $S(x) = \frac{1}{2}(R(x+1) - R(x))$. Then $\deg S(x) = d-1$ and for all $x \in [0, d-1]$, we have $|S(x)| \leq 1$. Hence by the induction hypothesis, we have $S(d) \leq 2^d - 1$. Since $R(d+1) = 2S(d) + R(d)$, we get

$$R(d+1) \leq 2^{d+1} - 2 + 1 = 2^{d+1} - 1,$$

and we are done. ■

Example 6.22. Let $P(x)$ be a polynomial with real coefficients with $\deg P < 2d$. Prove that

$$|P(d)| \le 2\sqrt{d}\max\{|P(0)|,\ldots,|P(d-1)|,|P(d+1)|,\ldots,|P(2d)|\}.$$

Komal

Solution. To solve this problem, we will need the well-known inequality

$$\binom{2d}{d} \ge \frac{2^{2d-1}}{\sqrt{d}}.$$

for $d \ge 1$. This inequality is easy to prove by induction on d. In the base case $d = 1$ it reads $2 \ge 2$, which is true. For the inductive step, we use the inequality $(2d-1)^2 \ge 4d(d-1)$ and then the inductive hypothesis to show that

$$\binom{2d}{d} = \frac{2(2d-1)}{d}\binom{2d-2}{d-1} \ge \frac{4\sqrt{d-1}}{\sqrt{d}}\binom{2d-2}{d-1} \ge \frac{2^{2d-1}}{\sqrt{d}}.$$

Turning to our problem, we rewrite the Lemma for degree $2d$, which reads

$$\sum_{i=0}^{2d}(-1)^i\binom{2d}{i}P(i) = 0,$$

as

$$\binom{2d}{d}P(d) = \sum_{i=0,i\ne d}^{2d}(-1)^{d-i-1}\binom{2d}{i}P(i).$$

Hence by triangle inequality,

$$\binom{2d}{d}|P(d)| = \left|\sum_{i=0,i\ne d}^{2d}(-1)^{d-i-1}\binom{2d}{i}P(i)\right| \le \sum_{i=0,i\ne d}^{2d}\binom{2d}{i}|P(i)|.$$

Let $M = \max\{|P(0)|,\ldots,|P(d-1)|,|P(d+1)|,\ldots,|P(2d)|\}$. Then the left-hand side is at most

$$M\sum_{i=0,i\ne d}^{2d}\binom{2d}{i} = M\left(2^{2d} - \binom{2d}{d}\right).$$

Hence using the inequality above,

$$|P(d)| \le \frac{2^{2d} - \binom{2d}{d}}{\binom{2d}{d}}M < \frac{2^{2d}}{\binom{2d}{d}}M \le 2\sqrt{d}M. \qquad \blacksquare$$

We finish this section with an example that was the substantial part of the solution of a recent USA TST problem. It uses the following notation. If m is an integer, then $(m \mod n)$ denotes the remainder after dividing m by n, which is a number in the set $\{0,1,\ldots,n-1\}$.

Example 6.23. The function $g(x)$ from $\{0,1,\ldots,n-1\}$ onto $\{0,1,\ldots,n-1\}$ is a bijective function such that the functions

$$(g(x)+x \mod n),\ldots,(g(x)+(p-1)x \mod n)$$

are all bijective for some odd prime p. Prove that for all $1 \le k \le p-1$ the number $k!\sum_{i=0}^{n-1} i^k$ is divisible by n.

Solution. If $h(x)$ is a bijective function from $\{0,1,\ldots,n-1\}$ to $\{0,1,\ldots,n-1\}$, then we have

$$\sum_{x=0}^{n-1}h(x)^k = \sum_{i=0}^{n-1}i^k,$$

since the terms in the two sums are the same but possibly reordered.
Hence from the bijectivity hypothesis of the problem, we find that for all $1 \le k \le p-1$,

$$\sum_{x=0}^{n-1}g(x)^k \equiv \sum_{x=0}^{n-1}(g(x)+x)^k \equiv \ldots \equiv \sum_{x=0}^{n-1}(g(x)+(p-1)x)^k \equiv \sum_{i=0}^{n-1}i^k \pmod n.$$

Now treat $(g(x)+yx)^k$ as a polynomial of degree k in the variable y.
Then our special case of the L.I.F. reads

$$(g(x)+yx)^k = \sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}(g(x)+jx)^k \cdot \frac{y(y-1)\cdot\ldots\cdot(y-k)}{k!(y-j)}.$$

Taking the coefficient of y^k on both sides, and multiplying through by $k!$, we get

$$k!x^k = \sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}(g(x)+jx)^k.$$

Summing over x, we get

$$k!\sum_{x=0}^{n-1}x^k = \sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}\sum_{x=0}^{n-1}(g(x)+jx)^k.$$

Hence by the result above, we get

$$k!\sum_{x=0}^{n-1}x^k \equiv \sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}\cdot\sum_{i=0}^{n-1}i^k = 0 \pmod{n},$$

where we have used the fact that since $k \geq 1$ the binomial theorem gives

$$\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j} = (1-1)^k = 0.$$

Hence for all $0 \leq k \leq p-1$, the number $k!\sum_{x=0}^{n-1}x^k$ is divisible by n. ■

6.5 The uniqueness/existence proofs

While the Lagrange Interpolation Formula is incredibly powerful, there are some problems where what matters is just the existence/uniqueness parts of the theorem and not the formula itself.
Let us see some examples.

Example 6.24. Let $d \geq 2$ be an integer. Find the total number of polynomials $Q(x)$ of degree at most $d-1$ such that

$$x(x-1)(x-2)\cdot\ldots\cdot(x-d)Q(x)+x^2+1 = f(x)^2$$

for some polynomial $f(x)$ with real coefficients.

Solution. Comparing degrees we see that the condition that $\deg Q(x) \leq d-1$ is equivalent to $\deg f(x) \leq d$. Thus the possible polynomials $f(x)$ are the polynomials of degree at most d such that there is some choice of signs for which $f(k) = \pm\sqrt{1+k^2}$ for $k = 0,\ldots,d$.
We have 2^{d+1} choices for the $d+1$ signs, and the L.I.F. implies that for each choice, we will get a unique polynomial $f(x)$ of degree at most d. Thus we have 2^{d+1} distinct polynomials $f(x)$. For any such $f(x)$, the polynomial $f(x)^2-x^2-1$ has roots at $x = 0,1,\ldots,d$, so the quotient

$$Q(x) = \frac{f(x)^2-x^2-1}{x(x-1)(x-2)\cdot\ldots\cdot(x-d)}$$

will be a polynomial $Q(x)$ of degree at most $d-1$. However, we must be careful that we want to count possibilities for $Q(x)$, and not for $f(x)$. If two polynomials $f_0(x)$ and $f_1(x)$ give the same polynomial $Q(x)$, then $f_0(x)^2 = f_1(x)^2$ and hence $f_1(x) = \pm f_0(x)$. We see that flipping all the signs on $f(0),\ldots,f(d)$ will replace $f(x)$ by its negative, and hence give the same $Q(x)$. Thus the 2^{d+1} possibilities for $f(x)$ split into 2^d pairs, each of which gives the same polynomial $Q(x)$. Thus the total number of $Q(x)$ is 2^d. ■

Example 6.25. Let $P(x) = (x-1)(x-2)(x-3)$. For how many polynomials $Q(x)$ there exists a polynomial $R(x)$ of degree 3 such that

$$P(Q(x)) = P(x)R(x)?$$

Solution. Note that

$$P(Q(x)) = (Q(x)-1)(Q(x)-2)(Q(x)-3) = R(x)(x-1)(x-2)(x-3).$$

Therefore

$$P(Q(1)) = P(Q(2)) = P(Q(3)).$$

Hence $Q(1), Q(2), Q(3) \in \{1,2,3\}$.
Moreover, it is easy to find that $\deg Q(x) = 2$. Now, we have 3^3 total possibilities for $Q(x)$. According to the L.I.F., each possibility produces a polynomial of degree at most 2. It is easy to check that $Q(x) = 1,2,3,x,4-x$ are the only nonquadratic polynomials produced from the set of choices. Therefore we have 22 different possibilities for $Q(x)$. ■

We continue this section with a good instructive example about applications of the L.I.F.

Example 6.26. Six members of the Italian team for the International Mathematical Olympiad are to be selected from 13 candidates. At the TST the candidates got scores $a_1, \ldots, a_{13}$ with $a_i \neq a_j$ whenever $i \neq j$. The team leader has already selected the 6 candidates he wants to put on the team. With this in mind, he constructs a polynomial $P(x)$ and he claims that $c_i = P(a_i)$ is the creative potential of candidate i, and that the team should be the six candidates with highest creative potential. Find the least possible d such that he can always find a polynomial $P(x)$ of degree not exceeding d such that the creative potential of all 6 already selected candidates is strictly more than that of remaining 7 candidates.

Solution. The answer is 12. First, we will show that $d \geq 12$.
Assume that the six selected candidates get scores 2, 4, 6, 8, 10, 12 and the other members get scores 1, 3, 5, 7, 9, 11, 13. For any polynomial $P(x)$ the coach wants there is a real number C greater than $P(1), P(3), \ldots, P(13)$, but less than $P(2), \ldots P(12)$. In this case, the polynomial $P(x) - C$ assumes values with opposite signs at the ends of the intervals $[i, i+1]$ for $i = 1, \ldots, 12$. Hence $P(x)$ has at least 12 distinct real roots, and therefore

$$\deg(P(x) - C) = \deg P(x) \geq 12.$$

Now, we will prove it is always possible to construct a polynomial of degree at most 12 satisfying the problem conditions. Let us arrange the numbers as $a_1 < a_2 < \ldots < a_{13}$. Now, we construct a polynomial that assumes positive values at the scores of the six already selected candidates and assumes negative values at other 7 scores. By the L.I.F. there is a polynomial of degree at most 12 with these values the coach can choose, and this polynomial will put his chosen candidates on the team. ■

Next examples have more subtle implications, that is finding a polynomial of degree d passing through d points in the plane. All of them have L.I.F. as an essential part in line with some adequate refinements.

Example 6.27. Prove that for any set of d ordered pairs of real numbers $(x_1, y_1), \ldots, (x_d, y_d)$ with $x_i \neq x_j$ for all $i \neq j$, there exists a unique monic polynomial with real coefficients of degree d such that $P(x_i) = y_i$ for all $i = 1, 2, \ldots, d$.

First Solution. By the L.I.F. there is a polynomial $Q(x)$ of degree at most $d-1$ such that $Q(x_i) = y_i$ for all $i = 1, 2, \ldots, d$. Then adding to this polynomial $(x - x_1) \cdot \ldots \cdot (x - x_d)$ we get a polynomial

$$P(x) = Q(x) + (x - x_1) \cdot \ldots \cdot (x - x_d)$$

which is monic, has degree d, and still passes through these d points. To prove uniqueness, assume we have another such polynomial $R(x)$. Then the polynomial $R(x) - P(x)$ has degree at most $d - 1$ and has d real roots. Hence $R(x) = P(x)$. ■

Second Solution. By the L.I.F. there is a unique polynomial $Q(x)$ of degree at most $d - 1$ such that $Q(x_i) = y_i - x_i^d$. Therefore if we choose

$$P(x) = Q(x) + x^d$$

we will get a monic polynomial of degree d that passes through all d points. Uniqueness is proved as in the first solution. ■

Example 6.28. A teacher gives the students a task of the following kind. He informs them that he has in mind a monic polynomial $P(x)$ of degree 2017 with integer coefficients. Then he tells them k integers $n_1, n_2, \ldots, n_k$ and also informs them of the value of the expression $P(n_1)P(n_2) \cdot \ldots \cdot P(n_k)$. The teacher then asks the students to find a polynomial that, according to this data, could be the one he has in mind. What is the smallest k such that the teacher can compose a task of this kind so that the polynomial found by the students must necessarily coincide with the one he has in mind?

Russian Mathematical Olympiad 2017

Solution. If $k \leq 2016$, write $Q(x) = P(x) + (x - n_1) \cdot \ldots \cdot (x - n_k)$. Then $Q(x)$ is monic, has $\deg Q(x) = 2017$, and $P(n_i) = Q(n_i)$ for each $i = 1, \ldots, k$. Thus

$$P(n_1)P(n_2) \cdot \ldots \cdot P(n_k) = Q(n_1)Q(n_2) \cdot \ldots \cdot Q(n_k),$$

hence $P(x)$ cannot be uniquely determined.
Now, we prove that $k = 2017$ works. Put $n_i = 4i$, $i = 1, \ldots, k$. Suppose the teacher chooses

$$P(x) = 1 + (x - n_1) \cdot \ldots \cdot (x - n_{2017}).$$

Then $P(n_1)P(n_2) \cdot \ldots \cdot P(n_k) = 1$. Suppose a student finds that the monic polynomial $Q(x)$ with integer coefficients of degree 2017 works. Then

$$Q(n_1)Q(n_2) \cdot \ldots \cdot Q(n_k) = 1,$$

so we must have $Q(n_i) = \pm 1$. If two different signs occur, then there are indices r, s with $1 \leq r, s \leq k$ such that $Q(n_r) = 1$, $Q(n_s) = -1$. Since $Q(x)$ has integer coefficients, we find that $n_r - n_s = 4(r - s)$ divides $Q(n_r) - Q(n_s) = 2$. Hence $4 \mid 2$, which is impossible. Thus all the $Q(n_r)$ are equal. Since they are all ± 1, there are an odd number of them, and their product is 1, we must have

$$Q(n_1) = Q(n_2) = \ldots = Q(n_k) = 1.$$

Hence $P(x) - Q(x)$ has 2017 distinct real roots but its degree is at most 2016. Thus $Q(x) = P(x)$, and so the student must have found the polynomial chosen by the teacher. ■

Example 6.29. Prove that every monic polynomial of degree d with real coefficients is the average of two monic polynomials of degree d with d real roots.

Titu Andreescu - USA Mathematical Olympiad 2002

Solution. Choose a strictly decreasing sequence of d real numbers $x_1 > \ldots > x_d$. For each odd i choose y_i such that $y_i < \min\{0, 2P(x_i)\} \leq 0$, and for each even i choose $y_i > \min\{0, 2P(x_i)\} \geq 0$. Let $R(x)$ be a monic polynomial of degree d such that

$$\deg R(x) = d, \quad R(x_i) = y_i.$$

Let $Q(x) = 2P(x) - R(x)$. Since $y_{2k} > 0 > y_{2k+1}$, the signs of $R(x)$ at the ends of each interval (x_{i+1}, x_i) are different, hence $R(x)$ has a root in the interval (x_{i+1}, x_i), for each $i = 1, \ldots, d - 1$. Moreover,

$$Q(x_{2k+1}) = 2P(x_{2k+1}) - y_{2k+1} > 0 > 2P(x_{2k}) - y_{2k} = Q(x_{2k}),$$

so $Q(x)$ also has a root in each interval (x_{i+1}, x_i). This forces $R(x)$ and $Q(x)$ to each have at least $d-1$ real roots. However, since complex roots must come in conjugate pairs and $\deg R(x) = \deg Q(x) = d$, this means that $R(x)$ and $Q(x)$ actually have d real roots each. Finally, $R(x)$ and $Q(x)$ average to $P(x)$ since

$$P(x) = \frac{Q(x) + R(x)}{2}.$$ ■

We continue this section by extending one corollary of the L.I.F. to rational functions.

Example 6.30. Prove that if a rational function that is not a polynomial assumes rational values at each positive integer point, then it is the quotient of two relatively prime polynomials with integer coefficients.

Solution. Let the rational function in question be

$$R(x) = \frac{P(x)}{Q(x)},$$

where $P(x)$ and $Q(x)$ are relatively prime polynomials.
Let $r = \deg P(x) + \deg Q(x)$. We prove the statement by induction on r.
For $r = 0$, $R(x)$ is constant and the problem is obvious.
Now we turn to the induction step. If $\deg Q(x) > \deg P(x)$, then we may consider $\frac{1}{R(x)}$ instead of $R(x)$. Thus we may assume that $\deg P(x) \geq \deg Q(x)$.
Look at

$$R_1(x) = \frac{R(x+1) - R(1)}{x}.$$

Since $R(1)$ is rational, $R_1(x)$ is a rational function that assumes rational values at each positive integer point. Since

$$R_1(x) = \frac{1}{Q(x+1)} \cdot \frac{P(x+1)Q(1) - Q(x+1)P(1)}{Q(1)x},$$

and the second factor is a polynomial, we see that we can write $R_1(x)$ as a quotient whose denominator $Q(x+1)$ has the same degree as $Q(x)$, but whose numerator has lower degree than $P(x)$. Thus by the induction hypothesis, we can write

$$R_1(x) = \frac{P_1(x)}{Q_1(x)},$$

where $P_1(x)$ and $Q_1(x)$ are relatively prime polynomials with integer coefficients. Writing $R(1) = \frac{p}{q}$ for integer p, q, we see that

$$R(x) = \frac{q(x-1)P_1(x-1) + pQ_1(x-1)}{qQ_1(x-1)}$$

is a quotient of two polynomials with integer coefficients. Furthermore, since $\gcd(P_1(x), Q_1(x)) = 1$, we have $\gcd(P_1(x-1), Q_1(x-1)) = 1$ and since $R(1)$ is rational we have $Q_1(0) \neq 0$. Thus the numerator and denominator are relatively prime polynomials. ■

Example 6.31. [2] Prove that there is a polynomial $P(x)$ of degree 99 with positive leading coefficient such that $0, \frac{1}{50}, \frac{2}{50}, \ldots, \frac{49}{50}, 1$ are roots of $P(x)$ and

$$P'\left(\frac{1}{50}\right) = P'\left(\frac{2}{50}\right) = \ldots = P'\left(\frac{49}{50}\right) = -1.$$

Solution. From the given list of roots we know that we can write

$$P(x) = Q(x)R(x)$$

with

$$Q(x) = x\left(x - \frac{1}{50}\right)\left(x - \frac{2}{50}\right) \cdot \ldots \cdot \left(x - \frac{49}{50}\right)(x-1)$$

[2] If you are not familiar with derivatives, you can skip this example.

and $R(x)$ a polynomial of degree 48. Note that

$$P'\left(\frac{i}{50}\right) = Q\left(\frac{i}{50}\right)P'\left(\frac{i}{50}\right) + Q'\left(\frac{i}{50}\right)R\left(\frac{i}{50}\right) = Q'\left(\frac{i}{50}\right)R\left(\frac{i}{50}\right).$$

Therefore

$$R\left(\frac{i}{50}\right) = \frac{P'\left(\frac{i}{50}\right)}{Q'\left(\frac{i}{50}\right)} = -\frac{1}{Q'\left(\frac{i}{50}\right)}, \quad i = 1, 2, \ldots, 49.$$

By the L.I.F., there is a unique polynomial $R(x)$ of degree at most 48 with these values, but we need to prove that $\deg R(x) = 48$. To see this, note that in the sequence $Q'\left(\frac{1}{50}\right), \ldots, Q'\left(\frac{49}{50}\right)$, we have 48 sign changes and hence $R(x)$ has at least 48 real roots. Thus $\deg R(x) \geq 48$, and so $R(x)$ has degree 48. ■

6.6 A novel interpretation of $\binom{x}{d}$

The standard expression for a polynomial $P(x) = a_d x^d + \cdots + a_0$ writes a polynomial as a linear combination of the polynomials $1, x, \ldots, x^{d-1}$. The L.I.F. writes a polynomial of degree at most d as a linear combination of certain polynomials of degree d, i.e.,

$$\frac{Q_i(x)}{Q_i(r_i)} = \frac{(x-r_1)\cdot\ldots\cdot\widehat{(x-r_i)}\cdot\ldots\cdot(x-r_d)}{(r_i-r_1)\cdot\ldots\cdot\widehat{(r_i-r_i)}\cdot\ldots\cdot(r_i-r_d)}.$$

(The hat here is a common notation telling you to omit one term in the product, the one with the hat.) Both of these representations tell us interesting things about the polynomial. In this section, we will consider a different representation. We will use the formula

$$\binom{x}{d} = \frac{x(x-1)\cdot\ldots\cdot(x-d+1)}{d!}$$

to view the binomial coefficient $\binom{x}{d}$ as a polynomial of degree d with rational coefficients. Then we would like to consider $P(x)$ as a linear combination of these polynomials. The first result says that we can always do this.

Example 6.32. Prove that every polynomial $P(x)$ of degree d can be written uniquely as

$$P(x) = a_0\binom{x}{0} + a_1\binom{x}{1} + a_2\binom{x}{2} + \ldots + a_d\binom{x}{d}$$

for some numbers $a_0, \ldots, a_d$.

Solution. First we will prove this by induction on the degree d of $P(x)$ that every polynomial has such a representation. For the base case, if $d = 0$, then $P(x) = C$ is a constant polynomial and we have $P(x) = C\binom{x}{0}$. For the inductive step, suppose every polynomial of degree less than d has such a representation. Write $P(x) = bx^d + Q(x)$, where $b \neq 0$ and $\deg Q(x) < d$. Then the polynomial

$$P(x) - d!b\binom{x}{d} = b\left(x^d - d!\binom{x}{d}\right) + Q(x)$$

has degree at most $d-1$. Hence by the inductive hypothesis we have

$$P(x) - d!b\binom{x}{d} = a_0\binom{x}{0} + a_1\binom{x}{1} + a_2\binom{x}{2} + \ldots + a_{d-1}\binom{x}{d-1},$$

and so defining $a_d = d!b$, we have

$$P(x) = a_0\binom{x}{0} + a_1\binom{x}{1} + a_2\binom{x}{2} + \ldots + a_d\binom{x}{d}.$$

To see that this representation is unique, suppose the contrary. Then there is some polynomial $P(x)$ which we can write in two different ways as

$$\begin{aligned} P(x) &= a_0\binom{x}{0} + a_1\binom{x}{1} + a_2\binom{x}{2} + \ldots + a_d\binom{x}{d} \\ &= b_0\binom{x}{0} + b_1\binom{x}{1} + b_2\binom{x}{2} + \ldots + b_d\binom{x}{d}. \end{aligned}$$

Then there is some largest index k such that $a_k \neq b_k$, and we have

$$0 = (a_0 - b_0)\binom{x}{0} + (a_1 - b_1)\binom{x}{1} + \ldots + (a_k - b_k)\binom{x}{k}.$$

Taking the coefficient of x^k on both sides, we find that

$$0 = \frac{a_k - b_k}{k!},$$

hence $a_k = b_k$, a contradiction. ■

Remark. We have been a little vague in the above argument about what the numbers a_i are. If $P(x)$ has rational, real, or complex coefficients, then the argument implies that the a_i are rational, real, or complex, respectively.

The cases where the a_i are integers and where $P(x)$ has integer coefficients do not quite align, but still they are interesting as the next two results show.

Example 6.33. Prove that if $P(x)$ is an integer-valued polynomial (i.e., $P(\mathbb{Z}) \subseteq \mathbb{Z}$) of degree d and

$$P(x) = a_0\binom{x}{0} + a_1\binom{x}{1} + a_2\binom{x}{2} + \ldots + a_d\binom{x}{d},$$

then a_i must be an integer for all $i = 0, 1, \ldots, d$.

Solution. Note that the converse to this example is something you already know. If the a_i are integers, then

$$P(n) = a_0\binom{n}{0} + a_1\binom{n}{1} + \ldots + a_d\binom{n}{d}$$

is an integer for any integer n. Hence

$$P(x) = a_0\binom{x}{0} + a_1\binom{x}{1} + \ldots + a_d\binom{x}{d}$$

is an integer-valued polynomial.

Now suppose $P(x)$ is an integer-valued polynomial and by the previous example write

$$P(x) = a_0\binom{x}{0} + a_1\binom{x}{1} + \ldots + a_d\binom{x}{d}.$$

Suppose on the contrary that the a_i are not all integers. Then there is some largest index k such that a_k is not an integer. Then

$$P(x) - a_{k+1}\binom{x}{k+1} - \ldots - a_d\binom{x}{d} = a_0\binom{x}{0} + a_1\binom{x}{1} + \ldots + a_k\binom{x}{k}.$$

All of $a_{k+1}, \ldots, a_d$ are integers, so the left-hand side is an integer-valued polynomial. However, if we plug in $x = k$, then the right-hand side becomes a_k, which is not an integer, a contradiction. Thus the a_i are all integers. ■

Example 6.34. If $P(x)$ is a polynomial with integer coefficients and

$$P(x) = a_0 + a_1\binom{x}{1} + a_2\binom{x}{2} + \ldots + a_d\binom{x}{d},$$

then each a_k is an integer and a multiple of $k!$.

Solution. As in the previous example, the converse is obvious since

$$k!\binom{x}{k} = x(x-1)\cdot\ldots\cdot(x-(k-1))$$

is a polynomial with integer coefficients.
Now suppose $P(x)$ has integer coefficients and write

$$P(x) = 0!b_0\binom{x}{0} + 1!b_1\binom{x}{1} + \ldots + d!b_d\binom{x}{d}.$$

Suppose on the contrary that the b_i are not all integers. Then there is some largest index k such that b_k is not an integer. Then

$$P(x) - (k+1)!b_{k+1}\binom{x}{k+1} - \ldots - d!b_d\binom{x}{d} = 0!b_0\binom{x}{0} + \ldots + k!b_k\binom{x}{k}.$$

All of $b_{k+1}, \ldots, b_d$ are integers, so the left-hand side is polynomial with integer coefficients, but the leading coefficient of the right-hand side is b_k, which is not an integer, a contradiction. Thus the b_i are all integers. ■

Example 6.35. Consider the set of integers $\{a_0, a_1, \ldots, a_d\}$.
Prove that there exists an integer-valued polynomial $P(x)$ of degree at most d such that $P(k) = a_k$ for all $k = 0, 1, \ldots, d$.

Solution. We shall prove the statement by induction on d. The base case $d = 0$ is easy, since we can just take $P(x) = a_0$. Now for the inductive step, suppose there exists a polynomial $P_1(x)$ of degree at most $d-1$ such that $P_1(k) = a_k$ for all $k = 0, 1, \ldots, d-1$. Setting

$$P(x) = P_1(x) + (a_d - P_1(d))\binom{x}{d}$$

gives a polynomial $P(x)$ of degree at most d with $P(k) = P_1(k) = a_k$ for $k = 0, 1, \ldots, d-1$, and with $P(d) = a_d$. This completes the proof. ■

Remark. This last example shows that the polynomials $\binom{x}{k}$ provide an alternative to the L.I.F. in the special case of points $0, 1, \ldots, d$, since they allow us to inductively build up polynomials with prescribed values. They have the advantage of giving formulas which are usually simpler than the L.I.F. formulas, but the disadvantage that the process is inductive instead of a single formula like the L.I.F. is.
There are a few special cases where with the binomial theorem we can write down the polynomials instantly. For example, the binomial formula shows that

$$1 + \binom{k}{1} + \binom{k}{2} + \ldots + \binom{k}{d} = 2^k$$

for all $k = 0, 1, \ldots, d$, hence

$$P(x) = 1 + \binom{x}{1} + \binom{x}{2} + \ldots + \binom{x}{d}$$

is a polynomial of degree d such that $P(k) = 2^k$ for all $k = 0, 1 \ldots, d$.
More generally,

$$P(x) = 1 + (a-1)\binom{x}{1} + (a-1)^2\binom{x}{2} + \ldots + (a-1)^d\binom{x}{d}$$

is a polynomial of degree d such that $P(k) = a^k$ for all $k = 0, 1 \ldots, d$.

Example 6.36. How many polynomials $P(x)$ of integer coefficients and degree at most 4 satisfy $0 \le P(x) < 72$ for all $x \in \{0, 1, 2, 3, 4\}$?

Solution. Write

$$P(x) = a_0 + a_1\binom{x}{1} + a_2\binom{x}{2} + a_3\binom{x}{3} + a_4\binom{x}{4}.$$

Since $P(x)$ has integer coefficients, Example 6.34 shows that $a_0, \ldots, a_4$ are integers, a_4 must be multiple of 24, a_3 must be a multiple of 6, and a_2 must be a multiple of 2.
Note that the conditions $0 \le P(x) < 72$ can be translated to the following inequalities:

$$0 \le a_0 < 72, \quad 0 \le a_0 + a_1 < 72, \quad 0 \le a_0 + 2a_1 + a_2 < 72,$$

$$0 \le a_0 + 3a_1 + 3a_2 + a_3 < 72, \quad 0 \le a_0 + 4a_1 + 6a_2 + 4a_3 + a_4 < 72.$$

We have 72 choices for a_0. Since $-a_0 \le a_1 < 72 - a_0$, we have 72 choices also for a_1. Since $-a_0 - 2a_1 \le a_2 < 72 - a_0 - 2a_1$ and a_2 must be even, we only have 36 choices for a_2. Since $-a_0 - 3a_1 - 3a_2 \le a_3 < 72 - a_0 - 3a_1 - 3a_2$ and a_3 is a multiple of 6, we only have 12 choices for a_3. Finally, since

$$-a_0 - 4a_1 - 6a_2 - 4a_3 \le a_4 < 72 - a_0 - 4a_1 - 6a_2 - 4a_3$$

and a_4 is a multiple of 24, we have only 3 choices for a_4. Thus the total number of choices is

$$72^2 \cdot 36 \cdot 12 \cdot 3 = 2592^2.$$

■

Example 6.37. Given that $P(x)$ is a real polynomial of degree at most 2012 that satisfies $P(n) = 2^n$ for all $n = 1, 2, \ldots, 2012$, what choice(s) of $P(0)$ produce(s) the minimum value of $P(0)^2 + P(2013)^2$?

Solution. Look at

$$P(x) - \left(1 + \binom{x}{1} + \binom{x}{2} + \ldots + \binom{x}{2012}\right).$$

This is a polynomial of degree at most 2012 and we compute that

$$P(1) = P(2) = \cdots = P(2012) = 0.$$

Therefore

$$P(x) = 1 + \binom{x}{1} + \binom{x}{2} + \ldots + \binom{x}{2012} + C(x-1)(x-2)\cdot\ldots\cdot(x-2012)$$

for some constant C.
Putting $x = 0$, we find that

$$P(0) = 1 + (-1)^{2012}2012! \cdot C = 1 + 2012! \cdot C,$$

and putting $x = 2013$, we get

$$P(2013) = 2^{2013} - 1 + 2012! \cdot C.$$

Hence

$$P(0)^2 + P(2013)^2 = (1 + 2012! \cdot C)^2 + (2^{2013} - 1 + 2012! \cdot C)^2.$$

This is a quadratic function of C, so we find that the minimum is achieved when

$$C = -\frac{2^{2012}}{(2012)!}$$

and this minimum is

$$P(0) = 2(2^{2012} - 1)^2.$$

■

Example 6.38. Prove that for each polynomial $P(x)$ there are polynomials $Q(x)$ and $R(x)$ such that

$$Q(R(x)) - R(Q(x)) = P(x).$$

Solution. The sneaky trick here is to just try $R(x) = x + 1$. Then the given equation reduces to $Q(x+1) - Q(x) = P(x) + 1$. We saw in Section 3.6 that we can always find a polynomial $Q(x)$ that satisfies this condition, so that solves the problem. However, with the notation of this section we can do much better by giving an explicit formula for $Q(x)$. The usual Pascal's triangle identity

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

holds for all positive integers k and $n \geq k$. Since this is infinitely values of n, we deduce that as polynomials

$$\binom{x+1}{k} = \binom{x}{k} + \binom{x}{k-1}.$$

This can also be easily checked by writing out the right-hand side and pulling out the common factors. Interpret this formula as saying that the polynomial $q(x) = \binom{x}{k}$ is a polynomial such that

$$q(x+1) - q(x) = \binom{x+1}{k} - \binom{x}{k} = \binom{x}{k-1}.$$

Then we have proven the following improvement on the result of Section 3.6:

Theorem

For any polynomial $P(x)$ of degree d, there is a polynomial $Q(x)$ of degree $d+1$ such that $Q(x+1) - Q(x) = P(x)$. In fact, if we write

$$P(x) = a_0\binom{x}{0} + a_1\binom{x}{1} + \ldots + a_d\binom{x}{d},$$

then the polynomials satisfying this are

$$Q(x) = C\binom{x}{0} + a_0\binom{x}{1} + a_1\binom{x}{2} + \ldots + a_d\binom{x}{d+1},$$

where C is an arbitrary constant.

Returning to our problem, this says that if we write

$$P(x) + 1 = b_0 + b_1\binom{x}{1} + \ldots + b_d\binom{x}{d},$$

then

$$R(x) = x + 1, \quad Q(x) = b_0\binom{x}{1} + b_1\binom{x}{2} + \ldots + b_d\binom{x}{d+1}$$

is a solution to the problem. ■

6.7 Proposed problems

Problem 6.1. Let $P(x)$ be a polynomial with integer coefficients of degree d such that for some prime $q > d$ we have $P(k) \equiv 0 \pmod{q}$ for all k. Prove that all the coefficients of $P(x)$ are divisible by q.

Problem 6.2. Prove that any polynomial

$$P(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$$

can be written as

$$P(z) = \frac{1}{n}\sum_{k=1}^{n} \omega_k P(\omega_k)\frac{z^n - 1}{z - \omega_k},$$

where $\omega_1, \omega_2, \ldots, \omega_n$ are the n-th roots of unity.

Radu Gologan

Problem 6.3. Let $Q(x)$ be a polynomial with real coefficients of degree d. Consider the real numbers $b_1 < \ldots < b_{d+1}$. Prove that the polynomial

$$f(x) = \sum_{i=1}^{d+1} a_i Q(x + b_i),$$

with $a_i = \prod_{i \neq j} \frac{1}{b_i - b_j}$, is constant.

Problem 6.4. Let $\sigma_m(x_1,\ldots,x_n)$ be the sum of all products of subsets of size m of $x_1,\ldots,x_n$. Let $m,k\geq 0$ be any integers with $m+k<n$ and let $x_1,\ldots,x_n$ be real numbers. Prove that

$$\sum_{i=1}^{n}\frac{x_i^k\sigma_m(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)}{\prod_{j\neq i}(x_i-x_j)}=\begin{cases}(-1)^m & m+k=n-1,\\ 0 & \text{otherwise.}\end{cases}$$

Problem 6.5. Let $a_1,\ldots,a_n$ be distinct real numbers. Consider arbitrary real numbers $b_1,\ldots,b_n$.

(i) Prove that if $b_i>0$, then there exists a polynomial $P(x)$ with real coefficients of degree less than $2n$ that has no real roots and $P(a_i)=b_i$.

(ii) Prove that there exists a polynomial $P(x)$ with real coefficients of degree less than $2n$ that has only real roots and $P(a_i)=b_i$.

Problem 6.6. Prove that there exists a polynomial P such that for all $k=1,2,\ldots,2019$, P assumes the value k at exactly k different points.

Chapter 7

Newton's Identities

7.1 Two forms of Newton's Identities

Suppose we are handed a polynomial $P(x)$ of degree d. As we have seen repeatedly, a very powerful way of studying $P(x)$ is to look at its roots, $r_1,r_2,\ldots,r_d$. This leads to the natural question: What interesting things can we build from the roots of $P(x)$?

There are of course innumerable things we could build from the roots, but some are just not natural, and therefore tend not to arise. For example, we could look at $r_1+2r_2+\cdots+dr_d$. We don't, because this depends on the order in which we right down the roots. Taking this as a principle, we should focus on functions of the roots that are symmetric, that is, which don't change when we reorder the roots. This still leaves a vast number of possibilities, so let's further restrict to the easiest sorts of functions, namely polynomials.

Thus by thinking about the roots of polynomials, we are somewhat naturally lead to the topic of symmetric polynomials. This turns out to be a huge subject within polynomials, and we won't have the space to do more than study a few simple symmetric polynomials. The symmetric polynomials one usual encounters first are the elementary symmetric polynomials, usually denoted $\sigma_k(x_1,x_2,\ldots,x_n)$. Informally, $\sigma_k(x_1,x_2,\ldots,x_n)$ is the sum of all monomials in the variables $x_1,x_2,\ldots,x_n$ which consist of products of k of these variables.

In formulas, we can write

$$\sigma_k(x_1, x_2, \ldots, x_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k},$$

or

$$\sigma_k(x_1, x_2, \ldots, x_n) = \sum_{I \subseteq \{1,2,\ldots,n\}, |I| = k} \prod_{i \in I} x_i.$$

The main reason one encounters these first is of course Vieta's formulas. If we further assume that $P(x)$ is monic, then we have

$$P(x) = (x - r_1)(x - r_2) \cdot \ldots \cdot (x - r_d) = x^d - \sigma_1 x^{d-1} + \cdots + (-1)^d \sigma_d,$$

where $\sigma_k = \sigma_k(r_1, r_2, \ldots, r_d)$ are the elementary symmetric polynomials in the roots.

Vieta's formulas give us one answer to the question we asked above. We can easily find the value of any elementary symmetric polynomial in the roots of $P(x)$. Indeed, we can read them off almost instantly from the coefficients of $P(x)$. The only problem with the elementary symmetric polynomials is that they can get quite large. If we write out $\sigma_k(x_1, x_2, \ldots, x_n)$ completely, then we will get $\binom{n}{k}$ terms and the binomial coefficients grow pretty fast. A few moments of thought will lead you to another set of symmetric polynomials which avoid this problem, the power sums

$$S_k(x_1, x_2, \ldots, x_n) = x_1^k + x_2^k + \cdot \ldots \cdot + x_n^k.$$

These are just n terms and still give us one polynomial of every possible total degree. (By convention, one often sets $\sigma_0(x_1, x_2, \ldots, x_n) = 1$ and $S_0(x_1, x_2, \ldots, x_n) = n$.)

The topic of this chapter is basically to understand how these two lists of elementary symmetric polynomials relate. Given the elementary symmetric polynomials, we could obviously write down the polynomial $P(x)$ above, find its roots, and then calculate S_k. Is there a better way to get S_k from σ_k? What about the other direction, if we know the S_k, can we find σ_k? The answer is that we can, and the way we will go from one to the other are Newton's identities.

We already saw one very special case of Newton's identities back in Chapter 2. We showed that we can write $x^k + \frac{1}{x^k}$ as a polynomial in $x + \frac{1}{x}$. The first few steps of this were

$$x^2 + \frac{1}{x^2} = \left(x + \frac{1}{x}\right)^2 - 2, \quad x^3 + \frac{1}{x^3} = \left(x + \frac{1}{x}\right)^3 - 3\left(x + \frac{1}{x}\right),$$

and for larger k, we could use the recursion

$$x^{k+1} + \frac{1}{x^{k+1}} = \left(x + \frac{1}{x}\right)\left(x^k + \frac{1}{x^k}\right) - \left(x^{k-1} + \frac{1}{x^{k-1}}\right).$$

This lead us to a family of polynomials $T_k(x)$ such that

$$T_k\left(x + \frac{1}{x}\right) = x^k + \frac{1}{x^k}.$$

So now let's take this idea and use it to derive Newton's identities for the special case of two variables. Call the two variables a, b. Then the elementary symmetric polynomials are $\sigma_1 = a + b$ and $\sigma_2 = ab$, and we want formulas for $S_k = a^k + b^k$. We can implement the same approach as above. We can certainly find formulas for S_k for small k. We have $S_0 = 2$ (by convention), $S_1 = a + b = \sigma_1$, and you probably are already aware that

$$S_2 = a^2 + b^2 = (a + b)^2 - 2ab = \sigma_1^2 - 2\sigma_2.$$

To extend this list, we define a monic quadratic polynomial $P(x)$ with roots a and b, that is,

$$P(x) = (x - a)(x - b) = x^2 - (a + b)x + ab = x^2 - \sigma_1 x + \sigma_2.$$

Then since a and b are roots of $P(x)$, we have

$$a^2 = \sigma_1 a - \sigma_2, \quad b^2 = \sigma_1 b - \sigma_2.$$

Now multiplying the first equality by a^{k-1} and the second equality by b^{k-1} yields

$$a^{k+1} = \sigma 1 a^k - \sigma_2 a^{k-1}, \quad b^{k+1} = \sigma_1 b^k - \sigma_2 b^{k-1}.$$

Adding these equalities side by side, we find that

$$S_{k+1} = \sigma_1 S_k - \sigma_2 S_{k-1}.$$

Thus we could inductively write down formulas for each S_k as a polynomial in σ_1 and σ_2 (with integer coefficients). The next few are

$$S_3 = \sigma_1 S_2 - \sigma_2 S_1 = \sigma_1^3 - 3\sigma_1\sigma_2,$$

and

$$S_4 = \sigma_1 S_3 - \sigma_2 S_2 = \sigma_1^4 - 4\sigma_1\sigma_2 + 2\sigma_2^2.$$

Example 7.1. Let c and d be complex numbers. What can be said about

$$T_k = ca^k + db^k?$$

Solution. Multiply the equality $a^{k+1} = \sigma_1 a^k - \sigma_2 a^{k-1}$ by c and the equality $b^{k+1} = \sigma_1 b^k - \sigma_2 b^{k-1}$ by d and add them side by side. The result is

$$T_{k+1} = \sigma_1 T_k - \sigma_2 T_{k-1}.$$

Surprisingly, T_k satisfies the same recursion as S_k. (As you may suspect, there is something deeper going on here. In this case, the theory of constant coefficient linear recursions.) ■

Let's generalize this one more step, to three variables.
If we have variables a, b, c, then the elementary symmetric polynomials are $\sigma_1 = a+b+c$, $\sigma_2 = ab+ac+bc$, $\sigma_3 = abc$. Can we do the same thing we did before and find polynomial formulas for $S_k = a^k + b^k + c^k$? The answer is yes! Again, we can find a few starting values $S_0 = 3$, $S_1 = \sigma_1$, and as you are doubtless aware we still have

$$S_2 = a^2 + b^2 + c^2 = (a+b+c)^2 - 2(ab+bc+ca) = \sigma_1^2 - 2\sigma_2.$$

So as for the two-variable case, it would suffice to find a recursive formula for S_k. Define the polynomial

$$P(x) = (x-a)(x-b)(x-c) = x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3.$$

Then $a^3 = \sigma_1 a^2 - \sigma_2 a + \sigma_3$, and the same holds for b and c. Multiplying the first equality by a^{k-2}, the second equality by b^{k-2} and the last one by c^{k-2}, and adding all three, we find that

$$S_{k+1} = \sigma_1 S_k - \sigma_2 S_{k-1} + \sigma_3 S_{k-2}.$$

Thus we can write each S_k as a polynomial with integer coefficients in $\sigma_1, \sigma_2, \sigma_3$. The next two are

$$S_3 = \sigma_1 S_2 - \sigma_2 S_1 + \sigma_3 S_0 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3,$$

$$S_4 = \sigma_1 S_3 - \sigma_2 S_2 + \sigma_3 S_1 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3.$$

Example 7.2. If $\sigma_3 \neq 0$, can we similarly find the value of

$$S_{-k} = a^{-k} + b^{-k} + c^{-k}$$

for some positive integer k?

First Solution. The answer is of course yes. Multiplying the equality

$$a^3 = \sigma_1 a^2 - \sigma_2 a + \sigma_3$$

by a^{-1}, we get

$$a^2 = \sigma_1 a - \sigma_2 + \sigma_3 a^{-1}.$$

Adding the three similar equalities we get

$$S_2 = \sigma_1 S_1 + \sigma_2 S_0 + \sigma_3 S_{-1}.$$

Therefore S_{-1} can be determined in terms of S_2, S_1, S_0. By the same approach, after multiplying the equality

$$a^3 = \sigma_1 a^2 - \sigma_2 a + \sigma_3$$

by a^{-k-2} and adding the two similar equalities side by side, we find that

$$S_{-k-1} = \sigma_1 S_{-k} - \sigma_2 S_{-k+1} + \sigma_3 S_{-k+2}.$$

Thus we find that S_{-k} are rational functions in $\sigma_1, \sigma_2, \sigma_3$, and in fact the denominator is always σ_3^k. ■

Second Solution. The answer is of course yes. For positive k, we used the polynomial

$$P(x) = (x-a)(x-b)(x-c) = x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3.$$

For negative k, we simply use the reciprocal polynomial

$$-\frac{x^3}{\sigma_3} P\left(\frac{1}{x}\right) = \left(x - \frac{1}{a}\right)\left(x - \frac{1}{b}\right)\left(x - \frac{1}{c}\right) = x^3 - \frac{\sigma_2}{\sigma_3}x^2 + \frac{\sigma_1}{\sigma_3}x - \frac{1}{\sigma_3}. \quad \blacksquare$$

Example 7.3. Let a, b, c be real numbers and $S_n = a^n + b^n + c^n$. It is known that $S_1 = 2$, $S_2 = 6$, $S_3 = 14$. Show that $|S_n^2 - S_{n-1}S_{n+1}| = 8$ for each positive integer $n > 1$.

Solution. By the formulas above

$$\sigma_1 = S_1 = 2, \quad \sigma_2 = \frac{1}{2}(\sigma_1^2 - S_2) = -1, \quad \sigma_3 = -\frac{1}{3}(\sigma_1 S_2 - S_3 - \sigma_1\sigma_2) = 0.$$

Therefore $abc = 0$. Assume without loss that $c = 0$. Then

$$\begin{aligned} S_n^2 - S_{n-1}S_{n+1} &= (a^n + b^n)^2 - (a^{n+1} + b^{n+1})(a^{n-1} + b^{n-1}) \\ &= (ab)^{n-1}(2ab - a^2 - b^2) \\ &= -(ab)^{n-1}(a-b)^2 \\ &= -(ab)^{n-1}((a+b)^2 - 4ab). \end{aligned}$$

Note that $\sigma_2 = ab = -1$, $S_1 = a + b = 2$, so $(a-b)^2 = (a+b)^2 - 4ab = 8$. Therefore

$$-(ab)^{n-1}((a+b)^2 - 4ab) = 8 \cdot (-1)^n.$$

That is, $|S_n^2 - S_{n-1}S_{n+1}| = 8$. $\blacksquare$

Example 7.4. How about $T_k = c_1 a^k + c_2 b^k + c_3 c^k$ for some complex numbers c_1, c_2, c_3?

Solution. Multiplying the equality $a^{k+1} = \sigma_1 a^k - \sigma_2 a^{k-1} + \sigma_3 a^{k-2}$ by c_1, the equality $b^{k+1} = \sigma_1 b^k - \sigma_2 b^{k-1} + \sigma_3 b^{k-2}$ by c_2 and the equality $c^{k+1} = \sigma_1 c^k - \sigma_2 c^{k-1} + \sigma_3 c^{k-2}$, by c_3, and adding them side by side, we find that

$$T_{k+1} = \sigma_1 T_k - \sigma_2 T_{k-1} + \sigma_3 T_{k-2}. \quad \blacksquare$$

Example 7.5. Let a, b, c be positive real numbers such that

$$abc = 1, \quad a^3 + b^3 + c^3 = 4.$$

Prove that

$$\frac{a^5}{(a-b)(a-c)} + \frac{b^5}{(b-c)(b-a)} + \frac{c^5}{(c-a)(c-b)} = 5 + (a^2b + b^2c + c^2a + a^2c + b^2a + c^2b).$$

Solution. Let $T_n = (c-b)a^n + (a-c)b^n + (b-a)c^n$. As we have just seen, T_n satisfies the recursion

$$T_{n+3} = \sigma_1 T_{n+2} - \sigma_2 T_{n+1} + \sigma_3 T_n.$$

Since $T_0 = T_1 = 0$ and $T_2 = (a-b)(b-c)(c-a)$, we compute that

$$T_3 = \sigma_1 T_2,$$

$$T_4 = \sigma_1 T_3 - \sigma_2 T_2 = \sigma_1^2 T_2 - \sigma_2 T_2,$$

and

$$T_5 = \sigma_1 T_4 - \sigma_2 T_3 + \sigma_3 T_2 = (\sigma_1^3 - 2\sigma_1\sigma_2 + \sigma_3) T_2.$$

Thus we compute

$$\frac{a^5}{(a-b)(a-c)} + \frac{b^5}{(b-c)(b-a)} + \frac{c^5}{(c-a)(c-b)} = \frac{a^5(c-b) + b^5(a-c) + c^5(b-a)}{(a-b)(b-c)(c-a)} = \frac{T_5}{T_2} = \sigma_1^3 - 2\sigma_1\sigma_2 + \sigma_3.$$

Since $a^3+b^3+c^3 = S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$, and we compute that

$$\begin{aligned} a^2b+b^2c+c^2a+a^2c+b^2a+c^2b &= a^2(\sigma_1-a)+b^2(\sigma_1-b)+c^2(\sigma_1-c) \\ &= \sigma_1 S_2 - S_3 = \sigma_1\sigma_2 - 3\sigma_3, \end{aligned}$$

we have

$$\begin{aligned} \frac{T_5}{T_2} &= \sigma_1^3 - 2\sigma_1\sigma_2 + \sigma_3 = (S_3+\sigma_3)+(\sigma_1\sigma_2-3\sigma_3) \\ &= 5+(a^2b+b^2c+c^2a+a^2c+b^2a+c^2b). \end{aligned}$$

So we are done. ■

Having done the cases of 2 and 3 variables, it is time to see what we can do with the general case. It should be clear how the derivation of the recursion generalizes to more variables. Let $z_1,\ldots,z_n$ be complex numbers and define $S_k = z_1^k+\ldots+z_n^k$. The monic polynomial

$$P(x) = (x-z_1)\cdot\ldots\cdot(x-z_n) = x^n - \sigma_1 x^{n-1} + \ldots + (-1)^n\sigma_n$$

vanishes at each z_k, therefore multiplying by z_k^r, we get

$$z_k^{n+r} = \sigma_1 z_k^{n+r-1} - \sigma_2 z^{n+r-2} + \cdots + (-1)^{n-1}\sigma_n z_k^r.$$

Adding these n equalities for $k = 1,2,\ldots,n$, we get

$$S_{n+r} = \sigma_1 S_{n+r-1} - \sigma_2 S_{n+r-2} + \ldots + (-1)^{n-1}\sigma_n S_r.$$

This is one form of Newton's identities

Newton's Identities - First Form

Let S_k and σ_k be the power sum and elementary symmetric polynomials in n variables. Then

$$S_{n+r} = \sigma_1 S_{n+r-1} - \sigma_2 S_{n+r-2} + \ldots + (-1)^{n-1}\sigma_n S_r.$$

The same argument as in the preceding example also gives the following result:

Theorem

Let $c_1,\ldots,c_n$ be complex numbers, σ_k the elementary symmetric polynomials in n variables $z_1,\ldots,z_n$, and let $T_k = c_1z_1^k+\ldots+c_nz_n^k$. Then for each non-negative integer r,

$$T_{n+r} = \sigma_1 T_{n+r-1} - \sigma_2 T_{n+r-2} + \ldots + (-1)^{n-1}\sigma_n T_r.$$

Example 7.6. Let $P(x) = x^6-x^5-x^3-x^2-x+1$ and $Q(x) = x^4-x^3-x^2-1$. If $z_1,\ldots,z_4$ are roots of $Q(x)$, find the value of $P(z_1)+P(z_2)+P(z_3)+P(z_4)$.

Solution. Note that $P(x) = Q(x)(x^2+1)+x^2+2$. Therefore $P(z_i) = z_i^2+2$. Hence

$$\begin{aligned} P(z_1)+P(z_2)+P(z_3)+P(z_4) &= 8+\sum_{i=1}^4 z_i^2 \\ &= 8+S_2 \\ &= S_1\sigma_1 - 2\sigma_2 \\ &= 1+2 \\ &= 3. \end{aligned}$$ ■

It is great that we found a recursion for the power sums, but to exploit this recursion, we also need some initial values. We could derive a few of these. We always have $S_1 = \sigma_1$, and we know that

$$S_1 = \sigma_1, \quad S_2 = z_1^2+\ldots+z_n^2 = (z_1+\ldots+z_n)^2 - 2\sum_{1\le i<j\le n} z_iz_j = \sigma_1^2 - 2\sigma_2.$$

You might even be able to compute that for $n \ge 3$,

$$\begin{aligned} S_3 = z_1^3+\ldots+z_n^3 &= (z_1+\ldots+z_n)^3 - 3(z_1+\ldots+z_n)\left(\sum_{1\le i<j\le n} z_iz_j\right) \\ &\quad + 3\sum_{1\le i<j<k\le n} z_iz_jz_k = \sigma_1^3 - 3\sigma_2\sigma_1 + 3\sigma_3. \end{aligned}$$

Unfortunately, the formulas are starting to get a little long. The thing you will very quickly notice is that we are getting the same formulas for S_k with $k > 0$, as long as $n \geq k$.

Let's suppose for a second that this is always true. For $n = k$, we proved the formula

$$S_k = \sigma_1 S_{k-1} - \sigma_2 S_{k-2} + \ldots + (-1)^k \sigma_{k-1} S_1 + (-1)^{k+1} k \sigma_k,$$

where we have written k instead of S_0 because something weird is happening with S_0. If we already have $S_1, \ldots, S_{k-1}$ as polynomials in the σ_i, then this will give us S_k as such a polynomial. If it really is the same polynomial for every n, then we have the following educated guess:

Newton's Identities - Second Form

Let S_i and σ_i be the power sum and elementary symmetric polynomials in $n \geq k$ variables. Then

$$S_k = \sigma_1 S_{k-1} - \sigma_2 S_{k-2} + \ldots + (-1)^k \sigma_{k-1} S_1 + (-1)^{k+1} k \sigma_k.$$

Guessing the correct answer is often a big step towards a proof, but now we have to prove this formula. We will give three proofs. First, let's give a combinatorial proof. The advantage to this proof is that it really dives in and shows how the terms align.

Proof. (Combinatorial proof) Writing out the formula we are trying to prove

$$S_k - \sigma_1 S_{k-1} + \sigma_2 S_{k-2} + \ldots + (-1)^{k-1} \sigma_{k-1} S_1 + (-1)^k k \sigma_k = 0,$$

we get

$$\sum_{r=0}^{k-1} (-1)^r \left(\sum_{1 \leq i_1 < \ldots < i_r \leq n} z_{i_1} \ldots z_{i_r} \right) \left(\sum_{j=1}^{n} z_j^{k-r} \right)$$
$$+ (-1)^k k \left(\sum_{1 \leq i_1 < \ldots < i_k \leq n} z_{i_1} \ldots z_{i_k} \right) = 0.$$

Now think about the monomials that occur. First, let us focus on monomials where one variable occurs with an exponent greater than 1. These can only arise from the first sum. For a subset $A \subset \{1, 2, \ldots, n\}$, let $Z_A = \prod_{a \in A} z_a$. Then the monomials coming from the first sum have the form $Z_A z_j^{k-r}$ for some subset A with $|A| = r < k$. An exponent greater than 1 means that either $k - r > 1$ or $k - r = 1$ and $j \in A$. In fact, from this we see that there is a little ambiguity here, since we may have $j \in A$. Let's remove this by insisting that $j \notin A$, which we can always arrange by removing j from A and raising the exponent of z_j. Thus we only need to think about monomials $z_A z_j^{k-|A|}$, where $|A| = s < k - 1$ is a set that does not contain j. Such a monomial can arise in only two ways in the sum above. It could come from the $r = s$ term in the first sum, when $i_1 < i_2 < \cdots < i_r$ are the elements of A. The coefficient of such a monomial is $(-1)^r$. It could also arise from the $r = s + 1$ term in the first sum, when $i_1 < i_2 < \cdots < i_{r+1}$ are the elements of A and also j. The coefficient of such a monomial is $(-1)^{r+1}$. Thus this monomial arises exactly twice with opposite signs, hence they cancel.

Now consider a monomial where every exponent is equal to 1. Any such monomial is Z_A for some set $A \subset \{1, 2, \ldots, n\}$ with $|A| = k$. These can arise in two ways. They could come from the first sum in the case where $r = k - 1$ and $i_1 < i_2 < \cdots < i_{k-1}$ are all but one of the elements of A, and the missing element comes from the $\sigma_1 = z_1 + z_2 + \cdots + z_n$ factor. There are k such terms, one for each element of A, and they all occur with a sign of $(-1)^{k-1}$, so the total contribution of these terms is $(-1)^{k-1} k$. These terms also arise from the second sum, where of course they have the cancelling coefficient $(-1)^k k$. Thus these terms cancel as well.

Since we have shown that every monomial that occurs cancels, it follows that the whole sum is 0, as desired. ❑

Now let's give an algebraic proof. This proof has the advantage of justifying our intuition above. We were not just guessing the answer above, we were proving it but didn't know that yet.

Proof. (Algebraic proof) Let $S_k = z_1^k + z_2^k + \cdots + z_n^k$ and let

$$R_k = \sigma_1 S_{k-1} - \sigma_2 S_{k-2} + \ldots + (-1)^k \sigma_{k-1} S_1 + (-1)^{k+1} k \sigma_k$$

be the polynomial given by the recursion. Note that R_k is a polynomial in the variables $z_1, \ldots, z_n$, but because of the recursion we can also think of R_k as a polynomial in the elementary symmetric functions $\sigma_i(z_1, z_2, \ldots, z_n)$ for $i \leq k$. We want to prove that $S_k = R_k$.

Look at what happened to the elementary symmetric function $\sigma_i(z_1, z_2, \ldots, z_n)$ when we set one of the variables, say z_n, to zero. Every monomial involving z_n vanishes. Hence we are just left with monomials with i out of the variables $z_1, z_2, \ldots, z_{n-1}$. Thus

$$\sigma_i(z_1, z_2, \ldots, z_{n-1}, 0) = \sigma_i(z_1, z_2, \ldots, z_{n-1}).$$

This says something very nice about R_k. If we set any $n-k$ of the variables $z_1, \ldots, z_n$ to zero, then R_k will be the polynomial that satisfies the recursion above for the remaining k variables. But this is the case were we have already proved the recursion for the Newton's identities. Thus if we set any $n-k$ variables equal to 0, leaving only the variables with indices $i_1 < i_2 < \cdots < i_k$, then

$$R_k = z_{i_1}^k + z_{i_2}^k + \cdots z_{i_k}^k = S_k.$$

Now suppose $S_k - R_k$ is nonzero. Then when we write it out, there will be some monomial that has a nonzero coefficient. Since every term in S_k and R_k has total degree k, this monomial must be $z_{i_1} z_{i_2} \cdots z_{i_k}$ for some $i_1 < i_2 < \cdots < i_k$. But then if we set all the other variables equal to 0 and these k variables to 1, all the other monomials will vanish and we will find that $S_k - R_k \neq 0$. But we just saw that in this case $S_k = R_k$, so this is a contradiction. So $S_k = R_k$. ❑

The proof above also says something important, that we already had observed but hadn't proven. There is really only one formula for S_k as a polynomial in the elementary symmetric polynomials σ_i. If the number of variables is at least k, then this is exactly the formula we get. If not, then we just set any σ_m with m larger than the number of variables to 0. So for example, from the general formula for S_3,

$$S_3 = \sigma_1^3 - 3\sigma_2\sigma_1 + 3\sigma_3,$$

we get the formula for two variables

$$a^3 + b^3 = (a+b)^3 - 3ab(a+b)$$

by just setting σ_3 to zero.

Finally we give a calculus proof. If you haven't had calculus, please feel free to skip this proof. Two proofs should be enough. However, the power series at the end, which you can think of as "infinite degree polynomials", provide fabulous identities you should be able to understand without calculus.

Proof. (Calculus proof) Consider the polynomial

$$Q(t) = (1 - z_1 t) \cdot \ldots \cdot (1 - z_n t) = 1 - \sigma_1 t + \sigma_2 t^2 - \ldots + (-1)^n \sigma_n t^n.$$

Then we compute

$$\begin{aligned} Q'(t) = &- z_1(1 - z_2 t) \cdot \ldots \cdot (1 - z_n t) - z_2(1 - z_1 t)(1 - z_3 t) \cdot \ldots \cdot (1 - z_n t) - \ldots \\ &- z_n(1 - z_2 t) \cdot \ldots \cdot (1 - z_{n-1} t) = -\sigma_1 + 2\sigma_2 t - \ldots + n(-1)^n \sigma_n t^{n-1}. \end{aligned}$$

Therefore

$$-\frac{tQ'(t)}{Q(t)} = \frac{tz_1}{1 - z_1 t} + \ldots + \frac{tz_n}{1 - z_n t} = \sum_{k=1}^{\infty} \left(\sum_{i=1}^{n} z_i^k \right) t^k = \sum_{k=1}^{\infty} S_k t^k.$$

Therefore

$$\sigma_1 t - 2\sigma_2 t^2 - \ldots + n(-1)^{n-1} \sigma_n t^n = (1 - \sigma_1 t + \sigma_2 t^2 - \ldots + (-1)^n \sigma_n t^n) \sum_{k=1}^{\infty} S_k t^k.$$

Comparing the coefficients of t^r on both sides, our educated guess is proved. This calculus proof is incredibly powerful. Pulling out the higher coefficients gives the previous result for S_{n+r} with $r \geq 0$. You can even go further. Dividing by t and integrating both sides, we get

$$-\log Q(t) = \sum_{k=1}^{\infty} \frac{S_k}{k} t^k.$$

If we plug in the Taylor series for the function $-\log(1-x)$, then we get

$$\sum_{k=1}^{\infty} \frac{S_k}{k} t^k = \sum_{m=1}^{\infty} \frac{1}{m} \left(\sigma_1 t - \sigma_2 t^2 + \cdots + (-1)^{n-1} t^n \right)^m.$$

If we take the coefficient of t^k in this formula, we get a non-recursive formula for S_k as a polynomial in the σ_i. If we exponentiate, then we get

$$Q(t) = \exp\left(-\sum_{k=1}^{\infty} \frac{S_k}{k} t^k\right) = \sum_{m=0}^{\infty} \frac{(-1)^m}{m!} \left(\sum_{k=1}^{\infty} \frac{S_k}{k} t^k\right)^m.$$

Taking the coefficient of t^k in this formula, we get a formula for the elementary symmetric polynomials in terms of the power sums. ❑

Remark. The identities

$$S_{n+r} = \sigma_1 S_{n+r-1} - \sigma_2 S_{n+r-2} + \ldots + (-1)^{n-1} \sigma_n S_r$$

for $r \geq 0$ and

$$S_k = \sigma_1 S_{k-1} - \sigma_2 S_{k-2} + \ldots + (-1)^k \sigma_{k-1} S_1 + (-1)^{k+1} k \sigma_k$$

for $n \geq k$ are called *Newton's Identities*. The interesting issue is that for $r = 0$, the former coincides to the latter for $k = n$. The algebraic and calculus proofs (and the combinatorial proof with a little more work) above show that you can just use the last formula for all k, with the convention that $\sigma_k = 0$ if k exceeds the number of variables.

Example 7.7. Let $r_1, \ldots, r_n$ be the roots of polynomial

$$x^n - 2x^{n-1} + 3x^{n-2} + \ldots + (-1)^n (n+1).$$

Prove that for all $m = 1, 2, \ldots, n$

$$r_1^m + \ldots + r_n^m = 2(-1)^{m-1}.$$

Solution. From Vieta's formulas we read off $\sigma_1 = S_1 = 2$, $\sigma_2 = 3$, ..., $\sigma_n = n + 1$. Hence Newton's Identities for $m \leq n$ read

$$S_m = 2S_{m-1} - 3S_{m-2} + \ldots + (-1)^m m S_1 + (-1)^{m+1} m(m+1).$$

An easy induction proof, with induction step,

$$S_m = (-1)^{m-2}(4 + 6 + \ldots + 2m - m(m+1)) = 2(-1)^{m-1}.$$

shows that $S_i = 2(-1)^{i-1}$ for $i = 1, \ldots, m-1$. ■

Example 7.8. Let $P(x)$ be a monic polynomial of degree n, with integer coefficients and d complex roots $z_1, \ldots, z_n$. Prove that $S_k = z_1^k + \ldots + z_n^k$ is an integer for each k.

Solution. This was really all proved above, but it is important enough to be worth emphasizing. Since $P(x)$ is monic with integer coefficients, Vieta's formulas say that all the elementary symmetric polynomials σ_k are all integers. However, Newton's identities imply that each power sum is a polynomial with integer coefficients in the σ_k. Hence all the power sums are also integers. ■

7.2 Newton's Identity and number theory: elementary problems

Example 7.9. Let n be an integer and let a, b, c, d be integers such that

$$a + b + c + d \text{ and } a^2 + b^2 + c^2 + d^2$$

are divisible by n. Prove that

$$n \mid (a^4 + b^4 + c^4 + d^4 + 4abcd).$$

Solution. Let

$$P(x) = (x-a)(x-b)(x-c)(x-d) = x^4 - \sigma_1 x^3 + \sigma_2 x^2 - \sigma_3 x + \sigma_4.$$

We know that $S_1 = \sigma_1$ and S_2 are divisible by n. Now by Newton's Identities, we have

$$S_4 = \sigma_1 S_3 - \sigma_2 S_2 + \sigma_3 S_1 - 4\sigma_4.$$

Hence reducing modulo n, we get

$$S_4 \equiv -4\sigma_4 \pmod{n}.$$

Therefore n divides $S_4 + 4\sigma_4 = a^4 + b^4 + c^4 + d^4 + 4abcd$. ■

Example 7.10. Let p be an odd prime numbers and a, b, c, d, e be integers such that $a+b+c+d+e$ and $a^2+b^2+c^2+d^2+e^2$ are divisible by p. Prove that $a^5+b^5+c^5+d^5+e^5-5abcde$ is divisible by p.

Solution. Let

$$(x-a)(x-b)(x-c)(x-d)(x-e) = x^5 - \sigma_1 x^4 + \sigma_2 x^3 - \sigma_3 x^2 + \sigma_4 x - \sigma_5.$$

We know that $S_1 = \sigma_1$ and $S_2 = S_1^2 - 2\sigma_2$ are divisible by p. Hence σ_1 and σ_2 are divisible by p. According to Newton's Identities

$$S_5 = \sigma_1 S_4 - \sigma_2 S_3 + \sigma_3 S_2 - \sigma_4 S_1 + 5\sigma_5.$$

Taking this equation modulo p, we find that $S_5 \equiv 5\sigma_5 \pmod{p}$. Hence p divides

$$S_5 - 5\sigma_5 = a^5+b^5+c^5+d^5+e^5-5abcde. \qquad \blacksquare$$

Example 7.11. Three real numbers a, b, c satisfy the following conditions: for each positive integer n, the sum $a^n+b^n+c^n$ is an integer. Prove that there exist three integers p, q, r such that a, b, c are the roots of the equation

$$x^3 - px^2 + qx - r = 0.$$

Vietnamese Mathematical Olympiad 2009

Solution. Writing $(x-a)(x-b)(x-c) = x^3 - px^2 + qx - r$, we want to prove that p, q, r are integers. According to Newton's Identities,

$$S_{n+3} = pS_{n+2} - qS_{n+1} + rS_n.$$

It is clear that $p = S_1$ is an integer. Moreover, from $S_2 = p^2 - 2q$, we find that $2q$ is an integer. Furthermore, since

$$S_3 = pS_2 - qS_1 + 3r = p^3 - 3pq + 3r,$$

we get $2S_3 = 2p^3 - 3p \cdot 2q + 6r$. Therefore $6r$ is an integer. Now note that

$$S_4 = pS_3 - qS_2 + rS_1 = p(p^3 - 3pq + 3r) - q(p^2 - 2q) + pr = p^4 - 4qp^2 + 4pr + 2q^2.$$

Multiplying both sides by 3, we get that $6q^2$ is an integer.
Therefore $2q^2 = 6q^2 - (2q)^2$ is an integer. However, this means that $(2q)^2 = 4q^2$ is an even integer, hence $2q$ is an even integer, and we find that q is an integer. Now, the formula above $S_3 = p^3 - 3pq + 3r$ gives that $3r$ is an integer. Assume that r is not an integer. Then $r = \frac{k}{3}$ for some integer k which is not a multiple of 3. From the formula above for S_4, we conclude that $\frac{4pk}{3}$ is an integer, so $3 \mid p$. From the Newton Identity for S_6,

$$S_6 = pS_5 - qS_4 + \frac{k}{3}S_3,$$

we find that $3 \mid S_3$.
However, this means that from the identity $S_3 = p^3 - 3pq + k$, we conclude that k is a multiple of 3, a contradiction. Thus r is an integer. $\blacksquare$

Remark. There is a general statement that was posed in American Mathematical Monthly by early 80s. The solution needs more advanced tools. We shall discuss it in the next volume.

Let $z_1, z_2, \ldots, z_n$ be complex numbers such that $\sum_{j=1}^{n} z_i^m$ is an integer for every positive integer m. Show that the polynomial $(x-z_1)\cdot\ldots\cdot(x-z_n)$ has integer coefficients.

Michael Larsen - American Mathematical Monthly, Problem E2993

Example 7.12. Let a, b, c be integers such that $a+b+c=0$. Prove that for all positive integer n we have

$$a^2+b^2+c^2 \mid a^{n^2+1} + b^{n^2+1} + c^{n^2+1}.$$

Solution. Note that

$$\sigma_1 = a+b+c = 0, \quad \sigma_2 = ab+ac+bc = -\frac{1}{2}(a^2+b^2+c^2) = -\frac{1}{2}S_2.$$

Thus

$$S_m = -\sigma_2 S_{m-2} + \sigma_3 S_{m-3} = \frac{1}{2}(a^2+b^2+c^2)S_{m-2} + \sigma_3 S_{m-3}.$$

Since $a+b+c=0$, we find that S_m is even for each m. Therefore we can write

$$S_m = \frac{S_{m-2}}{2}(a^2+b^2+c^2) + \sigma_3 S_{m-3}.$$

Hence $S_m \equiv \sigma_3 S_{m-3} \pmod{S_2}$. If $m \equiv 1 \pmod 3$, we have $S_m \equiv \sigma_3 S_1 \equiv 0 \pmod{S_2}$ and if $m \equiv 2 \pmod 3$, we have $S_m \equiv \sigma_3 S_2 \equiv 0 \pmod{S_2}$. Since $n^2+1 \equiv 1, 2 \pmod 3$, we are done. ∎

Example 7.13. Prove that for all positive integers we have

$$2^{n+1} \mid \left\lfloor \left(1+\sqrt{3}\right)^{2n+1} \right\rfloor.$$

Solution. Let $z_1 = 1+\sqrt{3}$ and $z_2 = 1-\sqrt{3}$. Then $\sigma_1 = z_1+z_2 = 2$ and $\sigma_2 = z_1 z_2 = -2$. Set $S_n = z_1^n + z_2^n$. Then Newton's Identities read

$$S_{n+1} = 2S_n + 2S_{n-1}.$$

An easy induction on n shows that S_{2n-1} and S_{2n} are divisible by 2^n.
In particular,

$$S_{2n+1} = z_1^{2n+1} + z_2^{2n+1} = 2^{n+1}k$$

for some positive integer k. Therefore

$$z_1^{2n+1} = 2^{n+1}k - z_2^{2n+1}.$$

Since $0 < -z_2^{2n+1} < 1$, we find that $\lfloor z_1^{2n+1} \rfloor = 2^{n+1}k$.
Thus $2^{n+1} \mid \lfloor (1+\sqrt{3})^{2n+1} \rfloor$ ∎

7.3 Newton's Identities and polynomials

One interesting feature of the power sums $S_k = z_1^k + \ldots + z_n^k$ is that as k gets large the term (or terms if there is a tie) with largest modulus dominate the sum. This is particularly dramatic in the case when all but one of the roots have modulus less than 1. In this special case, one term is growing and all the other terms are getting small.

This leads to many interesting problems which require Newton's Identities. Newton's Identities allow you to say some things about what happens to the power sums for large k (maybe just that they are integers), and the largest term lets you say something else about it. When you compare the two, you get interesting conclusions.

Example 7.14. Let α be the greatest root of the polynomial $x^3 - 3x^2 + 1$. Prove that $\lfloor \alpha^{2020} \rfloor$ is divisible by 17.

Solution. First, let us look at what Newton's Identities tell us about the power sums of the roots. Let $\alpha > \beta > \gamma$ be the three roots (which we will see below are all real, but we don't need this yet). Let $S_k = \alpha^k + \beta^k + \gamma^k$ be the power sum. Then Newton's Identities let us compute $S_0 = S_1 = 3$, $S_2 = 9$, and $S_{n+3} = 3S_{n+2} - S_n$ for $n \geq 0$. Since the current problem asks for a result modulo 17, we look at this recursion modulo 17. Stepping it out (which takes a little work) modulo 17, we find that $S_{n+16} \equiv S_n \pmod{17}$. Thus

$$S_{2020} = S_{16\cdot 126+4} \equiv S_4 \equiv 1 \pmod{17},$$

This says that

$$S_{2020} = \alpha^{2020} + \beta^{2020} + \gamma^{2020} = 17k+1$$

for some positive integer k.
Now, let us look at what the sizes of the roots tell us. Write $P(x) = x^3 - 3x^2 + 1$, we have

$$P(-1) = -3 < 0, \quad P(0) = 1 > 0, \quad P(1) = -1 < 0, \quad P(3) = 1 > 0.$$

Hence, using the notation we set in the previous paragraph, we find that $-1 < \gamma < 0 < \beta < 1 < \alpha < 3$. Thus we have two roots of absolute value less than 1, and one root α which is greater than 1. Thus for large k, S_k will be very close to α^k. More precisely, combining this with the result above, we find that

$$\alpha^{2020} = 17k + 1 - \beta^{2020} - \gamma^{2020}.$$

Since 2020 is even, we see that $\alpha^{2020} < 17k+1$, so to complete the proof, we only need to show that

$$\beta^{2020} + \gamma^{2020} < 1.$$

Unfortunately the bounds above only get us $\beta^{2020}+\gamma^{2020}<2$, so we have to improve them a little. Here is one way. Note that $P\left(2\sqrt{2}\right)=16\sqrt{2}-23<0$, so we find $2\sqrt{2}<\alpha<3$. This gives

$$0<\beta^{2020}+\gamma^{2020}<\beta^2+\gamma^2=9-\alpha^2<9-\left(2\sqrt{2}\right)^2=1.$$

Therefore $\beta^{2020}+\gamma^{2020}\in(0,1)$, and we conclude that $\lfloor\alpha^{2020}\rfloor=17k$. ■

Example 7.15. Let n be a positive integer. Prove that $\lfloor(\sqrt[3]{28}-3)^{-n}\rfloor$ is not divisible by 6.

German Team Selection Test 2011

Solution. Let $z_1=\sqrt[3]{28}-3$. Then $(3+z_1)^3=28$, which yields

$$z_1^3+9z_1^2+27z_1-1=0.$$

Thus z_1 is a root of $x^3+9x^2+27x-1$, and the other two roots are

$$z_2=\omega\sqrt[3]{28}-3,\quad z_3=\omega^2\sqrt[3]{28}-3,$$

where ω is a primitive third root of unity. Note that $|z_2|=|z_3|$. Furthermore,

$$|z_2|^2=\frac{1}{|z_1|}>1,$$

so $|z_2|=|z_3|>1$. By Newton's Identities, we know that

$$S_{-n}\equiv -9S_{-n-1}-27S_{-n-2}+S_{-n-3}.$$

Since

$$S_{-n}\equiv S_{-n-1}+S_{-n-2}+S_{-n-3}\pmod 2$$

and

$$S_2=27,\quad S_1=-9,\quad S_0=3,\quad S_{-1}=27,\ldots.$$

we find that S_n is odd for each n. Notice that $S_{-n}\equiv S_{-n-3}\pmod 3$. Thus S_{-n} is divisible by 3. Thus

$$S_{-n}=z_1^{-n}+z_2^{-n}+z_3^{-n}=6t+3,$$

for some positive integer t.
Finally, assume that $\lfloor z_1^{-n}\rfloor=k$. Then $|k-z_1^{-n}|<1$, and so

$$|k-6t-3|=|k-S_{-n}|=|k-z_1^{-n}-z_2^{-n}-z_3^{-n}|<|k-z_1^{-n}|+|z_2^{-n}|+|z_3^{-n}|<3.$$

Hence $k=6t\pm1$, $6t\pm2$. In each case, k is not divisible by 6. ■

There is a general strategy here for problems that ask about integers close to a power of some algebraic number α. (The problem might for example ask about some property of $\lfloor\alpha^n\rfloor$, or of the ceiling.)

Strategy

(i) Find a polynomial $P(x)$ satisfied by α, usually the minimal one.

(ii) Factor $P(x)=(x-z_1)\cdot\ldots\cdot(x-z_d)$ and analyze the roots.

(iii) Check if α^n is close to S_n.

(iv) Apply Newton's Identities to find the recursion satisfied by S_n.

(v) Use some algebraic or number theoretic facts, and possibly induction, to prove something about S_n

(vi) Hey presto!

Example 7.16. Let α and β be the roots of the polynomial x^2-qx+1, where q is a rational number greater than 2. Let $S_1=\alpha+\beta$ and $T_1=1$. For $n\geq2$, define $S_n=\alpha^n+\beta^n$ and

$$T_n=S_{n-1}+2S_{n-2}+\ldots+(n-1)S_1+n.$$

Prove that for odd n, T_n is a rational number.

Centro-American Mathematical Olympiad 2014

First Solution. Since $\alpha\beta = 1$, we have $S_{n+1} = S_1 S_n - S_{n-1}$. A simple induction implies that S_n is a rational number for all n. Now, we will prove by induction that

$$T_{2m+1} = (1 + S_1 + \ldots + S_m)^2$$

for each positive integer m. The base case $m = 0$ is trivial. For the inductive step, we have

$$T_{2m+1} = T_{2m-1} + S_{2m} + 2 + 2(S_1 + \ldots + S_{2m-1}).$$

By the inductive hypothesis $T_{2m-1} = (1 + S_1 + \ldots + S_{m-1})^2$, so this implies that

$$T_{2m+1} = (1 + S_1 + \ldots + S_{m-1})^2 + S_{2m} + 2 + 2(S_1 + \ldots + S_{2m-1}).$$

Note that

$$S_{2m} + 2 = \alpha^{2m} + \beta^{2m} + 2(\alpha\beta)^m = (\alpha^m + \beta^m)^2 = S_m^2.$$

Furthermore,

$$S_1 + \ldots + S_{2m-1} = (\alpha + \alpha^2 + \cdots + \alpha^{2m-1}) + (\beta + \beta^2 + \cdots + \beta^{2m-1})$$
$$= \alpha^m(\alpha^{1-m} + \alpha^{2-m} + \ldots + \alpha^{m-1}) + \beta^m(\beta^{1-m} + \beta^{2-m} + \ldots + \beta^{m-1}).$$

Since

$$\alpha^{1-m} + \alpha^{2-m} + \ldots + \alpha^{-1} = \beta + \beta^2 + \ldots + \beta^{m-1},$$

and similary for β, we have that

$$S_1 + \ldots + S_{2m-1} = (\alpha^m + \beta^m)(1 + \alpha + \beta + \ldots + \alpha^{m-1} + \beta^{m-1})$$
$$= S_m(1 + S_1 + \ldots + S_{m-1}).$$

Therefore

$$\begin{aligned} T_{2m+1} &= (1 + S_1 + \ldots + S_{m-1})^2 + S_{2m} + 2(1 + S_1 + \ldots + S_{2m-1}) \\ &= (1 + S_1 + \ldots + S_{m-1})^2 + S_m^2 + 2S_m(1 + S_1 + \ldots + S_{m-1}) \\ &= (1 + S_1 + \ldots + S_m)^2. \end{aligned}$$

Since $1 + S_1 + \ldots + S_m$ is a rational number, our proof is complete. ■

Second Solution. Since $\beta = \alpha^{-1}$, we have

$$1 + S_1 + \ldots + S_m = 1 + \alpha + \alpha^2 + \ldots + \alpha^m + \alpha^{-1} + \ldots + \alpha^{-m}.$$

Look at what happens when we square this. A term in the product will be α^{r+s} for some r, s with $-m \le r, s \le m$. Thus we get a term of α^j for each solution to $r+s = j$ with r, s in this range. If $j \ge 0$, we see that $j - m \le r = s - j \le j + m$, so we must have $j - m \le r \le m$. Conversely, for any r in the range, we can define $s = j - r$ and we will have $-m \le r, s \le m$. Thus there are $2m + 1 - j$ terms which equal α^j. Since we get the same number for α^{-j}, we find that

$$(1+\ldots+S_m)^2 = (\alpha^{2m}+\alpha^{-2m}) + 2(\alpha^{2m-1}+\alpha^{1-2m}) + \ldots + 2m(\alpha+\alpha^{-1}) + 2m + 1$$
$$= S_{2m} + 2S_{2m-1} + \ldots + (2m-1)S_1 + 2m + 1 = T_{2m+1}.$$

Hence

$$T_{2m+1} = (1 + S_1 + \ldots + S_m)^2.$$

Now, by the above argument, we know that $1 + S_1 + \ldots + S_m$ is rational. ■

Example 7.17. Let $a_1, \ldots, a_n$ be integers and $A = (a_1^2 - 1) \cdot \ldots \cdot (a_n^2 - 1)$. If

$$A \sum_{i=1}^{n} \frac{1}{(a_i^2 - 1)(a_i + 1)}$$

is an integer, prove that $\frac{A}{(a_i^2-1)(a_i+1)}$ is integer for $i = 1, 2, \ldots, n$.

Solution. Let $z_i = \dfrac{A}{(a_i^2 - 1)(a_i + 1)}$. Then $\sigma_1 = \displaystyle\sum_{i=1}^{n} z_i$ is an integer by hypothesis. Since

$$A^2 = (a_1^2 - 1)^2 \cdot \ldots \cdot (a_n^2 - 1)^2$$

is a multiple of $(a_i^2)(a_i + 1)(a_j^2 - 1)(a_j + 1)$ for every i, j, we see that

$$\sigma_2 = \sum_{1 \le i < j \le n} z_i z_j = A^2 \sum_{1 \le i < j \le n} \frac{1}{(a_i^2 - 1)(a_j^2 - 1)(a_i + 1)(a_j + 1)}$$

is an integer. By the same argument,

$$\sigma_k = \sum_{1\le i_1<i_2<\ldots<i_k\le n} z_{i_1}z_{i_2}\cdot\ldots\cdot z_{i_k}$$

is an integer for each $k = 1,\ldots,n$. Hence the polynomial

$$P(x) = (x-z_1)\cdot\ldots\cdot(x-z_n) = x^n - \sigma_1 x^{n-1} + \ldots + (-1)^n\sigma_n$$

is monic, has integer coefficients and has rational roots. Therefore its roots are integers. ■

Example 7.18. Solve the following system in complex numbers

$$\begin{cases} x_1 + x_2 + \ldots + x_n &= a \\ x_1^2 + x_2^2 + \ldots + x_n^2 &= a^2 \\ \qquad\qquad \vdots & \vdots \\ x_1^n + x_2^n + \ldots + x_n^n &= a^n. \end{cases}$$

Solution. Let $(x-x_1)\cdot\ldots\cdot(x-x_n) = x^n - \sigma_1 x^{n-1} + \ldots + (-1)^n\sigma_n$. Since $\sigma_1 = S_1 = a$, iteratively looking at Newton's Identities

$$k\sigma_k = (-1)^{k-1}S_k + (-1)^{k-2}\sigma_1 S_{k-1} + \ldots + \sigma_{k-1}S_1, \quad k = 2,\ldots,n,$$

shows that $\sigma_2 = \ldots = \sigma_n = 0$. Thus

$$(x-x_1)\cdot\ldots\cdot(x-x_n) = x^n - ax^{n-1}.$$

and hence $(x_1, x_2, \ldots, x_n) = (a, 0, 0, \ldots, 0)$, or a permutation of this. ■

Now, we provide two correlated number theoretic examples. We shall prove the first by classical number theoretic approaches, but second by Newton's Identities.

Example 7.19. Let p be an odd prime number and let

$$(x-1)\cdot\ldots\cdot(x-p+1) = x^{p-1} - \sigma_1 x^{p-2} + \ldots + \sigma_{p-1}.$$

Prove that $\sigma_1, \ldots, \sigma_{p-2}$ are all divisible by p.

Solution. It is known that

$$\sigma_i = \sum_{1\le j_1<\ldots<j_i\le p-1} j_1\ldots j_i.$$

Let g be a primitive root modulo p. Note that the set $\{g, 2g, \ldots, (p-1)g\}$ coincides with the set $\{1, 2, \ldots, p-1\}$. Thus

$$g^i\sigma_i = \sum_{1\le j_1<\ldots<j_i\le p-1} gj_1\ldots gj_i \equiv \sum_{1\le j_1<\ldots<j_i\le p-1} j_1\ldots j_i \equiv \sigma_i \pmod p.$$

Therefore $(g^i - 1)\sigma_i \equiv 0 \pmod p$. Since g is a primitive root and $i < p-1$, $g^i - 1$ is not divisible by p. Hence $\sigma_i \equiv 0 \pmod p$. ■

Example 7.20. Let p be an odd prime number, k a positive integer, and $S_k = 1^k + \ldots + (p-1)^k$. Prove that

$$S_k \equiv \begin{cases} 0, & \text{if } p-1 \nmid k \\ -1, & \text{if } p-1 \mid k \end{cases} \pmod p.$$

Solution. By Fermat's Little Theorem, it is enough to restrict k in the set $\{1, 2, \ldots, p-1\}$. According to Newton's Identities,

$$S_k = \sigma_1 S_{k-1} - \sigma_2 S_{k-2} + \ldots + (-1)^{k+1}k\sigma_k,$$

for $k = 1, 2, \ldots, p-1$. Now, for $k = 1$, $S_1 = \sigma_1 \equiv 0 \pmod p$. Thus for all $k = 1, 2, \ldots, p-2$, we find that $S_k \equiv 0 \pmod p$. Now, for $k = p-1$ we have

$$S_{p-1} = \sigma_1 S_{p-1} - \sigma_2 S_{p-2} + \ldots + (-1)^p(p-1)\sigma_{p-1}.$$

Proceeding as in the above example, $\sigma_1, \ldots, \sigma_{p-2}$ are all divisible by p, thus

$$S_{p-1} \equiv \sigma_{p-1} \pmod p.$$

By Wilson's Theorem,

$$\sigma_{p-1} = (p-1)! \equiv -1 \pmod p.$$

Therefore $S_{p-1} \equiv -1 \pmod p$. ■

7.4 Newton's Identity and number theory: advanced problems

Finally, we arrive at the last part of this chapter. We have learned many interesting aspects of Newton's Identities. We have found that it has different applications in Number Theory, Polynomials etc.. Here are some more advanced problems, where Newton's Identities can be used to help solve the problem.

Example 7.21. Let a, b, c be the roots of the polynomial

$$P(x) = x^3 - 3x^2 + 1.$$

Prove that for each $n \geq 1$,

$$\frac{a^n + b^n + c^n - 4^n - 5^n - 11^n}{17}$$

is an integer.

Solution. Let $S_n = a^n + b^n + c^n$ be the power sums of the roots of $P(x)$ and $T_n = 4^n + 5^n + 11^n$ the power sums for $4, 5, 11$. From Newton's Identities, we know that $S_0 = S_1 = 3$, $S_2 = 9$ and S_n satisfies $S_{n+3} = 3S_{n+2} - S_n$ for $n \geq 0$. We also get that $T_0 = 3$, $T_1 = 20$, $T_2 = 162$, and

$$T_{n+3} = 20T_{n+2} - 119T_{n+1} + 220T_n$$

for $n \geq 0$. Reducing these modulo 17, we see that $T_1 \equiv S_1$, $T_2 \equiv S_2$, and

$$T_{n+3} \equiv 3T_{n+2} - T_n \pmod{17}.$$

Thus $T_n \equiv S_n \pmod{17}$ for all n and we are done. ■

Example 7.22. Let $p = a^2 + b^2$ for some positive integers a and b. Prove that there are infinitely many natural numbers n such that $(a^n + b^n + a + b)(1 + (ab)^n)$ is divisible by p.

Solution. Let D be the order of $(ab)^2$ modulo p, that is, D is the smallest positive integer such that $(ab)^{2D} \equiv 1 \pmod{p}$. If $D = 2m$ is even, then $x = (ab)^m \pmod{p}$ cannot be 1 (since D is minimal) and satisfies $x^2 \equiv 1 \pmod{p}$. Thus $x \equiv -1 \pmod{p}$, and hence $(ab)^m \equiv -1 \pmod{p}$. In this case, we can just take $n = (2k+1)m = kD + m$. This will give $(ab)^n \equiv (ab)^m \equiv -1 \pmod{p}$, which means that p will divide $1 + (ab)^n$.
Thus we may assume that D is odd. Note that Newton's Identities give

$$a^{k+4} + b^{k+4} = (a^2 + b^2)(a^{k+2} + b^{k+2}) - (ab)^2(a^k + b^k).$$

Hence

$$a^{k+4} + b^{k+4} \equiv -(ab)^2(a^k + b^k) \pmod{p},$$

and iterating this we get

$$a^{4k+1} + b^{4k+1} \equiv (-1)^k(ab)^{2k}(a + b) \pmod{p}.$$

Now choose $k = (2m+1)D$. Since k is odd and $(ab)^{2D} \equiv 1 \pmod{p}$, we get

$$a^{4(2m+1)D+1} + b^{4(2m+1)D+1} \equiv -(a + b) \pmod{p}.$$

Hence if we let $n = 4(2m+1)D + 1$, then we find $a^n + b^n + a + b$ is divisible by p. ■

Example 7.23. Let $a_1, \ldots, a_n$ be integers and assume that for all $i = 1, 2, \ldots, k-1$ we have the following equality:

$$a_1 + 2^i a_2 + \ldots + n^i a_n = 0.$$

Prove that $k! \mid (a_1 + 2^k a_2 + \ldots + n^k a_n)$.

Polish Mathematical Olympiad

Solution. Let $T_k = a_1 + 2^k a_2 + \cdots + n^k a_n$ and define

$$Q(x) = x(x-1) \cdot \ldots \cdot (x-k+1) = x^k - b_{k-1}x^{k-1} + \ldots + (-1)^{k-1}(k-1)!x.$$

For each positive integer m, $Q(m) = k!\binom{m}{k}$ is divisible by $k!$. Hence we see that $\sum_{j=1}^{n} a_j Q(j)$ is a multiple of $k!$. However, we compute that

$$\sum_{j=1}^{n} a_j Q(j) = T_k - b_{k-1}T_{k-1} + \ldots + (-1)^{k-1}(k-1)!T_1 = T_k.$$

Therefore T_k is a multiple of $k!$, as desired.

Remark. We could carry this further using Newton's Identities. The T_k satisfy the recurrence

$$T_{n+k} = b_{k-1}T_{n+k-1} + \ldots + (-1)^k(k-1)!T_{n+1}$$

for $n \geq 0$. Hence an easy induction shows that T_n is a multiple of $k!$ for all n.

Example 7.24. Let p be a prime number and let k be a positive integer, $k < p$. If $x_1, \ldots, x_k \in \mathbb{Z}$ and

$$x_1 + \ldots + x_k, \ldots, {x_1}^k + \ldots + {x_k}^k$$

are all divisible by p, prove that $p \mid x_1, \ldots, x_k$.

Mongolian Mathematical Olympiad 2013

Solution. By Newton's Identities, we have

$$S_k = \sigma_1 S_{k-1} - \sigma_2 S_{k-2} + \ldots + (-1)^{k+1} k\sigma_k.$$

Since $p \mid S_i$ for all $i = 1, \ldots, k$ and $k < p$, we find that $p \mid \sigma_k = x_1 \cdot \ldots \cdot x_k$. Then p divides at least one of $x_1, \ldots, x_k$. Assume that $p \mid x_k$. Hence the power sums for $x_1, \ldots, x_{k-1}$ are all multiples of p. Therefore we can repeat the same argument to we find that p divides $x_1 \cdot \ldots \cdot x_{k-1}$. Continuing in this way, we conclude that $p \mid x_1, \ldots, x_k$. ∎

By the last example, we adopt a synthetic approach based on Newton's Identities and complex numbers.

Example 7.25. Let p be a prime number and $n \geq p$. Prove that p divides

$$\sum_{r \geq 0} (-1)^r \binom{n}{rp}.$$

Solution. Let

$$A = \sum_{r \geq 0} (-1)^r \binom{n}{rp}.$$

Take $Q(x) = (1-x)^n$. If ω is a primitive p-th root of unity, then

$$\begin{aligned} Q(1) + Q(\omega) + \ldots + Q(\omega^{p-1}) &= \sum_{k=0}^{p-1} \sum_{j=0}^{n} \binom{n}{j} (-1)^j \omega^{kj} \\ &= \sum_{j=0}^{n} \binom{n}{j} (-1)^j \sum_{k=0}^{p-1} \omega^{kj}. \end{aligned}$$

If $p \nmid j$, then we have $\sum_{k=0}^{p-1} \omega^{kj} = \frac{\omega^{jp}-1}{\omega^j - 1} = 0$. If $p \mid j$, then $\sum_{k=0}^{p-1} \omega^{kj} = \sum_{k=0}^{p-1} 1 = p$. Thus we find that

$$\frac{Q(1) + Q(\omega) + \ldots + Q(\omega^{p-1})}{p} = A.$$

Now, it suffices to prove

$$Q(1) + Q(\omega) + \ldots + Q(\omega^{p-1}) = (1-1)^n + (1-\omega)^n + \ldots + (1-\omega^{p-1})^n$$

is divisible by p^2. Let $z_j = 1 - \omega^j$, $j = 0, \ldots, p-1$, and consider the polynomial

$$(x - z_0) \cdot \ldots \cdot (x - z_{p-1}) = x^p - \sigma_1 x^{p-1} + \ldots + (-1)^p \sigma_p.$$

Note that this choice means that

$$Q(1) + Q(\omega) + \ldots + Q(\omega^{p-1}) = S_n,$$

so it suffices to show that S_n is a multiple of p^2 for $n \geq p$. Since

$$(z_j - 1)^p = (-\omega^j)^p = (-1)^p,$$

each z_j is a root of $(x-1)^p - (-1)^p$, and we see that this polynomial is

$$(x - z_0) \cdot \ldots \cdot (x - z_{p-1}) = (x-1)^p + (-1)^p = \sum_{k=1}^{p} (-1)^{p-k} \binom{p}{k} x^k.$$

Thus $\sigma_1, \ldots, \sigma_{p-1}$ are all divisible by p and $\sigma_p = 0$. Since Newton's Identities show that all the power sums S_k are polynomials in the elementary symmetric polynomials σ_k with integer coefficients, it follows that S_k are all divisible by p. Moreover, for $r \geq 0$, Newton's Identities read

$$\begin{aligned} S_{p+r} &= \sigma_1 S_{p+r-1} - \sigma_2 S_{p+r-2} + \ldots - S_r \sigma_p \\ &= \sigma_1 S_{p+r-1} - \sigma_2 S_{p+r-2} + S_{r+1} \sigma_{p-1}. \end{aligned}$$

Every term on the right is a product of two factors both of which are divisible by p. Hence it follows that S_{p+r} is divisible by p^2, and thus that S_n is divisible by p^2 for $n \geq p$.

7.5 Proposed problems

Problem 7.1. Let a, b, c be distinct real numbers with $a + b + c = 2019$. Evaluate the sum

$$\frac{a(b-c)^2}{(c-a)(a-b)} + \frac{b(c-a)^2}{(a-b)(b-c)} + \frac{c(a-b)^2}{(b-c)(c-a)}.$$

Problem 7.2. Find all positive integers a, b, c such that

$$\frac{a^4}{(a-b)(a-c)} + \frac{b^4}{(b-c)(b-a)} + \frac{c^4}{(c-a)(c-b)} = 47.$$

Problem 7.3. Let x, y and z be distinct integers and n be a non-negative integer. Prove that

$$\frac{x^n}{(x-y)(y-z)} + \frac{y^n}{(y-z)(y-x)} + \frac{z^n}{(z-x)(x-y)}$$

is an integer.

Kürschák Competition 1959

Problem 7.4. Find all positive integers n such that for all real numbers x, y, z with $x+y+z = 0$ and $xyz = 1$, the expression $S_n = x^n + y^n + z^n$ is constant.

Problem 7.5. Let

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= y_1 + y_2 + y_3 + y_4, \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 &= y_1^2 + y_2^2 + y_3^2 + y_4^2, \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 &= y_1^3 + y_2^3 + y_3^3 + y_4^3. \end{aligned}$$

Prove that

$$(x_1 - y_2)(x_1 - y_3)(x_1 - y_4) = (y_1 - x_2)(y_1 - x_3)(y_1 - x_4).$$

Problem 7.6. Show that there is a positive integer k with the following property: if a, b, c, d, f are integers and m is a divisor of $a^n + b^n + c^n - d^n - e^n - f^n$ for all integers $n = 1, 2, \ldots, k$ then m is a divisor of

$$a^n + b^n + c^n - d^n - e^n - f^n$$

for all positive integers n.

Problem 7.7. Let $a_1, \ldots, a_n$ be distinct real numbers such that no subset of them sums to zero. Solve following system of equations:

$$\begin{cases} a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = 0, \\ a_1 x_1^2 + a_2 x_2^2 + \ldots + a_n x_n^2 = 0, \\ \qquad\qquad \vdots \\ a_1 x_1^n + a_2 x_2^n + \ldots + a_n x_n^n = 0. \end{cases}$$

Problem 7.8. Let $z_1, \ldots, z_n$ be complex numbers and k be a positive integer such that

$$z_1^k + \ldots + z_n^k = z_1^{k+1} + \ldots + z_n^{k+1} = \ldots = z_1^{k+n-1} + \ldots + z_n^{k+n-1} = 0.$$

Prove that $z_1 = \ldots = z_n = 0$.

Problem 7.9. Prove that for any $z_1, z_2, \ldots, z_n \in \mathbb{C}$ there exists a positive integer $k \leq 2n+1$ such that

$$\mathrm{Re}(z_1^k + z_2^k + \ldots + z_n^k) \geq 0.$$

Problem 7.10. Let a, b, c be complex numbers and let

$$S_n = a^n + b^n + c^n.$$

Assume that S_1, S_2, S_3 are integers and $5S_1 - 3S_2 - 2S_3$ is divisible by 6. Prove that S_n is an integer for each n.

Problem 7.11. Let p and q be prime numbers and let $a_1, \ldots, a_p, b_1, \ldots, b_q$ be integers such that $a_i + b_j$ form a complete residue system modulo pq. Prove that $a_1, \ldots, a_p$ form a complete residue system modulo p.

Sergei Ivanov - Saint Petersburg Mathematical Olympiad 2006

Problem 7.12. Let (a_n) and (b_n) be two sequences such that

$$\begin{cases} 4a_1 - 2b_1 = 7, \\ a_{n+1} = a_n^2 - 2b_n \\ b_{n+1} = b_n^2 - 2a_n. \end{cases}$$

Find the value of $2^{512}a_{10} - b_{10}$.

Belarusian Mathematical Olympiad

Chapter 8

Additional Problems

Problem 8.1. Suppose that

$$(x^2 - x + 1)^3(x^3 + 4x^2 + 4x + 1)^5 = a_{21}x^{21} + a_{20}x^{20} + \ldots + a_0.$$

What is the value of $a_1 + \ldots + a_{10}$?

Problem 8.2. Let $P(x)$ be an irreducible monic polynomial with rational coefficients. Assume that $P(x)$ has two roots whose product is equal to 1. Prove that the degree of the polynomial is even.

Problem 8.3. Consider a third degree polynomial. We are allowed to perform the following two operations arbitrarily many times:

(i) reverse the order of its coefficients including zeroes (for instance, from the polynomial $x^3 - 2x^2 - 3$ we can obtain $-3x^3 - 2x + 1$);

(ii) change polynomial $P(x)$ to the polynomial $P(x+1)$.

Is it possible to obtain the polynomial $x^3 - 3x^2 + 3x - 3$ from the polynomial $x^3 - 2$?

Alexander Golovanov

Problem 8.4. Let $z_1, \ldots, z_{2n}$ be nonreal $2n+1$-th roots of unity. Prove that

$$\sum_{k=1}^{2n} \frac{1-\overline{z_k}}{1+z_k} = 2n+1.$$

Problem 8.5. Prove that for any integer a the polynomial $3x^{2n} + ax^n + 2$ is not divisible by $2x^{2m} + ax^m + 3$.

Moscow Mathematical Olympiad 1952

Problem 8.6. Assume that $\alpha^{2005} + \beta^{2005}$ can be expressed as a polynomial in $\alpha+\beta$ and $\alpha\beta$. Find the sum of the coefficients of the polynomial.

China Western Mathematical Olympiad 2005

Problem 8.7. Determine all polynomials with non-negative real coefficients satisfying the following conditions:

$$p(0) = 0, \quad p(|z|) \leq x^4 + y^4 \quad \forall z \in \mathbb{C},$$

where $|z|$ is the modulus of the complex number $z = x + iy$.

Spanish Mathematical Olympiad 1982

Problem 8.8. Let m be a positive integer and

$$P(x) = \sum_{k=0}^{6m-1} x^{2^k} = x + x^2 + \ldots + x^{2^{6m-1}},$$

$$Q(x) = x^{2^{2m+1}-2} + x^{2^{2m}-1} + 1.$$

Prove that $P(x)$ is divisible by $Q(x)$.

Problem 8.9. Let n, k be positive integers with $k < n$ and let α be a real number with $|\alpha| \leq 1$.
Prove that all the roots of polynomial $x^n + \alpha x^{n-k} + \alpha x^k + 1$ are on the unit circle.

Problem 8.10. (a) Prove that there exists a polynomial P with integer coefficients of degree 502 such that

$$1 + x^4 + x^8 + x^{12} + \ldots + x^{2008} = P(x)P(-x)P(ix)P(-ix) \qquad \forall x \in \mathbb{C}.$$

(b) Prove that if $a_0, a_1, \ldots, a_n \in \mathbb{C}$, $a_n \neq 0$, then there exists a polynomial Q with complex coefficients of degree n such that

$$a_0 + a_1 x^4 + a_2 x^8 + \ldots + a_n x^{4n} = Q(x)Q(-x)Q(ix)Q(-ix) \qquad \forall x \in \mathbb{C}.$$

Marcel Țena - Nicolae Teodorescu Competition 2008

Problem 8.11. Let d be an integer greater than 1 and let $a_0, a_1 \ldots, a_d$ be real numbers with $a_1 = a_{d-1} = 0$. Prove that for any real number k,

$$|a_0| - |a_d| \leq \sum_{i=0}^{d-2} |a_i - k a_{i+1} - a_{i+2}|.$$

Canadian Mathematical Olympiad 2019

Problem 8.12. Let $(a_n)_{n \in \mathbb{N}}$ be a sequence of real numbers defined by

$$a_{n+1} = a_n^3 - 3a_n^2 + 3$$

for all $n \geq 0$. For how many values of a_0 do we have $a_{2017} = a_0$?

Problem 8.13. Let $d \geq 3$ be an odd number, let $r > 0$ be a real number and let $a_1, \ldots, a_{d-1}$ be complex numbers. The polynomial

$$P(z) = z^d + a_1 z^{d-1} + \ldots + a_{d-1} z - 1$$

has roots $r_1, \ldots, r_d$ such that $|r_j| = r$ for $j = 1, \ldots, d$. Prove that

$$\mathrm{Im}(r_j + r_1 \ldots r_{j-1} r_{j+1} \ldots r_d) = 0$$

for each j. Moreover, prove that $\mathrm{Im}(a_k) = \mathrm{Im}(a_{d-k})$ for each k.

Problem 8.14. Let $n \geq 3$ be an integer. Do there exist positive real numbers $a_1, a_2, a_3, \ldots a_n$ such that for any $k = 1, 2, \ldots, n$ every root of the polynomial $a_{k+n-1}x^{n-1} + \ldots + a_{k+1}x + a_k$ (where $a_{i+n} = a_i$ for all $i = 1, 2, \ldots, n-1$) satisfies the inequality $|\text{Im } z| \leq |\text{Re } z|$?

Chinese Team Selection Test 2003

Problem 8.15. Let $P(x) = x^{d+1} + a_1x^{d-1} + a_2x^{d-2} + \ldots + a_d$ be a polynomial with complex coefficients. Consider $r = \max\{|a_1|, \ldots, |a_d|\}$. Prove that for each of its roots r_i we have $|r_i|(|r_i| - 1) \leq r$.

Marcel Chiriță

Problem 8.16. Let a and b be two positive integers. Prove that

$$2(a^2 - ab + b^2) \mid (a-b)^{2^n} + a^{2^n} + b^{2^n}.$$

Gazeta Matematică

Problem 8.17. Let $P(x)$ be a polynomial with integer coefficients and let ω be a complex number such that $|\omega| = 1$. Let $P(\omega) = c$, where c is a real number. Prove that there exists a polynomial $Q(x)$ with integer coefficients such that

$$c = Q\left(\omega + \frac{1}{\omega}\right).$$

Problem 8.18. Let z be a complex number of modulus 1. Prove that there exists a polynomial of degree d such that all of its coefficients are $+1$ or -1 and $|P(z)| \leq 4$.

Komal

Problem 8.19. Let r be the real root of the polynomial $x^3 - x^2 - 1$. A real number a is *good* if it is equal to the sum of the elements of a finite subset of the set $\{1, r, r^2, \ldots\}$. Is it true that for each $\varepsilon > 0$ there are two good numbers a and b such that $0 < a - b < \varepsilon$?

Problem 8.20. Let $C \in (0, 1)$ and let d be a positive integer. Prove that the moduli of all the roots of polynomial

$$P(x) = \sum_{k=0}^{d} \binom{d}{k} C^{k(d-k)} x^k$$

are equal to 1.

Chinese Team Selection Test 2018

Problem 8.21. Find all nonconstant polynomials $P(z)$ with complex coefficients for which all complex roots of $P(z)$ and $P(z) - 1$ have absolute value 1.

Ankan Bacharia - USA Team Selection Test 2021

Problem 8.22. Let $D = \{z \in \mathbb{C} : \text{Re}(z) < 1\}$. Let $d \geq 1$ be a positive integer and let $a_0, \ldots, a_d$ be real numbers such that $0 < a_0 \leq a_1 \leq \ldots \leq a_{d-1}$ and $a_{d-1} > a_d > 0$. Prove that all the roots of $P(x) = a_dx^d + a_{d-1}x^{d-1} + \ldots + a_0$ lie in D.

Problem 8.23. The polynomial

$$P(x) = rx^3 + qx^2 + px + 1$$

has positive real coefficients and only one real root. Define the sequence $a_1 = 1$, $a_2 = -p$, $a_3 = p^2 - q$ and for each $n \geq 1$,

$$a_{n+3} + pa_{n+2} + qa_{n+1} + ra_n = 0.$$

Prove that the sequence has infinitely many terms which are negative real numbers.

Vietnamese Team Selection Test 2009

Problem 8.24. Let $P(x)$ and $Q(x)$ be monic polynomials with complex coefficients such that

$$P(x) - Q(y) = \prod_{j=1}^{n} (a_jx + b_jy + c_j)$$

for some nonzero complex numbers a_j, b_j, c_j. Prove that there are complex numbers a, b, c such that

$$P(x) = (x+a)^n + c, \quad Q(x) = (x+b)^n + c.$$

Problem 8.25. Find all positive integers n such that the polynomial

$$a^n(b-c) + b^n(c-a) + c^n(a-b)$$

has $a^2+b^2+c^2+ab+ac+bc$ as factor.

American Mathematical Monthly, Problem 10306

Problem 8.26. Let P and Q be two nonzero polynomials with complex coefficients. Prove that P and Q have the same roots with the same multiplicity for correspondent roots if and only if the function $f : \mathbb{C} \to \mathbb{R}$ defined by $f(x) = |P(x)| - |Q(x)|$ has constant sign on $\mathbb{C}$ (it can also vanish).

Marcel Ţena - Romanian Mathematical Olympiad 1978

Problem 8.27. Let $f = x^{2n} + a_{2n-1}x^{2n-1} + \ldots + a_1x + 1 \in \mathbb{C}[x]$ be a polynomial such that $a_{2n-k} = a_k$, $\forall k \in \{1, 2, \ldots, n-1\}$ and

$$|a_1| + |a_2| + \ldots + |a_{2n-1}| < 2.$$

If α is a root of f, prove that $\left|\alpha + \frac{1}{\alpha}\right| < 2$.

Alin Pop - Gazeta Matematică B 12/2003, *Problem* C:2694

Problem 8.28. Let $a, b, c, d > 0$. Prove that

$$\sqrt{\left(a+\sqrt{\frac{bcd}{a}}\right)\left(b+\sqrt{\frac{acd}{b}}\right)\left(c+\sqrt{\frac{abd}{c}}\right)\left(d+\sqrt{\frac{abc}{d}}\right)} + 2\sqrt{abcd}$$

$$\geq ab+bc+cd+da+ac+bd.$$

Problem 8.29. Find all positive integers n such that there are n points $P_1, \ldots, P_n$ on the unit circle satisfying the following property: for any point M on the unit circle, $\sum_{i=1}^{n} MP_i^k$ is a fixed value for

(i) $k = 2018$;
(ii) $k = 2019$.

Chinese Team Selection Test 2019

Problem 8.30. Polynomials $u_i(x) = a_ix + b_i$ ($a_i, b_i \in \mathbb{R}$, $i = 1, 2, 3$) satisfy

$$(u_1(x))^n + (u_2(x))^n = (u_3(x))^n$$

for some natural number $n > 2$. Prove that there exist real numbers A, B, c_1, c_2, c_3 such that $u_i(x) = c_i(Ax + B)$ for $i = 1, 2, 3$.

Polish Mathematical Olympiad 1972

Problem 8.31. Determine all pairs of polynomials P and Q with complex coefficients such that for all complex numbers x, we have

$$P(P(x)) - Q(Q(x)) = 1 + i, \quad P(Q(x)) - Q(P(x)) = 1 - i.$$

Problem 8.32. Let $P(x) = a_0 + a_1x + a_2x^2 + a_{10}x^{10} + a_{11}x^{11} + a_{12}x^{12} + a_{13}x^{13}$, $a_{13} \neq 0$ and $Q(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + b_{10}x^{10} + b_{11}x^{11} + b_{12}x^{12} + b_{13}x^{13}$, $b_3 \neq 0$. Let $D(x) = \gcd(P(x), Q(x))$. Find the maximum value of $\deg D(x)$.

Problem 8.33. Determine all polynomials P such that for every real number x,

$$(P(x))^2 + P(-x) = P(x^2) + P(x).$$

P. Calábec - Czech-Slovak Mathematical Olympiad 2001

Problem 8.34. Find all monic polynomials $P(x)$, $Q(x)$ of the same degree such that for all real numbers x,

$$P(x)^2 - P(x^2) = Q(x).$$

Problem 8.35. Find all monic polynomials $P(x)$, $Q(x)$ such that $P(1) = 1$ and

$$2P(x) = Q\left(\frac{(x+1)^2}{2}\right) - Q\left(\frac{(x-1)^2}{2}\right).$$

Greek Mathematical Olympiad 2016

Problem 8.36. Find all polynomials $P(x)$ with real coefficients such that for all $|x| < 1$,

$$P\left(x\sqrt{2}\right) = P\left(x + \sqrt{1-x^2}\right).$$

USA TSTST 2014

Problem 8.37. Find all polynomials $P(x)$ with real coefficients for which there is a unique polynomial $Q(x)$ with $Q(0) = 0$ such that

$$x + Q(y + P(x)) = y + Q(x + P(y)) \qquad \forall x, y.$$

Problem 8.38. Do there exist a polynomial $P(x)$ of degree $d > 0$ with rational coefficients such that some of its coefficients are not integers and a polynomial $Q(x)$ with integer coefficients and a set S of $d+1$ integers such that $P(s) = Q(s)$ for each $s \in S$?

Problem 8.39. Find all the polynomials $P(x)$ with real coefficients such that $|P(x)| \leq x$ for all real numbers x.

Romanian Mathematical Olympiad 1974

Problem 8.40. Let $P \in \mathbb{R}[x]$ such that $P(\sin t) = P(\cos t)$ for all $t \in \mathbb{R}$. Prove that there exists a polynomial $Q \in \mathbb{R}[x]$ such that $P(x) = Q(x^4 - x^2)$.

Vladimir Maşek - Romanian IMO Team Selection Test 1983

Problem 8.41. Let $P(x)$ be a polynomial with real coefficients satisfying the condition

$$P(\cos\theta + \sin\theta) = P(\cos\theta - \sin\theta)$$

for every real number θ. Prove that $P(x) = Q((1-x^2)^2)$ for some polynomial $Q(x)$ with real coefficients.

Problem 8.42. Find all the polynomials $P \in \mathbb{R}[x]$ such that

$$P(\sin x) = P(\tan x)P(\cos x) \text{ for any } x \in \left(\frac{\pi}{3}, \frac{\pi}{2}\right).$$

Vladimir Maşek - Romanian Mathematical Olympiad 1986

Problem 8.43. Find all quadruples of polynomials $P_1(x)$, $P_2(x)$, $P_3(x)$, $P_4(x)$ with real coefficients such that for each quadruple of integers x, y, z, t such that $xy - zt = 1$, one has

$$P_1(x)P_2(y) - P_3(z)P_4(t) = 1.$$

Alexander Golovanov - Saint Petersburg Mathematical Olympiad 1996

Problem 8.44. Suppose that F, G, H are polynomials of degree at most $2n+1$ with real coefficients such that:
(i) For all real x we have $F(x) \leq G(x) \leq H(x)$.
(ii) There exist distinct real numbers $x_1, x_2, \ldots, x_n$ such that

$$F(x_i) = H(x_i) \quad \text{for } i = 1, 2, 3, \ldots, n.$$

(iii) There exists a real number x_0 different from $x_1, x_2, \ldots, x_n$ such that

$$F(x_0) + H(x_0) = 2G(x_0).$$

Prove that $F(x) + H(x) = 2G(x)$ for all real numbers x.

Baltic Way 2007

Problem 8.45. Consider two polynomials P and Q with real coefficients having the property that the sets

$$\{n \in \mathbb{N} \mid P(n) \leq Q(n)\} \quad \text{and} \quad \{n \in \mathbb{N} \mid Q(n) \leq P(n)\}$$

are infinite. Prove that $P = Q$.

Laurenţiu Panaitopol, Laurenţiu Panaitopol Competition 2010

Problem 8.46. Prove that there doesn't exist a rational function $R(z)$ such that $R(n) = n!$ for all natural numbers n.

Jacques Marion - Crux Mathematicorum 5/1976

Problem 8.47. Find all polynomials $P(x)$ such that

$$P(x)P(2x^2) = P(x + x^3).$$

Mathematics and Youth Journal

Problem 8.48. Prove that for each positive integer n, there exists a polynomial of degree n with n distinct real roots such that

$$P(x(4 - x)) = P(x)P(4 - x).$$

Mongolian Mathematical Olympiad

Problem 8.49. Find all polynomials P with real coefficients such that

$$\frac{P(x)}{yz} + \frac{P(y)}{zx} + \frac{P(z)}{xy} = P(x - y) + P(y - z) + P(z - x)$$

holds for all nonzero real numbers x, y, z satisfying

$$2xyz = x + y + z.$$

Titu Andreescu and Gabriel Dospinescu - USA Mathematical Olympiad 2019

Problem 8.50. Find all polynomials $P(x)$ for which:

$$P(a + b) = 6\left(P(a) + P(b)\right) + 15a^2b^2(a + b),$$

for all complex numbers a and b such that $a^2 + b^2 = ab$.

Titu Andreescu and Mircea Becheanu - Mathematical Reflections, Problem U484

Problem 8.51. Find all polynomials P with complex coefficients such that

$$P(a) + P(b) = 2P(a + b),$$

whenever a and b are complex numbers satisfying $a^2 + 5ab + b^2 = 0$.

Titu Andreescu and Mircea Becheanu - Mathematical Reflections, Problem U491

Problem 8.52. Let a be a positive integer such that

$$f(x) = x^2 + ax + 2017!,$$

has no real roots. Prove that there is no integer k such that $f(x^k)$ is reducible over $\mathbb{Z}[x]$.

Problem 8.53. Find all ordered pairs (m, n) of positive integers such that there exist polynomials $P(x)$, $Q(x)$ of degree m, n respectively, and with real coefficients, such that the numbers $1, 2, \ldots, mn$ are roots of $P(Q(x))$.

Problem 8.54. Find all monic polynomials $P(x)$, $Q(x)$ such that

$$P(Q(x)) = x^{2019}.$$

Problem 8.55. Let P, Q, R be nonconstant polynomials with integer coefficients such that for any real number x,

$$P(Q(x)) = Q(R(x)) = R(P(x)).$$

Show that $P = Q = R$.

Polish Mathematical Olympiad 2009

Problem 8.56. Find all polynomials $P(x)$, $Q(x)$ with real coefficients such that $P(P(x)) = Q(Q(1 - x))$.

Belarusian Mathematical Olympiad 2001

Problem 8.57. Let k be odd. Let $f_1, \ldots, f_k$ be polynomials with real coefficients such that

$$f_1(f_2(x)) = f_2(f_3(x)) = \ldots = f_k(f_1(x)).$$

Prove that $f_1 = \ldots = f_k$.

Problem 8.58. Do there exist polynomials $P(x)$ and $Q(x)$ with integer coefficients of degree at least 2018 such that

$$P(Q(x)) - 3Q(P(x)) = 1?$$

Problem 8.59. Let $P(x)$ be a nonconstant polynomial with integer coefficients such that for all but finitely many positive integer n, $P(1) + \ldots + P(n)$ divides $nP(n+1)$. Prove that there is a non-negative integer k such that for each positive integer n we have

$$P(n) = \binom{n+k}{n-1} P(1).$$

Problem 8.60. Find all polynomials $P(x)$ with integer coefficients such that for all positive integers a, b, c that are the side lengths of a right-angled triangle, the numbers $P(a), P(b), P(c)$ are also the side lengths of a right-angled triangle.

Problem 8.61. Find all polynomials P, Q with real coefficients such that

$$P(Q(x)) = P(x)^{2017}.$$

Problem 8.62. Evaluate the sum

$$\sum_{k=1}^{1000} \frac{(2^k - 3^1) \cdot \ldots \cdot (2^k - 3^{1000})}{(2^k - 2^1) \cdot \ldots \cdot (2^k - 2^{k-1})(2^k - 2^{k+1}) \cdot \ldots \cdot (2^k - 2^{1000})}.$$

Problem 8.63. Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$. Prove that

$$\sum_{k=1}^{n} \frac{\prod_{i=1}^{n} (a_k + b_i)}{\prod_{i \neq k} (a_k - a_i)} = \sum_{k=1}^{n} \frac{\prod_{i=1}^{n} (b_k + a_i)}{\prod_{i \neq k} (b_k - b_i)}.$$

Chinese Team Selection Test 2010

Problem 8.64. Let $b_i = (a_i - a_1) \cdot \ldots \cdot (a_i - a_{i-1})(a_i - a_{i+1}) \cdot \ldots \cdot (a_i - a_n)$. Prove that $(n-1)!$ divides $\operatorname{lcm}(b_1, \ldots, b_n)$.

Fedor Petrov - Saint Petersburg Mathematical Olympiad 2005

Problem 8.65. Let $P(x)$ be a nonconstant polynomial with real coefficients. For all positive real numbers M, prove that there is a positive integer m such that for any monic polynomial $Q(x)$ of degree greater than or equal to m, the total number of integer solutions of the inequality $|P(Q(x))| \leq M$ does not exceed $\deg Q(x)$.

Navid Safaei - Iranian Mathematical Olympiad 2018

Problem 8.66. Find all distinct positive integers $a_1, \ldots, a_n$ such that for each positive integer $k = 1, \ldots, n$ the number $a_1 \cdot \ldots \cdot a_n$ divides $(k+a_1) \cdot \ldots \cdot (k+a_n)$.

Problem 8.67. Let d be a positive integer. Find the largest value of the constant $C(d)$ such that for any polynomial $P(x) = a_0 + \ldots + a_d x^d$ of degree d with complex coefficients and every permutation $(x_0, \ldots, x_d)$ of $(0, 1, \ldots, d)$, we have

$$\sum_{k=0}^{d} |P(x_k) - P(x_{k+1})| \geq C|a_d|,$$

where $x_{d+1} = x_0$.

Chinese Team Selection Test 2010

Problem 8.68. Let $d > 1$ be an odd integer and let $P(x)$ be a polynomial of degree d. Suppose that $P(k) = 2^k$ for $k = 0, 1, 2, \ldots, d$. Prove that $P(x)$ is divisible by $x + 1$, but it is not divisible by $(x + 1)^2$.

Navid Safaei

Problem 8.69. Let $d > 1$ be an odd integer and $P(x)$ be a polynomial of degree d. Suppose that $P(k) = 2^k$ for $k = 0, 1, 2, \ldots, d$. Prove that there exist at most finitely many integers x such that $P(k)$ is some power of 2.

Taiwanese Team Selection Test 2018

Problem 8.70. A polynomial $P(x)$ of degree d satisfies $P(k) = 2^k$ for all integers $k = 0, 1, \ldots, d$.
Prove that $P(k) \geq 2^{k-1}$ for all integers $k = d + 1, d + 2, \ldots, 2d + 1$.

Problem 8.71. Let $P(x)$ be a polynomial with complex coefficients of degree d such that $P(0) = 0$. Show that for each complex number α, $|\alpha| < 1$, there are complex numbers $z_1, \ldots, z_{d+2}$ on the unit circle such that

$$P(\alpha) = \sum_{i=1}^{d+2} P(z_i).$$

American Mathematical Monthly 11432

Problem 8.72. Let a, b, c be integers such that $a + b + c = 0$. Prove that:

(i) $(a^2b^2 + c^2b^2 + a^2c^2) \mid (a^5b^5 + c^5b^5 + a^5c^5)$;

(ii) If $n - 1$ is divisible by 3, then $(a^2 + b^2 + c^2) \mid (a^n + b^n + c^n)$;

(iii) if $n - 2$ is divisible by 3, then $(a^2b^2 + c^2b^2 + a^2c^2) \mid (a^nb^n + c^nb^n + c^na^n)$.

Kvant, Problem M2023

Problem 8.73. Let $x_1, \ldots, x_n \in \mathbb{Z}$ satisfy $\gcd(x_1, \ldots, x_n) = 1$.
Define $s_k = x_1^k + \ldots + x_n^k$. Prove that

$$\gcd(s_1, \ldots, s_n) \mid \operatorname{lcm}(1, 2, \ldots, n).$$

Komal

Problem 8.74. Let $x_1, \ldots, x_{1000}$ be integers such that

$$\sum_{i=1}^{1000} x_i^k \equiv 0 \pmod{2017} \quad \text{for all} \quad k = 1, 2, \ldots, 672.$$

Prove that $2017 \mid x_i$ for all $i = 1, 2, \ldots, 1000$.

Japanese Mathematical Olympiad 2017

Problem 8.75. Let n be an integer not divisible by 3. Find all integer solutions of the equation

$$(a^2 - bc)^n + (b^2 - ac)^n + (c^2 - ab)^n = 1.$$

H. Van Der Berg - Mathematical Reflections, Problem O52

Problem 8.76. Let $r > 0$ and $r = r^{\frac{2}{3}} + 1$. Prove that there exists a positive integer N such that

$$4^{100} \left| N - r^{300} \right| < 1.$$

Problem 8.77. Find all integers n such that for any positive real numbers a, b, c, x, y, z such that

$$\max(a, b, c, x, y, z) = a, \quad a + b + c = x + y + z, \quad abc = xyz,$$

the inequality $a^n + b^n + c^n \geq x^n + y^n + z^n$ holds.

Chinese Team Selection Test 2018

Part II

Solutions to the Proposed Problems

Chapter 1

On the Form $x^d P\left(\frac{1}{x}\right)$

Problem 1.1. Let $a_1, \ldots, a_n$ be natural numbers whose sum is 2020. Find the least positive real number t such that the equation

$$\sum_{i=1}^{n} \frac{a_i x^i}{1+x^{2i}} = t.$$

has only one positive real root.

Solution. Let $f(x) = \sum_{i=1}^{n} \frac{a_i x^i}{1+x^{2i}}$. It is easy to check that $f(x) = f\left(\frac{1}{x}\right)$. Hence if r is any root of $f(x) = t$, then $\frac{1}{r}$ is another root of the same equation unless $r = \frac{1}{r}$, that is $r = \pm 1$. Thus if there is exactly one positive real root it must be $r = 1$. Plugging in $x = 1$, we find that $t = 1010$. Moreover,

$$\sum_{i=1}^{n} \frac{a_i x^i}{1+x^{2i}} - 1010 = -\sum_{i=1}^{n} \frac{a_i (x^i - 1)^2}{1+x^{2i}} \leq 0$$

with equality only at $x = 1$. Thus for $t = 1010$, $x = 1$ is the only root. ■

Problem 1.2. Let $a_0 + a_1 x + a_2 x^2 + \ldots + a_{2n} x^{2n}$ be the polynomial obtained expanding $(1 + x + x^2)^n$. Compute:

(i) $a_0 + a_2 + \ldots + a_{2n}$;
(ii) $a_1 + a_3 + \ldots + a_{2n-1}$;
(iii) $a_0a_1 - a_1a_2 + a_2a_3 - \ldots - a_{2n-1}a_{2n}$.

Italian Mathematical Olympiad 1994

Solution. Let $P(x) = (1 + x + x^2)^n = a_0 + a_1x + a_2x^2 + \ldots + a_{2n}x^{2n}$. We have

$$P(1) = a_0 + a_1 + \ldots + a_{2n} = (1 + 1 + 1)^n = 3^n,$$

and

$$P(-1) = a_0 - a_1 + a_2 - \ldots + a_{2n} = (1 - 1 + 1)^n = 1.$$

Adding and subtracting side by side the two identities, we get

$$\begin{aligned} a_0 + a_2 + \ldots + a_{2n} &= \frac{P(1) + P(-1)}{2} = \frac{3^n + 1}{2}, \\ a_1 + a_3 + \ldots + a_{2n-1} &= \frac{P(1) - P(-1)}{2} = \frac{3^n - 1}{2}. \end{aligned}$$

Now, for point (iii), observe that

$$P\left(\frac{1}{x}\right) = \frac{1}{x^{2n}}P(x),$$

so $a_i = a_{2n-i}$ for all $i = 0, 1, \ldots, n-1$. It follows that $a_ia_{i+1} = a_{2n-1-i}a_{2n-i}$ for all $i = 0, 1, \ldots, n-1$. So

$$\begin{aligned} a_0a_1 - a_1a_2 + a_2a_3 - \ldots - a_{2n-1}a_{2n} &= \sum_{i=0}^{n-1}(-1)^i(a_ia_{i+1} - a_{2n-1-i}a_{2n-i}) \\ &= 0. \end{aligned}$$

■

Problem 1.3. Let $P(x) = a_nx^n + \ldots + a_0$ be a nonzero polynomial with complex coefficients. We say that $P(x)$ is *reciprocal* if $a_k = a_{n-k}$ for all $k \in \{0, 1, \ldots, n\}$ or $a_k = -a_{n-k}$ for all $k \in \{0, 1, \ldots, n\}$. To each such polynomial we associate the symbol $[P(x)]$ defined as follows: $[P(x)] = 1$ if $a_k = a_{n-k}$ for all $k \in \{0, 1, \ldots, n\}$ and $[P(x)] = -1$ if $a_k = -a_{n-k}$ for all $k \in \{0, 1, \ldots, n\}$.

(a) Prove that if $P(x)$ and $Q(x)$ are reciprocal, then $PQ(x)$ is reciprocal and $[PQ(x)] = [P(x)][Q(x)]$.

(b) Prove that if $P(x)$ and $PQ(x)$ are reciprocal, then $Q(x)$ is reciprocal and $[Q(x)] = \dfrac{[PQ(x)]}{[P(x)]}$.

Marcel Ţena - Nicolae Teodorescu Competition 2007

Solution. If $P(x)$ is a reciprocal polynomial, we observe that the following are equivalent:

$$[P] = 1 \iff P\left(\frac{1}{x}\right) = \frac{1}{x^n}P(x), \qquad [P] = -1 \iff P\left(\frac{1}{x}\right) = -\frac{1}{x^n}P(x).$$

Hence

$$P\left(\frac{1}{x}\right) = \frac{[P(x)]}{x^n}P(x). \tag{1.1}$$

(a) If $P(x)$ and $Q(x)$ are reciprocal, $\deg P(x) = n$, $\deg Q(x) = m$, then from (1.1), we have

$$P\left(\frac{1}{x}\right) = \frac{[P(x)]}{x^n}P(x), \quad Q\left(\frac{1}{x}\right) = \frac{[Q(x)]}{x^m}Q(x).$$

Multiplying these equations side by side, we get

$$PQ\left(\frac{1}{x}\right) = \frac{[P(x)][Q(x)]}{x^{n+m}}PQ(x),$$

which proves that $PQ(x)$ is a reciprocal polynomial and

$$[PQ(x)] = [P(x)][Q(x)].$$

(b) Let $\deg P(x) = n$ and $\deg Q(x) = m$. If $P(x)$ and $PQ(x)$ are reciprocal, from (1.1) we have

$$P\left(\frac{1}{x}\right) = \frac{[P(x)]}{x^n}P(x), \quad PQ\left(\frac{1}{x}\right) = \frac{[PQ(x)]}{x^{n+m}}PQ(x).$$

Dividing the second equation by the first, we get

$$Q\left(\frac{1}{x}\right) = \frac{\frac{[PQ(x)]}{[P(x)]}}{x^m} Q(x),$$

which proves that $Q(x)$ is a reciprocal polynomial and $[Q(x)] = \frac{[PQ(x)]}{[P(x)]}$. ■

Problem 1.4. A self-reciprocal polynomial $P(x) = \sum_{j=0}^{d} a_j x^j$ satisfies

$$a_1 = a_{d-1},\ a_2 = a_{d-2}, \ldots, a_d = a_0.$$

Consider all the self-reciprocal polynomials with integer coefficients that are factors of $x^{1234} - x^3 - x + 1$. Find the factor that has the largest degree.

Solution. Assume that $Q(x)$ be a self-reciprocal factor of $x^{1234} - x^3 - x + 1$ and let $d = \deg Q(X)$. Then we can write $x^{1234} - x^3 - x + 1 = Q(x) R(x)$, where $\deg R(x) = 1234 - d$. Moreover, by the substitution $x \mapsto \frac{1}{x}$ and the fact that Q is self-reciprocal, we get

$$x^{1234} - x^{1233} - x^{1231} + 1 = Q(x)\left(x^{1234-d} R\left(\frac{1}{x}\right)\right).$$

Hence $Q(x)$ is a common divisor of $x^{1234} - x^3 - x + 1$ and $x^{1234} - x^{1233} - x^{1231} + 1$. Note that

$$x^3\left(x^{1234} - x^{1233} - x^{1231} + 1\right) - \left(x^3 - x^2 - 1\right)\left(x^{1234} - x^3 - x + 1\right) = (x-1)^2\left(x^2+1\right)\left(x^2+x+1\right).$$

Whence $Q(x)$ divides $(x-1)^2\left(x^2+1\right)\left(x^2+x+1\right)$.
First, we will show that $x^{1234} - x^3 - x + 1$ is divisible by $x^2 + 1$ and

$$(x^2 + x + 1)(x - 1) = x^3 - 1.$$

For $x^2 + 1$, writing the polynomial as $x^{1234} + 1 - x\left(x^2 + 1\right)$, it remains to show that $x^{1234} + 1$ is divisible by $x^2 + 1$, which is clear, because

$$x^{1234} + 1 = (x^2)^{617} + 1^{617} = \left(x^2 + 1\right)\left((x^2)^{616} - (x^2)^{615} + \cdots - x^2 + 1\right).$$

For $x^3 - 1$, writing the polynomial as $x\left(x^{1233} - 1\right) - \left(x^3 - 1\right)$, we have that $x^{1233} - 1$ is divisible by $x^3 - 1$ because 1233 is divisible by 3.
Next, we prove that $(x-1)^2$ doesn't divide $x^{1234} - x^3 - x + 1$. Assume on the contrary, that $x^{1234} - x^3 - x + 1 = (x-1)^2 T(x)$ for some polynomial $T(x)$ with real coefficients. By the substitution $x \mapsto x + 1$, we get

$$(x+1)^{1234} - (x+1)^3 - x = x^2 T(x+1).$$

The coefficient of x on the left-hand side is $1234 - 3 - 1 = 1230$, but on the right-hand side it is 0, a contradiction. Therefore $Q(x)$ cannot be divisible by $(x-1)^2$ and so $Q(x)$ must divide $(x-1)\left(x^2+1\right)\left(x^2+x+1\right)$.
However, if $x-1$ is a factor of $Q(x)$, then since Q is self-reciprocal $(x-1)^2$ must be a factor. Thus Q must divide $\left(x^2+1\right)\left(x^2+x+1\right)$. Hence Q has degree at most 5 and $\left(x^2+1\right)\left(x^2+x+1\right)$ is a self-reciprocal factor of $x^{1234} - x^3 - x + 1$ of degree 5. Thus it is the highest degree self-reciprocal factor. ■

Problem 1.5. If the monic polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$ has all its roots $x_1, x_2, \ldots, x_n$ in the interval $[-1, 1]$ and its coefficients satisfy the property $a_{n-i} = a_i$, $i = 0, 1, \ldots, n$, prove that $f(x) = (x+1)^p (x-1)^{2q}$, where $p, q \in \mathbb{N}$ and $p + 2q = n$.

Marcel Ţena - Gazeta Matematică B 5/2009, *Problem* 26158

Solution. Since f is monic, $a_n = a_0 = 1$, so $f(0) = 1 \neq 0$. So $x_k \neq 0$ for all $k = 1, 2, \ldots, n$. We have

$$\begin{aligned} f\left(\frac{1}{x_k}\right) &= \sum_{i=0}^{n} \frac{a_i}{x_k^i} = \frac{1}{x_k^n} \sum_{i=0}^{n} a_i x_k^{n-i} \\ &= \frac{1}{x_k^n} \sum_{i=0}^{n} a_{n-i} x_k^{n-i} = \frac{1}{x_k^n} f(x_k) \\ &= 0, \end{aligned}$$

so $\frac{1}{x_k} \in [-1, 1]$ for all $k = 1, 2, \ldots, n$. Since $x_k \in [-1, 1]$, we conclude that $x_k \in \{-1, 1\}$ for all $k = 1, 2, \ldots, n$ and therefore $f(x) = (x+1)^p (x-1)^{n-p}$,

where p is the multiplicity of the root -1. As $f(0) = 1$, we get $1 = (-1)^{n-p}$, so $n - p = 2q$ for some $q \in \mathbb{N}$. ■

Problem 1.6. Let $P(x) = a_{2n}x^{2n} + a_{2n-1}x^{2n-1} + \ldots + a_0$ such that $a_k = a_{2n-k}$ for $k = 0, 1, \ldots, n$.

(i) Prove that there exists a polynomial Q such that

$$P(x) = x^n Q\left(x + \frac{1}{x}\right).$$

(ii) If $a_0 = a_{2n} = 1$ and $|a_n| < 2$, prove that $P(x)$ has at least one complex root.

Romanian Mathematical Olympiad

Solution. (i) Divide the polynomial $P(x)$ by x^n. Then

$$\begin{aligned} \frac{P(x)}{x^n} &= \frac{a_{2n}x^{2n} + a_{2n-1}x^{2n-1} + \ldots + a_0}{x^n} \\ &= a_{2n}x^n + \frac{a_0}{x^n} + a_{2n-1}x^{n-1} + \frac{a_1}{x^{n-1}} + \ldots + a_n. \end{aligned}$$

Since $a_k = a_{2n-k}$, we find that

$$\frac{P(x)}{x^n} = a_{2n}\left(x^n + \frac{1}{x^n}\right) + a_{2n-1}\left(x^{n-1} + \frac{1}{x^{n-1}}\right) + \ldots + a_n.$$

We can easily prove by induction that $x^r + \frac{1}{x^r}$ is a polynomial in $x + \frac{1}{x}$ for all positive integer r. Thus the left-hand side of the above equality is a polynomial in $x + \frac{1}{x}$. Therefore there is a polynomial $Q(x)$ such that

$$\frac{P(x)}{x^n} = Q\left(x + \frac{1}{x}\right).$$

(ii) We have $P(x) = x^{2n} + a_{2n-1}x^{2n-1} + \ldots + 1$.
Since P is a self-reciprocal polynomial of even degree, it follows from Example 1.7 that we can write the roots, with multiplicity, as $\left\{x_1, \ldots, x_n, \frac{1}{x_1}, \ldots, \frac{1}{x_n}\right\}$.

Letting $g(x) = (x - x_1) \cdot \ldots \cdot (x - x_n)$ and $h(x) = \left(x - \frac{1}{x_1}\right) \cdot \ldots \cdot \left(x - \frac{1}{x_n}\right)$, we have $P(x) = g(x)h(x)$. By Vieta's Formulas, we have

$$g(x) = x^n + b_1x^{n-1} + \ldots + b_{n-1}x + b_n, \quad h(x) = x^n + \frac{b_{n-1}}{b_n}x^{n-1} + \ldots + \frac{b_1}{b_n}x + \frac{1}{b_n}.$$

Comparing the coefficients of x^n in $P(x)$ and in $g(x)h(x)$, we find that

$$a_n = b_n + \frac{1}{b_n} + \frac{b_{n-1}^2}{b_n} + \frac{b_{n-2}^2}{b_n} + \ldots + \frac{b_1^2}{b_n}.$$

Hence

$$-b_n^2 - a_nb_n - 1 = b_{n-1}^2 + b_{n-2}^2 + \ldots + b_1^2.$$

Let $Q(x) = -x^2 - a_nx - 1$. Note that the discriminant of the quadratic polynomial $Q(x)$ is $a_n^2 - 4 < 0$. Since the leading coefficient of $Q(x)$ is negative, we have that $Q(x) < 0$ for all x. Now, if all the roots of the polynomial $P(x)$ were real, then by Vieta's Formulas we would find that all the values of $b_1, \ldots, b_{n-1}$ are real. Thus $Q(b_n) = b_{n-1}^2 + b_{n-2}^2 + \ldots + b_1^2 \geq 0$, a contradiction. Thus P must have a complex root. ■

Problem 1.7. Let $P(x) = a_dx^d + \ldots + a_1x + a_0$ and define

$$C(P(x)) = a_d^2 + a_{d-1}^2 + \ldots + a_1^2 + a_0^2.$$

Let $P(x) = 3x^2 + 7x + 2$. Find a polynomial $Q(x)$ with real coefficients such that $Q(0) = 1$ and $C((P(x))^n) = C((Q(x))^n)$ for every positive integer n.

Solution. It is easy see that the coefficient of x^0 in $P(x)P\left(\frac{1}{x}\right)$ is equal to $C(P(x))$. If we find a polynomial Q with $Q(0) = 1$ and

$$Q(x)Q\left(\frac{1}{x}\right) = P(x)P\left(\frac{1}{x}\right),$$

then we will have $Q(x)^nQ\left(\frac{1}{x}\right)^n = P(x)^nP\left(\frac{1}{x}\right)^n$ for all positive integer n and hence $C(Q(x)^n) = C(P(x)^2)$ for all positive integer n. Thus we will have the desired example.

To find such a Q, note that $P(x) = (3x+1)(x+2)$, so if we take

$$Q(x) = (3x+1)(2x+1) = 6x^2 + 5x + 1,$$

then we will have $Q(0) = 1$ and

$$\begin{aligned} P(x)P\left(\frac{1}{x}\right) &= (3x+1)(x+2)\left(\frac{3}{x}+1\right)\left(\frac{1}{x}+2\right) \\ &= \frac{(3x+1)(x+3)(x+2)(2x+1)}{x^2} \end{aligned}$$

and

$$\begin{aligned} Q(x)Q\left(\frac{1}{x}\right) &= (3x+1)(2x+1)\left(\frac{3}{x}+1\right)\left(\frac{2}{x}+1\right) \\ &= \frac{(3x+1)(x+3)(x+2)(2x+1)}{x^2} \end{aligned}$$

will be equal. ∎

Remark. There are many other possibilities for the polynomial $Q(x)$. For example, the polynomials $Q(x) = (3x^k+1)(2x^k+1)$ and $Q(x) = (3x^k-1)(2x^k-1)$ would also work.

Problem 1.8. Find all positive integers n for which there is a polynomial $P(x)$ with real coefficients satisfying

$$P(x^{1998} - x^{-1998}) = x^n - x^{-n} \qquad \forall x \neq 0.$$

Vietnamese Mathematical Olympiad 1998

Solution. We prove the general case, i.e., we find all positive integers k, n for which there is a polynomial $P(x)$ with real coefficients satisfying

$$P(x^k - x^{-k}) = x^n - x^{-n} \qquad \forall x \neq 0.$$

Let $P(x) = \sum_{i=0}^{m} a_i x^i$, where $a_m \neq 0$. Then $P(x^k - x^{-k}) = x^n - x^{-n}$ is equivalent to

$$\sum_{i=0}^{m} a_i \frac{(x^{2k}-1)^i}{x^{ki}} = \frac{x^{2n}-1}{x^n}, \tag{1.2}$$

i.e.,

$$\sum_{i=0}^{m} a_i x^n (x^{2k}-1)^i x^{k(m-i)} = x^{km}(x^{2n}-1) \qquad \forall x \neq 0.$$

Since the polynomial on the left-hand side is of degree $n+2km$ and the polynomial on the right-hand side is of degree $2n+km$, then $n+2km = 2n+km$, which gives $n = km$. We will prove that m must be odd. Indeed, assume that m is even. Setting $y = x^k$, we can write the given equation as

$$P\left(y - \frac{1}{y}\right) = y^m - \frac{1}{y^m} \qquad \forall y \neq 0. \tag{1.3}$$

Substituting $y = 2$ and $y = -\frac{1}{2}$ into (1.3), we get

$$P\left(\frac{3}{2}\right) = 2^m - \frac{1}{2^m} > 0 \quad \text{and} \quad P\left(\frac{3}{2}\right) = \frac{1}{2^m} - 2^m < 0,$$

a contradiction. Hence if there exists a polynomial satisfying the given properties, it follows that $n = km$ with m odd.

Now we prove that the converse is also true. Assume that $n = km$ with m odd. Setting again $y = x^k$, we prove by induction on m that there exists a polynomial $P(x)$ satisfying (1.3)

If $m = 1$, we see that $P_1(y) = y$ satisfies (1.3). If $m = 3$, then $P_3(y) = y^3 + 3y$ satisfies (1.3). Suppose that $P_1, P_3, \ldots, P_m$ satisfy (1.3). Let

$$P_{m+2}(x) = (x^2+2)P_m(x) - P_{m-2}(x).$$

By the inductive hypothesis, we have ($y \neq 0$)

$$\begin{aligned} P_{m+2}\left(y - \frac{1}{y}\right) &= \left(\left(y - \frac{1}{y}\right)^2 + 2\right) P_m\left(y - \frac{1}{y}\right) - P_{m-2}\left(y - \frac{1}{y}\right) \\ &= \left(y^2 + \frac{1}{y^2}\right)\left(y^m - \frac{1}{y^m}\right) - \left(y^{m-2} - \frac{1}{y^{m-2}}\right) \\ &= y^{m+2} - \frac{1}{y^{m+2}}. \end{aligned}$$

The conclusion follows from the principle of mathematical induction.
Now, we go back to the given problem and we conclude that $n = 1998m$, where m is an odd positive integer. ■

Problem 1.9. Let $n \not\equiv 2 \pmod 3$.
Prove that the polynomial $P(x) = x^n + x + 1$ is irreducible over $\mathbb{Z}[x]$.

Solution. Assume the contrary. Then there are polynomials $g(x)$ and $h(x)$ with integer coefficients such that $x^n + x + 1 = g(x)h(x)$.
Let $Q(x) = g(x)h\left(\frac{1}{x}\right) = c_1x^{m_1} + \ldots + c_lx^{m_l}$, where $c_1, \ldots, c_l$ are integers and $m_1, \ldots, m_l$ are distinct integers. Note that

$$P(x)P\left(\frac{1}{x}\right) = g(x)g\left(\frac{1}{x}\right)h(x)h\left(\frac{1}{x}\right) = Q(x)Q\left(\frac{1}{x}\right).$$

Considering the constant terms on both sides, we find that $3 = c_1^2 + \ldots + c_l^2$. Hence $l = 3$ and $c_i = \pm 1$. So $Q(x) = ax^r + bx^s + cx^t$, where $a, b, c = \pm 1$ and $r > s > t$. Note that

$$P(x)P\left(\frac{1}{x}\right) = x^n + x^{n-1} + x + 3 + x^{-1} + x^{1-n} + x^{-n}.$$

On the other hand,

$$Q(x)Q\left(\frac{1}{x}\right) = acx^{r-t} + abx^{r-s} + bcx^{s-t} + 3 + bcx^{t-s} + abx^{s-r} + acx^{t-r}.$$

Hence by comparing the coefficients of both rational functions, we find that $a = b = c = \pm 1$. We also see that $r - t$ is the highest degree exponent in $Q(x)Q\left(\frac{1}{x}\right)$, so $r - t = n$. Since we do not know which of $r - s$ and $s - t$ is larger, all we can conclude from those terms is that $\{r - s, s - t\} = \{n - 1, 1\}$. However if we interchange the roles of g and h, then we replace Q by $Q\left(\frac{1}{x}\right)$, so we may assume $s - t = 1$. Thus $r = t + n$, $s = t + 1$ and so $Q(x) = \pm x^t P(x)$. Hence

$$\pm x^t = \frac{Q(x)}{P(x)} = \frac{g(x)h\left(\frac{1}{x}\right)}{g(x)h(x)} = \frac{h\left(\frac{1}{x}\right)}{h(x)},$$

so $h\left(\frac{1}{x}\right) = \pm x^t h(x)$. In particular, if a is any root of $h(x)$, then $\frac{1}{a}$ is also a root. But that means a and $\frac{1}{a}$ are both roots of $P(x)$. This implies that

$$a^n + a + 1 = 0, \qquad a^n + a^{n-1} + 1 = 0.$$

Therefore $a^{n-2} = 1$, and hence $a^2 + a + 1 = 0$. However, the roots of this quadratic are the primitive cube roots of unity, and since $n \not\equiv 2 \pmod 3$, we have $a^{n-2} \neq 1$, a contradiction. ■

Remark. The same approach is applicable for the proof of the irreducibility of the polynomial $P(x) = x^n - x - 1$, which is called the *Selmer Polynomial*.

Problem 1.10. Let n be an even positive integer, and let $c_1, \ldots, c_n$ be real numbers such that

$$\sum_{i=1}^{n} |c_i - 1| < 1.$$

Prove that the polynomial $P(x) = 2x^n - c_{n-1}x^{n-1} + c_{n-2}x^{n-2} - \ldots - c_1x + 2$ has no real roots.

Po Shen Loh - USA Team Selection Test 2014

Solution. Note that $x^nP\left(\frac{1}{x}\right) = 2x^n - c_1x^{n-1} + c_2x^{n-2} - \ldots - c_{n-2}x + 2$ also satisfies the hypotheses of the problem. Thus it suffices to show that $P(x)$ has no roots in $[-1, 1]$. Applying this easier result to both $P(x)$ and $x^nP\left(\frac{1}{x}\right)$, will show that $P(x)$ has no real roots.
Since $|c_i - 1| < 1$, we find that $c_i \in (0, 2)$ for all i. Putting $c_i = 1 + d_i$ with $d_i \in (-1, 1)$, we rewrite the polynomial expression as

$$2x^n - (1 + d_{n-1})x^{n-1} + (1 + d_{n-2})x^{n-2} - \ldots - (1 + d_1)x + 2.$$

The above expression is equal to $P_1(x) + P_2(x) + P_3(x)$ where

$$P_1(x) = x^n - x^{n-1} + x^{n-2} - \ldots - x + 1, \; P_2(x) = x^n + 1 \text{ and}$$

$$P_3(x) = \sum_{i=1}^{n-1} (-1)^i d_i x^i.$$

For negative x every term of $P_1(x)$ is positive, and hence $P_1(x) > 0$, and for positive x, we have $P_1(x) = \frac{x^{n+1}+1}{x+1} > 0$. Thus $P_1(x) > 0$ for all real x.
We will be done if we prove that $P_2(x) + P_3(x) > 0$ for $x \in [-1, 1]$. Since $P_2(0) + P_3(0) = 1$, it suffices to show that $P_2(x) + P_3(x)$ has no roots in $[-1, 1]$. Assume that $x \in [-1, 1]$. By Triangle Inequality,

$$\left|\sum_{i=1}^{n-1}(-1)^i d_i x^i\right| \le \sum_{i=1}^{n-1}|d_i| < 1.$$

Thus

$$P_2(x) + P_3(x) = x^n + 1 + \sum_{i=1}^{n-1}(-1)^i d_i x^i \ge x^n + 1 - \left|\sum_{i=1}^{n-1}(-1)^i d_i x^i\right| > x^n > 0.$$

Remark. Rather than using the reciprocal polynomial of P, we could have given the following direct proof that $P_2(x) + P_3(x)$ has no roots for $|x| > 1$: If $|x| > 1$, then $-1 < \frac{1}{x} < 1$, so we have

$$\left|\sum_{i=1}^{n-1}(-1)^i d_i \left(\frac{1}{x}\right)^{n-i}\right| \le \sum_{i=1}^{n-1}|d_i| < 1$$

Therefore $\left|\sum_{i=1}^{n-1}(-1)^i d_i x^i\right| < x^n$, which implies that

$$P_2(x) + P_3(x) \ge x^n + 1 - \left|\sum_{i=1}^{n-1}(-1)^i d_i x^i\right| > x^n + 1 - x^n > 1 > 0.$$

Problem 1.11. Let $a_1, \ldots, a_n$ be complex numbers with modulus $r > 0$. Denote by T_s the sum of products of any s numbers from $a_1, \ldots, a_n$. Assume that $T_{n-s} \neq 0$. Prove that $\left|\frac{T_s}{T_{n-s}}\right| = r^{2s-n}$.

Solution. Let $P(z) = (z+a_1)\cdot\ldots\cdot(z+a_n) = z^n + T_1 z^{n-1} + T_2 z^{n-2} + \ldots + T_n$. The roots of $P(z)$ are $-a_1, \ldots, -a_n$ (which are nonzero since $r > 0$), hence the roots of the reciprocal polynomial $z^n P\left(\frac{1}{z}\right) = T_n z^n + \ldots + 1$ are

$$-\frac{1}{a_1} = -\frac{\overline{a_1}}{r^2}, \ldots, -\frac{1}{a_n} = -\frac{\overline{a_n}}{r^2}.$$

Hence the roots of the polynomial $\overline{T_n} z^n + \overline{T_{n-1}} z^{n-1} \ldots + 1$ are $-\frac{a_1}{r^2}, \ldots, -\frac{a_n}{r^2}$. By Vieta's Formulas, we easily deduce that

$$\sum_{i_1<\cdots<i_s} \frac{a_{i_1}}{r^2}\cdot\frac{a_{i_2}}{r^2}\cdot\ldots\cdot\frac{a_{i_s}}{r^2} = \left(\frac{1}{r^2}\right)^{n-s} T_{n-s} = \frac{\overline{T_s}}{\overline{T_n}}.$$

This implies

$$\left|\frac{\overline{T_s}}{\overline{T_n}}\right| = \left|\frac{T_s}{T_n}\right| = \frac{|T_{n-s}|}{r^{2n-2s}}.$$

Hence $\left|\frac{T_s}{T_{n-s}}\right| = \frac{|T_n|}{r^{2n-2s}}$. It remains to note that

$$|T_n| = |a_1 \cdot \ldots \cdot a_n| = |a_1| \cdot \ldots \cdot |a_n| = r^n,$$

whence $\left|\frac{T_s}{T_{n-s}}\right| = r^{2s-n}$. ■

Problem 1.12. For a polynomial $P(x) = b_d x^d + \ldots + b_0$, we define the BB-sum of $P(x)$ as the number $b_0 b_1 + b_1 b_2 + \ldots + b_{d-1} b_d$. Determine whether there exist real numbers r and s such that for every positive integer k, the BB-sum of $(x^2 + rx + s)^k$ is equal to the BB-sum of $(2x^2 + 7x + 3)^k$.

Solution. The BB-sum of the polynomial $P(x) = b_d x^d + \ldots + b_0$ is equal to the coefficient of x in the product $P(x)P\left(\frac{1}{x}\right)$. Since $2x^2 + 7x + 3 = (2x+1)(x+3)$, the BB-sum of $(2x^2 + 7x + 3)^k$ is the coefficient of x in

$$\left((2x+1)(x+3)\left(\frac{2}{x}+1\right)\left(\frac{1}{x}+3\right)\right)^k = \left((x+2)(x+3)\left(\frac{1}{x}+2\right)\left(\frac{1}{x}+3\right)\right)^k.$$

Whence the coefficient of x in the latter expression is the BB-sum of the polynomial $((x+2)(x+3))^k = (x^2 + 5x + 6)^k$. So $r = 5$ and $s = 6$ are such numbers. ■

Problem 1.13. Let $P(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0$ be a polynomial of degree $d \geq 3$ with integer coefficients such that $a_k + a_{d-k}$ is even for $k = 1, 2, \ldots, d-1$ and a_0 is also even. If $P(x) = Q(x)R(x)$, where $R(x)$ and $Q(x)$ are nonconstant polynomials with integer coefficients and $\deg Q(x) \leq \deg R(x)$ and all the coefficients of $R(x)$ are odd, show that $P(x)$ has at least one integer root.

Solution. We may assume that $Q(x)$ and $R(x)$ are both monic.
Let $s = \deg R(x)$. Then the hypotheses say $d/2 \leq s < d$. Let

$$Q_1(x) = x^{d-s}Q\left(\frac{1}{x}\right).$$

We will work modulo 2, that is, with polynomials in $\mathbb{Z}_2[x]$. For a polynomial with integer coefficients, we will use a hat on it to denote that we have reduced all its coefficients modulo 2.
The hypotheses of the problem then say that the polynomial $P_1(x) = \hat{P}(x)+\hat{1}$ is self-reciprocal in $\mathbb{Z}_2[x]$, that $P_1(x) + \hat{1} = \hat{P}(x) = \hat{Q}(x)\hat{R}(x)$, and that $\hat{R}(x) = x^s + x^{s-1} + \cdots + x + \hat{1}$. Putting this together we have

$$P_1(x) + \hat{1} = \hat{Q}(x)\left(x^s + x^{s-1} + \ldots + x + \hat{1}\right).$$

Now, using the substitution $x \mapsto \frac{1}{x}$ and multiplying both sides by x^d, and using the fact that $P_1(x)$ and $\hat{R}(x)$ are self-reciprocal we have

$$P_1(x) + x^d = \hat{Q}_1(x)\left(x^s + x^{s-1} + \ldots + x + \hat{1}\right).$$

Therefore by adding the above equations, we find that

$$x^d + \hat{1} = \left(x^s + x^{s-1} + \ldots + x + \hat{1}\right)\left(\hat{Q}(x) + \hat{Q}_1(x)\right).$$

Since $x^d + \hat{1} = (x^d + x^{d-s-1}) + (x^{d-s-1} + \hat{1})$ and

$$x^d + x^{d-s-1} = x^{d-s-1}(x + \hat{1})\left(x^s + x^{s-1} + \ldots + x + \hat{1}\right),$$

it follows that $x^s + x^{s-1} + \ldots + x + \hat{1}$ divides $x^{d-s-1} - \hat{1}$. Hence either $d = s+1$ so that this is the zero polynomial or $d - s - 1 \geq s$. Since we assumed $s \geq d/2$, the second possibility does not occur. Thus $d = s + 1$ and hence Q is a linear polynomial and its real root is an integer root of P. ■

Chapter 2

Complex Numbers and Polynomials. Part I

Problem 2.1. Let $n \equiv 3 \pmod 8$ and let

$$(x^2 + 1)^n = a_{2n}x^{2n} + a_{2n-1}x^{2n-1} + \ldots + a_1x + a_0.$$

Find $a_0 + a_8 + \ldots + a_{2n-6}$.

Alessandro Ventullo

Solution. Observe that in $x^2 + 1$ appear only terms with even degree, so in $(x^2+1)^n$ appear only terms with even degree, i.e., $a_1 = a_3 = \ldots = a_{2n-1} = 0$. Setting $x = 1$ and $x = i$, we get the system of equations

$$\begin{cases} a_0 + a_2 + \ldots + a_{2n} &= 2^n \\ a_0 - a_2 + \ldots - a_{2n} &= 0. \end{cases}$$

Adding these two equations, we get

$$a_0 + a_4 + \ldots + a_{2n-2} = 2^{n-1}. \tag{2.1}$$

Then setting $x = \sqrt{i}$, we get

$$(1+i)^n = (a_0 - a_4 + \ldots + a_{2n-6} - a_{2n-2}) + i(a_2 - a_6 + \ldots + a_{2n-4} - a_{2n}).$$

Since $1+i=\sqrt{2}e^{\frac{i\pi}{4}}$, using De Moivre's Formula, we have

$$(-\sqrt{2^{n-1}}+i\sqrt{2^{n-1}})=(a_0-a_4+\ldots+a_{2n-6}-a_{2n-2})+i(a_2-a_6+\ldots+a_{2n-4}-a_{2n}).$$

Comparing the real parts, we get

$$a_0-a_4+\ldots+a_{2n-6}-a_{2n-2}=-\sqrt{2^{n-1}},$$

and summing this equation to equation (2.1), we get

$$a_0+a_8+\ldots+a_{2n-6}=\sqrt{2^{n-1}}(\sqrt{2^{n-1}}-1). \quad \blacksquare$$

Problem 2.2. Let x_1,x_2,x_3,x_4 be the roots of the equation

$$x^4-(m+2)x^3+(m^2+m+1)x^2+2x-2=0, \qquad m\in\mathbb{R}.$$

(a) If $x_1=1+i$, find $m\in\mathbb{R}$ and solve the equation.

(b) Under conditions of point (a), evaluate $x_1^{2006}+x_2^{2006}+x_3^{2006}+x_4^{2006}$.

Trident Competition 2006

Solution. **(a)** We compute that $x_1^2=2i$, $x_1^3=-2+2i$, and $x_1^4=-4$.
Thus the equation $x_1^4-(m+2)x_1^3+(m^2+m+1)x_1^2+2x_1-2=0$, becomes

$$-4-2(-1+i)(m+2)+2i(m^2+m+1)+2(1+i)-2=0.$$

This simplifies to $m+im^2=0$, and since m is real this means $m=0$.
For $m=0$, the given equation becomes $x^4-2x^3+x^2+2x-2=0$.
Since

$$\begin{aligned}x^4-2x^3+x^2+2x-2&=x^2(x-1)^2+2(x-1)=(x-1)(x^3-x^2+2)\\&=(x-1)(x+1)(x^2-2x+2),\end{aligned}$$

we get the equation

$$(x-1)(x+1)(x^2-2x+2)=0.$$

We get the solutions $x_1=1+i$, $x_2=1-i$, $x_3=1$, $x_4=-1$.
(b) Using the exponential form for complex numbers, we have $x_1=\sqrt{2}e^{i\frac{\pi}{4}}$ and $x_2=\sqrt{2}e^{-i\frac{\pi}{4}}$. Therefore we get

$$\left(\frac{x_1}{\sqrt{2}}\right)^8=\left(\frac{x_2}{\sqrt{2}}\right)^8=x_3^8=x_4^8=1.$$

As $2006\equiv 6 \pmod 8$, we get

$$\begin{aligned}x_1^{2006}+x_2^{2006}+x_3^{2006}+x_4^{2006}&=\sqrt{2}^{2006}\left(\left(\frac{x_1}{\sqrt{2}}\right)^6+\left(\frac{x_2}{\sqrt{2}}\right)^6\right)+x_3^6+x_4^6\\&=2^{1003}\left(\left(e^{i\frac{\pi}{4}}\right)^6+\left(e^{-i\frac{\pi}{4}}\right)^6\right)+1^6+(-1)^6\\&=2^{1003}(-i+i)+1+1=2. \quad \blacksquare\end{aligned}$$

Problem 2.3. **(a)** Solve in $\mathbb{C}$ the equation

$$x^6+3x^5+12x^4+19x^3+15x^2+6x+1=0.$$

(b) Evaluate $\sum_{k=1}^{6}\left|1+\frac{1}{x_k}\right|$ and $\sum_{k=1}^{6}|x_k|^2$, where x_1,x_2,x_3,x_4,x_5,x_6 are the roots of the given equation.

Vasile Berghea - Gazeta Matematică B 9/2007 *Problem* C:3217

Solution. **(a)** Setting $y=\frac{1}{x}$, the equation becomes

$$y^6+6y^5+15y^4+19y^3+12y^2+3y+1=0,$$

i.e.,

$$(y+1)^6-(y+1)^3+1=0.$$

Let $t=(y+1)^3$. Then the last equation becomes $t^2-t+1=0$, i.e., $t^3=-1$ with $t\neq -1$. Hence $(y+1)^9=-1$ and $(y+1)^3\neq -1$, which gives

$$y+1=\cos\frac{(2k+1)\pi}{9}+i\sin\frac{(2k+1)\pi}{9}$$

or equivalently

$$y_k = -1 + \cos\frac{(2k+1)\pi}{9} + i\sin\frac{(2k+1)\pi}{9}, \qquad k \in \{0,2,3,5,6,8\}.$$

So

$$\begin{aligned} x_k = \frac{1}{y_k} &= \frac{1}{-2\sin^2\frac{(2k+1)\pi}{18} + 2i\sin\frac{(2k+1)\pi}{18}\cos\frac{(2k+1)\pi}{18}} \\ &= \frac{1}{-2\sin\frac{(2k+1)\pi}{18}\left(\sin\frac{(2k+1)\pi}{18} - i\cos\frac{(2k+1)\pi}{18}\right)} \\ &= \frac{\sin\frac{(2k+1)\pi}{18} + i\cos\frac{(2k+1)\pi}{18}}{-2\sin\frac{(2k+1)\pi}{18}} \\ &= -\frac{1}{2}\left(1 + i\cot\frac{(2k+1)\pi}{18}\right), \end{aligned}$$

where $k \in \{0,2,3,5,6,8\}$. Note (for use in part (b)) that the first part of this calculation shows that

$$|y_k| = 2\left|\sin\frac{(2k+1)\pi}{18}\right| = 2\left|\cos\frac{(4-k)\pi}{9}\right|.$$

(b) Let $A = \{0,2,3,5,6,8\}$. For all $k \in A$, we have

$$\left|1 + \frac{1}{x_k}\right| = |1 + y_k| = \left|\cos\frac{(2k+1)\pi}{9} + i\sin\frac{(2k+1)\pi}{9}\right| = 1,$$

so $\sum_{k\in A}\left|1 + \frac{1}{x_k}\right| = 6$. Likewise, for all $k \in A$, we have

$$|x_k| = \frac{1}{|y_k|} = \frac{1}{2\left|\sin\frac{(2k+1)\pi}{18}\right|} = \frac{1}{2\left|\cos\frac{(4-k)\pi}{9}\right|}.$$

Hence

$$\begin{aligned} \sum_{k\in A}|x_k|^2 &= \frac{1}{4}\left(\frac{1}{\cos^2\frac{4\pi}{9}} + \frac{1}{\cos^2\frac{2\pi}{9}} + \frac{1}{\cos^2\frac{\pi}{9}} + \frac{1}{\cos^2\frac{\pi}{9}} + \frac{1}{\cos^2\frac{2\pi}{9}} + \frac{1}{\cos^2\frac{4\pi}{9}}\right) \\ &= \frac{1}{4}\left(\sum_{k=0}^{8}\frac{1}{\cos^2\frac{k\pi}{9}} - \sum_{k=0}^{2}\frac{1}{\cos^2\frac{k\pi}{3}}\right) \end{aligned}$$

If n is odd, we have the identity

$$\sum_{k=0}^{n-1}\frac{1}{\cos^2\frac{k\pi}{n}} = n^2,$$

so

$$\sum_{k\in A}|x_k|^2 = \frac{1}{4}(9^2 - 3^2) = 18. \qquad \blacksquare$$

Remark. One can also compute $\sum_{k\in A}|x_k|^2$ using Vieta's formulas. Note that all the roots x_k have $\operatorname{Re}(x_k) = -\frac{1}{2}$, hence

$$\overline{x_k} = 2\operatorname{Re}(x_k) - x_k = -1 - x_k$$

and

$$|x_k|^2 = x_k\overline{x_k} = -x_k - x_k^2.$$

Since Vieta's formulas give

$$\sum_{k\in A}x_k = -3$$

and

$$\sum_{k\in A}x_k^2 = \left(\sum_{k\in A}x_k\right)^2 - 2\sum_{j<k\in A}x_jx_k = (-3)^2 - 2\cdot 12 = -15,$$

we get

$$\sum_{k\in A}|x_k|^2 = -\sum_{k\in A}x_k - \sum_{k\in A}x_k^2 = 3 + 15 = 18.$$

Problem 2.4. Let $P(x) = (x-r)(x-r^2)(x-r^3)(x-r^4)$ be a polynomial with real coefficients. Find all possible values of r.

Solution. Clearly if r is real, then $P(x)$ has real coefficients. If r is not real, then since the polynomial has real coefficients, $\overline{r}$ must also be a root, which means that either $\overline{r} = r^2$ or $\overline{r} = r^3$ or $\overline{r} = r^4$. In each case, taking the modulus of both sides, we find that $|r| = 1$. Hence $\overline{r} = \frac{1}{r}$.

If $\overline{r} = r^2$, then $r^3 = 1$. But in this case one of the remaining roots is real ($r^3 = 1$) and the other ($r^4 = r$) is complex and not paired with its conjugate. Thus $P(x)$ does not have real coefficients. If $\overline{r} = r^3$, then $r^4 = 1$, which implies that $r^2 = -1$, hence $r = \pm i$. In this case

$$P(x) = (x \pm i)(x \mp i)(x-1)(x+1) = x^4 - 1$$

has real coefficients. Finally, if $\overline{r} = r^4$, then $r^5 = 1$. This implies that r, r^2, r^3, and r^4 are the four primitive fifth roots of unity and

$$P(x) = (x-r)(x-r^2)(x-r^3)(x-r^4) = x^4 + x^3 + x^2 + x + 1$$

has real coefficients. ■

Problem 2.5. Let $r_1, \ldots, r_{10}$ be the nonreal roots of polynomial $x^{11}+11x+1$. Find the largest positive integer less than or equal to $\left|\sum_{j=1}^{10} r_j^{10}\right|$.

Korean Mathematical Olympiad, 2nd Round 2010

Solution. Let $P(x) = x^{11}+11x+1$. The problem statement implies that $P(x)$ has exactly one real root, and this is easy to verify. The function $x^{11} + 11x$ is a strictly increasing function of x and hence for each t there is exactly one real solution to $x^{11} + 11x = t$. The case $t = -1$ says that P has exactly one real root, which we will denote by r. It is easy to see that $P\left(-\frac{1}{11}\right) < 0$ and $P\left(-\frac{1}{12}\right) > 0$, so we find that $-12 < \frac{1}{r} < -11$. By Vieta's Formulas, we get

$$\frac{1}{r} + \sum_{j=1}^{10} \frac{1}{r_j} = -11.$$

Now,

$$\sum_{j=1}^{10} r_j^{10} = \sum_{j=1}^{10} \frac{r_j^{11}}{r_j}.$$

Since $r_j^{11} = -11r_j - 1$, we have

$$\sum_{j=1}^{10} \frac{r_j^{11}}{r_j} = \sum_{j=1}^{10} \frac{-11r_j - 1}{r_j} = -110 - \sum_{j=1}^{10} \frac{1}{r_j} = -99 + \frac{1}{r}.$$

Because $-99 + \frac{1}{r} \in (-111, -110)$, we find that $\left|\sum_{j=1}^{10} r_j^{10}\right| \in (110, 111)$. Hence the desired value is 110. ■

Problem 2.6. Let r_1, r_2, r_3 be the roots of polynomial $P(x) = x^3+111x^2+1$. Let $Q(x)$ be a polynomial of degree 3 such that

$$Q\left(r_i + \frac{1}{r_i}\right) = 0 \text{ for all } i = 1, 2, 3.$$

Find $\dfrac{Q(1)}{Q(-1)}$.

Solution. Let C be the leading coefficient of Q, then

$$Q(x) = C\left(x - \left(r_1 + \frac{1}{r_1}\right)\right)\left(x - \left(r_2 + \frac{1}{r_2}\right)\right)\left(x - \left(r_3 + \frac{1}{r_3}\right)\right).$$

Hence

$$\frac{Q(1)}{Q(-1)} = \prod_{i=1}^{3} \frac{r_i^2 - r_i + 1}{r_i^2 + r_i + 1}.$$

Note that $r_i^2 - r_i + 1 = (r_i + \omega)(r_i + \omega^2)$ and $r_i^2 - r_i + 1 = (r_i - \omega)(r_i - \omega^2)$, where $\omega = \frac{-1+i\sqrt{3}}{2}$ is a primitive third root of unity. Therefore

$$\frac{Q(1)}{Q(-1)} = \prod_{i=1}^{3} \frac{(r_i + \omega)(r_i + \omega^2)}{(r_i - \omega)(r_i - \omega^2)} = \frac{P(-\omega)\,P(-\omega^2)}{P(\omega)\,P(\omega^2)}.$$

Since we compute $P(\omega) = 111\omega^2 + 2$ and either noting that $P(\omega^2)$ is the conjugate or by direct computation, we have $P(\omega^2) = 11\omega + 2$. Thus

$$\begin{aligned} P(\omega)P(\omega^2) &= |P(\omega)|^2 = (111\omega^2 + 2)(111\omega + 2) = 111^2 + 222(\omega + \omega^2) + 4 \\ &= 12321 - 222 + 4 = 12103. \end{aligned}$$

Similarly, we compute $P(-\omega) = 111\omega^2$ and hence $P(-\omega^2) = 111\omega$, so

$$P(-\omega)P(-\omega^2) = |P(-\omega)|^2 = 111^2 = 12321.$$

Thus

$$\frac{Q(1)}{Q(-1)} = \frac{|P(-\omega)|^2}{|P(\omega)|^2} = \frac{12321}{12103}.$$

■

Problem 2.7. Find the product of the roots of the equation

$$\sum_{k=1}^{2017} \frac{1}{z - \varepsilon_k} = 0,$$

where ε_k are the roots of the polynomial $x^{2018} - 1$, other than 1.

Solution. We consider the more general case, i.e., the equation

$$\sum_{k=1}^{n-1} \frac{1}{z - \varepsilon_k} = 0,$$

where ε_k are the roots of the polynomial $x^n - 1$, other than 1. Let

$$P(x) = (x - \varepsilon_1) \cdot \ldots \cdot (x - \varepsilon_{n-1}) = \frac{x^n - 1}{x - 1}.$$

Then we have

$$\log P(z) = \sum_{k=1}^{n-1} \log(z - \varepsilon_k) = \log(z^{n-1} + z^{n-2} + \cdots + z + 1)$$

so that taking a derivative gives

$$\frac{P'(z)}{P(z)} = \sum_{k=1}^{n-1} \frac{1}{z - \varepsilon_k} = \frac{(n-1)z^{n-2} + (n-2)z^{n-3} + \cdots + 1}{z^{n-1} + z^{n-2} + \cdots + z + 1}.$$

Thus the roots of desired equation are exactly the roots of the polynomial

$$P'(z) = (n-1)z^{n-2} + (n-2)z^{n-3} + \cdots + 1.$$

Hence by Vieta's formula the product of the roots is $\frac{(-1)^n}{n-1}$. In the case of our problem, we get $\frac{1}{2017}$. ■

Problem 2.8. Let x and y be complex number and let n be a positive integer. Prove that

$$x^{2n} - x^n y^n + y^{2n} = \prod_{\substack{1 \le k < 3n \\ \gcd(k,6)=1}} \left(x^2 - 2\cos\left(\frac{k\pi}{3n}\right) xy + y^2 \right).$$

Roman Witula, Ddyta Hetmaniok, Damian Slota - The College Mathematics Journal, Problem 1876

Solution. First look at the product on the right.
The values of k with $1 \le k < 3n$ that are not multiples of 3 are the numbers $3m + 1$ and $3m + 2$ for $m = 0, \ldots, n - 1$. For each such pair exactly one of the two is odd and hence gives a term in the product. Thus the product on the right-hand side has exactly n factors of degree 2. Hence both sides of the proposed equality are homogeneous polynomials of degree $2n$. Thus dividing both sides by y^{2n} and setting $z = \frac{x}{y}$, it suffices to prove

$$z^{2n} - z^n + 1 = \prod_{\substack{1 \le k < 3n \\ \gcd(k,6)=1}} \left(z^2 - 2\cos\left(\frac{k\pi}{3n}\right) z + 1 \right).$$

The left-hand side can be written as

$$z^{2n} - z^n + 1 = \frac{z^{3n} + 1}{z^n + 1}.$$

Thus the roots are the $3n$-th roots of -1 (the roots of $z^{3n} + 1 = 0$) which are not n-th roots of -1 (the roots of $z^n + 1 = 0$). From Theorem 2.9, we see that the $3n$-th roots of -1 are the numbers

$$z = \cos\left(\frac{(2m+1)\pi}{3n}\right) + i\sin\left(\frac{(2m+1)\pi}{3n}\right),$$

for $0 \leq m < 3n$, which we can also describe as the numbers

$$z = \cos\left(\frac{k\pi}{3n}\right) \pm i \sin\left(\frac{k\pi}{3n}\right),$$

for all odd $k, 1 \leq k < 3n$. Since the same argument shows that the n-th roots of -1 will be the cases where k is a multiple of 3, we conclude that the roots of the right-hand side are given by the above formula for all k with $1 \leq k < 3n$ and $\gcd(k, 6) = 1$. Thus the left-hand side equals

$$\prod_{\substack{1 \leq k < 3n \\ \gcd(k,6)=1}} \left(z - \cos\left(\frac{k\pi}{3n}\right) - i \sin\left(\frac{k\pi}{3n}\right)\right)\left(z - \cos\left(\frac{k\pi}{3n}\right) + i \sin\left(\frac{k\pi}{3n}\right)\right)$$

$$= \prod_{\substack{1 \leq k < 3n \\ \gcd(k,6)=1}} \left(z^2 - 2\cos\left(\frac{k\pi}{3n}\right) z + 1\right),$$

as desired. ■

Problem 2.9. Consider the polynomial

$$f(x) = x^n + 2x^{n-1} + 3x^{n-2} + \ldots + nx + n + 1$$

and let $\varepsilon = \cos\frac{2\pi}{n+2} + i \sin\frac{2\pi}{n+2}$. Prove that

$$f(\varepsilon) f(\varepsilon^2) \cdot \ldots \cdot f(\varepsilon^{n+1}) = (n+2)^n.$$

Mihai Piticari - Alexandru Myller Competition 2003

Solution. Let $g(x) = x^{n+1} + x^n + \ldots + x + 1$. The roots of g are $\varepsilon, \varepsilon^2, \ldots, \varepsilon^{n+1}$, so we also have

$$g(x) = (x - \varepsilon)(x - \varepsilon^2) \cdots (x - \varepsilon^{n+1}).$$

Expanding gives

$$(x-1) f(x) = x^{n+1} + x^n + \ldots + x - n - 1,$$

so we have $g(x) = (x-1) f(x) + n + 2$. Hence

$$0 = g(\varepsilon^k) = (\varepsilon^k - 1) f(\varepsilon^k) + n + 2, \qquad k = 1, 2, \ldots, n+1,$$

which we can rewrite as

$$(1 - \varepsilon^k) f(\varepsilon^k) = n + 2, \qquad k = 1, 2, \ldots, n+1.$$

Multiplying these equations side by side, we get

$$(1-\varepsilon)(1-\varepsilon^2) \cdot \ldots \cdot (1 - \varepsilon^{n+1}) f(\varepsilon) \cdot \ldots \cdot f(\varepsilon^{n+1}) = (n+2)^{n+1}.$$

However,

$$(1-\varepsilon)(1-\varepsilon^2) \cdot \ldots \cdot (1 - \varepsilon^{n+1}) = g(1) = n + 2,$$

which gives

$$(n+2) f(\varepsilon) \cdot \ldots \cdot f(\varepsilon^{n+1}) = (n+2)^{n+1},$$

and hence

$$f(\varepsilon) f(\varepsilon^2) \cdot \ldots \cdot f(\varepsilon^{n+1}) = (n+2)^n.$$ ■

Problem 2.10. Let n be a positive integer and let $z_1, \ldots, z_n$ be the roots of $1 + z^n$. For each $a > 0$, prove that

$$\frac{1}{n} \sum_{k=1}^{n} \frac{1}{|z_k - a|^2} = \frac{1 + a^2 + \ldots + a^{2(n-1)}}{(1 + a^n)^2}.$$

Gheorghe Stoica - American Mathematical Monthly, Problem 11947

Solution. Let $P(z) = z^n + 1 = (z - z_1) \cdot \ldots \cdot (z - z_n)$. Then

$$t_1 = a - z_1, \ldots, t_n = a - z_n$$

are the roots of

$$\begin{aligned} P(a - z) &= (a - z)^n + 1 = (-1)^n (z - a)^n + 1 \\ &= (-1)^n z^n + \ldots - n a^{n-1} z + a^n + 1. \end{aligned}$$

By Vieta's Formulas, we have

$$t_1 \ldots t_n = a^n + 1, \quad \text{and} \quad t_1 \ldots t_{n-1} + \ldots + t_2 \ldots t_n = na^{n-1}.$$

Hence

$$\frac{1}{t_1} + \ldots + \frac{1}{t_n} = \frac{t_1 \ldots t_{n-1} + \ldots + t_2 \ldots t_n}{t_1 \ldots t_n} = \frac{na^{n-1}}{1+a^n}.$$

That is,

$$\sum_{k=1}^{n} \frac{1}{a - z_k} = \frac{na^{n-1}}{1+a^n},$$

which yields

$$\sum_{k=1}^{n} \frac{a - z_k + a + z_k}{a - z_k} = \frac{2na^n}{1+a^n}.$$

Whence

$$n + \sum_{k=1}^{n} \frac{a + z_k}{a - z_k} = \frac{2na^n}{1+a^n}.$$

That is,

$$\frac{1}{n} \sum_{k=1}^{n} \frac{a + z_k}{a - z_k} = \frac{2a^n - a^n - 1}{1+a^n} = \frac{a^n - 1}{a^n + 1}.$$

Taking the real parts on both sides and keeping in mind that

$$\operatorname{Re}\left(\frac{a+b}{a-b}\right) = \frac{|a|^2 - |b|^2}{|a-b|^2},$$

we find that

$$\frac{1}{n} \sum_{k=1}^{n} \frac{a^2 - 1}{|a - z_k|^2} = \frac{a^n - 1}{a^n + 1} = \frac{a^{2n} - 1}{(1+a^n)^2}.$$

Therefore dividing both sides by $a^2 - 1$, we get

$$\frac{1}{n} \sum_{k=1}^{n} \frac{1}{|z_k - a|^2} = \frac{1 + a^2 + \ldots + a^{2(n-1)}}{(1+a^n)^2}.$$

The case $a = 1$ follows by continuity. ∎

Problem 2.11. Let $a \neq 0, b, c$ be real numbers. Prove that there is a polynomial $P(x)$ with real coefficients such that $aP(x)^2 + bP(x) + c$ is divisible by $x^2 + 1$.

Alexander Golovanov

Solution. Since $aP(x)^2 + bP(x) + c$ will be a polynomial with real coefficients, being divisible by $x^2 + 1$ is the same as saying it vanishes at $x = i$, hence that

$$aP(i)^2 + bP(i) + c = 0.$$

Treating this as a quadratic equation in the unknown $P(i)$ we get

$$P(i) = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

If $b^2 - 4ac \geq 0$, then the roots are real and we can simply take $P(x)$ to be the constant polynomial

$$P(x) = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

If $b^2 - 4ac < 0$, then the roots are complex

$$P(i) = \frac{-b \pm i\sqrt{4ac - b^2}}{2a}$$

and we can take $P(x)$ to be the linear polynomial

$$P(x) = -\frac{b}{2a} + \frac{\sqrt{4ac - b^2}}{2a} x.$$

Problem 2.12. Prove that if k, m, n are non-negative integers, then the polynomial

$$P(x) = x^{3k+2} + x^{3m+1} + x^{3n}$$

is divisible by $x^2 + x + 1$.

Polish Mathematical Olympiad 1966

First Solution. For a non-negative integer p, the polynomial

$$x^{3p} - 1 = (x^3)^p - 1$$

is divisible by $x^3 - 1$, and thus by $x^2 + x + 1$. So the difference

$$P(x) - (x^2 + x + 1) = x^2(x^{3k} - 1) + x(x^{3m} - 1) + x^{3n} - 1$$

is divisible by $x^2 + x + 1$.
Hence the polynomial $P(x)$ is divisible by $x^2 + x + 1$. ■

Second Solution. Since P is a polynomial with real coefficients, being divisible by $x^2 + x + 1$ is the same as having a root at the cube root of unity $\omega = \frac{-1+i\sqrt{3}}{2}$. Since $\omega^3 = 1$, we compute

$$P(\omega) = \omega^{3k+2} + \omega^{3m+1} + \omega^{3n} = \omega^2 + \omega + 1 = 0,$$

as desired. ■

Problem 2.13. Prove that for every positive integer k the polynomial

$$(x^4 - 1)(x^3 - x^2 + x - 1)^k + (x + 1)x^{4k-1}$$

is divisible by $x^5 + 1$.

Polish Mathematical Olympiad 1986

First Solution. Let $P(x) = (x^4 - 1)(x^3 - x^2 + x - 1)^k + (x + 1)x^{4k-1}$.
Note that

$$x^3 - x^2 + x - 1 = \frac{x^4 - 1}{x + 1}.$$

Therefore we can write

$$\begin{aligned} x^{k+1}P(x) &= x^{k+1}(x+1)\left(\frac{x^4-1}{x+1}\right)^{k+1} + (x+1)x^{5k} \\ &= (x+1)\left[\left(\frac{x(x^4-1)}{x+1}\right)^{k+1} - (-1)^{k+1}\right] + (x+1)\left(x^{5k} - (-1)^k\right). \end{aligned}$$

Since $a^n - b^n$ is always a multiple of $a - b$, we see that the first term is a multiple of

$$(x+1)\left[\frac{x(x^4-1)}{x+1} + 1\right] = x^5 - x + x + 1 = x^5 + 1$$

and the second term is a multiple of $x^5 + 1$. Hence $x^{k+1}P(x)$ is a multiple of $x^5 + 1$ which implies that $P(x)$ is as well. ■

Second Solution. Let

$$P_k(x) = (x^4 - 1)(x^3 - x^2 + x - 1)^k + (x + 1)x^{4k-1}.$$

Define the polynomials

$$p(x) = x^3 - x^2 + x - 1, \qquad q(x) = x^4 - p(x)$$

and notice that

$$\begin{aligned} x^4 - 1 &= (x+1)p(x) \\ x^5 + 1 &= (x+1)q(x) \\ P_k(x) &= (x^4-1)\left(p(x)\right)^k + (x+1)x^{4k-1}, \end{aligned}$$

i.e.,

$$P_k(x) = (x+1)\left(\left(p(x)\right)^{k+1} + x^{4k-1}\right).$$

We prove by induction on k that $P_k(x)$ is divisible by $x^5 + 1$ for all positive integers k. If $k = 1$, we have

$$\begin{aligned} P_1(x) &= (x^4-1)(x^3 - x^2 + x - 1) + (x+1)x^3 \\ &= x^7 - x^6 + x^5 + x^2 - x + 1 \\ &= (x^2 - x + 1)(x^5 + 1). \end{aligned}$$

From $x^5 + 1 = (x + 1)q(x)$, we see that the divisibility of P_k by $x^5 + 1$ is equivalent to the divisibility of the polynomial

$$Q_k(x) = \left(p(x)\right)^{k+1} + x^{4k-1}$$

by the polynomial $q(x)$. Assume that $q(x)$ divides the polynomial $Q_k(x)$ for some positive integer k. Then

$$\begin{aligned} Q_{k+1}(x) - x^4 Q_k(x) &= \left((p(x))^{k+2} + x^{4k+3}\right) - x^4\left((p(x))^{k+1} + x^{4k-1}\right) \\ &= (p(x))^{k+1}\left(p(x) - x^4\right) \\ &= -(p(x))^{k+1} q(x). \end{aligned}$$

It follows that $q(x)$ divides also the polynomial $Q_{k+1}(x)$. The conclusion follows from the principle of mathematical induction. ∎

Problem 2.14. Let $f(x)$ be a polynomial and let n be a positive integer. Prove that if $f(x^n)$ is divisible by $x-1$, then it is also divisible by

$$x^{n-1} + x^{n-2} + \ldots + x + 1.$$

Polish Mathematical Olympiad 1988

Solution. Let $F(x) = f(x^n)$. Since $F(x)$ is divisible by $x-1$, we have $F(1) = 0$. It follows that $f(1) = 0$. Thus the polynomial $f(x)$ is divisible by $x-1$. In other words, there is a polynomial $g(x)$ such that

$$f(x) = (x-1)g(x).$$

Hence

$$\begin{aligned} F(x) &= f(x^n) \\ &= (x^n - 1)g(x^n) \\ &= (x-1)(x^{n-1} + x^{n-2} + \ldots + x + 1)g(x^n), \end{aligned}$$

which gives the desired conclusion. ∎

Problem 2.15. Determine all pairs (n, r), where n is a positive integer and r is a real number for which the polynomial $(x+1)^n - r$ is divisible by the polynomial $2x^2 + 2x + 1$.

Polish Mathematical Olympiad 1996

First Solution. Let us denote by $Q_n(x)$ and $R_n(x)$, respectively, the quotient and the remainder of the division of the polynomial $(x+1)^n$ by $2x^2 + 2x + 1$. The pair (n, r) is one of the pairs sought if and only if $R_n(x)$ is a constant polynomial identically equal to r. For $n = 1, 2, 3, 4$ we have:

$$\begin{aligned} (x+1)^1 &= 0 \cdot (2x^2 + 2x + 1) + (x+1) \\ (x+1)^2 &= \frac{1}{2} \cdot (2x^2 + 2x + 1) + \left(x + \frac{1}{2}\right) \\ (x+1)^3 &= \left(\frac{1}{2}x + 1\right)(2x^2 + 2x + 1) + \frac{1}{2}x \\ (x+1)^4 &= \left(\frac{1}{2}x^2 + \frac{3}{2}x + \frac{5}{4}\right)(2x^2 + 2x + 1) - \frac{1}{4}. \end{aligned}$$

Thus

$$\begin{aligned} &R_1(x) = x + 1, \quad R_2(x) = x + \frac{1}{2}, \\ &R_3(x) = \frac{1}{2}x, \qquad R_4(x) = -\frac{1}{4}. \end{aligned} \tag{2.2}$$

For all integers $n \geq 0$ we have

$$\begin{aligned} (x+1)^{n+4} &= (x+1)^n (x+1)^4 \\ &= \left(Q_n(x)(2x^2 + 2x + 1) + R_n(x)\right)\left(Q_4(x)(2x^2 + 2x + 1) - \frac{1}{4}\right) \\ &= P(x) - \frac{1}{4}R_n(x), \end{aligned}$$

where $P(x)$ is a polynomial divisible by $2x^2 + 2x + 1$. Therefore

$$R_{n+4}(x) = -\frac{1}{4}R_n(x).$$

Hence from formulas (2.2), we obtain by induction the following equations for

$k = 1, 2, 3, \ldots$

$$\begin{aligned} R_{4k}(x) &= \left(-\frac{1}{4}\right)^k \\ R_{4k+1}(x) &= \left(-\frac{1}{4}\right)^k (x+1) \\ R_{4k+2}(x) &= \left(-\frac{1}{4}\right)^k \left(x+\frac{1}{2}\right) \\ R_{4k+3}(x) &= \left(-\frac{1}{4}\right)^k \left(\frac{1}{2}x\right). \end{aligned}$$

We immediately see that $R_n(x)$ is a constant polynomial only for $n = 4k$ and its value is $\left(-\frac{1}{4}\right)^k$. In conclusion, the required pairs (n, r) have the form $\left(4k, \left(-\frac{1}{4}\right)^k\right)$, where k is a positive integer. ■

Second Solution. Since the roots of $2x^2 + 2x + 1$ are $-\frac{1}{2} \pm \frac{i}{2}$ and the polynomial $(x+1)^n - r$ has real coefficients, we see that a pair (n, r) is a solution to the problem exactly when $-\frac{1}{2} + \frac{i}{2}$ is a root of $(x+1)^n - r$. Thus we get a solution for n exactly when

$$\left(-\frac{1}{2} + \frac{i}{2} + 1\right)^n = \left(\frac{1}{2} + \frac{i}{2}\right)^n$$

is a real number and the corresponding r is just its value. Since

$$\frac{1}{2} + \frac{i}{2} = \frac{1}{\sqrt{2}}(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}),$$

we compute that

$$\left(\frac{1}{2} + \frac{i}{2}\right)^n = 2^{-\frac{n}{2}}\left(\cos\frac{n\pi}{4} + i\sin\frac{n\pi}{4}\right).$$

This is real exactly when $\sin\frac{n\pi}{4} = 0$, hence when $n = 4k$ is a multiple of 4 and the corresponding value for r is

$$r = 2^{-\frac{n}{2}}\cos\frac{n\pi}{4} = 2^{-2k}\cos(k\pi).$$

In conclusion, the required pairs (n, r) have the form $\left(4k, 2^{-2k}\cos(k\pi)\right)$, where k is a positive integer. ■

Problem 2.16. Using a given sequence of positive real numbers $q_1, q_2, \ldots$, a sequence of polynomials is constructed in the following way:

$$\begin{aligned} f_0(x) &= 1 \\ f_1(x) &= x \\ f_{n+1}(x) &= (1+q_n)xf_n(x) - q_n f_{n-1}(x) \qquad \text{if } n \geq 1. \end{aligned}$$

Prove that all real roots of these polynomials belong to the interval $[-1, 1]$.

Moscow Mathematical Olympiad 1968

Solution. We prove by induction on n that if $|x| > 1$, then

$$|f_{n+1}(x)| > |f_n(x)|.$$

If $n = 0$ this is obvious. Now, assume that if $|x| > 1$, then

$$|f_n(x)| > |f_{n-1}(x)|.$$

For $|x| > 1$ we have

$$\begin{aligned} |f_{n+1}(x)| &\geq (1+q_n)|xf_n(x)| - q_n|f_{n-1}(x)| \\ &> (1+q_n)|f_n(x)| - q_n|f_n(x)| \\ &= |f_n(x)|. \end{aligned}$$

Therefore if $|x| > 1$, we have $|f_n(x)| > |f_{n-1}(x)| > \ldots > |f_1(x)| > 1$ and so $f_n(x) \neq 0$ for all $n \in \mathbb{N}$. ■

Problem 2.17. Find all complex numbers $a \neq 0$ and b such that for every complex root z of the equation $x^4 - ax^3 - bx - 1 = 0$, we have $|a - z| \geq |z|$.

Nikolai Nikolov - Bulgarian Mathematical Olympiad 2006

Solution. Let z_1, z_2, z_3, z_4 be the roots of the polynomial $x^4 - ax^3 - bx - 1$. By Vieta's Formulas,

$$z_1 + z_2 + z_3 + z_4 = a \quad \text{and} \quad \sum_{1 \leq i < j \leq 4} z_i z_j = 0.$$

Hence ${z_1}^2 + {z_2}^2 + {z_3}^2 + {z_4}^2 = a^2$. Write $t_k = \frac{2z_k}{a} = x_k + iy_k$ for $k = 1, 2, 3, 4$. Then $t_1 + t_2 + t_3 + t_4 = 2$, so $x_1 + x_2 + x_3 + x_4 = 2$ and $t_1^2 + t_2^2 + t_3^2 + t_4^2 = 4$ which combined with ${t_k}^2 = {x_k}^2 - {y_k}^2 + 2ix_k y_k$ gives

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 4 + y_1^2 + y_2^2 + y_3^2 + y_4^2 \geq 4.$$

On the other hand, $|a - z_k| \geq |z_k|$, which gives $|2 - t_k| \geq |t_k|$. This yields the inequality

$$(2 - x_k)^2 + {y_k}^2 \geq {x_k}^2 + {y_k}^2,$$

which simplifies to $x_k \leq 1$. Moreover, since $x_1 + x_2 + x_3 + x_4 = 2$, we get

$$x_k + 3 \geq x_1 + x_2 + x_3 + x_4 = 2$$

and hence $x_k \geq -1$. Thus $-1 \leq x_k \leq 1$ which implies $x_k^2 \leq 1$. Summing these we get

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \leq 4.$$

Thus we must have $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 4$ and we must have had equality in all the inequalities above. This implies that $y_k = 0$ and $t_k = x_k = \pm 1$ for all k. Since $t_1 + t_2 + t_3 + t_4 = 2$, we have without loss of generality $t_1 = t_2 = t_3 = 1$ and $t_4 = -1$. Hence $z_1 = z_2 = z_3 = -z_4 = \frac{a}{2}$. Since Vieta's formulas also give $z_1 z_2 z_3 z_4 = -1$, we conclude that $\left(\frac{a}{2}\right)^4 = 1$. Thus $a = 2, -2, 2i$, or $-2i$. From the roots, we compute that $b = -\frac{a^3}{4}$. This results in the four solutions

$$(a, b) \in \{(2, -2), (-2, 2), (2i, 2i), (-2i, -2i)\}.$$

■

Problem 2.18. If a non-real number z_0 is a root of the polynomial

$$z^{n+1} - z^2 + az + 1,$$

where a is any real number and $n \geq 2$, prove that

$$|z_0| > \frac{1}{\sqrt[n]{n}}.$$

German Team Selection Test 2009

Solution. Let $z_0 = r(\cos\alpha + i\sin\alpha)$ so that $|z_0| = r$. Since z_0 is a root of the given polynomial, dividing by z_0 we see that

$$z_0^n = z_0 - a - \frac{1}{z_0}.$$

Since

$$z_0^n = r^n(\cos n\alpha + i\sin n\alpha)$$

and

$$\frac{1}{z_0} = \frac{1}{r}(\cos\alpha - i\sin\alpha),$$

taking imaginary parts gives

$$r^n \sin n\alpha = \frac{1 + r^2}{r}\sin\alpha.$$

Since $\sin\alpha \neq 0$, we have $\sin n\alpha \neq 0$ and we can write this as

$$\frac{\sin\alpha}{\sin n\alpha} = \frac{r^{n+1}}{1 + r^2}.$$

Furthermore, since $\frac{r^{n+1}}{1+r^2} > 0$, we find that

$$\frac{r^{n+1}}{1 + r^2} = \frac{\sin\alpha}{\sin n\alpha} = \left|\frac{\sin\alpha}{\sin n\alpha}\right| \geq \frac{1}{n}.$$

Moreover, $r^n > \frac{r^{n+1}}{1+r^2}$, so $r^n > \frac{1}{n}$. ■

Problem 2.19. Prove that if the roots of the polynomial

$$P(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + (-1)^n \in \mathbb{C}[x]$$

have the same modulus, then $P(-1) \in \mathbb{R}$.

N. Micu - Romanian Mathematical Olympiad 1974

Solution. Let $x_1, x_2, \ldots, x_n$ be the roots of the polynomial $P(x)$. Since the roots of P have the same modulus and $x_1 x_2 \cdot \ldots \cdot x_n = 1$, we see that

$$|x_1| = |x_2| = \ldots = |x_n| = 1.$$

As

$$P(x) = (x - x_1)(x - x_2) \cdot \ldots \cdot (x - x_n),$$

we have

$$\begin{aligned} P(-1) &= (-1 - x_1)(-1 - x_2) \cdot \ldots \cdot (-1 - x_n) \\ &= (-1)^n (1 + x_1)(1 + x_2) \cdot \ldots \cdot (1 + x_n). \end{aligned}$$

Furthermore, since $\overline{x_i} = 1/x_i$ for $i = 1, 2, \ldots, n$, we have

$$\begin{aligned} \overline{P(-1)} &= (-1)^n \overline{(1 + x_1)(1 + x_2) \cdot \ldots \cdot (1 + x_n)} \\ &= (-1)^n (1 + \overline{x_1})(1 + \overline{x_2}) \cdot \ldots \cdot (1 + \overline{x_n}) \\ &= (-1)^n \left(1 + \frac{1}{x_1}\right)\left(1 + \frac{1}{x_2}\right) \cdot \ldots \cdot \left(1 + \frac{1}{x_n}\right) \\ &= (-1)^n \frac{(x_1 + 1)(x_2 + 2) \cdot \ldots \cdot (x_n + 1)}{x_1 x_2 \cdot \ldots \cdot x_n} \\ &= (-1)^n (1 + x_1)(1 + x_2) \cdot \ldots \cdot (1 + x_n). \end{aligned}$$

So $P(-1) = \overline{P(-1)}$, which implies $P(-1) \in \mathbb{R}$. ∎

Problem 2.20. Let d be an odd positive integer and let

$$P(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0$$

be a polynomial with complex coefficients such that all of its roots lie on the unit circle and $a_0 \neq 1$. Prove that $\frac{a_{d-1} - a_1}{1 - a_0}$ is a real number.

Solution. Denote the roots of $P(x)$ by $r_1, \ldots, r_d$. Therefore

$$r_1 + \ldots + r_d = -a_{d-1}, \quad r_1 \cdot \ldots \cdot r_d \left(\frac{1}{r_1} + \ldots + \frac{1}{r_d}\right) = a_1, \quad r_1 \cdot \ldots \cdot r_d = -a_0.$$

Hence

$$\frac{a_{d-1} - a_1}{1 - a_0} = \frac{r_1 + \ldots + r_d + r_1 \cdot \ldots \cdot r_d \left(\frac{1}{r_1} + \ldots + \frac{1}{r_d}\right)}{1 + r_1 \cdot \ldots \cdot r_d}.$$

Now, taking the conjugate, we find that the conjugate of $\frac{a_{d-1} - a_1}{1 - a_0}$ is

$$\frac{\overline{r_1} + \ldots + \overline{r_d} + \overline{r_1 \cdot \ldots \cdot r_d}\left(\frac{1}{\overline{r_1}} + \ldots + \frac{1}{\overline{r_d}}\right)}{1 + \overline{r_1 \cdot \ldots \cdot r_d}}.$$

Because $r_1, \ldots, r_d$ lie on the unit circle, we find that

$$\overline{r_i} = \frac{1}{r_i}.$$

Hence we find that the above expression is equal to

$$\frac{\frac{1}{r_1} + \ldots + \frac{1}{r_d} + \frac{1}{r_1 \cdot \ldots \cdot r_d}(r_1 + \ldots + r_d)}{1 + \frac{1}{r_1 \cdot \ldots \cdot r_d}} = \frac{r_1 \cdot \ldots \cdot r_d \left(\frac{1}{r_1} + \ldots + \frac{1}{r_d}\right) + r_1 + \ldots + r_d}{1 + r_1 \cdot \ldots \cdot r_d}$$

$$= \frac{a_{d-1} - a_1}{1 - a_0}.$$

Since it is equal to its conjugate, we conclude that it must be real. ∎

Problem 2.21. Let $a \neq 0$, $m > n$, $m \neq 2n$ and assume that the absolute values of all roots of polynomial $ax^m + bx^n + c$ are the same. Prove that $b = 0$.

Solution. Let us denote the roots of the polynomial by $r_1, \ldots, r_m$. Then

$$\sigma_{m-n} = \sum_{i_1 < i_2 < \cdots < i_{m-n}} r_{i_1} \cdot \ldots \cdot r_{i_{m-n}} = (-1)^{m-n} \frac{b}{a}$$

and since $m-n \neq n$ the coefficient of x^{m-n} is zero and hence

$$\sigma_n = \sum_{i_1<\cdots<i_n} r_{i_1} \cdot \ldots \cdot r_{i_n} = 0.$$

Let $|r|$ be the common modulus of all the roots. Then we see that

$$\begin{aligned}
\sigma_{m-n} &= r_1 r_2 \cdot \ldots \cdot r_m \sum_{i_1<\cdots<i_n} \frac{1}{r_{i_1} \cdot \ldots \cdot r_{i_n}} \\
&= r_1 r_2 \cdot \ldots \cdot r_m \sum_{i_1<\cdots<i_n} \frac{\overline{r_{i_1}} \cdot \ldots \cdot \overline{r_{i_n}}}{|r_{i_1}|^2 \cdot \ldots \cdot |r_{i_n}|^2} \\
&= \frac{r_1 r_2 \cdot \ldots \cdot r_m}{|r|^{2n}} \sum_{i_1<\cdots<i_n} \overline{r_{i_1}} \cdot \ldots \cdot \overline{r_{i_n}} = \frac{r_1 r_2 \cdot \ldots \cdot r_m}{|r|^{2n}} \overline{\sigma_n} = 0.
\end{aligned}$$

Hence $b = 0$. ■

Problem 2.22. Let $P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0$ be a polynomial with complex coefficients such that all of its roots lie inside the unit circle. Let

$$P^*(x) = x^d \overline{P}\left(\frac{1}{x}\right).$$

Prove that all the roots of $P(z) + P^*(z)$ lie on the unit circle.

Solution. We can write $P(x) = a_d(x - z_1) \cdot \ldots \cdot (x - z_d)$, where $z_1, \ldots, z_d$ are the roots of P and by hypothesis $|z_i| < 1$ for $1 \leq i \leq d$. Hence we have

$$\overline{P}(x) = \overline{a_d}(1 - x\overline{z_1}) \cdot \ldots \cdot (1 - x\overline{z_d}).$$

Now, let r be any root of $P(z) + P^*(z)$. Then

$$|r - z_1| \cdot \ldots \cdot |r - z_d| = |1 - r\overline{z_1}| \cdot \ldots \cdot |1 - r\overline{z_d}|.$$

Now, we have

$$|r - z_j|^2 - |1 - r\overline{z_j}|^2 = |r|^2 + |z_j|^2 - 1 - |rz_j|^2 = (1 - |z_j|^2)(|r|^2 - 1).$$

Since $|z_j| < 1$, we find that if $|r| > 1$, then $|r - z_j| > |1 - r\overline{z_j}|$ for all j and if $|r| < 1$, then $|r - z_j| < |1 - r\overline{z_j}|$ for all j. In both cases the equality

$$|r - z_1| \cdot \ldots \cdot |r - z_d| = |1 - r\overline{z_1}| \cdot \ldots \cdot |1 - r\overline{z_d}|$$

cannot happen. Hence we must have $|r| = 1$. ■

Problem 2.23. Let $|a| \leq 1$ be a real number. Prove that all the roots of the equation $x^{n+1} - ax^n - ax + 1 = 0$ lie on the unit circle.

Solution. Assume that z is a root of polynomial $x^{n+1} - ax^n - ax + 1$. Then

$$z^n(z - a) = az - 1.$$

Hence $z^n = \frac{az-1}{z-a}$. Thus $|z|^n = \left|\frac{az-1}{z-a}\right|$. We have

$$|z|^{2n} = \left|\frac{az-1}{z-a}\right|^2 = \frac{az-1}{z-a} \cdot \frac{a\overline{z}-1}{\overline{z}-a} = \frac{1 + a^2|z|^2 - 2\mathrm{Re}(az)}{a^2 + |z|^2 - 2\mathrm{Re}(az)}.$$

Hence

$$|z|^{2n} - 1 = \frac{(1-a^2)(1-|z|^2)}{\underbrace{a^2 + |z|^2 - 2\mathrm{Re}(az)}_{+}}.$$

Since $|a| \leq 1$, we find that $|z|^{2n} - 1$ and $1 - |z|^2$ must have the same sign. This cannot occur unless $|z| = 1$. ■

Problem 2.24. Let a, b, c, d be real numbers such that $b - d \geq 5$ and all roots x_1, x_2, x_3, and x_4 of the polynomial $P(x) = x^4 + ax^3 + bx^2 + cx + d$ are real. Find the smallest value the product

$$(x_1^2 + 1)(x_2^2 + 1)(x_3^2 + 1)(x_4^2 + 1)$$

can take.

Titu Andreescu - USA Mathematical Olympiad 2014

Solution. Since x_1, x_2, x_3, x_4 are the roots of $P(x)$, we can write

$$P(x) = (x - x_1)(x - x_2)(x - x_3)(x - x_4).$$

We have

$$\begin{aligned}\prod_{k=1}^{4}(x_k^2+1) &= \prod_{k=1}^{4}(x_k - i)(x_k + i)\\ &= P(i)P(-i)\\ &= (1 - b + d - i(a-c))\,(1 - b + d + i(a-c))\\ &= (b - d - 1)^2 + (a - c)^2\\ &\geq 16,\end{aligned}$$

and the equality is attained when $b - d = 5$ and $a = c$. ■

Chapter 3

Finding Polynomials. Part I

Problem 3.1. Let $P(x) = x^2 + a$, $(a \neq 0)$ and $Q(x) = x^3 + bx + c$. If $Q(P(x)) = P(Q(x))$ for all real numbers x, find the value of $Q(10)$.

Solution. According to the problem statement the following identity holds:

$$(x^3 + bx + c)^2 + a = (x^2 + a)^3 + b(x^2 + a) + c.$$

Examining the coefficient of x^3 on the both sides, we find that $2c = 0$. Hence $c = 0$. Therefore

$$(x^3 + bx)^2 + a = (x^2 + a)^3 + b(x^2 + a).$$

Examining the coefficients of x^4, x^2 and x^0 on both sides, we find that

$$2b = 3a, \quad b^2 = 3a^2 + b, \quad a = a^3 + ab.$$

The first of these equations gives $b = \frac{3}{2}a$ and plugging this into the second we get $\frac{9}{4}a^2 = 3a^2 + \frac{3}{2}a$ which means $0 = a^2 + 2a$. Since $a \neq 0$, get $a = -2$ and hence $b = -3$. These also satisfy the third equation, thus we have found that the only solution is

$$P(x) = x^2 - 2, \qquad Q(x) = x^3 - 3x.$$

Therefore $Q(10) = 970$. ■

Problem 3.2. Find all polynomials $P(x)$ of degree d such that

$$P(1) + P(x) + \ldots + P(x^d) = (1 + x + \ldots + x^d)P(x).$$

Solution. The left-hand side of the equality has degree d^2 and the right-hand side has degree $2d$, hence we must have $d = 2$. Then

$$P(1) + P(x) + P(x^2) = (x^2 + x + 1)P(x).$$

That is, $P(1) + P(x^2) = (x^2 + x)P(x)$. Setting $P(x) = ax^2 + bx + c$, we find that

$$ax^4 + bx^2 + a + b + 2c = (x^2 + x)(ax^2 + bx + c).$$

Considering the coefficient of x^3, we get $a + b = 0$. Therefore

$$ax^4 - ax^2 + 2c = (x^2 + x)(ax^2 - ax + c).$$

Examining the constant terms, we get $c = 0$. Hence

$$ax^4 - ax^2 = (x^2 + x)(ax^2 - ax).$$

The latter equality is indeed a true identity. Hence $P(x) = a(x^2 - x)$. ■

Problem 3.3. Find all polynomials $P(x)$ such that

$$P(2x) = 8P(x) + (x - 2)^2 \qquad \forall x \in \mathbb{R}.$$

P. Černek - Czech-Slovak Mathematical Olympiad 2001

Solution. Let $P(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$. Taking the coefficient of x^k in the given equation we get $2^k a_k = 8a_k$ for $k \geq 3$, $2^2 a_2 = 8a_2 + 1$ for $k = 2$, $2a_1 = 8a_1 - 4$ for $k = 1$, and $a_0 = 8a_0 + 4$ for $k = 0$. Therefore we conclude that $a_k = 0$ for $k \geq 4$, a_3 is unconstrained, $a_2 = -\frac{1}{4}$, $a_1 = \frac{2}{3}$, and $a_0 = -\frac{4}{7}$. So

$$P(x) = ax^3 - \frac{1}{4}x^2 + \frac{2}{3}x - \frac{4}{7},$$

where $a \in \mathbb{R}$. ■

Problem 3.4. Let

$$3P(x^2) + 2122x^2 = 2(x^2 + 2)P(x) + x^4 + 4024x^3 + 8048x + 1959.$$

Find $P(2013)$.

Solution. Let $\deg P(x)) = d$. If $d < 2$, then the left-hand side has degree less than 4 and the right-hand side is degree 4. If $d > 2$, then the left-hand side has degree $2d$ and the right-hand side has degree $d + 2 < 2d$. Thus these fail the degree condition, and it follows that $\deg P(x) = 2$. Writing $P(x) = ax^2 + bx + c$, we find that

$$3(ax^4 + bx^2 + c) + 2122x^2 = 2(x^2 + 2)(ax^2 + bx + c) + x^4 + 4024x^3 + 8048x + 1959.$$

Examining the coefficients of x^4 yields $3a = 2a + 1$ hence $a = 1$. Examining the coefficients of x^3 yields $0 = 2b + 4024$ hence $b = -2012$ and examining the constant terms, we get $3c = 4c + 1959$ hence $c = -1959$. Therefore

$$P(x) = x^2 - 2012x - 1959.$$

Plugging in to check the remaining coefficients, we see that this is a solution. Hence $P(2013) = 54$. ■

Problem 3.5. Find all polynomials $P(x)$ with real coefficients such that for all nonzero real numbers x we have $P(x)P\left(\frac{1}{x}\right) = 1$.

Solution. If $P(x) = cx^d$ for some real number c and integer $d \geq 0$, then the equation becomes $c^2 = 1$ and we see that the only solutions of this form are $P(x) = \pm x^d$. If P is not of this form, then it has at least two terms and hence we can write $P(x) = a_d x^d + \ldots + a_k x^k$ where $k < d$ and a_k, a_d are both nonzero. Then the equation becomes

$$(a_d x^d + \ldots + a_k x^k)(a_d x^{-d} + \ldots + a_k x^{-k}) = 1$$

which we can write as a polynomial equation as

$$(a_d x^d + \ldots + a_k x^k)(a_k x^{d-k} + \ldots + a_d) = x^d.$$

Looking at the coefficient of x^k on both sides, we get $a_k a_d = 0$, a contradiction. Thus the only solutions are $P(x) = \pm x^d$. ■

Problem 3.6. Find all polynomials $P(x)$ and $Q(x)$ such that

$$(x+1)P(x-1) - x^2Q(x+1) = x^2 - x - 1,$$
$$P(x+1) - (x+2)Q(x+3) = -1.$$

Solution. Using the substitution $x \mapsto x+2$, the first equation becomes

$$(x+3)P(x+1) - (x+2)^2Q(x+3) = x^2 + 3x + 1.$$

Multiply the second equation by $-(x+2)$ and adding these two equations, we find that

$$P(x+1) = (x+2)^2 - 1.$$

Therefore $P(x) = x(x+2)$. Thus

$$(x+2)Q(x+3) = 1 + P(x+1) = (x+2)^2,$$

which gives $Q(x) = x - 1$. ■

Problem 3.7. Find all polynomials $P(x)$ and $Q(x)$ with rational coefficients such that

$$2x + 1 + (3x+1)P(x) = Q(x)^2.$$

Solution. Putting $x = -\frac{1}{3}$, then $Q\left(-\frac{1}{3}\right)^2 = \frac{1}{3}$. Hence $Q\left(-\frac{1}{3}\right) = \pm\frac{1}{\sqrt{3}}$, which is impossible. Hence there are no such polynomials. ■

Remark. There exist polynomials $P(x)$ and $Q(x)$ with real coefficients satisfying the statement of the problem. For example $P(x) = x - 1$ and $Q(x) = \pm\sqrt{3}x$.

Problem 3.8. Find all polynomials $P(x)$ and $Q(x)$ with real coefficients such that

$$P(Q(x) + 1) = 1 + Q(P(x)),$$
$$Q(P(x) + 1) = 1 + P(Q(x)),$$
$$P(0) = Q(0) = 0.$$

Solution. Putting $x = 0$, we get $P(1) = Q(1) = 1$. Now, putting $x = 1$ implies that $P(2) = Q(2) = 2$.
Proceeding by induction, we find that $P(k) = Q(k) = k$ for all positive integers k. Therefore $P(x) = Q(x) = x$ for all real numbers x. ■

Problem 3.9. Find all polynomials $P(x)$ with real coefficients such that

$$P(x)P(y) = P\left(\frac{x+y}{2}\right)^2 - P\left(\frac{x-y}{2}\right)^2.$$

Solution. Setting $x = y = 0$, we get $P(0) = 0$. Putting $y = 3x$, we find that

$$P(x)P(3x) = P(2x)^2 - P(-x)^2.$$

Writing $P(x) = a_d x^d + \ldots + a_0$ with $a_d \neq 0$ and comparing the leading coefficients, we find that

$$3^d a_d^2 = 4^d a_d^2 - (-1)^{2d} a_d^2.$$

Hence $3^d = 4^d - 1$. But, if $d > 1$, then $4^d - 3^d > 1$. Therefore $d = 1$ and $P(x) = a_1 x$. It is easy to check that this gives a solution. ■

Problem 3.10. Find all polynomials $P(x)$ with complex coefficients such that $P(0) = 0$ and for all integers $n > 2$ and for all real numbers $a_1, a_2, \ldots, a_n$ with $a_1 + a_2 \ldots + a_n \neq 0$,

$$P\left(\frac{a_1}{a_1 + a_2 + \ldots + a_n}\right) + \ldots + P\left(\frac{a_n}{a_1 + a_2 + \ldots + a_n}\right) = 0.$$

Solution. Assume that $\deg P(x) = d$.
Then for each positive integer $k = 1, 2, \ldots, d+1$, plugging $a_1 = \ldots = a_k = 1$, $a_{k+1} = \ldots = a_n = 0$, we get $P\left(\frac{1}{k}\right) = 0$. Hence $P(x) = 0$ for all x. ■

Problem 3.11. Let $P(x)$ be a nonzero polynomial such that

$$P(x)(x-1)^{20} = (x^2 + ax + 1)^{30} + (x^2 + bx + c)^{10}$$

for some real numbers a, b, c. Evaluate $P(1) + a^2 + b^2 + c^2$.

Solution. Plugging $x = 1$, we find that $(2+a)^{30} + (1+b+c)^{10} = 0$. Thus $2 + a = 1 + b + c = 0$. Hence $a = -2$ and $b + c = -1$. Thus

$$x^2 + bx + c = (x-1)(x-c).$$

Rewrite the original identity as

$$\begin{aligned} P(x)(x-1)^{20} &= (x^2 - 2x + 1)^{30} + (x-1)^{10}(x-c)^{10} \\ &= (x-1)^{60} + (x-1)^{10}(x-c)^{10}. \end{aligned}$$

If $c \neq 1$, then the right-hand side is only divisible by $(x-1)^{10}$. Thus $c = 1$ and $b = -2$ and

$$P(x)(x-1)^{20} = (x-1)^{60} + (x-1)^{20}.$$

This implies that $P(x) = (x-1)^{40} + 1$. That is, $P(1) = 1$, which gives

$$P(1) + a^2 + b^2 + c^2 = 1 + 4 + 4 + 1 = 10. \quad \blacksquare$$

Problem 3.12. Find all monic polynomials $P(x)$ with real coefficients such that for each real number x

$$P(x + P(x)) = x^2 + P(P(x)).$$

Solution. Clearly $P(x)$ cannot be a constant polynomial, so

$$\deg P(x) = d > 0,$$

and we can write

$$P(x) = x^d + Q(x)$$

for some polynomial $Q(x)$ with $\deg Q(x) = k \leq d-1$. Then we compute that

$$P(x + P(x)) - P(P(x)) = [(x + P(x))^d - P(x)^d] + Q(x + P(x)) - Q(P(x)).$$

The last two terms have degree at most $kd \leq d(d-1)$. For the term in square brackets, the binomial theorem gives

$$(x + P(x))^d - P(x)^d = dxP(x)^{d-1} + \frac{d(d-1)}{2}x^2P(x)^{d-2} + \ldots + x^d.$$

The first term in this expansion has degree $1 + d(d-1)$ and the remaining terms have lower degree. Thus we see that $P(x + P(x)) - P(P(x))$ has degree $d^2 - d + 1$.

Now if the given equation holds we have $P(x + P(x)) - P(P(x)) = x^2$, so comparing degrees we get $d^2 - d + 1 = 2$. However, this equation has no integer solution, so there is no such polynomial $P(x)$. $\blacksquare$

Problem 3.13. Find all monic polynomials $P(x)$ with real coefficients such that for each real number x

$$P(x + P(x)) = 2x^3 + x^2 + P(P(x)).$$

Solution. As in the preceding solution, $P(x)$ cannot be a constant polynomial and therefore if we let $\deg P(x) = d > 0$, we find that the polynomial

$$P(x + P(x)) - P(P(x))$$

has degree $d^2 - d + 1$.

In the current problem, we have

$$P(x + P(x)) - P(P(x)) = 2x^3 + x^2,$$

hence equating degrees gives $d^2 - d + 1 = 3$ and hence $d = 2$. Writing

$$P(x) = x^2 + bx + c$$

(since $P(x)$ was assumed to be monic), we compute

$$\begin{aligned} P(x + P(x)) &- P(P(x)) \\ &= (x + P(x))^2 + b(x + P(x)) + c - (P(x))^2 - bP(x) - c \\ &= 2xP(x) + x^2 + bx = 2x^3 + (2b+1)x^2 + (2c+b)x. \end{aligned}$$

Therefore we see that $2b + 1 = 1$ and $2c + b = 0$, so that $b = c = 0$. Thus $P(x) = x^2$ is the only solution. $\blacksquare$

Problem 3.14. (a) Determine the set of all polynomials $P(x)$ with real coefficients such that

$$(x-4)P(x+1) - xP(x) + 20 = 0 \qquad \forall x \in \mathbb{R}.$$

(b) From the set determined in point (a), find the polynomial satisfying $P(0) = 29$.

I. V. Maftei - Romanian Mathematical Olympiad 1971

Solution. (a) Let $P(x) = Q(x) + 5$. Then the given relation becomes

$$(x-4)Q(x+1) = xQ(x) \qquad \forall x \in \mathbb{R}.$$

Setting $x = 0, 1, 2, 3$ successively, we get $Q(1) = Q(2) = Q(3) = Q(4) = 0$, so there exists a polynomial $G(x)$ with real coefficients such that

$$Q(x) = G(x)(x-1)(x-2)(x-3)(x-4).$$

Substituting this expression into $(x-4)Q(x+1) = xQ(x)$, we get

$$G(x+1) = G(x) \qquad \forall x \in \mathbb{R}.$$

From the result of Section 3.5, we see that $G(x)$ must be constant and we get

$$P(x) = C(x-1)(x-2)(x-3)(x-4) + 5$$

for some $C \in \mathbb{R}$.
(b) Setting $x = 0$ into the previous equation, we get $29 = 24C + 5$, which gives $C = 1$. So $P(x) = (x-1)(x-2)(x-3)(x-4) + 5$. ■

Problem 3.15. Let $P(x)$ be a polynomial with integer coefficients such that $P(a) = 1$, $P(b) = 2$, $P(17) = 3$ for some integers $a < b < 17$.
(i) Prove that the equation $P(x) = 5$ has at most one integer solution.
(ii) Find all polynomials $P(x)$ for which the equation $P(x) = 5$ has exactly one integer solution.

Solution. (i) We will make repeated use of the fact that if $P(x)$ is a polynomial with integer coefficients, then for any integers r, s, we have $r - s$ divides $P(r) - P(s)$. Using this fact, we see that $17 - b$ divides $P(17) - P(b) = 1$, and hence $17 - b = \pm 1$. Since we assumed $b < 17$, this forces $b = 16$. Similarly, $b - a = 16 - a$ divides $P(b) - P(a) = 1$ and $a = 15$.
Now suppose that $P(r) = 5$. Using the result above, $r - 17$ divides

$$P(r) - P(17) = 2,$$

hence $r - 17 \in \{\pm 1, \pm 2\}$. Thus $r \in \{15, 16, 18, 19\}$. Also $r - 16 = r - b$ divides $P(r) - P(b) = 3$, hence $r - 16 \in \{\pm 1, \pm 3\}$ and hence $r \in \{13, 15, 17, 19\}$. Comparing these two lists, and excluding the case $r = 15$ since we cannot have $r = a$, we see that $r = 19$. Thus $P(x) = 5$ has at most one solution, and if it has one solution, then it is $x = 19$.
(ii) Suppose P is such a polynomial. From the solution to (i), we see that if we define $Q(x) = P(x) + 14 - x$, then

$$Q(15) = Q(16) = Q(17) = Q(19) = 0.$$

Hence we can write

$$Q(x) = (x-15)(x-16)(x-17)(x-19)R(x)$$

for some polynomial $R(x)$ with integer coefficients, which gives

$$P(x) = x - 14 + (x-15)(x-16)(x-17)(x-19)R(x).$$

By construction such a polynomial $P(x)$ has the desired properties. ■

Problem 3.16. Anna is playing a mathematical computer game. The computer is hiding a polynomial $P(x)$. The degree and coefficients of $P(x)$ are unknown to Anna, but she knows that the coefficients are strictly positive real numbers. At each move, Anna inputs a real number a and the computer outputs $P(a)$. This is repeated until Anna can determine what $P(x)$ must be. For a strategy S used by Anna, denote by $S(P)$ the number of moves she needs to determine $P(x)$. Call a strategy S *optimal* if $S(P) \leq S'(P)$ for all possible strategies S' and all polynomials P with strictly positive coefficients. Does there exist an optimal strategy?

Solution. The answer is yes. The following strategy is optimal: choose positive integers $1, 2, 3, \ldots$ in ascending order. Further, this strategy gives $S(P) = \deg P + 2$ for all polynomials with strictly positive real coefficients. To prove this, it suffices to prove the following two claims:

(i) $S(P) \leq \deg P + 2$.

(ii) $S'(P) \geq \deg P + 2$ for each possible strategy S'.

We shall prove (i) by induction on $d = \deg P$. In the base case where $d = 0$, we need to show $S(P) \leq 2$. This means that if $P(x)$ is constant, then Anna will know $P(x)$ from $P(1)$ and $P(2)$. If $P(x)$ is not constant, then since all the coefficients of $P(x)$ are strictly positive, we will have $P(1) < P(2)$. On the other hand, if $P(x)$ is constant, then $P(1) = P(2)$. Hence from $P(1)$ and $P(2)$, Anna will know whether $P(x)$ is constant and if it is, then she will clearly know $P(x)$.
Now suppose that $d > 0$ and assume that (i) is true for each polynomial of degree at most $d - 1$. Our claim is that if $Q(x)$ is a polynomial with strictly positive coefficients such that $Q(i) = P(i)$, $i = 1, 2, \ldots, d + 2$, then $P(x) = Q(x)$ for all x. To see this, consider the polynomials

$$R(x) = P(x + 1) - P(x), \quad S(x) = Q(x + 1) - Q(x).$$

It is clear that $R(x)$ and $S(x)$ both have positive real coefficients and $R(i) = S(i)$ for $i = 1, 2, \ldots, d+1$. Since $\deg R(x) = d-1$, by the inductive hypothesis we find that $R(x) = S(x)$. Therefore $(Q - P)(x + 1) = (Q - P)(x)$ for all x. This implies that $Q - P$ is constant. Since $P(1) = Q(1)$, we find that $P = Q$.
Now, we will prove (ii) by contradiction. Suppose that there is a strategy S' and a polynomial $P(x)$ with strictly positive coefficients of degree d such that $S'(P) \leq d + 1$. Let the first $d + 1$ moves of S' be $r_1, \ldots, r_{d+1}$. Since the coefficients of P are positive, there is some $\varepsilon > 0$ such that the coefficients of

$$T(x) = P(x) + \varepsilon(x - r_1) \cdot \ldots \cdot (x - r_{d+1})$$

are strictly positive. However, the polynomials $T(x)$ and $P(x)$ are different, but they assume the same values at $r_1, \ldots, r_{d+1}$. This contradicts our assumption that $P(x)$ can uniquely be determined after $d + 1$ moves. ∎

Problem 3.17. Find all polynomials P and Q such that for all real numbers x,

$$Q(x^2) = (x + 1)^4 - x\,(P(x))^2\,.$$

P. Černek - Czech-Slovak Mathematical Olympiad 2001

Solution. Let $\deg P(x) = n$. If $n \geq 2$, then the right side of the equation will have degree $2n + 1$ which is odd, but the left side clearly has even degree. Hence $n \leq 1$. Writing $P(x) = ax + b$, we get

$$\begin{aligned} Q(x^2) &= (x + 1)^4 - x(ax + b)^2 \\ &= x^4 + (4 - a^2)x^3 + (6 - 2ab)x^2 + (4 - b^2)x + 1. \end{aligned}$$

Since $Q(x^2)$ has only even powers of x, the coefficients of odd powers of x on the right must be equal to zero. Thus $4 - a^2 = 4 - b^2 = 0$, which means $a, b \in \{-2, 2\}$ and $Q(x^2) = x^4 + (6 - 2ab)x^2 + 1$. Substituting each of the four possible pairs of numbers a, b we find four solutions:

$$\begin{aligned} P(x) &= 2x + 2, \quad Q(x) = x^2 - 2x + 1 \\ P(x) &= 2x - 2, \quad Q(x) = x^2 + 14x + 1 \\ P(x) &= -2x + 2, \quad Q(x) = x^2 + 14x + 1 \\ P(x) &= -2x - 2, \quad Q(x) = x^2 - 2x + 1. \end{aligned}$$

∎

Problem 3.18. Find all polynomials $P(x)$ with real coefficients such that

$$P\left(x^2\right) P\left(x^3\right) = (P(x))^5 \qquad \forall x \in \mathbb{R}.$$

Polish Mathematical Olympiad 2008

First Solution. We observe first that the only constant polynomials that satisfy the given condition are $P(x) \equiv 0$ and $P(x) \equiv 1$. Now, assume that the polynomial $P(x)$ is not constant.
If the polynomial $P(x)$ is of the form $P(x) = cx^n$ for some real number $c \neq 0$ and $n \geq 1$, then

$$c^2 x^{5n} = P\left(x^2\right) P\left(x^3\right) = (P(x))^5 = c^5 x^{5n},$$

which implies $c^2 = c^5$, so $c = 1$. Therefore among these polynomials the only polynomials satisfying the given condition are $P(x) = x^n$ for $n \geq 1$.
There is still a case to be considered, i.e., when the polynomial $P(x)$ is the sum of at least two nonzero monomials. We can write

$$P(x) = a_n x^n + a_l x^l + G(x),$$

where $n > l \geq 0$, $a_n \neq 0$, $a_l \neq 0$, and $G(x)$ has degree at most $l-1$. Therefore

$$\begin{aligned} P\left(x^2\right) P\left(x^3\right) &= \left(a_n x^{2n} + a_l x^{2l} + G\left(x^2\right)\right)\left(a_n x^{3n} + a_l x^{3l} + G\left(x^3\right)\right) \\ &= a_n^2 x^{5n} + a_l a_n x^{3n+2l} + a_l a_n x^{2n+3l} + H(x), \end{aligned}$$

where $H(x)$ is a polynomial of degree at most $2n + 3l - 1$ and

$$(P(x))^5 = (a_n x^n + a_l x^l + G(x))^5 = a_n^5 x^{5n} + 5a_n a_l x^{4n+l} + Q(x),$$

where $Q(x)$ is a polynomial of degree at most $3n + 2l$. Observe that

$$2n + 3l < 3n + 2l < 4n + l.$$

Therefore the coefficient of the term x^{4n+l} in the polynomial $P\left(x^2\right) P\left(x^3\right)$ is zero, and in the polynomial $(P(x))^5$ is $5a_n a_l \neq 0$, a contradiction. In conclusion, the only polynomials satisfying the given condition are $P(x) \equiv 0$, $P(x) \equiv 1$ and $P(x) = x^n$ for $n = 1, 2, \ldots$. ■

Second Solution. As in the first solution, consider first the case where the polynomial $P(x)$ is constant. We get solutions $P(x) \equiv 0$ and $P(x) \equiv 1$ and from now on we assume that the polynomial $P(x)$ is not constant.
Substituting $x = 0$ in the given relation, we get $P(0)^2 = P(0)^5$. Therefore $P(0) = 0$ or $P(0) = 1$.
Suppose first that $P(0) = 1$. The polynomial $P(x) - 1$ is not constant and $x = 0$ is a root of this polynomial. Therefore there exists a positive integer k and a polynomial $G(x)$ such that

$$P(x) = 1 + x^k G(x), \qquad \text{where } G(0) \neq 0.$$

By the Binomial Theorem, we have

$$\begin{aligned} P\left(x^2\right) P\left(x^3\right) &= \left(1 + x^{2k} G(x^2)\right)\left(1 + x^{3k} G(x^3)\right) \\ &= 1 + x^{2k} R(x), \end{aligned}$$

$$(P(x))^5 = \left(1 + x^k G(x)\right)^5 = 1 + 5x^k G(x) + x^{2k} S(x),$$

where $R(x)$, $S(x)$ are some polynomials with real coefficients. Hence the coefficient of x^k on the left-hand side of the equation is zero, but on the right-hand side is $5G(0) \neq 0$, a contradiction.
Now, we need to consider the case $P(x) \neq 0$, $P(0) = 0$. We can write

$$P(x) = x^m G(x) \tag{3.1}$$

for some positive integer m and some polynomial $G(x)$ such that $G(0) \neq 0$. From the given relation and (3.1), we have

$$x^{5m} G\left(x^2\right) G\left(x^3\right) = P\left(x^2\right) P\left(x^3\right) = (P(x))^5 = x^{5m} (G(x))^5,$$

so for any real number x we have

$$G\left(x^2\right) G\left(x^3\right) = (G(x))^5.$$

In other words, the polynomial $G(x)$ also satisfies the given condition. Since $G(0) \neq 0$, then from what we have seen, we conclude that $G(x) \equiv 1$. Therefore $P(x) = x^m$. It remains to observe that each such polynomial $P(x)$ satisfies the given condition. ■

Problem 3.19. Determine all pairs of polynomials $P(x)$ and $Q(x)$ with real coefficients such that

$$x^3 Q(x) = P(Q(x))$$

for all real numbers x.

Solution. If $Q(x) = 0$, then $P(Q(x)) = 0$, so $P(0) = 0$. Conversely, it is easy to check that if $Q(x) = 0$ and $P(0) = 0$ then we have a solution.

Otherwise, let $\deg P(x) = p$ and $\deg Q(x) = q \geq 0$. Then

$$\deg(x^3 Q(x)) = 3 + q, \quad \deg(P(Q(x))) = pq.$$

Hence $pq = 3 + q$. Writing this as $q(p-1) = 3$, we see that $q \mid 3$ and hence that $(p, q) = (4, 1)$ or $(2, 3)$.
If $(p, q) = (4, 1)$, then we can write $Q(x) = ax + b$, for some real numbers $a \neq 0$, b. Then the equation becomes

$$x^3(ax + b) = P(ax + b).$$

Using the substitution $x \mapsto \frac{x-b}{a}$, we find that

$$P(x) = x\left(\frac{x-b}{a}\right)^3.$$

If $(p, q) = (2, 3)$, then we can write $P(x) = ax^2 + bx + c$ where $a \neq 0$. Then the equation becomes

$$x^3 Q(x) = aQ(x)^2 + bQ(x) + c.$$

But this forces $Q(x)$ to divide c, and since $\deg Q(x) = 3 > 0$, this means $c = 0$. Cancelling a factor of $Q(x)$, we get $x^3 = aQ(x) + b$. Hence we find the solutions

$$P(x) = ax^2 + bx, \qquad Q(x) = \frac{1}{a}x^3 - \frac{b}{a}. \quad \blacksquare$$

Problem 3.20. Find all polynomials $P(x)$ such that

$$\frac{1}{\frac{1}{P(x)} - \frac{1}{P(P(x))}}$$

is also a polynomial.

Adapted from Oleg Mushkarov

First Solution. First assume that neither $P(x)$ nor $P(P(x)) - P(x)$ is a constant polynomial. Rewrite the expression as

$$\frac{P(P(x))P(x)}{P(P(x)) - P(x)}$$

and note that

$$\frac{P(P(x))P(x)}{P(P(x)) - P(x)} = P(x) + \frac{P(x)^2}{P(P(x)) - P(x)}.$$

Hence

$$\frac{P(x)^2}{P(P(x)) - P(x)}$$

must be a polynomial. If $\deg P(x) = d > 2$, then the numerator has degree $2d$, but the denominator has degree $d^2 > 2d$, an impossibility. This implies that $\deg P(x) \in \{1, 2\}$.
If $\deg P(x) = 1$, then we can write $P(x) = ax + b$, where $a \neq 0$ and $a \neq 1$ since $P(P(x)) - P(x)$ is not constant. Then

$$\frac{P(x)^2}{P(P(x)) - P(x)} = \frac{(ax + b)^2}{(a^2 - a)x + ab} = cx + d$$

for some c, d. This yields

$$(ax + b)^2 = \left((a^2 - a)x + ab\right)(cx + d).$$

Checking the coefficient of x^2 we find that $c = \frac{a}{a-1}$ and checking the constant terms, we find that $d = \frac{b}{a}$. Thus

$$(ax + b)^2 = \left((a^2 - a)x + ab\right)\left(\frac{a}{a-1}x + \frac{b}{a}\right).$$

Examining the coefficient of x, we find that

$$2ab = b(a-1) + \frac{a^2 b}{a-1},$$

which simplifies to $b = 0$. Thus $P(x) = ax$ and it is easy to see that this gives a solution.
If $\deg P(x) = 2$, then since the degrees of the numerator and the denominator of

$$\frac{P(x)^2}{P(P(x)) - P(x)}$$

are both two, we find that

$$P(P(x)) - P(x) = aP(x)^2$$

for some constant a. Hence there are infinitely many t (all t with $t = P(x)$ for some x) such that $P(t) = at^2 + t$. Hence

$$P(x) = ax^2 + x.$$

Finally, if $P(x)$ is constant, then we have a solution, and if $P(P(x)) - P(x) = C$ for some constant C, then $P(x) = x + C$. This is also a solution. ■

Second Solution. As in the first solution if $P(x)$ and $P(P(x)) - P(x)$ are not constant, then

$$\frac{P(x)^2}{P(P(x)) - P(x)}$$

must be a polynomial. Hence all the roots of $P(P(x)) - P(x)$ must be the roots of $P(x)^2$. Thus they must be roots of $P(x)$.
Let r be any root of $P(P(x)) - P(x)$. Then $P(r) = 0$ and so

$$P(P(r)) = P(r) = 0.$$

Therefore $P(P(r)) = P(0) = 0$. Thus 0 is a root of $P(x)$, and so we can write $P(x) = xS(x)$ for some polynomial $S(x)$. Hence $P(P(x)) = P(x)S(P(x))$, and therefore

$$\frac{P(x)^2}{P(P(x)) - P(x)} = \frac{P(x)^2}{P(x)S(P(x)) - P(x)} = \frac{P(x)}{S(P(x)) - 1}$$

is a polynomial. Again, either $S(x)$ is constant (and hence $P(x) = ax$) or $S(P(x)) - 1$ has a root r which is necessarily a root of $P(x)$ as well. Hence $S(0) = 1$. Writing $S(x) = 1 + xT(x)$, we find that

$$S(P(x)) = 1 + P(x)T(P(x)).$$

Therefore

$$\frac{P(x)}{S(P(x)) - 1} = \frac{P(x)}{P(x)T(P(x))} = \frac{1}{T(P(x))}$$

is a polynomial. Hence $T(x)$ must be constant.
This implies that $S(x) = 1 + ax$ and $P(x) = x(1 + ax) = ax^2 + x$. ■

Problem 3.21. Find all polynomials $P(x)$ satisfying

$$P(P(x)) + x = P(x + P(x)).$$

Solution. As in Problem 3.12, we see that $P(x)$ cannot be constant and hence if we let $\deg P(x) = d > 0$, then $P(x + P(x)) - P(P(x))$ has degree $d^2 - d + 1$. Writing the equation as $P(x+P(x)) - P(P(x)) = x$ and comparing the degrees of the two sides, we get $d^2 - d + 1 = 1$ and hence $d = 1$. Thus we can write $P(x) = ax + b$ with $a \neq 0$. Then we find that

$$P(x + P(x)) - P(P(x)) = a((a + 1)x + b) + b - a(ax + b) - b = ax.$$

Hence $a = 1$ and $P(x) = x + b$. ■

Problem 3.22. Find all polynomials $P(x)$ such that

$$\begin{aligned} P(x) + \binom{2018}{2} P(x+2) + \ldots + \binom{2018}{2016} P(x+2016) + P(x+2018) \\ = \binom{2018}{1} P(x+1) + \binom{2018}{3} P(x+3) + \ldots + \binom{2018}{2015} P(x+2015) \\ + \binom{2018}{2017} P(x+2017). \end{aligned}$$

Nordic Mathematical Contest 2018

Solution. Recall from Section 3.6, that if $\deg P(x) = d > 0$ and the leading coefficient is a_d, then $P(x+1) - P(x)$ is a polynomial of degree $d-1$ with leading coefficient da_d. We denote the polynomial $P(x+1) - P(x)$ by ΔP. Using this twice, we find that

$$\Delta^2 P = \Delta(\Delta P) = P(x+2) - 2P(x+1) + P(x).$$

Similarly, iterating this k times we find that

$$\Delta^k P = P(x+k) - \binom{k}{1} P(x+k-1) + \ldots + (-1)^k P(x).$$

Further if $\deg P(x) = d \geq k$ has leading coefficient a_d, then the polynomial $\Delta^k P$ has degree $d-k$ and leading coefficient

$$d(d-1)\cdots(d-k+1)a_d = \frac{d!}{(d-k)!}a_d$$

(and if $d < k$, then $\Delta^k P \equiv 0$). In particular, $\Delta^d P = d! a_d$.
In terms of this Δ-notation, we see that the problem is asking for all polynomials $P(x)$ such that $\Delta^{2018} P = 0$. From the above discussion, the answer is that these are exactly the polynomials with $\deg P(x) \leq 2017$. ∎

Problem 3.23. Given a positive integer k, find all polynomials $P(x)$ with real coefficients such that $P(P(x)) = (P(x))^k$.

Canadian Mathematical Olympiad 1975

Solution. We have that $P(x)$ is a constant or $P(x)$ takes infinitely many values. If $P(x)$ is a constant, say $P(x) = c$ where $c \in \mathbb{R}$, then

$$c = P(c) = P(P(x)) = (P(x))^k = c^k$$

for all real numbers x. So either $k = 1$ and c is arbitrary, or $k \neq 1$ and $c \in \{0, 1\}$. If $P(x)$ is not constant, then $P(t) = t^k$ for infinitely many real numbers t. Thus $Q(x) = P(x) - x^k$ is a polynomial with infinitely many roots and so it must vanish identically. Therefore $k \geq 1$ and $P(x) = x^k$. ∎

Problem 3.24. Let $n \geq 3$ be an integer.
Find all polynomials $f_1(x), \ldots, f_n(x)$ such that for all $1 \leq k \leq n$

$$f_k(x) f_{k+1}(x) = f_{k+1}(f_{k+2}(x)),$$

where $f_{n+1}(x) = f_1(x)$, $f_{n+2}(x) = f_2(x)$.

Oleg Mushkarov - Bulgarian Mathematical Olympiad 2012

Solution. Let $\deg f_k(x) = d_k$ for $k = 1, 2, \ldots, n$. We have

$$d_k + d_{k+1} = d_{k+1} d_{k+2}.$$

Hence $d_{k+1} \mid d_k$ for all $k = 1, 2 \ldots, n$. However, the only way this can happen all the way around the cycle is if d_k is constant. Thus all the polynomials f_k have the same degree d and we find that $2d = d^2$. If $d = 0$, then all the polynomials f_k are constant and we find that $f_k(x) = 1$ for all k. If all the polynomials f_k are quadratic, then we can write

$$f_k(x) = a_k x^2 + b_k x + c_k$$

with $a_k \neq 0$ for each $k = 1, 2 \ldots, n$. Examining the coefficient of x^4, we find that $a_k = a_{k+2}^2$ for $k = 1, 2, \ldots, n$. If $n = 2m$, then

$$a_1 = a_3^2 = \ldots = a_{2m-1}^{2^{m-1}} = a_1^{2^m},$$

hence $a_1 = a_3 = \ldots = a_{2m-1} = 1$.
Analogously, we find $a_2 = a_4 = \ldots = a_{2m} = 1$. For odd n the argument is similar, but there is only one cycle of length n. In either case, we get

$$a_1 = a_2 = \ldots = a_n = 1.$$

Now, examining the coefficient of x^3 we get

$$b_k + b_{k+1} = 2b_{k+2}, \quad k = 1, 2, \ldots, n.$$

Let $\min\{b_1, \ldots, b_n\} = b$ and suppose the minimum is attained for $b_s = b$. From the equation for $k = s-2$, we get $2b \leq b_{s-1} + b_{s-2} = 2b_s = 2b$. Thus we

must have equality in the inequalities, which means $b_{s-1} = b_{s-2} = b$. Iterating this, we find that $b_1 = \ldots = b_n = b$.
Considering the coefficient of x^2, we find that

$$c_k + c_{k+1} = 2c_{k+2} + b, \quad k = 1, 2, \ldots, n.$$

Adding all these equations, we find that $nb = 0$, which gives $b = 0$. Therefore

$$c_k + c_{k+1} = 2c_{k+2}.$$

By the same argument given above, this implies $c_1 = c_2 = \ldots = c_n = c$ for some c. Hence $f_k(x) = x^2 + c$ for all k. Plugging this in, we get

$$(x^2 + c)^2 + c = (x^2 + c)^2,$$

from which we obtain $c = 0$. So $f_k(x) = x^2$ for all k. ∎

Problem 3.25. Find all polynomials $P(x)$ with real coefficients such that

$$P(x)^2 - P(x-1)P(x+1) = 2P(x).$$

Solution. If $P(x)$ is a constant polynomial, then we easily see that $P(x) = 0$. Otherwise, let $\deg P(x) = d > 0$ and write

$$P(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$$

with $a_d \neq 0$. First, let us find the degree and leading coefficient of the left hand side $P(x)^2 - P(x-1)P(x+1)$. We have

$$P(x)^2 = a_d^2 x^{2d} + 2a_d a_{d-1} x^{2d-1} + (2a_d a_{d-2} + a_{d-1}^2)x^{2d-2} + \ldots.$$

We also compute

$$P(x \pm 1) = a_d(x \pm 1)^d + a_{d-1}(x \pm 1)^{d-1} + \ldots$$

$$= a_d x^d + (a_{d-1} \pm d a_d)x^{d-1} + \left(a_{d-2} \pm (d-1)a_{d-1} + \frac{d(d-1)}{2}a_d\right)x^{d-2} + \ldots,$$

so that

$$P(x-1)P(x+1) = a_d^2 x^{2d} + 2a_d a_{d-1} x^{2d-1} + (a_{d-1}^2 + 2a_d a_{d-2} - d a_d^2)x^{2d-2} + \ldots.$$

Hence

$$P(x)^2 - P(x-1)P(x+1) = d a_d^2 x^{2d-2} + \ldots.$$

Thus the left-hand side has degree $2d-2$ and leading coefficient da_d^2.
Since the right-hand side has degree d and leading coefficient $2a_d$, we conclude that $2d - 2 = d$, hence $d = 2$, and that $a_2 = 1$. Let r be a root of $P(x)$. Then setting $x = r$, we get

$$P(r+1)P(r-1) = 0.$$

That is, either $r+1$ or $r-1$ is a root of $P(x)$. Switching the roles of the two roots, if necessary, we find that the two roots of $P(x)$ are r and $r+1$ for some r. Hence

$$P(x) = (x-r)(x-r-1).$$

Since $P(x)$ has real coefficients, we see that r is real and it is easy to check that this gives a solution. ∎

Problem 3.26. Find all polynomials $P(x)$ with real coefficients such that

$$P(x-1)P(x+1) > P(x)^2 - 1$$

for all real numbers x.

Nikolai Nikolov

Solution. If $P(x) = c$ is a constant polynomial, then the inequality becomes $c^2 > c^2 - 1$. This always holds, hence all constant polynomials are solutions. Otherwise, write the inequality as

$$P(x)^2 - P(x-1)P(x+1) < 1.$$

From the calculation in the preceding solution, if we let $\deg P(x) = d > 0$ and suppose $P(x)$ has leading coefficient $a_d \neq 0$, then $P(x)^2 - P(x-1)P(x+1)$ is a polynomial of degree $2d-2$ with leading coefficient da_d^2. If $d \geq 2$, then

$P(x)^2 - P(x-1)P(x+1)$ will be a nonconstant polynomial with positive leading coefficient. Thus the desired inequality will fail for all sufficiently large x. If $d = 1$, then $P(x)^2 - P(x-1)P(x+1) = a_1^2$ is constant polynomial, and the inequality just reduces to $a_1^2 < 1$. Hence all polynomials of the form $P(x) = ax + b$ with $a \in (-1, 1)$ are also solutions. ■

Problem 3.27. Determine all polynomials $P(x)$ with real coefficients such that

$$(x+1)P(x-1) - (x-1)P(x)$$

is a constant polynomial.

Canadian Mathematical Olympiad 2013

First Solution. The answer is $P(x)$ any constant polynomial or

$$P(x) = ax^2 + ax + c,$$

where $a, c \in \mathbb{R}$, $a \neq 0$. Let

$$T(x) = (x+1)P(x-1) - (x-1)P(x). \tag{3.2}$$

Setting $x = -1$, we get $T(-1) = 2P(-1)$ and setting $x = 1$, we get

$$T(1) = 2P(0).$$

Since $T(x)$ is a constant polynomial, we get $2P(-1) = 2P(0)$, i.e.,

$$P(-1) = P(0).$$

Let $c = P(-1) = P(0)$ and $Q(x) = P(x) - c$. Then $Q(-1) = Q(0) = 0$, i.e., -1 and 0 are roots of $Q(x)$. Hence $Q(x) = x(x+1)R(x)$, where $R(x)$ is a polynomial with real coefficients. Then $P(x) - c = x(x+1)R(x)$, i.e.,

$$P(x) = x(x+1)R(x) + c. \tag{3.3}$$

Substituting (3.3) into (3.2) yields

$$\begin{aligned} T(x) &= (x+1)\left((x-1)xR(x-1) + c\right) - (x-1)\left(x(x+1)R(x) + c\right) \\ &= x(x-1)(x+1)\left(R(x-1) - R(x)\right) + 2c. \end{aligned}$$

Since $T(x)$ is constant, so is $x(x-1)(x+1)\left(R(x-1) - R(x)\right)$. Therefore $R(x-1) - R(x)$ is the zero polynomial, which gives $R(x) = R(x-1)$ for all $x \in \mathbb{R}$. From the result of Section 3.5, it follows that $R(x) = a$ is a constant polynomial. If $a = 0$, we get from (3.3) that $P(x)$ is constant. If $a \neq 0$, we get from (3.3) that $P(x) = ax(x+1) + c$ for some $a \in \mathbb{R}$. Therefore $P(x) = ax^2 + ax + c$, where $a \neq 0$. An easy check shows that these polynomials satisfy the given condition. ■

Second Solution. Observe that any constant polynomial P satisfies the given condition. Assume that P is not a constant polynomial.
Let $n = \deg P \geq 1$ and write

$$P(x) = \sum_{k=0}^{n} a_k x^k,$$

with $a_n \neq 0$. Then we compute that

$$(x-1)P(x) = a_n x^{n+1} + (a_{n-1} - a_n)x^n + \ldots - a_0$$

and that

$$\begin{aligned} P(x-1) &= a_n(x-1)^n + a_{n-1}(x-1^{n-1} + \ldots + a_0 \\ &= a_n x^n + (a_{n-1} - na_n)x^{n-1} + \ldots + P(-1) \end{aligned}$$

so that

$$(x+1)P(x-1) = a_n x^{n+1} + (a_{n-1} - (n-1)a_n)x^n + \ldots + P(-1).$$

Thus

$$(x+1)P(x-1) - (x-1)P(x) = (2-n)a_n x^n + \ldots + P(-1) - a_0.$$

Thus the coefficient of x^n is $(2-n)a_n$. Since we want the left-hand side to be a constant polynomial, this coefficient must be equal to 0 and since $a_n \neq 0$, we obtain $n = 2$. Hence P is a quadratic polynomial, i.e.,

$$P(x) = ax^2 + bx + c, \qquad a, b, c \in \mathbb{R}, a \neq 0.$$

Then

$$(x+1)(a(x-1)^2+b(x-1)+c)-(x-1)(ax^2+bx+c)=C.$$

Simplifying the left-hand side we get

$$(b-a)(x-1)+2c=2C.$$

Hence $b-a=0$ and $2c=2C$. So $P(x)=ax^2+ax+c$, where $a,c\in\mathbb{R}$ and $a\neq 0$. ∎

Problem 3.28. Find all polynomials $P(x)$ with real coefficients such that for all real numbers x,

$$(x+1)P(x-1)+(x-1)P(x+1)=2xP(x).$$

E. Kováč - Czech-Slovak Mathematical Olympiad 2002

First Solution. We will show that the polynomials satisfying the required condition are precisely the polynomials of the form

$$P(x)=ax^3-ax+d,$$

where a and d are arbitrary real numbers.
It is easy to check that all constant polynomials are solutions, so assume $P(x)$ is nonconstant. Then $\deg P(x)=n>0$ and we let the leading coefficient of $P(x)$ be $a_n\neq 0$. Write the equation as

$$x(P(x+1)-2P(x)+P(x-1))=P(x+1)-P(x-1).$$

Recall the result of Section 3.6, that if $P(x)$ is a polynomial of degree n with leading coefficient $a_n\neq 0$, then $P(x+1)-P(x)$ is a polynomial of degree $n-1$ with leading coefficient na_n.
From this, we see that $P(x+1)-P(x-1)$ is a polynomial of degree $n-1$ with leading coefficient $2na_n$ and $P(x+1)-2P(x)+P(x-1)$ is a polynomial of degree $n-2$ with leading coefficient $n(n-1)a_n$. Thus both sides of this

equality are polynomials of degree $n-1$ and equating the leading coefficients gives $n(n-1)a_n=2a_n$, and since $n\geq 1$ and $a_n\neq 0$, we conclude that $n=3$. Hence we can write

$$P(x)=ax^3+bx^2+cx+d.$$

In this case the two sides of our equation will be polynomials of degree $n-1=2$ and we have already seen that the leading coefficients agree. That means that if we write the equation as

$$(x+1)P(x-1)+(x-1)P(x+1)-2xP(x)=0,$$

then the left-hand side will be a linear polynomial. Hence to check that it vanishes it suffices to plug in any two distinct values of x. For $x=1$, we get $2P(0)-2P(1)=0$ which easily reduces to $a+b+c=0$. For $x=-1$, we get $-2P(0)+2P(-1)=0$ which easily reduces to $a-b+c=0$. Hence $b=0$ and $c=-a$. Thus the solutions are $P(x)=ax^3-ax+d$ (where the case $a=0$ corresponds to the constant solutions we found earlier). ∎

Second Solution. Let $P(x)$ be a polynomial satisfying the relation

$$(x+1)P(x-1)+(x-1)P(x+1)=2xP(x). \tag{3.4}$$

If we set $x=1$ in (3.4), we get $P(0)=P(1)$ and if we set $x=-1$ in (3.4), we get $P(0)=P(-1)$. Therefore if we define d by $P(0)=d$, then the equation $P(x)=d$ has roots $x=0$, $x=1$ and $x=-1$. Thus there exists a polynomial $Q(x)$ such that $P(x)=x(x-1)(x+1)Q(x)+d$. We substitute this expression into equation (3.4) to find out what conditions must be satisfied by the polynomial $Q(x)$ and the coefficient d. This gives

$$\begin{aligned}&(x+1)x(x-1)(x-2)Q(x-1)\\&+d(x+1)+(x-1)(x+1)x(x+2)Q(x+1)+d(x-1)\\&=2x^2(x-1)(x+1)Q(x)+2dx.\end{aligned}$$

The terms with the coefficient d cancel in the last equation, and the remaining terms all have a common factor of $x(x-1)(x+1)$. So cancelling this factor, we get the equation

$$(x-2)Q(x-1)+(x+2)Q(x+1)=2xQ(x) \tag{3.5}$$

for an unknown polynomial $Q(x)$. Since $a(x-2)+a(x+2) = 2ax$, every constant polynomial $Q(x) = a$ satisfies equation (3.5). Therefore equation (3.4) is satisfied by all polynomials of the form

$$P(x) = x(x-1)(x+1)a + d = ax^3 - ax + d, \qquad a, d \in \mathbb{R}.$$

In order to prove that no other polynomials $P(x)$ satisfy (3.4), we must show that any polynomial $Q(x)$ satisfying equation (3.5) is constant. To see this suppose $Q(x)$ is such polynomial and denote $Q(2) = a$. Setting $x = 2$ in equation (3.5), we obtain $Q(3) = Q(2) = a$. Now, we will prove by induction that $Q(n) = a$ for all $n \geq 2$. We have already established the base cases. If for some $n \geq 2$ we have $Q(n) = Q(n+1) = a$, then by plugging $x = n+1$ into equation (3.5), we get

$$\begin{aligned} Q(n+2) &= \frac{2(n+1)Q(n+1) - (n-1)Q(n)}{n+3} \\ &= \frac{2(n+1)a - (n-1)a}{n+3} \\ &= a. \end{aligned}$$

This completes the induction. Thus $Q(n) = a$ for all integers $n \geq 2$ (hence for infinitely many numbers). Thus $Q(x) = a$ is a constant polynomial, and we are done. ■

Problem 3.29. Find all polynomials $P(x)$ with real coefficients such that

$$(x-1)P(x+1) - (x+1)P(x-1) = 4P(x).$$

Belarusian Mathematical Olympiad 2013

Solution. Substituting $x = 1$ and then $x = -1$, we get

$$2P(1) = -P(0), \quad 2P(-1) = -P(0).$$

Setting $x = 0$, we get

$$-P(1) - P(-1) = 4P(0).$$

Therefore $P(0) = P(1) = P(-1) = 0$, which means that

$$P(x) = x(x-1)(x+1)Q(x)$$

for some polynomial $Q(x)$. Hence

$$(x+2)Q(x+1) - (x-2)Q(x-1) = 4Q(x).$$

Setting $x = 2$, then $Q(1) = Q(2)$.
Now, we prove by induction on n that $Q(n) = Q(1)$ for each positive integer n. Clearly, the statement is true for $n = 1$ and we have proven it for $n = 2$. Assume that the statement is true for $2, 3, \ldots, n-1$. Setting $x = n-1$, we have

$$(n+1)Q(n) - (n-3)Q(n-2) = 4Q(n-1).$$

Since $Q(n-2) = Q(n-1) = Q(1)$, we find that $Q(n) = Q(1)$ for each positive integer n. Hence the equation $Q(x) = Q(1)$ has infinitely many solutions and so $Q(x)$ is constant. Thus $P(x) = C(x^3 - x)$ for some constant C and it is easy to check that these are solutions. ■

Problem 3.30. Let a, b be real numbers with $a \neq 0$. Find all polynomials $P(x)$ such that

$$xP(x-a) = (x-b)P(x) \qquad \forall x.$$

Vietnamese Mathematical Olympiad 1984

Solution. If $b = 0$, then $xP(x-a) = xP(x)$ for all x, which implies that $P(x)$ is a constant polynomial.
Now, let $b \neq 0$. We will prove that if $b/a \notin \mathbb{N}^*$, then $P(x) \equiv 0$. We have two cases.

(i) If $\deg P(x) = 0$, i.e., $P(x) = C$ for some $C \in \mathbb{R}$, then $xC = (x-b)C$ for all x, so $C = 0$ and $P(x) \equiv 0$.

(ii) Let $\deg P(x) = n > 0$, where $P(x)$ is a polynomial satisfying the given property. We prove that $b/a \in \mathbb{N}^*$. The given equation can be written in the form

$$bP(x) = x\left(P(x) - P(x-a)\right) \qquad \forall x. \tag{3.6}$$

Assume that $P(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_0$, where $c_n \neq 0$ and $n \geq 1$. Then

$$\begin{aligned} P(x) - P(x-a) &= c_n\left(x^n - (x-a)^n\right) + Q(x) \\ &= nc_n a x^{n-1} + R(x), \end{aligned}$$

where $Q(x)$ and $R(x)$ are polynomials of degree at most $n-2$. Substituting expressions of $P(x)$ and $P(x) - P(x-a)$ into (3.6), we get

$$c_n b x^n + c_{n-1} b x^{n-1} + \ldots + bc_0 = nc_n a x^n + xR(x),$$

and $\deg(xR(x)) = n-1$. It follows that $c_n b = nc_n a$, i.e., $b/a = n$. Therefore if $b/a \notin \mathbb{N}^*$, then $P(x) \equiv 0$.

Now, assume that $b/a = n$, i.e., $b = na$, where $n \in \mathbb{N}^*$. The given equation becomes

$$xP(x-a) = (x - na)P(x) \qquad \forall x.$$

Plugging in successively $x = 0, a, 2a, \ldots, (n-1)a$, we conclude that

$$P(0) = P(a) = P(2a) = \ldots = P\left((n-1)a\right) = 0.$$

Since we have found n distinct roots and $P(x)$ has degree n, we must have

$$P(x) = Cx(x-a)(x-2a)\cdot\ldots\cdot(x-(n-1)a), \qquad C \in \mathbb{R},$$

and it is easy to check that these are solutions.

In conclusion, if $b = 0$, then $P(x)$ is a constant polynomial. If $b \neq 0$, then

$$P(x) = \begin{cases} 0 & \text{if } \dfrac{b}{a} \notin \mathbb{N}^* \\ Cx(x-a)(x-2a)\cdot\ldots\cdot(x-(n-1)a) & \text{if } \dfrac{b}{a} \in \mathbb{N}^*, \qquad C \in \mathbb{R}. \end{cases}$$

■

Problem 3.31. Find all polynomials $P(x)$ with real coefficients which satisfy

$$(x^3 + 3x^2 + 3x + 2)P(x-1) = (x^3 - 3x^2 + 3x - 2)P(x)$$

for all real numbers x.

Vietnamese Mathematical Olympiad 2003

Solution. The given equation is equivalent to

$$(x+2)(x^2 + x + 1)P(x-1) = (x-2)(x^2 - x + 1)P(x) \qquad \forall x \in \mathbb{R}. \quad (3.7)$$

Substituting $x = -2$ and $x = 2$ into (3.7), we get $P(-2) = P(1) = 0$.
Substituting $x = -1$ and $x = 1$ into (3.7), we get $P(-1) = P(0) = 0$.
It follows that

$$P(x) = (x-1)x(x+1)(x+2)Q(x) \qquad \forall x \in \mathbb{R},$$

where $Q(x)$ is a polynomial with real coefficients. Then

$$P(x-1) = (x-2)(x-1)x(x+1)Q(x-1) \qquad \forall x \in \mathbb{R}.$$

Substituting these expressions into (3.7), we get

$$\begin{aligned} &(x-2)(x-1)x(x+1)(x+2)(x^2 + x + 1)Q(x-1) \\ &= (x-2)(x-1)x(x+1)(x+2)(x^2 - x + 1)Q(x) \qquad \forall x \in \mathbb{R}, \end{aligned}$$

which implies that

$$(x^2 + x + 1)Q(x-1) = (x^2 - x + 1)Q(x) \qquad \forall x \neq 0, \pm 1, \pm 2.$$

Since both sides of this equation are polynomials of a variable x, then the equality is valid also for $x = 0, \pm 1, \pm 2$, i.e.,

$$(x^2 + x + 1)Q(x-1) = (x^2 - x + 1)Q(x) \qquad \forall x \in \mathbb{R}. \quad (3.8)$$

Now, observe that $\gcd(x^2 + x + 1, x^2 - x + 1) = 1$. Indeed, if

$$d(x) = \gcd(x^2 + x + 1, x^2 - x + 1),$$

then

$$d(x) \mid \frac{1}{2}\left((x+1)(x^2-x+1)-(x-1)(x^2+x+1)\right)=1.$$

It follows that $(x^2+x+1) \mid Q(x)$, i.e.,

$$Q(x)=(x^2+x+1)R(x) \qquad \forall x \in \mathbb{R},$$

where $R(x)$ is a polynomial with real coefficients. So

$$Q(x-1)=(x^2-x+1)R(x-1) \qquad \forall x \in \mathbb{R}.$$

Substituting these expressions into (3.8), we get

$$(x^2+x+1)(x^2-x+1)R(x-1)=(x^2-x+1)(x^2+x+1)R(x) \qquad \forall x \in \mathbb{R},$$

i.e.,

$$R(x-1)=R(x) \qquad \forall x \in \mathbb{R}$$

since $(x^2+x+1)(x^2-x+1) \neq 0$ for all $x \in \mathbb{R}$. The last equation implies that $R(x)$ is constant, so

$$P(x)=C(x-1)x(x+1)(x+2)(x^2+x+1),$$

where $C \in \mathbb{R}$. Conversely, by an easy check we wee that the above-mentioned polynomials satisfy the problem conditions, and so they are all the required polynomials. ■

Problem 3.32. Give an example of a polynomial $P(x)$ of degree 2001 for which the identity

$$P(x)+P(1-x)=1$$

holds.

V. Senderov - Moscow Mathematical Olympiad 2001

Solution. Plugging $x=\frac{1}{2}+t$ into the equation we get

$$P\left(\frac{1}{2}+t\right)+P\left(\frac{1}{2}-t\right)=1.$$

Hence if we define $Q(x)=P\left(\frac{1}{2}+x\right)-\frac{1}{2}$, then we get

$$Q(x)+Q(-x)=0.$$

The solutions to this are easily seen to be all polynomials $Q(x)$ with only odd powers of x. Since Q has the same degree as P, we want Q to have degree 2001. The easiest choice is $Q(x)=x^{2001}$, which gives

$$P(x)=\left(x-\frac{1}{2}\right)^{2001}+\frac{1}{2}.$$

One way to understand this problem is to note that the equation for P says that the graph of $y=P(x)$ has a center of symmetry at the point $(\frac{1}{2},\frac{1}{2})$. The graph of $y=Q(x)=x^{2001}$ has a center of symmetry at the origin, and we have translated both coordinates to move that center to the desired point. ■

Problem 3.33. Does there exist a positive integer d and a polynomial $P(x)$ with integer coefficients such that $x^d+x+2=P(P(x))$?

Solution. The answer is negative. For the case $d=1$, we want

$$P(P(x))=2x+2$$

to be linear. This forces $P(x)$ to be linear. However if we write $P(x)=ax+b$, we find that $P(P(x))=a^2x+(a+1)b$, hence $a^2=2$.
Now, for all integers x,

$$P(P(x))-x=(P(P(x))-P(x))+(P(x)-x)$$

is divisible by $P(x)-x$. Hence if $P(x)$ is a solution, then $P(x)-x$ divides x^d+2. Hence $P(0)-0$ divides $0^d+2=2$ and $P(0) \in \{\pm 1, \pm 2\}$.
If $P(0)=1$, then $P(1)=P(P(0))=2$. So $P(2)=P(P(1))=4$, but this is impossible since $2-0$ must divide $P(2)-P(0)$.
If $P(0)=-1$, then $P(-1)=P(P(0))=2$. So $P(2)=P(P(-1))=(-1)^d+1$. But again, this means $P(0)$ is odd and $P(2)$ is even, an impossibility.
If $P(0)=2$, then $P(2)=P(P(0))=2$. Thus $2=P(2)=P(P(2))=2^d+4$, a contradiction.

Finally, if $P(0) = -2$. We find that $P(-2) = P(P(0)) = 2$. So

$$P(2) = P(P(-2)) = (-2)^d.$$

If d is even, then this says $P(2) = 2^d$. However, we saw above that $P(2) - 2$ divides $2^d + 2$. So this forces $2^d - 2 \mid 2^d + 2$ so $2^d - 2 \mid 4$. Hence $2^d - 2 \leq 4$ which forces $d \leq 2$. The case $d = 2$ is impossible since $d = (\deg P(x))^2$ must be a perfect square.
If d is odd, then we see that $(P(-1) + 1) \mid 1$, so $P(-1) \in \{-2, 0\}$.
If $P(-1) = 0$, then $-2 = P(0) = P(P(-1)) = (-1)^d - 1 + 2 = 0$, a contradiction.
If $P(-1) = -2$, then $P(-2) = P(P(-1)) = 0$.
Hence $-2 = P(0) = P(P(-2)) = -2^d$. Hence $d = 1$, a contradiction. ∎

Chapter 4

Finding Polynomials. Part II

Problem 4.1. Let $R(t)$ be a polynomial of degree 2017. Prove that there exist infinitely many polynomials $P(x)$ such that

$$P((R^{2017}(t) + R(t) + 1)^2 - 2) = P(R^{2017}(t) + R(t) + 1)^2 - 2.$$

Find a relation between those polynomials $P(x)$.

Solution. Let $Q(t) = R^{2017}(t) + R(t) + 1$. Then $Q(t)$ is of degree 2017^2. Hence it is surjective on $\mathbb{R}$. Thus for each real number x there is a real number t such that $Q(t) = x$. Therefore we may rewrite the original equation as

$$P(x^2 - 2) = P(x)^2 - 2.$$

Comparing leading coefficients, we see that any such polynomial $P(x)$ must be monic. Hence, as we have seen in the chapter, there is at most one polynomial for each degree. Now, we will prove that for each positive integer d there is a polynomial $P_d(x)$ satisfying $P_d(x^2 - 2) = P_d(x)^2 - 2$. We know that two such polynomials are $P_1(x) = x$ and $P_2(x) = x^2 - 2$. Define a sequence of polynomials $P_d(x)$ by $P_{d+2}(x) + P_d(x) = xP_{d+1}(x)$ for $d \geq 0$. It is a trivial induction to show that $P_d(x)$ is a monic polynomial of degree d. We will prove by induction that the polynomials $P_d(x)$ are solutions. Hence it follows from the uniqueness lemma in the chapter that they are the only solutions.

We have already discussed the base cases $d = 1$ and 2. For the induction step, assume that the statement holds for all positive integers less than or equal to $d+1$. Now,

$$P_{d+2}(x^2-2) - P_{d+2}(x)^2 + 2$$
$$= (x^2-2)P_{d+1}(x^2-2) - P_d(x^2-2) - (xP_{d+1}(x) - P_d(x))^2 + 2.$$

We need to show this is zero. Using the induction hypothesis and rearranging, we see that it is

$$(x^2-2)(P_{d+1}(x)^2-2)-(P_d(x)^2-2)-x^2P_{d+1}(x)^2+2xP_{d+1}(x)P_d(x)-P_d(x)^2+2$$
$$= -2P_{d+1}(x)^2 - 2P_d(x)^2 + 2xP_{d+1}(x)P_d(x) - 2x^2 + 8.$$

Cancelling off a factor of -2 it suffices to show that

$$Q_d(x) = P_{d+1}(x)^2 + P_d(x)^2 - xP_{d+1}(x)P_d(x) + x^2 - 4$$

vanishes. Note that

$$Q_d(x) = (xP_d(x) - P_{d-1}(x))^2 + P_d(x)^2 - x(xP_d(x) - P_{d-1}(x))P_d(x) + x^2 - 4$$
$$= Q_{d-1}(x).$$

Hence $Q_d(x)$ is independent of d. Since we compute that

$$Q_1(x) = (x^2-2)^2 + x^2 - x^2(x^2-2) + x^2 - 4 = 0,$$

it follows that $Q_d(x)$ vanishes for all d, as desired. Thus

$$P_{d+2}(x^2-2) = P_{d+2}(x)^2 - 2.$$ ■

Problem 4.2. Find all polynomials $P(x)$ with real coefficients such that

$$P(x)P(x+1) = P(x^2-x+3).$$

Taiwanese Team Selection Test 2014

Solution. The uniqueness lemma applies, so we can have at most one solution in each degree. It is easy to check that $P(x) = x^2-2x-3$ satisfies the problem condition. If $P(x)$ has even degree, then

$$P(x) = (x^2-2x-3)^d.$$

If $P(x)$ has odd degree, then $P(x)^2$ satisfies the problem condition. Thus

$$P(x)^2 = (x^2-2x-3)^k,$$

for some k. But x^2-2x-3 has no double root. Therefore we have no such polynomial of odd degree. ■

Problem 4.3. Prove that if the polynomial f is nonzero and for every real number x, $f(x)f(x+3) = f(x^2+x+3)$, then f has no real roots.

Polish Mathematical Olympiad 1986

Solution. Suppose f is a solution that has a real root r. Let r be the largest real root of polynomial f. Then plugging in $x = r$, we find that

$$f(r^2+r+3) = 0.$$

Thus $r^2+r+3 > r$ is also a real root, a contradiction. ■

Problem 4.4. Find all linear and quadratic polynomials $P(x)$ such that

$$P(x)P(2-x) = P(2+2x-x^2).$$

Solution. Note that the uniqueness lemma does not apply in this case, hence there might be multiple solutions with the same degree. Looking at the leading coefficients of both sides, it is easy to see that any such $P(x)$ is monic.
For linear polynomials, this means we can write $P(x) = x+b$, and plugging in we get $(x+b)(b+2-x) = (2+2x-x^2+b)$. Expanding and factoring, this becomes just $(b-1)(b+2) = 0$. Thus we find the two linear polynomials $P(x) = x+1$ and $P(x) = x-2$.

For quadratic polynomials, first notice that the linear solutions give three quadratic solutions $P(x) = (x+1)^2$, $P(x) = (x+1)(x-2)$, and $P(x) = (x-2)^2$. Looking for additional solutions, we may write $P(x) = x^2 + bx + c$. Plugging this in

$$(x^2+bx+c)((2-x)^2+b(2-x)+c) = (-x^2+2x+2)^2+b(-x^2+2x+2)+c,$$

which after expanding becomes

$$(2c-b^2-b+4)x^2-2(2c-b^2-b+4)x+(c-1)(2b+c+4)=0.$$

If $2b+c+4=0$, then $P(2)=0$ and hence $P(x)$ must be $x-2$ times a linear solution. Thus we have already found these, and so we may assume $c=1$. In this case the equation reduces to $b^2+b-6=0$, hence to $(b-2)(b+3)=0$. The case $b=2$ gives the solution $P(x)=(x+1)^2$, which we have already found, but $b=-3$ gives a new solution $P(x)=x^2-3x+1$. ■

Problem 4.5. Find all nonconstant polynomials $P(x)$ such that

$$P(x)P(2x^2-2) = P(2x^3-5x).$$

Solution. Since the uniqueness lemma applies, we would be done if we could find one nonconstant solution. Since the input polynomials are all even or odd, we look for a solution $P(x)$ which is even or odd and of low degree.
It is not important for the solution why we decide to look for even/odd solutions, but one can justify this choice. Let $D(x) = \gcd(P(x), P(-x))$. Then $D(x)$ is either even or odd and we can write $P(x) = S(x)D(x)$, and hence $P(-x) = \pm S(-x)D(x)$. Also note that for any common root r of $P(2x^3-5x)$ and $P(-2x^3+5x)$, we have that $2r^3-5r$ is a common root of $P(x)$ and $P(-x)$. Hence $D(2x^3-5x) = \gcd(P(2x^3-5x), P(-2x^3+5x))$. Thus from the given equation we get

$$\frac{\pm S(-x)}{S(x)} = \frac{P(-x)}{P(x)} = \frac{P(-2x^3+5x)}{P(2x^3-5x)} = \frac{\pm S(-2x^3+5x)}{S(2x^3-5x)}.$$

Since the leftmost and rightmost expressions are rational functions with relatively prime numerator and denominator, we must have $S(x) = CS(2x^3-5x)$

for some constant C. However, comparing degrees we see that $S(x)$ must be constant, and hence $P(x) = D(x)$ is either even or odd.
Since comparing leading coefficients shows that $P(x)$ must be monic, we first try $P(x) = x^2 + a$. Plugging this in, we get

$$(x^2+a)((2x^2-2)^2+a) = (2x^3-5x)^2+a,$$

which expands to give

$$-2(2a+3)x^4+\left(7a+\frac{33}{4}\right)x^2-a(a+3)=0.$$

Since we easily see that the constant term and the coefficient of x^4 cannot both vanish, there is no such polynomial. We next try $P(x) = x^3 + ax$. This gives

$$(x^3+ax)((2x^2-2)^3+a(2x^2-2)) = (2x^3-5x)^3+a(2x^3-5x),$$

and hence

$$-2(4a+9)x^7+\frac{11(4a+9)}{2}x^5-\frac{(4a+9)(4a+31)}{8}x^3+\frac{a(4a+9)}{2}x=0.$$

Thus we have found a solution $P(x) = x^3 - \frac{9}{4}x$, and by the uniqueness lemma all nonconstant solutions are $P(x) = \left(x^3-\frac{9}{4}x\right)^n$ for some $n > 0$. ■

Problem 4.6. Find all nonconstant polynomials $P(x)$ such that

$$P(x)P(x+2) = P(x^2+1).$$

Solution. We will show that there are no such polynomials.
First suppose we have such a polynomial and $P(x)$ has a (complex) root r with $|r| \geq 2$. Choose a root of $P(x)$ with maximum modulus, call it α, and note that of course $|\alpha| \geq 2$. Plugging in $x = \alpha$, we find that α^2+1 is also a root. However, we compute

$$|\alpha^2+1| \geq |\alpha|^2-1 \geq 2|\alpha|-1 > |\alpha|,$$

contradicting the maximality of $|\alpha|$. Thus we conclude that every root r of $P(x)$ must have $|r| < 2$.
Let r be a root of $P(x)$ and let β be one of the two numbers r and $r-2$, chosen so that $|\mathrm{Re}(\beta)| \geq 1$. Then we can write $\beta = u + iv$ with $|u| \geq 1$. Plugging in $x = \beta$, we have that one of $P(\beta)$ or $P(\beta+2)$ is equal to $P(r)$ and hence vanishes. Thus we conclude that $P(\beta^2+1) = 0$, hence that $\beta^2+1 = (u^2+1-v^2)+2iuv$ is also a root of $P(x)$. By the preceding argument, we must have

$$(u^2 + 1 - v^2)^2 + 4u^2v^2 < 4,$$

which we can write as $(u^2+1)^2 + 2(u^2-1)v^2 + v^4 < 4$. But this is impossible since

$$(u^2+1)^2 + 2(u^2-1)v^2 + v^4 \geq (u^2+1)^2 \geq 4.$$

Therefore there are no such polynomials. ■

Problem 4.7. Find all nonconstant polynomials $P(x)$ such that

$$P(x^3 - 3x) = P(x)^3 - 3P(x).$$

Solution. The problem is asking for all polynomials $P(x)$ that are permutable with $T_3(x) = x^3 - 3x$. Notice that $T_3(x) = x^3 - 3x$ is the cubic polynomial in the family of polynomials $T_m(x)$ satisfying

$$T_m\left(x + \frac{1}{x}\right) = x^m + \frac{1}{x^m}$$

which were discussed in the chapter. Hence it is permutable with any polynomial $T_m(x)$. Also note that $T_3(-x) = -T_3(x)$. Thus $T_3(x)$ is also permutable with $-T_m(x)$ for any m. Now suppose that $P(x) = ax^d + \cdots$ is any degree d polynomial permutable with $T_3(x)$. Then comparing the leading coefficients we see that $a = a^3$, and hence $a = \pm 1$. Thus by the uniqueness lemma, for each degree there are at most two polynomials permutable with $T_3(x)$, one with leading coefficient 1 and one with -1. Since we have found two such polynomials, we have them all. Hence the answer is $P(x) = \pm T_m(x)$ for some $m > 0$. ■

Chapter 5

Finding Polynomials. Part III

Problem 5.1. Find all monic polynomials with only simple real roots such that $P(x^2) = \pm P(x)P(-x)$.

Solution. Let $r_1 < \ldots < r_d$ be the distinct real roots of $P(x)$. It follows that

$$(x^2 - r_1^2) \cdot \ldots \cdot (x^2 - r_d^2) = \pm(x^2 - r_1) \cdot \ldots \cdot (x^2 - r_d).$$

Thus the sets $\{r_1^2, \ldots, r_d^2\}$ and $\{r_1, \ldots, r_d\}$ are the same. This shows that $r_i > 0$ and hence

$$r_1^2 < \ldots < r_d^2.$$

It follows that $r_i^2 = r_i$. Therefore $r_i \in \{0, 1\}$.
Thus $P(x) \in \{1, x, x-1, x(x-1)\}$. ■

Problem 5.2. Let $P(x) \in \mathbb{Z}[x]$ be an irreducible polynomial having a root with absolute value greater than $\frac{3}{2}$. Prove that if $P(\alpha) = 0$, then $P(1+\alpha^3) \neq 0$.

Solution. Assume on the contrary that $P(1 + \alpha^3) = 0$.
Defining $Q(x) = P(1+x^3)$, we find that $P(x)$ and $Q(x)$ have a root in common. Since $P(x)$ is irreducible, it is the minimal polynomial of α. Whence $Q(x)$ is divisible by $P(x)$ and so we can write $P(1 + x^3) = P(x)R(x)$ for some polynomial $R(x)$. Let β be a root of $P(x)$ with the greatest modulus, say with

$|\beta| = r$. Since plugging in $x = \beta$ gives $P(1+\beta^3) = 0$, we see that β^3+1 is also a root. Since $r > \frac{3}{2}$, we have $r^3 - r - 1 > 0$, and hence $|1+\beta^3| \geq |\beta|^3 - 1 > |\beta|$, a contradiction. ∎

Problem 5.3. Find all polynomials $P(x)$ with complex coefficients such that $P(x^3-1)$ is divisible by $P(x^2+x+1)$.

Gazeta Matematică

Solution. The polynomial $P(x) = ax^d$ satisfies the problem condition as does the zero polynomial. If there is any other solution $P(x)$, then it will have a nonzero root z of maximum modulus. The equation $x^2+x+1 = z$ has two complex roots, call them x_1 and x_2. Since we can write

$$P(x^3-1) = P(x^2+x+1)Q(x)$$

for some polynomial $Q(x)$, we find that

$$P(x_1^3-1) = P(x_2^3-1) = 0.$$

Since $x_1 + x_2 = -1$, the triangle inequality gives

$$|x_1 - 1| + |x_2 - 1| \geq |x_1 + x_2 - 2| = 3.$$

Since

$$x_1^3 - 1 = z(x_1 - 1), \quad x_2^3 - 1 = z(x_2 - 1),$$

we get

$$|z| \cdot |x_1 - 1| + |z| \cdot |x_2 - 1| \geq 3|z|.$$

So one of $x_1^3 - 1$ and $x_2^3 - 1$ has modulus at least $\frac{3|z|}{2}$, so greater then $|z|$. This contradicts our choice of z, so there is no such polynomial. ∎

Problem 5.4. Find all polynomials $P(x)$ such that

$$P(x^2) = P\left(x+\frac{1}{2}\right)P\left(x-\frac{1}{2}\right).$$

First Solution. If $P(x)$ is nonconstant, then it has a root. Assume that α is a root with maximum modulus. Setting $x = \alpha + \frac{1}{2}$ and $x = \alpha - \frac{1}{2}$, we get $P\left(\left(\alpha \pm \frac{1}{2}\right)^2\right) = 0$. Therefore

$$\left|\left(\alpha \pm \frac{1}{2}\right)^2\right| \leq |\alpha|.$$

By the Triangle Inequality,

$$\left|\left(\alpha+\frac{1}{2}\right)^2\right| + \left|\left(\alpha-\frac{1}{2}\right)^2\right| \geq \left|\left(\alpha+\frac{1}{2}\right)^2 - \left(\alpha-\frac{1}{2}\right)^2\right| = 2|\alpha|.$$

Since $|\alpha|$ is maximal, we must have equality in every step, so we must have

$$\left(\alpha+\frac{1}{2}\right)^2 = \alpha \quad \text{and} \quad \left(\alpha-\frac{1}{2}\right)^2 = -\alpha,$$

whence $\alpha^2 + \frac{1}{4} = 0$. Thus $\alpha = \pm\frac{1}{2}i$ and these must both be roots. Hence

$$P(x) = \left(x^2+\frac{1}{4}\right)Q(x).$$

It is easy to check that $Q(x)$ satisfies the same equation as $P(x)$, hence the same procedure shows that either $Q(x)$ is constant or is divisible by $x^2+\frac{1}{4}$. Since the only constant solutions are 0 and 1, any easy induction shows that the solutions are either $P(x) = 0$ or

$$P(x) = \left(x^2+\frac{1}{4}\right)^n.$$

Second Solution. Since it is easy to check that $P(x) = x^2 + \frac{1}{4}$ is a solution, it follows from the uniqueness lemma that all nonconstant solutions are

$$P(x) = \left(x^2+\frac{1}{4}\right)^n$$

for some $n \geq 1$. The constant solutions add the case $n = 0$ and the zero polynomial. ∎

Problem 5.5. Find the largest $c \in \mathbb{R}$ for which there exists a nonconstant polynomial $P(x)$ such that $P(x^2) = P(x-c)P(x+c)$.

Brazilian Training Camp

Solution. The answer is $c = \frac{1}{2}$. The fact that there is a solution for $c = \frac{1}{2}$ is the previous problem, so we need only show that for $c > \frac{1}{2}$ there are no nonconstant solutions.
Suppose on the contrary, that $c > \frac{1}{2}$ and there is a nonconstant solution $P(x)$. Let r be a root of $P(x)$ with maximal modulus. Plugging in $x = r - c$ and $x = r + c$, shows that $(r-c)^2$ and $(r+c)^2$ are also roots of $P(x)$. Further the triangle inequality gives

$$|(r+c)^2| + |(r-c)|^2 \geq |(r+c)^2 - (r-c)^2| = 4c \cdot |r|.$$

Thus one of these two roots must have modulus at least $2c \cdot |r|$, which is greater than $|r|$. This is a contradiction, so there is no such polynomial. ∎

Problem 5.6. Find all polynomials $P(x) = x^3 + ax^2 + bx + c$ such that

$$P(x^2 - 2) = -P(x)P(-x).$$

John Murray - Irish Mathematical Olympiad 2012

Solution. Let $P(x) = (x - r_1)(x - r_2)(x - r_3)$. Then

$$P(-x) = -(x + r_1)(x + r_2)(x + r_3).$$

So

$$-P(x)P(-x) = (x^2 - r_1^2)(x^2 - r_2^2)(x^2 - r_3)^2$$

and

$$P(x^2 - 2) = (x^2 - 2 - r_1)(x^2 - 2 - r_2)(x^2 - 2 - r_3).$$

The sets of roots of both polynomials must be the same, hence

$$\{r_1^2, r_2^2, r_3^2\} = \{r_1 + 2, r_2 + 2, r_3 + 2\}.$$

We have three cases.
(i) $2 + r_i = r_i^2$ for all $i = 1, 2, 3$. In this case $r_i = -1, 2$ and we find that

$$P(x) \in \{(x+1)^3, (x+1)^2(x-2), (x+1)(x-2)^2, (x-2)^3\}.$$

(ii) $2 + r_i = r_i^2$ for exactly one i. Without loss, this says $2 + r_1 = r_1^2$, but $r_2 \neq r_3$ and $2 + r_2 = r_3^2$, $2 + r_3 = r_2^2$. In this case $r_1 = -1, 2$ as before. Let $Q(x) = x^2 - 2$, then the other two equations say that $r_2 = Q(r_3)$ and $r_3 = Q(r_2)$. Therefore we find that $Q(Q(r_2)) = r_2$ and $Q(Q(r_3)) = r_3$. Hence r_2 and r_3 are roots of $Q(Q(x)) = x$, but because $r_2 \neq r_3$, are not roots of $Q(x) = x$. Since we compute

$$Q(Q(x)) - x = (x^2 - 2)^2 - x = (x^2 - x - 2)(x^2 + x - 1),$$

and the first factor says $Q(x) = x$, r_2 and r_3 must be the two roots of $x^2 + x - 1$. Thus we have found two more examples

$$P(x) = (x+1)(x^2 + x - 1), \quad (x-2)(x^2 + x - 1).$$

(iii) There is no i such that $2 + r_i = r_i^2$. In this case after reordering the roots, we can suppose that $2 + r_{i+1} = r_i^2$. As in part (ii), it follows that r_i are roots of $Q(Q(Q(x))) = x$ but not roots of $Q(x) = x$. Since $Q(Q(x)) = x^4 - 4x^2 + 2$, we compute

$$Q(Q(Q(x))) - x = (x^4 - 4x^2 + 2)^2 - x = x^8 - 8x^6 + 20x^4 - 16x^2 - x + 2.$$

This has degree 8, but we know $Q(x) - x = x^2 - x - 2$ is a factor, so we get

$$Q(Q(Q(x))) - x = (x^2 - x - 2)(x^6 + x^5 - 5x^4 - 3x^3 + 7x^2 + x - 1).$$

Now we have a sixth degree polynomial and any solution $P(x)$ will be a monic cubic factor. Since the constant coefficient is -1, any cubic factors will have constant term ± 1. If one factor is $x^3 + \alpha x^2 + \beta x + 1$, then from the x^5 and x coefficients, we find that the other factor will be $x^3 + (1-\alpha)x^2 + (1+\beta)x - 1$. Hence

$$x^6 + x^5 - 5x^4 - 3x^3 + 7x^2 + x - 1 = (x^3 + \alpha x^2 + \beta x + 1)(x^3 + (1-\alpha)x^2 + (1+\beta)x - 1).$$

Looking at the coefficient of x^3, we find

$$-3 = -1 + \alpha(1+\beta) + \beta(1-\alpha) + 1 = \alpha + \beta,$$

so $\beta = -3 = \alpha$. Hence the coefficient of x^4 gives

$$-5 = 1 + \beta + \alpha(1-\alpha) + \beta = -5 - \alpha - \alpha^2,$$

and hence $\alpha = 0$ or -1. Hence $(\alpha, \beta) = (0, -3)$ or $(-1, -2)$. Finally, the coefficient of x^2 gives

$$7 = 1 - 2\alpha + \beta(1+\beta)$$

and we see that only $(\alpha, \beta) = (0, -3)$ is a solution. Thus we have found the factorization

$$x^6 + x^5 - 5x^4 - 3x^3 + 7x^2 + x - 1 = (x^3 + -3x + 1)(x^3 + x^2 - 2x - 1),$$

and hence

$$P(x) = x^3 + x^2 - 2x - 1, \quad \text{or} \quad x^3 - 3x + 1. \qquad \blacksquare$$

Remark. One could simplify factoring the sixth degree polynomial by arguing as follows. Starting from any root r_i of $P(x)$, we find the three roots of $P(x)$ are

$$r_i, \quad r_i^2 - 2, \quad (r_i^2 - 2)^2 - 2 = r_i^4 - 4r_i^2 + 2.$$

Since $P(x) = x^3 + ax^2 + bx + c$, we have that the sum of roots of $P(x)$ is equal to $-a$. Hence

$$r_i + r_i^2 - 2 + r_i^4 - 4r_i^2 + 2 = -a,$$

implying that r_i are the roots of the polynomial $R(x) = x^4 - 3x^2 + x + a$. Since the sum of the roots of $R(x)$ is zero, we find that the fourth root of $R(x)$ must be $x = a$. Thus

$$\begin{aligned} x^4 - 3x^2 + x + a &= (x-a)(x-r_1)(x-r_2)(x-r_3) \\ &= (x-a)P(x) = (x-a)(x^3 + ax^2 + bx + c). \end{aligned}$$

Examining the coefficients of x^2, x, x^0, we get

$$-a^2 + b = -3, \quad -ab + c = 1, \quad -ac = a.$$

From the last of these, we see that either $a = 0$ or $c = -1$. If $a = 0$, we find that $b = -3$ and $c = 1$, so we get

$$P(x) = x^3 - 3x + 1.$$

If $c = -1$, then we get $ab = -2$ and hence $a^3 - 3a = ab = -2$, so

$$a^3 - 3a + 2 = (a-1)^2(a+2) = 0.$$

Thus $a \in \{1, -2\}$ and $b = -\frac{2}{a}$. This gives us two more possibilities

$$P(x) = x^3 + x^2 - 2x - 1, \quad x^3 - 2x^2 + x - 1.$$

Thus we have three candidates for $P(x)$. The first two are indeed the factors of our sixth degree polynomial. The third, $x^3 - 2x^2 + x - 1$, does not actually satisfy the given equation. It is an artefact of our calculation. Still, we could have done this calculation first, then either plug the three candidates into the original equation or try dividing our sixth degree polynomial by them to find the actual solutions.

Problem 5.7. Let $P(x)$, $Q(x)$ be quadratic trinomials such that the numbers $-22, 7, 13$ are three roots of the equation $P(Q(x)) = 0$. Find the fourth root of this equation.

P. Černek - Czech-Slovak Mathematical Olympiad 2000

First Solution. If we let r_1 and r_2 be the roots of $P(x)$, then the four roots of $P(Q(x))$ will be the union of the roots s_1 and s_2 of $Q(x) = r_1$ and the roots s_3 and s_4 of $Q(x) = r_2$. Since the quadratic polynomials $Q(x) - r_1$ and $Q(x) - r_2$ have the same x^2 and x coefficients, Vieta's formula implies that $s_1 + s_2 = s_3 + s_4$. Thus we have three cases.
(i) One of the quadratic equations has roots -22, 7, the other has roots 13 and q. Then $-22 + 7 = 13 + q$, which gives $q = -28$.
(ii) One of the quadratic equations has roots -22, 13, the other has roots 7 and q. Then $-22 + 13 = 7 + q$, which gives $q = -16$.
(iii) One of the quadratic equations has roots 13, 7, the other has roots -22 and q. Then $13 + 7 = -22 + q$, which gives $q = 42$.

Clearly, each case above can be realized. If $s_1 + s_2 = s_3 + s_4 = C$, then we can take $Q(x) = x^2 - Cx$ to guarantee the pairs sum to C, and then take $P(x) = (x - s_1s_2)(x - s_3s_4)$ to get the desired roots. For example, in case (i) we find $C = -22+7 = 13-28 = -15$, so we can take $Q(x) = x^2 + 15x$. Since we want $r_1 = (-22) \cdot 7 = -154$ and $r_2 = 13 \cdot (-28) = -364$ to be the roots of $P(x)$, we can take $P(x) = (x + 154)(x + 364)$. ∎

Second Solution. We solve the problem by using some properties of the graphs of quadratic functions. Let r_1 and r_2 be the roots of $P(x)$. Then the four roots of $P(Q(x))$ will be the x-coordinates of the four points where the graphs of the quadratic functions $f_1 : y = Q(x) - r_1$ and $f_2 : y = Q(x) - r_2$ cross the x-axis. These graphs, which are parabolas, are just vertical shifts of one another, hence they have the same axis of symmetry. Suppose it is the line $x = C$. Then the four intersection points with the x-axis will be symmetric about $x = C$, hence they will have a center of symmetry at the point C on the x-axis. This leads to three cases as in the previous solution.

(i) The center of symmetry is the point $-7.5 = \dfrac{-22+7}{2}$ on the x-axis. The fourth root lies on the x-axis and is symmetrical to the the image of number 13 with respect to the point -7.5 on the x-axis. We get $-7.5 = \dfrac{13+q}{2}$, so $q = -28$.

(ii) The center of symmetry is the point $-4.5 = \dfrac{-22+13}{2}$ on the x-axis. The fourth root lies on the x-axis and is symmetrical to the the image of number 7 with respect to the point -4.5 on the x-axis. We get $-4.5 = \dfrac{7+q}{2}$, so $q = -16$.

(iii) The center of symmetry is the point $10 = \dfrac{13+7}{2}$ on the x-axis. The fourth root lies on the x-axis and is symmetrical to the the image of number -22 with respect to the point 10 on the x-axis. We get $10 = \dfrac{-22+q}{2}$, so $q = 42$.

Again these cases can all be realized since from the axis of symmetry $x = C$ and the points where it crosses the x-axis, we can choose a monic quadratic whose graph realizes these. The two quadratics arising for the two pairs of

roots are just vertical shifts of one another. This means that if we choose one of the graphs to be $y = Q(x)$, the other will be $y = Q(x) - a$ for some a, and so we can choose $P(x) = x(x - a)$. ∎

Problem 5.8. Let $P(x)$ and $Q(x)$ be polynomials with complex coefficients such that $P(x)$ and $P(Q(x))$ are monic, $P(X)$ is nonconstant, and $Q(x)$ is nonlinear. Let

$$A = \{x \in \mathbb{C} : P(x) = 0\}, \quad B = \{x \in \mathbb{C} : P(Q(x)) = 0\}.$$

Prove that the following statements are equivalent:
(i) $A = B$;
(ii) there is a complex number r such that

$$P(x) = (x - r)^n, \quad Q(x) = \omega(x - r)^m + r,$$

where $n > 0$, $m > 1$ are integers and ω is an $n-$ th root of unity.

Solution. Clearly if (ii) holds, then $A = B = \{r\}$, so (i) holds. Thus we need only prove that (i) implies (ii). Let $A = \{r_1, \ldots, r_k\}$ be the set of distinct roots of $P(x)$, $k \geq 1$. Then B is are the union of the set of roots of equations

$$Q(x) = r_1, \ldots, Q(x) = r_k.$$

Since the equations $Q(x) = r_1, \ldots, Q(x) = r_k$ have no common roots and each has at least one root, the cardinality of the union is at least k. Since (i) holds, this union is equal to A hence has cardinality k. Thus we find that each of the equations $Q(x) = r_1, \ldots, Q(x) = r_k$ has exactly one complex root. Thus there is a permutation σ such that $Q(r_{\sigma(i)}) = r_i$. Hence the polynomial $Q(x) - r_i$ has only $r_{\sigma(i)}$ as a root. Therefore $Q(x) = C(x - r_{\sigma(i)})^m + r_i$, where $C \neq 0$ is the leading coefficient of $Q(x)$. Considering the coefficient of x^{m-1} in $Q(x)$ (this is where we are using that $Q(x)$ is nonlinear and hence $m \geq 2$), we find that $r_{\sigma(i)} = r_{\sigma(j)}$ for each i, j. Since by definition the r_i are distinct, it follows that $k = 1$. This means that

$$Q(x) = C(x - r)^m + r \quad \text{and} \quad P(x) = (x - r)^n.$$

Since $P(Q(x))$ is monic, we find that $C^n = 1$, that is, C is an n-th root of unity. Thus (ii) holds. ■

Problem 5.9. Let $f \in \mathbb{Z}[x]$ be a monic polynomial and let $(a_n)_{n\geq 1}$ be an arithmetic progression of natural numbers. Prove that if there exists $k \in \mathbb{Z}$ with $a_1 = f(k)$, then the set

$$\{a_n \mid n \geq 1\} \cap \{f(n) \mid n \in \mathbb{Z}\}$$

is infinite.

Gazeta Matematică B 11/2011, *Problem* 26536

Solution. Let $d > 0$ be the common difference of the arithmetic progression and let $n \in \mathbb{N}^*$. Since $nd = (k+nd) - k$ divides $f(k+nd) - f(k)$, there exists $m \in \mathbb{N}$ such that

$$m = \frac{f(k+nd) - f(k)}{nd}.$$

Then

$$a_{mn+1} = a_1 + mnd = f(k) + f(k+nd) - f(k) = f(k+nd) \in \{f(x) \mid x \in \mathbb{Z}\}.$$

Since $n \in \mathbb{N}^*$ is arbitrary, the conclusion follows. ■

Chapter 6

Lagrange's Interpolation Formula (L.I.F.)

Problem 6.1. Let $P(x)$ be a polynomial with integer coefficients of degree d such that for some prime $q > d$ we have $P(k) \equiv 0 \pmod{q}$ for all k. Prove that all the coefficients of $P(x)$ are divisible by q.

Solution. We write the L.I.F. for $P(x)$ and $0, 1, \ldots, d$, which gives

$$d!P(x) = \sum_{k=0}^{d} (-1)^{d-k} \binom{d}{k} Q_k(x) P(k).$$

Therefore each coefficient of $d!P(x)$ is a linear combination of $P(0), P(1), \ldots, P(d)$. Since $P(0), P(1), \ldots, P(d)$ are divisible by q, each coefficient of $d!P(x)$ is divisible by q. Since $q > d$, we see that $d!$ is not divisible by q. Hence each coefficient of $P(x)$ is divisible by q. ■

Problem 6.2. Prove that any polynomial

$$P(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$$

can be written as

$$P(z) = \frac{1}{n} \sum_{k=1}^{n} \omega_k P(\omega_k) \frac{z^n - 1}{z - \omega_k},$$

where $\omega_1, \omega_2, \ldots, \omega_n$ are the n-th roots of unity.

Radu Gologan

Solution. Write the L.I.F. for $P(x)$ and $\omega_1, \omega_2, \ldots, \omega_n$, which gives

$$P(z) = \sum_{i=1}^{n} \frac{Q_i(z)}{Q_i(\omega_i)} P(\omega_i),$$

where

$$Q(z) = (z-\omega_1)\cdot\ldots\cdot(z-\omega_n) \quad \text{and} \quad Q_i(z) = \frac{Q(z)}{z-\omega_i}$$

for $i = 0, \ldots, n$. Note that $Q(z) = z^n - 1$. Therefore

$$Q_i(z) = \frac{Q(z)}{z-\omega_i} = \frac{z^n-1}{z-\omega_i}.$$

Since

$$Q_i(z) = \frac{z^n-1}{z-\omega_i} = z^{n-1} + \omega_i z^{n-1} + \ldots + \omega_i^{n-2} z + \omega_i^{n-1},$$

we have

$$Q_i(\omega_i) = n\omega_i^{n-1} = n\frac{\omega_i^n}{\omega_i} = \frac{n}{\omega_i}.$$

Therefore

$$\frac{Q_i(z)}{Q_i(\omega_i)} = \frac{\frac{z^n-1}{z-\omega_i}}{\frac{n}{\omega_i}} = \frac{\omega_i}{n}\cdot\frac{z^n-1}{z-\omega_i}.$$

Hence

$$P(z) = \frac{1}{n}\sum_{k=1}^{n} \omega_k P(\omega_k)\frac{z^n-1}{z-\omega_k}.$$

Remark. Using calculus gives a different approach for finding $Q_i(\omega_i)$. That is, since

$$z^n - 1 = (z-\omega_1)\cdot\ldots\cdot(z-\omega_n),$$

differentiating both sides we find that

$$nz^{n-1} = (z-\omega_2)\cdot\ldots\cdot(z-\omega_n) + \ldots + (z-\omega_1)\cdot\ldots\cdot(z-\omega_{n-1}).$$

Now, putting $z = \omega_i$ and noticing that all but one term on the right vanishes, we find that

$$n\omega_i^{n-1} = \frac{n}{\omega_i} = Q_i(\omega_i).$$

Problem 6.3. Let $Q(x)$ be a polynomial with real coefficients of degree d. Consider the real numbers $b_1 < \ldots < b_{d+1}$. Prove that the polynomial

$$f(x) = \sum_{i=1}^{d+1} a_i Q(x+b_i),$$

with $a_i = \prod_{i\neq j} \frac{1}{b_i - b_j}$, is constant.

Solution. Notice that a_i is exactly the quantity which we denoted by $\frac{1}{Q_i(b_i)}$ in this chapter. Therefore taking the coefficient of x^d in the L.I.F. for the polynomials x^k, we find that in the notation of this problem

$$\sum_{i=1}^{d+1} a_i b_i^k = \begin{cases} 0, & k = 0, 1, \ldots, d-1, \\ 1, & k = d. \end{cases}$$

Let $Q(x) = c_d x^d + \ldots + c_0$. Then

$$Q(x+b_i) = c_d b_i^d + q_{d-1}(x) b_i^{d-1} + \ldots + q_0(x),$$

where $q_{d-1}(x), \ldots, q_0(x)$ are polynomials of degree at most d, which depend on $Q(x)$ but not on b_i. Hence

$$\sum_{i=1}^{d+1} a_i Q(x+b_i) = c_d \sum_{i=1}^{d+1} a_i b_i^d + q_{d-1}(x)\sum_{i=1}^{d+1} a_i b_i^{d-1} + \ldots + q_0(x)\sum_{i=1}^{d+1} a_i b_i.$$

Therefore using the summation formulas above, we get

$$\sum_{i=1}^{d+1} a_i Q(x+b_i) = c_d.$$

Hence $f(x)$ is constant, and in fact it is just the x^d coefficient of $Q(x)$. ■

Problem 6.4. Let $\sigma_m(x_1,\ldots,x_n)$ be the sum of all products of subsets of size m of $x_1,\ldots,x_n$. Let $m,k\geq 0$ be any integers with $m+k<n$ and let $x_1,\ldots,x_n$ be real numbers. Prove that

$$\sum_{i=1}^{n}\frac{x_i^k\sigma_m(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)}{\prod_{j\neq i}(x_i-x_j)}=\begin{cases}(-1)^m & m+k=n-1,\\ 0 & \text{otherwise.}\end{cases}$$

Solution. We solve the problem by writing the L.I.F for the polynomial $P(x)=x^k$ at the points $x_1,\ldots,x_n$, which reads

$$x^k=\sum_{i=1}^{n}\frac{(x-x_1)\cdot\ldots\cdot(x-x_{i-1})(x-x_{i+1})\cdot\ldots\cdot(x-x_n)}{\prod_{j\neq i}(x_i-x_j)}x_i^k.$$

Considering the coefficient of x^{n-m-1} on both sides, we find that

$$(-1)^m\sum_{i=1}^{n}\frac{x_i^k\sigma_m(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)}{\prod_{j\neq i}(x_i-x_j)}=\begin{cases}1, & n-m-1=k\\ 0, & \text{otherwise}\end{cases}.$$

This rearranges to give the desired formula. ∎

Problem 6.5. Let $a_1,\ldots,a_n$ be distinct real numbers. Consider arbitrary real numbers $b_1,\ldots,b_n$.

(i) Prove that if $b_i>0$, then there exists a polynomial $P(x)$ with real coefficients of degree less than $2n$ that has no real roots and $P(a_i)=b_i$.

(ii) Prove that there exists a polynomial $P(x)$ with real coefficients of degree less than $2n$ that has only real roots and $P(a_i)=b_i$.

Solution. (i) One solution is to define $Q_i(x)$ as in the L.I.F., and set

$$P(x)=\sum_{i=1}^{n}\left(\frac{Q_i(x)}{Q_i(a_i)}\right)^2 b_i.$$

When we evaluate at $x=a_i$, the only term for which $Q_i(a_i)$ is nonzero is the i-th term, and we see that $P(a_i)=b_i$. Clearly $P(x)>0$ for all x since $b_i>0$.

A second solution would be to let $0<b<\min\{b_1,\ldots,b_n\}$. Then we can define the polynomial $P(x)$ by

$$P(x)=b+\left(\sum_{i=1}^{n}\left(\sqrt{b_i-b}\frac{Q_i(x)}{Q_i(a_i)}\right)^2\right).$$

It is clear that $P(x)\geq b>0$ and the L.I.F. gives $P(a_i)=b_i$.
(ii) First, suppose none of the b_i equal zero. We may assume $a_1<\ldots<a_n$. Let I be the set of all indices i such that $b_ib_{i+1}>0$. For each $i\in I$ choose numbers c_i and d_i such that $c_i\in(a_i,a_{i+1})$ and $b_id_i<0$. Then use the L.I.F. to construct a polynomial $P(x)$ of degree at most $n+|I|-1$ such that

$$P(a_i)=b_i,\quad P(c_i)=d_i.$$

If $b_ib_{i+1}<0$, then $P(x)$ changes sign on the interval (a_i,a_{i+1}) and if $b_ib_{i+1}>0$, then $P(x)$ changes sign on both of the intervals (a_i,c_i) and (c_i,a_{i+1}). Thus $P(x)$ has $n+|I|-1$ distinct real roots, hence it has only real roots.
For the general case, let J be the set of all indices for which $b_i=0$, and define

$$R(x)=\prod_{i\in J}(x-a_i).$$

Since we want $P(x)$ to vanish at the a_i, we will look for a polynomial

$$P(x)=R(x)Q(x).$$

We see that we want

$$Q(a_i)=\frac{b_i}{R(a_i)}\neq 0 \text{ for all } i\notin J.$$

Thus we use the previous paragraph, to find a polynomial $Q(x)$ of degree at most $2(n-|J|)-1$ that has only real roots and satisfies

$$Q(a_i)=\frac{b_i}{R(a_i)} \text{ for all } i\notin J.$$

Then we simply set $P(x)=R(x)Q(x)$ to solve the problem. ∎

Problem 6.6. Prove that there exists a polynomial P such that for all $k = 1, 2, \ldots, 2019$, P assumes the value k at exactly k different points.

Solution. Write

$$P(x) = x^{2019} + CR(x) + \sum_{i=1}^{1009} (a_i x + b_i) R_i(x)$$

with

$$R(x) = (x-1)^2 \cdot \ldots \cdot (x-1009)^2, \quad R_i(x) = \frac{R(x)}{(x-i)^2}.$$

That is, $R(i) = R'(i) = 0$, $R_j(i) = R_j'(i) = 0$, $i \neq j$. Moreover,

$$P(i) = i^{2019} + (ia_i + b_i) R_i(i),$$

$$P'(i) = 2019 i^{2018} + (ia_i + b_i) R_i'(i) + a_i R_i(i).$$

Now, we want to find a_i, b_i in such a way that

$$P(i) = 2i, \quad P'(i) = 0$$

for $i = 1, \ldots, 1009$. Solving for a_i and b_i, we first find that

$$ia_i + b_i = \frac{2i - i^{2019}}{R_i(i)},$$

and from this we get

$$a_i = -\frac{2019 i^{2018} + R_i'(i) \left(\frac{2i - i^{2019}}{R_i(i)} \right)}{R_i(i)}.$$

Note that because $R_i(i) \neq 0$, this does define a_i. Plugging back into the first formula gives b_i.
Now, choose the real number C large enough that

$$P\left(\frac{1}{2}\right), P\left(\frac{3}{2}\right), \ldots, P\left(\frac{2017}{2}\right) > 2019.$$

Since $\lim_{x \to -\infty} P(x) = -\infty$,

$$P(1) = 2, \ P(3) = 6, \ldots, P(1009) = 2018,$$

we see that we must have a local maximum on each of the intervals $(-\infty, 1)$, $(1, 2), \ldots, (1008, 1009)$. Call these $x_1, \ldots, x_{1009}$. Thus we have 2018 critical points

$$x_1 < 1 < x_2 < 2 < \ldots < x_{1009} < 1009.$$

Since $P(x)$ has degree 2019, these must be the only critical points, and since the x_i are all local maxima, it follows that $1, 2, \ldots, 1009$ are all local minima. Therefore the polynomial $P(x)$ is monotone on each interval $(-\infty, x_1)$, $(x_1, 1), \ldots, (1009, +\infty)$. Since $P(i) = 2i$ and $P(x_i) > 2019$, we find that the equation $P(x) = k$ has exactly k distinct solutions for $k = 1, 2, \ldots, 2019$. ■

Chapter 7

Newton's Identities

Problem 7.1. Let a, b, c be distinct real numbers with $a + b + c = 2019$. Evaluate the sum

$$\frac{a(b-c)^2}{(c-a)(a-b)} + \frac{b(c-a)^2}{(a-b)(b-c)} + \frac{c(a-b)^2}{(b-c)(c-a)}.$$

Solution. Let $r = b - c$, $s = c - a$, $t = a - b$ and consider the sums

$$x_n = ar^n + bs^n + ct^n.$$

The current problem asks us to evaluate $\frac{x_3}{rst}$.
It is easy to see that $x_0 = a + b + c = 2019$ and $x_1 = 0$. Since $r + s + t = 0$, Newton's Identities give

$$\begin{aligned} x_3 &= (r+s+t)x_2 - (rs+st+tr)x_1 + rstx_0 \\ &= (a+b+c)rst = 2019rst. \end{aligned}$$

Hence the desired the answer is just 2019. ■

Problem 7.2. Find all positive integers a, b, c such that

$$\frac{a^4}{(a-b)(a-c)} + \frac{b^4}{(b-c)(b-a)} + \frac{c^4}{(c-a)(c-b)} = 47.$$

Solution. Consider the sums

$$T_n = a^n(b-c) + b^n(c-a) + c^n(a-b).$$

Then we easily see that $T_0 = T_1 = 0$, and a short computation gives

$$T_2 = -(a-b)(b-c)(c-a).$$

Letting $p = a+b+c$, $q = ab+ac+bc$, and $r = abc$, we see that Newton's Identities give

$$T_{n+3} = pT_{n+2} - qT_{n+1} + rT_n.$$

Therefore

$$T_3 = pT_2 = -(a+b+c)(a-b)(b-c)(c-a)$$

and

$$\begin{aligned} T_4 &= pT_3 - qT_2 = p^2T_2 - qT_2 = (p^2-q)T_2 \\ &= -(a-b)(b-c)(c-a)\left(\sum a^2 + \sum ab\right). \end{aligned}$$

Thus the requested condition, which says

$$-\frac{T_4}{(a-b)(b-c)(c-a)} = 47,$$

simplifies to

$$a^2+b^2+c^2+ab+bc+ca = 47.$$

Note that

$$a^2+b^2+c^2+ab+bc+ca \geq \frac{2}{3}(a+b+c)^2,$$

since this inequality rearranges to give the Cauchy-Schwartz inequality

$$a^2+b^2+c^2 \geq ab+bc+ca.$$

Thus we have $(a+b+c)^2 \leq \frac{141}{2}$, and hence $a+b+c \leq 8$. Since a, b, c must be distinct integers that sum to at most 8, we find that up to symmetry they must be $(1,2,3)$, $(1,2,4)$, $(1,2,5)$, or $(1,3,4)$. It is easy to check that only $(1,2,5)$ is a solution. Thus there are six solutions $(a,b,c) = (1,2,5)$ and its permutations. ■

Problem 7.3. Let x, y and z be distinct integers and n be a non-negative integer. Prove that

$$\frac{x^n}{(x-y)(y-z)} + \frac{y^n}{(y-z)(y-x)} + \frac{z^n}{(z-x)(x-y)}$$

is an integer.

Kürschák Competition 1959

First Solution. Let

$$P_n(x,y,z) = \frac{x^n(z-y) + y^n(x-z) + z^n(y-x)}{(x-y)(y-z)(z-x)}.$$

We prove by induction that $P_n(x,y,z)$ are polynomials in x, y, z with integer coefficients for all $n \geq 0$. If $n = 0$ or $n = 1$, we get $P_0(x,y,z) = P_1(x,y,z) = 0$. Assume that it is true for some $n \geq 2$. Then

$$\begin{aligned} P_{n+1}(x,y,z) - zP_n(x,y,z) &= \frac{x^{n+1} - zx^n}{(x-y)(x-z)} - \frac{y^{n+1} - zy^n}{(x-y)(y-z)} \\ &= \frac{x^n - y^n}{x-y}. \end{aligned}$$

Therefore

$$P_{n+1}(x,y,z) = zP_n(x,y,z) + (x^{n-1} + x^{n-2}y + \ldots + y^{n-1}),$$

and the conclusion follows from the principle of mathematical induction. ■

Second Solution. Let

$$P_n(x,y,z) = \frac{x^n(z-y) + y^n(x-z) + z^n(y-x)}{(x-y)(y-z)(z-x)}.$$

We prove by strong induction that $P_n(x,y,z)$ are polynomials in x, y, z with integer coefficients for all $n \geq 0$.
Clearly, $P_0(x,y,z) = P_1(x,y,z) = 0$ and $P_2(x,y,z) = 1$. Observe that

$$t^n(t-x)(t-y)(t-z) = t^{n+3} - (x+y+z)t^{n+2} + (xy+yz+zx)t^{n+1} - xyzt^n.$$

Hence if $t = x, y, z$, we get

$$t^{n+3} = (x+y+z)t^{n+2} - (xy+yz+zx)t^{n+1} + xyzt^n.$$

It follows that

$$P_{n+3}(x,y,z) = (x+y+z)P_{n+2}(x,y,z) - (xy+yz+zx)P_{n+1}(x,y,z) + xyzP_n(x,y,z).$$

If we assume that for a fixed $n \geq 0$, the expressions P_n, P_{n+1}, P_{n+2} are polynomials, it follows that also P_{n+3} is a polynomial. It follows that $P_n(x,y,z)$ are polynomials with integer coefficients for all $n \geq 0$. ■

Problem 7.4. Find all positive integers n such that for all real numbers x, y, z with $x+y+z = 0$ and $xyz = 1$, the expression $S_n = x^n + y^n + z^n$ is constant.

Solution. By Newton's Identities, we can write the power sums S_n as polynomials in the elementary symmetric polynomials

$$\sigma_1 = x+y+z,\ \sigma_2 = xy+yz+zx,\ \text{and}\ \sigma_3 = xyz.$$

Since $\sigma_1 = 0$ and $\sigma_3 = 1$ are fixed, this means that S_n will be a polynomial in σ_2. Note that σ_2 can take on infinitely many values. To prove this note that the quadratic polynomial $t^2 + zt + \frac{1}{z}$ has two real roots (which we can make x, y, so that Vieta's formulas will imply $x+y+z = 0$ and $xyz = 1$) if it has positive discriminant, that is, if $z^2 - \frac{4}{z} > 0$. Thus we get infinitely many triples (x,y,z) with $+y+z = 0$ and $xyz = 1$ and for these we compute that $\sigma_2 = -z^2 - \frac{1}{z}$ takes on infinitely many different values. In fact one can show that σ_2 can take on any value in $\left(-\infty, -\frac{3}{\sqrt[3]{4}}\right]$.[1]

[1]This is equivalent to the fact that the polynomial $x^3 + \sigma_2 x - 1$ has only real roots for such σ_2. As you have seen in chapter 4 of *117 Polynomial Problems*, this is equivalent to $\frac{\sigma_2^3}{27} + \frac{1}{4} \leq 0$. Therefore to $\sigma_2 \leq -\frac{3}{\sqrt[3]{4}}$.
For an alternative proof, without loss of generality, assume that $x+y > 0$.
Then $z = -x-y = \frac{1}{xy}$.
Thus $-\sigma_2 = x^2+xy+y^2 = (x+y)^2 - xy = (x+y)^2 + \frac{1}{x+y} = (x+y)^2 + \frac{1}{2(x+y)} + \frac{1}{2(x+y)} \geq \frac{3}{\sqrt[3]{4}}$.
That is, $\sigma_2 \leq -\frac{3}{\sqrt[3]{4}}$.

Thus the problem just reduces to the question of when S_n, thought of as a polynomial in σ_2, is a constant polynomial. Since we compute $S_1 = \sigma_1 = 0$, $S_2 = \sigma_1^2 - 2\sigma_2 = -2\sigma_2$, and $S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 = 3$, we see that $n = 1, 3$ are examples. The following Lemma shows there are no other examples.

Lemma. For each $d \geq 1$, S_{2d} is a polynomial of degree d in σ_2 with leading coefficient of $2(-1)^d$ and S_{2d+1} is a polynomial of degree $d-1$ in σ_2 with leading coefficient of $(-1)^{d-1}(2d+1)$.

Proof. Since $S_2 = -2\sigma_2$, $S_3 = 3$ for $d = 1$, the statement holds true. Assume that the statement holds for $1, 2, \ldots, d-1$. Since

$$S_{2d} = -\sigma_2 S_{2d-2} + S_{2d-3},$$

$$S_{2d-3} = (-1)^{d-1}(2d-3)\sigma_2^{d-3} + \ldots \quad \text{and} \quad S_{2d-2} = 2(-1)^{d-1}\sigma_2^{d-1} + \ldots,$$

we find that $S_{2d} = 2(-1)^d\sigma_2^d + \ldots$. Analogously, since

$$S_{2d+1} = -\sigma_2 S_{2d-1} + S_{2d-2},$$

we find that $S_{2d+1} = (-1)^{d-1}(2d+1)\sigma_2^{d-1} + \ldots$, and we are done. ❑

Problem 7.5. Let

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= y_1 + y_2 + y_3 + y_4, \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 &= y_1^2 + y_2^2 + y_3^2 + y_4^2, \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 &= y_1^3 + y_2^3 + y_3^3 + y_4^3. \end{aligned}$$

Prove that

$$(x_1 - y_2)(x_1 - y_3)(x_1 - y_4) = (y_1 - x_2)(y_1 - x_3)(y_1 - x_4).$$

Solution. Let $P(x) = (x - x_1)(x - x_2)(x - x_3)(x - x_4)$ and

$$Q(x) = (x - y_1)(x - y_2)(x - y_3)(x - y_4).$$

If $x_1 = y_1$, then we get

$$\begin{aligned} x_2 + x_3 + x_4 &= y_2 + y_3 + y_4, \\ x_2^2 + x_3^2 + x_4^2 &= y_2^2 + y_3^2 + y_4^2, \\ x_2^3 + x_3^3 + x_4^3 &= y_2^3 + y_3^3 + y_4^3. \end{aligned}$$

From the first two equations, we find that

$$x_2x_3 + x_3x_4 + x_2x_4 = y_2y_3 + y_3y_4 + y_2y_4.$$

Hence from this and the third equation, we obtain

$$x_2x_3x_4 = y_2y_3y_4.$$

Therefore all the coefficients of polynomials $(x - x_2)(x - x_3)(x - x_4)$ and $(x - y_2)(x - y_3)(x - y_4)$ are equal. So

$$S(x) = (x - x_2)(x - x_3)(x - x_4) = (x - y_2)(x - y_3)(x - y_4)$$

for all x. Hence

$$S(x_1) = (x_1 - y_2)(x_1 - y_3)(x_1 - y_4) = S(y_1) = (y_1 - x_2)(y_1 - x_3)(y_1 - x_4).$$

Now, without loss of generality, assume that $\{x_1, x_2, x_3, x_4\} \neq \{y_1, y_2, y_3, y_4\}$. From the first two identities, we get

$$\sum_{1 \le i < j \le 4} x_ix_j = \sum_{1 \le i < j \le 4} y_iy_j.$$

This and the third identity yield

$$\sum_{1 \le i < j < k \le 4} x_ix_jx_k = \sum_{1 \le i < j < k \le 4} y_iy_jy_k.$$

Thus

$$P(x) - Q(x) = x_1x_2x_3x_4 - y_1y_2y_3y_4.$$

Substituting $x = x_1$, $x = y_1$, we find that

$$-Q(x_1) = P(x_1) - Q(x_1) = x_1x_2x_3x_4 - y_1y_2y_3y_4,$$

and

$$P(y_1) = P(y_1) - Q(y_1) = x_1x_2x_3x_4 - y_1y_2y_3y_4.$$

Since $x_1 - y_1 \neq 0$, we get

$$(x_1 - y_2)(x_1 - y_3)(x_1 - y_4) = \frac{-Q(x_1)}{y_1 - x_1} = \frac{x_1x_2x_3x_4 - y_1y_2y_3y_4}{y_1 - x_1}$$

and

$$(y_1 - x_2)(y_1 - x_3)(y_1 - x_4) = \frac{P(y_1)}{y_1 - x_1} = \frac{x_1x_2x_3x_4 - y_1y_2y_3y_4}{y_1 - x_1}.$$

Therefore

$$(x_1 - y_2)(x_1 - y_3)(x_1 - y_4) = (y_1 - x_2)(y_1 - x_3)(y_1 - x_4)$$

and we are done. ■

Problem 7.6. Show that there is a positive integer k with the following property: if a, b, c, d, f are integers and m is a divisor of $a^n + b^n + c^n - d^n - e^n - f^n$ for all integers $n = 1, 2, \ldots, k$ then m is a divisor of

$$a^n + b^n + c^n - d^n - e^n - f^n$$

for all positive integers n.

Solution. We claim that $k = 6$ works. Let us define

$$T_n = a^n + b^n + c^n - d^n - e^n - f^n$$

and

$$(x - a)(x - b)(x - c)(x - d)(x - e)(x - f) = x^6 - \sigma_1x^5 + \ldots + \sigma_6.$$

Then Newton's Identities read

$$T_{n+6} = \sigma_1T_{n+5} - \sigma_2T_{n+4} + \ldots - \sigma_6T_n.$$

Hence if m divides T_1, T_2, ..., T_6, then m divides T_n for all positive integer n. ■

Problem 7.7. Let $a_1, \ldots, a_n$ be distinct real numbers such that no subset of them sums to zero. Solve following system of equations:

$$\begin{cases} a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0, \\ a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2 = 0, \\ \vdots \\ a_1x_1^n + a_2x_2^n + \ldots + a_nx_n^n = 0. \end{cases}$$

Solution. Let $P(x) = (x - x_1) \cdot \ldots \cdot (x - x_n) = x^n - \sigma_1 x^{n-1} + \ldots + (-1)^n \sigma_n$. Now, multiply the l-th equation by $(-1)^{n-l}\sigma_{n-l}$ for $l = 1, \ldots, n-1$. Adding all of these and the n-th equation, we find that

$$\sum_{k=1}^{n} a_k x_k^n + \sum_{l=1}^{n-1} (-1)^{n-l} \sigma_{n-l} \sum_{k=1}^{n} a_k x_k^l = 0.$$

Note that

$$x_k^n - \sigma_1 x_k^{n-1} + \ldots + (-1)^n \sigma_n = 0.$$

Multiplying this equation by a_k and summing all n such equations, we get

$$\sum_{k=1}^{n} a_k x_k^n + \sum_{l=1}^{n-1} (-1)^{n-l} \sigma_{n-l} \sum_{k=1}^{n} a_k x_k^l + (-1)^{n+1} \sigma_n \sum_{k=1}^{n} a_k = 0.$$

Comparing these we see that

$$\sigma_n(a_1 + a_2 + \ldots + a_n) = 0.$$

Since the sum of the a_k is nonzero, we see that $\sigma_n = x_1 x_2 \cdots x_n = 0$, and hence at least one of $x_1, \ldots, x_n$ is zero. Plugging this in, we reduce to an analogous problem in one few variables.
Hence we can repeat the argument above. Iterating this (or writing down a more formal induction), we get $x_1 = \ldots = x_n = 0$. ■

Problem 7.8. Let $z_1, \ldots, z_n$ be complex numbers and k be a positive integer such that

$$z_1^k + \ldots + z_n^k = z_1^{k+1} + \ldots + z_n^{k+1} = \ldots = z_1^{k+n-1} + \ldots + z_n^{k+n-1} = 0.$$

Prove that $z_1 = \ldots = z_n = 0$.

Solution. Since $S_k = S_{k+1} = \cdots = S_{n+k-1} = 0$, by Newton's Identities we have $S_m > 0$ for all $m \geq k$. Now, define $t_i = z_i^k$. Denote by S'_m the sum of the $m-$ th powers of $t_1, \ldots, t_n$. Since this gives $S'_m = S_{km}$, we conclude that $S'_1 = S'_2 = \ldots = S'_n = 0$. Thus by Example 7.19 (with $a = 0$) or the previous problem (with $a_1 = \cdots = a_n = 1$), we conclude that $t_1, \ldots, t_n$ are all zero, hence $z_1 = \ldots = z_n = 0$. ■

Problem 7.9. Prove that for any $z_1, z_2, \ldots, z_n \in \mathbb{C}$ there exists a positive integer $k \leq 2n + 1$ such that

$$\mathrm{Re}(z_1^k + z_2^k + \ldots + z_n^k) \geq 0.$$

Solution. Let $z_{n+1} = \overline{z_1}, \ldots, z_{2n} = \overline{z_n}$ and let

$$P(x) = (x - z_1) \cdot \ldots \cdot (x - z_{2n}) = x^{2n} - \sigma_1 x^{2n-1} + \ldots + \sigma_{2n}.$$

Then

$$S_k = z_1^k + z_2^k + \ldots + z_{2n}^k = \sum_{j=1}^{n} \left(z_j^k + \overline{z}_j^k \right) = 2\mathrm{Re}(z_1^k + z_2^k + \ldots + z_n^k).$$

Now, we must prove that there is a positive integer $k \leq 2n + 1$ such that $S_k \geq 0$. We will do this by assuming that $S_k < 0$ for each $1 \leq k < 2n + 1$ and proving that this implies $S_{2n+1} > 0$. By Newton's Identities, we have

$$S_r = \sigma_1 S_{r-1} - \sigma_2 S_{r-2} + \ldots + (-1)^{r+1} r \sigma_r,$$

for all $r = 1, 2, \ldots, 2n$. Since we assumed $S_k < 0$ for each $1 \leq k < 2n + 1$, an easy induction shows that $\sigma_1, \sigma_3, \ldots < 0$ and $\sigma_2, \sigma_4, \ldots > 0$. However, we then compute that

$$S_{2n+1} = \sigma_1 S_{2n} - \sigma_2 S_{2n-1} + \ldots - S_1 \sigma_{2n} > 0,$$

since every term on the right-hand side is positive. ■

Problem 7.10. Let a, b, c be complex numbers and let $S_n = a^n + b^n + c^n$. Assume that S_1, S_2, S_3 are integers and $5S_1 - 3S_2 - 2S_3$ is divisible by 6. Prove that S_n is an integer for each n.

Solution. Since $5S_1 - 3S_2 - 2S_3$ is divisible by 6, we find that $S_1 - S_2$ is divisible by 2 and $S_1 - S_3$ is divisible by 3. It follows that $S_1^2 - S_2$ is divisible by 2 and $S_1^3 - S_3$ is divisible by 3. Hence $\sigma_2 = \frac{1}{2}(S_1^2 - S_2)$ is an integer. Since we compute

$$\sigma_3 = \frac{1}{3}(S_3 - S_1S_2 + \sigma_2 S_1) = \frac{1}{3}(S_3 - S_1(S_1^2 - 2\sigma_2) + \sigma_2 S_1)$$
$$= \frac{1}{3}(S_3 - S_1^3 + 3\sigma_2 S_1) = \frac{1}{3}(S_3 - S_1^3) + \sigma_2 S_1,$$

we see that σ_3 is an integer. Since $\sigma_1, \sigma_2, \sigma_3$ are integers, Newton's Identities imply that S_n is an integer for all n. ■

Problem 7.11. Let p and q be prime numbers and let $a_1, \ldots, a_p, b_1, \ldots, b_q$ be integers such that $a_i + b_j$ form a complete residue system modulo pq. Prove that $a_1, \ldots, a_p$ form a complete residue system modulo p.

Solution. Define $S_k = 1^k + \ldots + (p-1)^k$ and recall from the chapter that $S_k \equiv 0 \pmod{p}$ for $k = 1, \ldots, p-2$ and $S_{p-1} \equiv -1 \pmod{p}$. We will prove that among $a_1, \ldots, a_p$ there is a multiple of p. Note that if we replace a_i by $a_i' = a_i - k$ for all $i = 1, \ldots, p$, then the numbers $a_i' + b_j = a_i + b_j - k$ also form a complete residue system modulo pq. Thus one of the a_i' is a multiple of p, and hence one of the a_i is congruent to $k \pmod{p}$. Thus we will have proved that $a_1, \ldots, a_p$ is a complete residue system modulo p.
Consider the sums

$$T_k = \sum_{i=1}^{p}\sum_{j=1}^{q}(a_i + b_j)^k.$$

Since the $a_i + b_j$ form a complete residue system modulo pq, we see that $a_i + b_j$ takes on every value modulo p exactly q times. Thus

$$T_k \equiv qS_k \equiv \begin{cases} 0, & \text{if } k = 1, \ldots, p-2 \\ -q, & \text{if } k = p-1 \end{cases} \pmod{p}.$$

We can also expand using the binomial theorem to get

$$T_k = \sum_{m=0}^{k}\binom{k}{m}\sum_{i=1}^{p}a_i^m\sum_{j=1}^{q}b_j^{k-m}.$$

In particular for $k = 1$, we get

$$T_k = p\sum_{i=1}^{q}b_i + q\sum_{i=1}^{p}a_i \equiv q\sum_{i=1}^{p}a_i \equiv 0 \pmod{p}.$$

Hence

$$\sum_{i=1}^{p}a_i \equiv 0 \pmod{p}.$$

Similarly for $k = 2$,

$$\sum(a_i + b_j)^2 = q\sum_{i=1}^{p}a_i^2 + 2\left(\sum_{i=1}^{q}b_i\right)\left(\sum_{i=1}^{p}a_i\right) + p\sum_{i=1}^{q}b_i^2 \equiv q\sum_{i=1}^{p}a_i^2 \pmod{p}.$$

Thus

$$\sum_{i=1}^{p}a_i^2 \equiv 0 \pmod{p}.$$

Continuing with this argument for $m = 3, \ldots, p-2$, we find that

$$\sum(a_i + b_j)^m \equiv q\sum_{i=1}^{p}a_i^m \equiv 0 \pmod{p}.$$

Hence

$$\sum_{i=1}^{p}a_i^m \equiv 0 \pmod{p}, \text{ for } m = 1, \ldots, p-2.$$

Doing the argument one more time gives

$$\sum(a_i + b_j)^{p-1} \equiv q\sum_{i=1}^{p}a_i^{p-1} \equiv -q \pmod{p},$$

and hence that

$$\sum_{i=1}^{p}a_i^{p-1} \equiv -1 \pmod{p}.$$

Since Fermat's little theorem says that if a is not a multiple of p, then

$$a^{p-1} \equiv 1 \pmod{p},$$

we conclude that there is exactly one a_i which is a multiple of p. ■

Problem 7.12. Let (a_n) and (b_n) be two sequences such that

$$\begin{cases} 4a_1 - 2b_1 = 7, \\ a_{n+1} = a_n^2 - 2b_n \\ b_{n+1} = b_n^2 - 2a_n. \end{cases}$$

Find the value of $2^{512}a_{10} - b_{10}$.

Belarusian Mathematical Olympiad

Solution. Let

$$P(x) = (x - z_1)(x - z_2)(x - z_3) = x^3 - a_1x^2 + b_1x - 1.$$

If we look at

$$P(x)P(-x) = (x^2 - z_1^2)(x^2 - z_2^2)(x^2 - z_3^2) = Q(x^2),$$

then we find

$$Q(x) = x^3 - (a_1^2 - 2b_1)x^2 + (b_1^2 - 2a_1)x - 1 = x^3 - a_2x^2 + b_2x - 1.$$

Since the roots of $Q(x)$ are z_1^2, z_2^2, z_3^2, we have

$$a_2 = a_1^2 - 2b_1 = z_1^2 + z_2^2 + z_3^2$$

and

$$b_2 = b_1^2 - 2a_1 = z_1^2z_2^2 + z_2^2z_3^2 + z_3^2z_1^2.$$

Iterating this

$$a_n = z_1^{2^{n-1}} + z_2^{2^{n-1}} + z_3^{2^{n-1}},$$
$$b_n = z_1^{2^{n-1}}z_2^{2^{n-1}} + z_2^{2^{n-1}}z_3^{2^{n-1}} + z_3^{2^{n-1}}z_1^{2^{n-1}}.$$

From the first criterion, we obtain that $P(2) = 0$. Hence $z_1 = 2$ and $z_2z_3 = \frac{1}{2}$. Therefore

$$a_{10} = 2^{2^9} + z_2^{2^9} + z_3^{2^9}, b_{10} = 2^{-2^9} + 2^{2^9}(z_2^{2^9} + z_3^{2^9}).$$

That is, $2^{512}a_{10} - b_{10} = 2^{2^{10}} - 2^{-2^9}$.

Chapter 8

Additional Problems

Problem 8.1. Suppose that

$$(x^2 - x + 1)^3(x^3 + 4x^2 + 4x + 1)^5 = a_{21}x^{21} + a_{20}x^{20} + \ldots + a_0.$$

What is the value of $a_1 + \ldots + a_{10}$?

Solution. Putting $P(x) = (x^2 - x + 1)^3(x^3 + 4x^2 + 4x + 1)^5$, it is easy to deduce that $x^{21}P\left(\frac{1}{x}\right) = P(x)$, therefore $a_{21} = a_0 = 1, a_{20} = a_1, \ldots$. Thus

$$a_1 + \cdots + a_{10} = \frac{1}{2}(a_0 + \cdots + a_{21} - 2a_0) = \frac{1}{2}(P(1) - 2P(0)) = 49999. \blacksquare$$

Problem 8.2. Let $P(x)$ be an irreducible monic polynomial with rational coefficients. Assume that $P(x)$ has two roots whose product is equal to 1. Prove that the degree of the polynomial is even.

Solution. Assume that $P(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_0$. Suppose that r and s are roots such that $rs = 1$. Let $Q(x) = \frac{1}{a_0} \cdot x^dP\left(\frac{1}{x}\right)$. If r is a root of $P(x)$, then $\frac{1}{r} = s$ is a root of $Q(x)$. Hence $P(x)$ and $Q(x)$ have a common root (i.e., $x = s$). Since $P(x)$ is irreducible and monic, it is the minimal polynomial of s. Thus $P(x)$ divides $Q(x)$. Since $P(x)$ and $Q(x)$ are monic polynomials of the same degree, this implies $P(x) = Q(x)$. Hence if r is root of $P(x)$, then

$\frac{1}{r}$ is also a root. Since $P(x)$ is irreducible (and at least quadratic since it has two roots), ± 1 cannot be roots of $P(x)$. Therefore we can partition the roots of $P(x)$ into pairs $\left\{r, \frac{1}{r}\right\}$. Hence the degree of the polynomial is even. ■

Problem 8.3. Consider a third degree polynomial. We are allowed to perform the following two operations arbitrarily many times:

(i) reverse the order of its coefficients including zeroes (for instance, from the polynomial $x^3 - 2x^2 - 3$ we can obtain $-3x^3 - 2x + 1$);

(ii) change polynomial $P(x)$ to the polynomial $P(x+1)$.

Is it possible to obtain the polynomial $x^3 - 3x^2 + 3x - 3$ from the polynomial $x^3 - 2$?

Alexander Golovanov

First Solution. Note that the polynomial $x^3 - 2$ is irreducible and has only one real root. The two transformations clearly preserve this property. Thus it suffices to track where the real root has moved to. If r is a root of $P(x)$, then the first operation produces a polynomial with $\frac{1}{r}$ as a root, and the second one gives a polynomial with $r-1$ as a root. Since the real root of the original polynomial is $\sqrt[3]{2}$ and that of desired ending polynomial is $1+\sqrt[3]{2}$, the problem reduces to the question whether it is possible to obtain $1+\sqrt[3]{2}$ from $\sqrt[3]{2}$ by operations $x \mapsto \frac{1}{x}$ and $x \mapsto x-1$. If it is, then we can apply one more operation $x \mapsto x-1$ to get back to $\sqrt[3]{2}$. Thus there is a sequence of moves ending with a $x \mapsto x-1$ taking $\sqrt[3]{2}$ to itself. Looking at the inverse moves, we see that we can go from $\sqrt[3]{2}$ to itself after a sequence of operations $x \mapsto x+1$ and $x \mapsto \frac{1}{x}$, starting with an $x \mapsto x+1$. An easy induction shows that the composition of such operations leads to $x \mapsto \frac{ax+b}{cx+d}$, where a, b, c, d are non-negative integers with $ad-bc=1$. Further each operation $x \mapsto x+1$ increases $a+b+c+d$ and the other operation preserves this sum. Thus $\sqrt[3]{2}$ must be a root of $x = \frac{ax+b}{cx+d}$, where $a+b+c+d \geq 3$. If we clear denominators, we will get a quadratic polynomial with x as a root and we cannot get the zero polynomial (since this occurs only for $(a,b,c,d) = (1,0,0,1)$ which has $a+b+c+d < 3$). However, the minimal polynomial of $\sqrt[3]{2}$ is of degree 3, so this is a contradiction. ■

Second Solution. The original polynomial has one real and two conjugate complex roots. We have seen that under the two operations these roots are subject to transformations $x \mapsto x-1$, $x \mapsto \frac{1}{x}$.
The imaginary roots of $x^3 - 2$ have negative real parts, and this property is preserved under the above transformations. But the desired polynomial has two imaginary roots with positive real parts. Thus we cannot reach it. ■

Third Solution. For $P(x) = ax^3+bx^2+cx+d$, we define $R(P(x)) = 3ad-bc$. The first operation transforms $P(x)$ into $x^3 P\left(\frac{1}{x}\right) = dx^3 + cx^2 + bx + a$, hence $R(P(x))$ doesn't change. The second transformation, transforms $P(x)$ into

$$P(x+1) = ax^3 + (b+3a)x^2 + (c+3a+2b)x + (d+a+b+c).$$

Hence the value of $R(P(x+1))$ is

$$3(d+a+b+c)a - (b+3a)(c+3a+2b) = R(P(x)) - 2\left(b^2+3ab+3a^2\right).$$

Since $b^2+3ab+3a^2 > 0$, we find that $R(P(x+1)) < R(P(x))$. Thus the above process cannot increase $R(P(x))$.
On the other hand $R(x^3-2) = -6$, $R(x^3-3x^2+3x-3) = 0$. Thus we cannot get from x^3-2 to x^3-3x^2+3x-3. ■

Problem 8.4. Let $z_1, \ldots, z_{2n}$ be nonreal $2n+1$-th roots of unity. Prove that

$$\sum_{k=1}^{2n} \frac{1-\overline{z_k}}{1+z_k} = 2n+1.$$

Solution. Since $\overline{z_k} = \frac{1}{z_k}$, we find that

$$\frac{1-\overline{z_k}}{1+z_k} = \frac{1-\frac{1}{z_k}}{1+z_k} = \frac{z_k-1}{z_k(1+z_k)}.$$

Hence

$$\sum_{k=1}^{2n} \frac{1-\overline{z_k}}{1+z_k} = \sum_{k=1}^{2n} \frac{z_k-1}{z_k(1+z_k)}.$$

Observe that $z_1, \ldots, z_{2n}$ can be partitioned into the sets

$$\left\{ z_k, \frac{1}{z_k} \right\}, \ k = 1, \ldots, n.$$

Therefore

$$\begin{aligned}
\sum_{k=1}^{2n} \frac{z_k - 1}{z_k(1+z_k)} &= \sum_{k=1}^{n} \left(\frac{z_k - 1}{z_k(1+z_k)} + \frac{\frac{1}{z_k} - 1}{\frac{1}{z_k}(\frac{1}{z_k} + 1)} \right) \\
&= \sum_{k=1}^{n} \left(\frac{z_k - 1}{z_k(1+z_k)} + \frac{z_k - z_k^2}{1+z_k} \right) \\
&= \sum_{k=1}^{n} \left(\frac{-1 + z_k + z_k^2 - z_k^3}{z_k(1+z_k)} \right) = \sum_{k=1}^{n} \left(\frac{(1-z_k)(z_k^2-1)}{z_k(1+z_k)} \right) \\
&= -\sum_{k=1}^{n} \left(\frac{(1-z_k)^2}{z_k} \right) = -\sum_{k=1}^{n} \left(z_k + \frac{1}{z_k} - 2 \right) \\
&= 2n - \sum_{k=1}^{n} \left(z_k + \frac{1}{z_k} \right) = 2n - \sum_{k=1}^{2n} z_k.
\end{aligned}$$

Since the sum of all the $2n+1$-th roots of unity is zero, we get $\sum_{k=1}^{2n} z_k = -1$. Hence the sum is $2n+1$. ∎

Problem 8.5. Prove that for any integer a the polynomial $3x^{2n} + ax^n + 2$ is not divisible by $2x^{2m} + ax^m + 3$.

Moscow Mathematical Olympiad 1952

Solution. Let α_1 and α_2 be the two roots of $2x^2 + ax + 3$, which are

$$\alpha_1, \alpha_2 = \frac{-a \pm \sqrt{a^2 - 24}}{4},$$

and let β_1 and β_2 be the two roots of $3x^2 + ax + 2$, which are

$$\beta_1, \beta_2 = \frac{-a \pm \sqrt{a^2 - 24}}{6}.$$

Then the roots $g(x)$ are m-th roots of α_1 and α_2 and similarly the roots of $f(x)$ are the n-th roots of β_1 and β_2.
Assume on the contrary, that $g(x) = 2x^{2m} + ax^m + 3$ divides

$$f(x) = 3x^{2n} + ax^n + 2.$$

Then every root of $g(x)$ is also a root of $f(x)$. Let x_1 and x_2 be roots of $g(x)$ with $x_1^m = \alpha_1$ and $x_2^m = \alpha_2$. We have two cases.
(i) $a^2 - 24 > 0$. In this case $|\alpha_1| \neq |\alpha_2|$, therefore $|x_1|^n \neq |x_2|^n$ and hence one of x_1 and x_2 is an n-th root of β_1 and the other is an n-th root of β_2. On one hand $|x_1 x_2| = \sqrt[n]{\beta_1 \beta_2} = \sqrt[n]{\frac{2}{3}} < 1$ and on the other $|x_1 x_2| = \sqrt[m]{\alpha_1 \alpha_2} = \sqrt[m]{\frac{3}{2}} > 1$, a contradiction.
(ii) $a^2 - 24 < 0$. In this case $|\alpha_1| = |\alpha_2| = \sqrt{\frac{3}{2}}$ and $|\beta_1| = |\beta_2| = \sqrt{\frac{2}{3}}$. Therefore on one hand $|x_1| = \sqrt[2m]{\frac{3}{2}} > 1$ and on the other $|x_1| = \sqrt[2n]{\frac{2}{3}} < 1$, a contradiction.

Problem 8.6. Assume that $\alpha^{2005} + \beta^{2005}$ can be expressed as a polynomial in $\alpha + \beta$ and $\alpha\beta$. Find the sum of the coefficients of the polynomial.

China Western Mathematical Olympiad 2005

First Solution. Let

$$\alpha^{2005} + \beta^{2005} = \sum_{i=0}^{2005} \sum_{j=0}^{i} a_{ij} (\alpha + \beta)^{i-j} (\alpha\beta)^j.$$

In order to find the sum of the coefficients of the polynomial on the right-hand side we set $\alpha + \beta = 1$ and $\alpha\beta = 1$. Let $S_k = \alpha^k + \beta^k$. It follows that the sum of the coefficients is S_{2005}. Since

$$(\alpha + \beta)(\alpha^{k-1} + \beta^{k-1}) = (\alpha^k + \beta^k) + \alpha\beta(\alpha^{k-2} + \beta^{k-2}),$$

we get

$$S_{k-1} = S_k + S_{k-2} \implies S_k = S_{k-1} - S_{k-2}.$$

Hence

$$\begin{aligned} S_k = S_{k-1} - S_{k-2} &= (S_{k-2} - S_{k-3}) - S_{k-2} = -S_{k-3} \\ &= S_{k-5} - S_{k-4} = S_{k-5} - (S_{k-5} - S_{k-6}) = S_{k-6}. \end{aligned}$$

So $\{S_k\}_{k\geq 1}$ is a periodic sequence with period 6 and we get $S_{2005} = S_1 = 1$. ■

Second Solution. Set $\alpha+\beta = 1$ and $\alpha\beta = 1$ and let $S_k = \alpha^k + \beta^k$. Then the sum of the coefficients is S_{2005}. Since α and β are solutions of the equation $x^2 - x + 1 = 0$, we have

$$\alpha = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}, \quad \beta = \cos\frac{\pi}{3} - i\sin\frac{\pi}{3}.$$

Hence

$$\begin{aligned} \alpha^k + \beta^k &= \left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right)^k + \left(\cos\frac{\pi}{3} - i\sin\frac{\pi}{3}\right)^k \\ &= \left(\cos\frac{k\pi}{3} + i\sin\frac{k\pi}{3}\right) + \left(\cos\frac{k\pi}{3} - i\sin\frac{k\pi}{3}\right) \\ &= 2\cos\frac{k\pi}{3}. \end{aligned}$$

If $k = 2005$, we get $S_{2005} = 1$. ■

Problem 8.7. Determine all polynomials with non-negative real coefficients satisfying the following conditions:

$$p(0) = 0, \qquad p(|z|) \leq x^4 + y^4 \quad \forall z \in \mathbb{C},$$

where $|z|$ is the modulus of the complex number $z = x + iy$.

Spanish Mathematical Olympiad 1982

Solution. As $p(0) = 0$, we can write $p(z) = a_n z^n + a_{n-1}z^{n-1} + \ldots + a_2 z^2 + a_1 z$, where $a_i \geq 0$ for all $i = 1, 2, \ldots, n$. We have

$$p\left(\sqrt{x^2+y^2}\right) \leq x^4 + y^4 \qquad \forall x, y \in \mathbb{R}. \tag{8.1}$$

Setting $y = 0$ and $x > 0$, we get $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x \leq x^4$, i.e.,

$$a_n x^{n-4} + \ldots + a_5 x + a_4 + \frac{a_3}{x} + \frac{a_2}{x^2} + \frac{a_1}{x^3} \leq 1. \tag{8.2}$$

If one of a_1, a_2, a_3 is different from zero, then $\lim\limits_{x\to 0^+} \dfrac{p(x)}{x^4} = \pm\infty$, which contradicts (8.2). So $a_1 = a_2 = a_3 = 0$. Also, $a_5 = a_6 = \ldots = a_n = 0$, because otherwise $\lim\limits_{x\to+\infty} \dfrac{p(x)}{x^4} = \pm\infty$, which again contradicts (8.2). So (8.2) gives $a_4 \leq 1$. Hence $p(z) = az^4$, where $a \geq 0$. Now, (8.1) gives

$$a(x^2+y^2)^2 \leq x^4 + y^4 \qquad \forall x, y \in \mathbb{R}.$$

Setting $x = y = 1$, we get $4a \leq 2$ and hence $a \leq \frac{1}{2}$. For $a = \frac{1}{2}$, the desired inequality factors as $\frac{1}{2}(x^2-y^2)^2 \geq 0$, hence it is true. This implies the inequality for all $a < \frac{1}{2}$. Thus the examples are $p(z) = az^4$ for $0 \leq a \leq \frac{1}{2}$. ■

Problem 8.8. Let m be a positive integer and

$$P(x) = \sum_{k=0}^{6m-1} x^{2^k} = x + x^2 + \ldots + x^{2^{6m-1}},$$
$$Q(x) = x^{2^{2m+1}-2} + x^{2^{2m}-1} + 1.$$

Prove that $P(x)$ is divisible by $Q(x)$.

Solution. Writing $Q(x) = \dfrac{x^{3(2^{2m+1}-1)} - 1}{x^{2^{2m+1}-1} - 1}$, we see that the roots of $Q(x)$ are the $3(2^{2m+1}-1)$-th roots of unity which are not $(2^{2m+1}-1)$-th roots of unity. To show that $Q(x)$ divides $P(x)$ it suffices to show these are all roots of $P(x)$. Let α be a root of $Q(x)$, then $\omega = \alpha^{2^{2m}-1} \neq 1$ is a primitive cube root of unity. Hence if k is not a multiple of 3, we have

$$1 + \omega^k + \omega^{2k} = \frac{1-\omega^{3k}}{1-\omega^k} = 0.$$

Then we compute

$$\begin{aligned} P(\alpha) &= \sum_{j=0}^{2m-1} (\alpha^{2^j} + \alpha^{2^{j+2m}} + \alpha^{2^{j+4m}}) \\ &= \sum_{j=0}^{2m-1} \alpha^{2^j}(1 + \alpha^{2^j(2^{2m}-1)} + \alpha^{2^j(2^{4m}-1)}) \\ &= \sum_{j=0}^{2m-1} \alpha^{2^j}(1 + \omega^{2^j} + \omega^{2^j(2^{2m}+1)}). \end{aligned}$$

Now note that $2^{2m} + 1 \equiv 2 \pmod 3$, so we can write this as

$$P(\alpha) = \sum_{j=0}^{2m-1} \alpha^{2^j}(1 + \omega^{2^j} + \omega^{2\cdot 2^j}),$$

and every term vanishes by the remark above. Therefore $P(\alpha) = 0$. ∎

Problem 8.9. Let n, k be positive integers with $k < n$ and let α be a real number with $|\alpha| \leq 1$.
Prove that all the roots of polynomial $x^n + \alpha x^{n-k} + \alpha x^k + 1$ are on the unit circle.

Solution. Let r be any root of polynomial $x^n + \alpha x^{n-k} + \alpha x^k + 1$.
Then $-r^{n-k}(r^k + \alpha) = 1 + \alpha r^k$.
If $r^k = -\alpha$, then $\alpha^2 = 1$ and we are done. Otherwise,

$$|r|^{n-k} = \left|\frac{\alpha r^k + 1}{r^k + \alpha}\right|.$$

Then we compute that

$$|r|^{2n-2k} - 1 = \frac{(1-\alpha^2)(1-|r|^{2k})}{|r^k + \alpha|^2}.$$

If $|r| > 1$, then the left-hand side is positive and the right-hand side is non-positive, and if $|r| < 1$, then the left-hand side is negative and the right-hand side is non-negative. Both are contradictions. Hence $|r| = 1$. ∎

Problem 8.10. **(a)** Prove that there exists a polynomial P with integer coefficients of degree 502 such that

$$1 + x^4 + x^8 + x^{12} + \ldots + x^{2008} = P(x)P(-x)P(ix)P(-ix) \qquad \forall x \in \mathbb{C}.$$

(b) Prove that if $a_0, a_1, \ldots, a_n \in \mathbb{C}$, $a_n \neq 0$, then there exists a polynomial Q with complex coefficients of degree n such that

$$a_0 + a_1 x^4 + a_2 x^8 + \ldots + a_n x^{4n} = Q(x)Q(-x)Q(ix)Q(-ix) \qquad \forall x \in \mathbb{C}.$$

Marcel Ţena - Nicolae Teodorescu Competition 2008

Solution. **(a)** The polynomial

$$P(x) = \frac{x^{503}+1}{x+1} = 1 - x + x^2 - x^3 + \ldots + x^{502}$$

has integer coefficients and satisfies the given condition. Indeed,

$$\begin{aligned} P(x)P(-x)P(ix)P(-ix) &= \frac{x^{503}+1}{x+1} \cdot \frac{-x^{503}+1}{-x+1} \cdot \frac{-ix^{503}+1}{ix+1} \cdot \frac{ix^{503}+1}{-ix+1} \\ &= \frac{(1-x^{1006})(1+x^{1006})}{(1-x^2)(1+x^2)} = \frac{1-x^{2012}}{1-x^4} \\ &= 1 + x^4 + x^8 + \ldots + x^{2008}. \end{aligned}$$

(b) Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$.
Then $f(x^4) = a_0 + a_1 x^4 + a_2 x^8 + \ldots + a_n x^{4n}$.
We can write $f(x) = a_n(x - x_1)(x - x_2)\cdot\ldots\cdot(x - x_n)$, where $x_1, x_2, \ldots, x_n \in \mathbb{C}$ are the roots of $f(x)$.

Choose $y_1, y_2, \ldots, y_n \in \mathbb{C}$ such that $y_k^4 = x_k$ for $k = 1, 2, \ldots, n$. Then

$$\begin{aligned} f(x^4) &= a_n \prod_{k=1}^{n} (x^4 - y_k^4) \\ &= a_n \prod_{k=1}^{n} (x - y_k)(x + y_k)(x - iy_k)(x + iy_k) \\ &= a_n \prod_{k=1}^{n} (x - y_k)(-(-x - y_k))(i(-ix - y_k))(-i(ix - y_k)) \\ &= (-1)^n a_n \prod_{k=1}^{n} (x - y_k) \prod_{k=1}^{n} (-x - y_k) \prod_{k=1}^{n} (-ix - y_k) \prod_{k=1}^{n} (ix - y_k). \end{aligned}$$

Choose $\lambda \in \mathbb{C}$ such that $\lambda^4 = (-1)^n a_n$ and define

$$Q(x) = \lambda \prod_{k=1}^{n} (x - y_k).$$

Then $a_0 + a_1 x^4 + a_2 x^8 + \ldots + a_n x^{4n} = Q(x)Q(-x)Q(ix)Q(-ix)$, as we wanted to prove. ■

Problem 8.11. Let d be an integer greater than 1 and let $a_0, a_1 \ldots, a_d$ be real numbers with $a_1 = a_{d-1} = 0$. Prove that for any real number k,

$$|a_0| - |a_d| \leq \sum_{i=0}^{d-2} |a_i - k a_{i+1} - a_{i+2}|.$$

Canadian Mathematical Olympiad 2019

Solution. Let $Q(x) = x^2 - kx - 1$ and $P(x) = a_d x^d + \cdots + a_0$. Note that the absolute value of the product of roots of $Q(x)$ is 1. Thus $Q(x)$ has a root r satisfying $|r| \leq 1$. Furthermore,

$$Q(x)P(x) = a_d x^{d+2} - k a_d x^{d+1} + \sum_{i=0}^{d-2} (a_i - k a_{i+1} - a_{i+2}) x^{i+2} - a_0(1 + kx).$$

Putting $x = r$, we find that

$$0 = a_d r^{d+2} - k a_d r^{d+1} + \sum_{i=0}^{d-2} (a_i - k a_{i+1} - a_{i+2}) r^{i+2} - a_0(1 + kr).$$

Since $r^2 = kr + 1$, we have $a_d r^{d+2} - k a_d r^{d+1} = a_d r^d$, $-a_0(1 + kr) = -a_0 r^2$, which gives

$$0 = -a_0 r^2 + \sum_{i=0}^{d-2} (a_i - k a_{i+1} - a_{i+2}) r^{i+2} + a_d r^d.$$

Thus

$$a_0 = \sum_{i=0}^{d-2} (a_i - k a_{i+1} - a_{i+2}) r^i + a_d r^{d-2}.$$

By the Triangle Inequality,

$$|a_0| \leq |a_d| \left| r^{d-2} \right| + \sum_{i=0}^{d-2} |a_i - k a_{i+1} - a_{i+2}| \cdot |r^i|.$$

Since $|r| \leq 1$, we get

$$|a_d| \left| r^{d-2} \right| + \sum_{i=0}^{d-2} |a_i - k a_{i+1} - a_{i+2}| \cdot |r^i| \leq |a_d| + \sum_{i=0}^{d-2} |a_i - k a_{i+1} - a_{i+2}|.$$

Thus $|a_0| \leq |a_d| + \sum_{i=0}^{d-2} |a_i - k a_{i+1} - a_{i+2}|$. ■

Problem 8.12. Let $(a_n)_{n \in \mathbb{N}}$ be a sequence of real numbers defined by

$$a_{n+1} = a_n^3 - 3a_n^2 + 3$$

for all $n \geq 0$. For how many values of a_0 do we have $a_{2017} = a_0$?

Solution. Let $P(x) = x^3 - 3x^2 + 3$. Rewrite the sequence in the form

$$a_{n+1} = P(a_n).$$

Note that $P(x) - x = x^3 - 3x^2 - x + 3 = (x-3)(x^2-1)$.
It is obvious that if $a_k > 3$ for some k, then $a_{k+1} > a_k > 3$ and if $a_k < -1$ for some k, then $a_{k+1} < a_k < -1$. Thus, if we have $a_{2017} = a_0$, then we must have $-1 \le a_0 \le 3$, implying that $-2 \le a_0 - 1 \le 2$ or equivalently $|a_0 - 1| \le 2$. Thus we can write $a_0 = 1 + \omega + \frac{1}{\omega}$, with $\omega = \cos\alpha + i\sin\alpha$. Thus

$$a_1 = a_0^3 - 3a_0^2 + 3 = (a_0-1)^3 - 3(a_0-1) + 1 = 1 + \omega^3 + \frac{1}{\omega^3}.$$

Iterating this we get $a_{2017} = 1 + \omega^{3^{2017}} + \frac{1}{\omega^{3^{2017}}}$. Note that $a_0 = 1 + 2\cos\alpha$ and $a_{2017} = 1 + 2\cos 3^{2017}\alpha$. If $a_{2017} = a_0$, then $\cos\alpha = \cos 3^{2017}\alpha$. That is,

$$\alpha \in \left\{0, \frac{2\pi}{3^{2017}-1}, \ldots, \pi\right\} \cup \left\{0, \frac{2\pi}{3^{2017}+1}, \ldots, \pi\right\}.$$

Since $\gcd(3^{2017}-1, 3^{2017}+1) = 2$, the only overlap between these two lists is the common first and last elements. Therefore we have 3^{2017} values for α. ■

Problem 8.13. Let $d \ge 3$ be an odd number, let $r > 0$ be a real number and let $a_1, \ldots, a_{d-1}$ be complex numbers. The polynomial

$$P(z) = z^d + a_1 z^{d-1} + \ldots + a_{d-1}z - 1$$

has roots $r_1, \ldots, r_d$ such that $|r_j| = r$ for $j = 1, \ldots, d$. Prove that

$$\mathrm{Im}(r_j + r_1 \ldots r_{j-1} r_{j+1} \ldots r_d) = 0$$

for each j. Moreover, prove that $\mathrm{Im}(a_k) = \mathrm{Im}(a_{d-k})$ for each k.

Solution. Since d is an odd integer, by Vieta's Formulas, we have

$$r_1 \cdot \ldots \cdot r_d = 1.$$

On the other hand, $|r_1 \cdot \ldots \cdot r_d| = r^d = 1$. Hence $r = 1$, which gives $\overline{r_j} = \frac{1}{r_j}$.

Now, it is easy to deduce that

$$r_j + r_1 \cdot \ldots \cdot r_{j-1} r_{j+1} \cdot \ldots \cdot r_d = r_j + \frac{1}{r_j} = r_j + \overline{r_j} = 2\mathrm{Re}(r_j) \in \mathbb{R}.$$

Moreover, since $|r_j| = 1$, we have $\mathrm{Re}(r_j) \in [-1, 1]$.
Hence $r_j + \overline{r_j} \in [-2, 2]$. Furthermore, letting $i_1 < \ldots < i_k$ be the k indices not included among $j_1 < \ldots < j_{d-k}$, we compute

$$\begin{aligned} a_k &= (-1)^{d-k} \sum_{1 \le j_1 < \ldots < j_{d-k} \le d} r_{j_1} \cdot \ldots \cdot r_{j_{d-k}} \\ &= (-1)^{d-k} \sum_{1 \le i_1 < \ldots < i_k \le d} \frac{1}{r_{i_1} \cdot \ldots \cdot r_{i_k}} \\ &= (-1)^{d-k} \sum_{1 \le i_1 < \ldots < i_k \le d} \overline{r_{i_1} \cdot \ldots \cdot r_{i_k}} \\ &= (-1)^d \overline{a_{d-k}} = -\overline{a_{d-k}}. \end{aligned}$$

Hence $\mathrm{Im}(a_k) = \mathrm{Im}(a_{d-k})$. ■

Problem 8.14. Let $n \ge 3$ be an integer. Do there exist positive real numbers $a_1, a_2, a_3, \ldots a_n$ such that for any $k = 1, 2, \ldots, n$ every root of the polynomial $a_{k+n-1}x^{n-1} + \ldots + a_{k+1}x + a_k$ (where $a_{i+n} = a_i$ for all $i = 1, 2, \ldots, n-1$) satisfies the inequality $|\mathrm{Im}\ z| \le |\mathrm{Re}\ z|$?

Chinese Team Selection Test 2003

Solution. The answer is no. Assume there exists $a_1, a_2, a_3, \ldots, a_n$ such that polynomial $a_{k+n-1}x^{n-1} + \ldots + a_{k+1}x + a_k$ has roots $z_1, \ldots, z_{n-1}$ satisfying $|\mathrm{Im}\ z| \le |\mathrm{Re}\ z|$ for all $j = 1, 2, \ldots, n-1$. Then we have

$$z_j^2 = (\mathrm{Re}\ z_j + i\ \mathrm{Im}\ z_j)^2 = (\mathrm{Re}\ z_j)^2 - (\mathrm{Im}\ z_j)^2 + 2(\mathrm{Re}\ z_j)(\mathrm{Im}\ z_j) \cdot i.$$

Thus $\mathrm{Re}\ z_j^2 = (\mathrm{Re}\ z_j)^2 - (\mathrm{Im}\ z_j)^2 \ge 0$. We have

$$\mathrm{Re}(z_1^2 + \ldots + z_{n-1}^2) = \mathrm{Re}(z_1^2) + \mathrm{Re}(z_2^2) + \ldots + \mathrm{Re}(z_{n-1}^2) \ge 0.$$

Note that since $n \geq 3$,

$$z_1 + \ldots + z_{n-1} = -\frac{a_{k+n-2}}{a_{k+n-1}} \quad \text{and} \quad \sum_{1 \leq i < j \leq n-1} z_i z_j = \frac{a_{k+n-3}}{a_{k+n-1}},$$

yielding the equality

$$\begin{aligned} z_1^2 + \ldots + z_{n-1}^2 &= (z_1 + \ldots + z_{n-1})^2 - 2 \sum_{1 \leq i < j \leq n-1} z_i z_j \\ &= \frac{a_{k+n-2}^2 - 2a_{k+n-1} \cdot a_{k+n-3}}{a_{k+n-1}^2}. \end{aligned}$$

Since the preceding value is real, we find that it is nonnegative. Thus

$$\frac{a_{k+n-2}^2 - 2a_{k+n-1} \cdot a_{k+n-3}}{a_{k+n-1}^2} \geq 0.$$

We get $a_{k+n-2}^2 - 2a_{k+n-1} \cdot a_{k+n-3} \geq 0$. As k varies over $1, \ldots, n$, $j = k+n-2$ interpreted cyclically also varies over $1, \ldots, n$.
Thus we find that for all $j = 1, 2, \ldots, n$ the inequality $a_j^2 - 2a_{j-1}a_{j+1} \geq 0$ is true. Now, let $a_s = \min\{a_1, a_2, a_3, \ldots a_n\}$. Then

$$a_s^2 - 2a_{s-1}a_{s+1} \leq a_s^2 - 2a_s \cdot a_s = -a_s^2 < 0,$$

contradiction. ∎

Problem 8.15. Let $P(x) = x^{d+1} + a_1 x^{d-1} + a_2 x^{d-2} + \ldots + a_d$ be a polynomial with complex coefficients. Consider $r = \max\{|a_1|, \ldots, |a_d|\}$. Prove that for each of its roots r_i we have $|r_i|(|r_i| - 1) \leq r$.

Marcel Chiriță

Solution. If $|r_i| \leq 1$, then the inequality is easy since $|r_i|(|r_i| - 1) \leq 0 \leq r$. Assume $|r_i| > 1$. Rewrite the equation that r_i is a root of $P(x)$ as

$$r_i = \frac{a_1}{r_i} + \frac{a_2}{r_i^2} + \ldots + \frac{a_d}{r_i^d}$$

and apply the triangle inequality to get

$$\begin{aligned} |r_i| &\leq \frac{|a_1|}{|r_i|} + \frac{|a_2|}{|r_i|^2} + \ldots + \frac{|a_d|}{|r_i|^d} \leq r\left(\frac{1}{|r_i|} + \frac{1}{|r_i|^2} + \ldots + \frac{1}{|r_i|^d}\right) \\ &= r \cdot \frac{1 - \frac{1}{|r_i|^d}}{|r_i| - 1} < \frac{r}{|r_i| - 1}. \end{aligned}$$

This rearranges to the desired inequality. ∎

Problem 8.16. Let a and b be two positive integers. Prove that

$$2(a^2 - ab + b^2) \mid (a-b)^{2^n} + a^{2^n} + b^{2^n}.$$

Gazeta Matematică

First Solution. Let $P(x) = \frac{1}{2}\left((x-b)^{2^n} + x^{2^n} + b^{2^n}\right)$. Note that since all the binomial coefficients $\binom{2^n}{k}$ with $k \neq 0, 2^n$ are even integers, $P(x)$ is a polynomial with integer coefficients. Let ε be a root of $\varepsilon^2 - \varepsilon + 1 = 0$, and recall that since $1 + \varepsilon^3 = (1+\varepsilon)(\varepsilon^2 - \varepsilon + 1) = 0$, this implies $\varepsilon^3 = -1$. Then

$$P(\varepsilon b) = \frac{1}{2} b^{2^n}(1 + \varepsilon^{2^n} + (1-\varepsilon)^{2^n}).$$

Note that $1 - \varepsilon = -\varepsilon^2$, which implies that

$$1 + \varepsilon^{2^n} + (1-\varepsilon)^{2^n} = 1 + \varepsilon^{2^n} + \varepsilon^{2^{n+1}} = \frac{\varepsilon^{3 \cdot 2^n} - 1}{\varepsilon^{2^n} - 1} = 0.$$

Thus $P(\varepsilon b) = 0$, which gives $P(\overline{\varepsilon} b) = 0$. Hence

$$(x - \varepsilon b)(x - \overline{\varepsilon} b) = x^2 - (\varepsilon + \overline{\varepsilon}) bx + b^2 = x^2 - bx + b^2$$

divides $P(x)$. Thus we can write

$$2P(x) = (x-b)^{2^n} + x^{2^n} + b^{2^n} = 2(x^2 - bx + b^2)Q(x)$$

for some polynomial $Q(x)$ with integer coefficients.
Hence $2(a^2 - ab + b^2)$ divides $(a-b)^{2^n} + a^{2^n} + b^{2^n}$. ∎

Second Solution. Let

$$P(x) = (x-a+b)(x+a)(x-b) = x^3 - (a^2+b^2-ab)x + ab(a-b).$$

Define $S_n = \frac{1}{2}\left((a-b)^n + (-a)^n + b^n\right)$. Then $S_1 = 0$, $S_2 = a^2+b^2-ab$, and $S_3 = \frac{3ab(b-a)}{2}$ are all integers (in the case of S_3, since at least one of a, b, and $b-a$ must be even). Since Newton's Identities give

$$S_{n+3} = (a^2+b^2-ab)S_{n+1} - ab(a-b)S_n,$$

we see that S_n is an integer for all $n \geq 1$. We also see that

$$S_{n+3} \equiv -ab(a-b)S_n \pmod{a^2+b^2-ab}.$$

Since $S_1 \equiv S_2 \equiv 0 \pmod{a^2+b^2-ab}$, we conclude that

$$S_n \equiv 0 \pmod{a^2+b^2-ab}$$

for all n which are not multiples of 3. In particular,

$$S_{2^n} \equiv 0 \pmod{a^2+b^2-ab},$$

which gives the desired result. ■

Problem 8.17. Let $P(x)$ be a polynomial with integer coefficients and let ω be a complex number such that $|\omega| = 1$. Let $P(\omega) = c$, where c is a real number. Prove that there exists a polynomial $Q(x)$ with integer coefficients such that

$$c = Q\left(\omega + \frac{1}{\omega}\right).$$

Solution. Let $P(x) = a_d x^d + \ldots + a_0$. Note that $P(\overline{\omega}) = \overline{P(\omega)} = \overline{c} = c$. Since $\overline{\omega} = \frac{1}{\omega}$, we get $P(\overline{\omega}) = a_d\omega^{-d} + \ldots + a_0$. Thus

$$\begin{aligned} c &= \frac{\omega P(\omega) - \overline{\omega}P(\overline{\omega})}{\omega - \overline{\omega}} = \sum_{k=0}^{d} a_k \cdot \frac{\omega^{k+1} - \omega^{-k-1}}{\omega - \omega^{-1}} \\ &= \sum_{k=0}^{d} a_k \left(\omega^k + \omega^{k-2} + \ldots + \omega^{-k}\right). \end{aligned}$$

Recall from Example 1.7, that there are polynomials $T_k(x)$ with integer coefficients such that

$$T_k\left(x + \frac{1}{x}\right) = x^k + \frac{1}{x^k}.$$

Thus we find that

$$Q(x) = \sum_{k=0}^{d} a_k \left(T_k(x) + T_{k-2}(x) + \ldots\right)$$

is a polynomial such that $c = Q\left(\omega + \frac{1}{\omega}\right)$. ■

Problem 8.18. Let z be a complex number of modulus 1. Prove that there exists a polynomial of degree d such that all of its coefficients are $+1$ or -1 and $|P(z)| \leq 4$.

Komal

First Solution. We must prove that there are $\varepsilon_i = \pm 1$ such that

$$\left|\sum_{i=0}^{d} \varepsilon_i z^i\right| \leq 4.$$

This will follow quickly from the following lemma.

Lemma. Let $z_1, \ldots, z_d$ be complex numbers lying on or inside the unit circle. Then there are $\varepsilon_i = \pm 1$ such that

$$\left|\sum_{i=0}^{d} \varepsilon_i z_i\right| \leq \sqrt{2}.$$

Proof. We prove this by induction on d. For $d = 1$, notice that

$$|z_1 - z_0|^2 + |z_1 + z_0|^2 = 2|z_1|^2 + 2|z_0|^2 \leq 4.$$

So either $|z_1 - z_0| \leq \sqrt{2}$ or $|z_1 + z_0| \leq \sqrt{2}$.

Now assume $d \geq 2$. Look at all the lines Oz_i through the origin and one of the $d+1$ points $z_0, \ldots, z_d$. Since $d+1 \geq 3$, there are two of these lines that make an angle of at most $\frac{\pi}{3}$ at O. Assume without loss that these are the lines Oz_{d-1} and Oz_d. Replacing z_d with $-z_d$ if necessary, we may further assume that the angle $\angle z_{d-1}Oz_d$ is at most $\frac{\pi}{3}$. Now, consider the triangle with vertices O, z_{d-1}, z_d. Since $\angle z_{d-1}Oz_d$ cannot be the largest angle of this triangle, we have

$$|z_{d-1} - z_d| \leq \max\{|z_{d-1}|, |z_d|\} \leq 1.$$

Thus $z_0, \ldots, z_{d-2}, z_{d-1} - z_d$ are d points inside or on the unit circle. Hence by the inductive hypothesis there are $\varepsilon_i = \pm 1$ such that

$$\left|\sum_{i=1}^{d-2} \varepsilon_i z_i + \varepsilon_{d-1} z_{d-1} - \varepsilon_{d-1} z_d\right| \leq \sqrt{2},$$

and defining $\varepsilon_d = -\varepsilon_{d-1}$ completes the induction. □

Appling the Lemma to the numbers $1, z, \ldots, z^d$, shows there are $\varepsilon_i = \pm 1$ such that

$$\left|\sum_{i=0}^{d} \varepsilon_i z^i\right| \leq \sqrt{2}.$$

Second Solution. Since we can replace $P(z)$ by $P(-z)$, we may assume that $\operatorname{Re}(z) \leq 0$. Consider $P(z) = 1 + z + \ldots + z^d$. Since

$$|1 - z|^2 = 1 + |z|^2 - 2\operatorname{Re}(z) \geq 1 + |z|^2 = 2,$$

we get

$$|P(z)| = \left|\frac{1 - z^{d+1}}{1 - z}\right| \leq \frac{|1 - z^{d+1}|}{\sqrt{2}} \leq \frac{1 + |z|^{d+1}}{\sqrt{2}} = \sqrt{2}.$$

Problem 8.19. Let r be the real root of the polynomial $x^3 - x^2 - 1$. A real number a is *good* if it is equal to the sum of the elements of a finite subset of the set $\{1, r, r^2, \ldots\}$. Is it true that for each $\varepsilon > 0$ there are two good numbers a and b such that $0 < a - b < \varepsilon$?

Solution. The answer is no. Let $P(x) = x^3 - x^2 - 1$. For $x \leq 1$, we have $P(x) = -x^2(1 - x) - 1 \leq -1$, hence $P(x)$ has no roots in this range. For $x > 1$, $x^2(x-1)$ is an increasing function of x, hence $P(x)$ has exactly one real root r which satisfies $r > 1$ (as the problem statement implies). The other two roots of $P(x)$ are nonreal and hence conjugate. Let us denote them by s and t. Since $|s| = |t|$ and Vieta's Formulas give $rst = 1$, we conclude that

$$|s|^2 = |t|^2 = \frac{1}{|r|} < 1.$$

Thus $|s| = |t| < 1$.

On the other hand, the polynomial $P(x)$ is irreducible over $\mathbb{Z}[x]$. Since if a cubic polynomial reduces it must have a linear factor, and hence a rational root. By the rational root theorem, we only need to check ± 1, and it is easy to see these are not roots of $P(x)$ (as the above argument also shows).

Assume that there are good numbers a, b with $0 < a - b < \varepsilon$. A good number is just a number which is the value $g(r)$ of a polynomial $g(x)$ with coefficients 0 and 1. Hence we can write $a = g_1(r)$ and $b = g_2(r)$ for two such polynomials. Then $f(x) = g_1(x) - g_2(x)$ is a polynomial with coefficients ± 1, 0 such that $0 < f(r) < \varepsilon$.

Look at the polynomial $F(r, s, t) = f(r) \cdot f(s) \cdot f(t)$. This is a symmetric polynomial in the variables r, s, t with integer coefficients. Hence it can be written as a polynomial with integer coefficients in the elementary symmetric polynomials $\sigma_1 = r + s + t$, $\sigma_2 = rs + st + tr$, and $\sigma_3 = rst$. If we set r, s, t to be the roots of $P(x)$, then these three quantities are integers ($\sigma_1 = 1$, $\sigma_2 = 0$, and $\sigma_3 = 1$). Thus $F(r, s, t)$ is an integer. Furthermore since $f(r) > 0$ is nonzero, and $P(x)$ is irreducible, we have that $f(s)$, $f(t)$ are nonzero, hence $F(r, s, t) \neq 0$. Since $F(r, s, t)$ is integer, we deduce that

$$|F(r, s, t)| = |f(r)| \cdot |f(s)| \cdot |f(t)| \geq 1.$$

Hence

$$|f(r)| \geq \frac{1}{|f(s)| \cdot |f(t)|}.$$

Note that,

$$|f(s)| \leq 1 + |s| + |s|^2 + \ldots = \frac{1}{1 - |s|},$$

and analogously, $|f(t)| \le \frac{1}{1-|t|}$. Hence

$$\varepsilon > |f(r)| \ge (1-|t|)\cdot(1-|s|).$$

Thus if ε is less than $(1-|t|)\cdot(1-|s|)$ such good numbers do not exist. ■

Problem 8.20. Let $C \in (0,1)$ and let d be a positive integer. Prove that the moduli of all the roots of polynomial

$$P(x) = \sum_{k=0}^{d} \binom{d}{k} C^{k(d-k)} x^k \text{ are equal to 1.}$$

Chinese Team Selection Test 2018

Solution. We prove the statement by induction on d. Define

$$P_d(x) = \sum_{k=0}^{d} \binom{d}{k} C^{k(d-k)} x^k.$$

Then $P_1(x) = x+1$. Assume that the statement holds for all positive integers less than or equal to d. That is, $P_d(x) = (x-z_1)\cdot\ldots\cdot(x-z_d)$, with $|z_i| = 1$, $i = 1, 2, \ldots, d$. Now, we can easily deduce that

$$\begin{aligned}
P_{d+1}(x) &= \sum_{k=0}^{d+1} \binom{d+1}{k} C^{k(d+1-k)} x^k \\
&= \sum_{k=0}^{d+1} \left(\binom{d}{k-1} + \binom{d}{k} \right) C^{k(d+1-k)} x^k \\
&= \sum_{k=0}^{d} \binom{d}{k} C^{(k+1)(d-k)} x^{k+1} + \sum_{k=0}^{d} \binom{d}{k} C^{k(d+1-k)} x^k \\
&= xC^d P_d\left(\frac{x}{C}\right) + P_d(Cx).
\end{aligned}$$

Now, assume that there is a complex number $z \neq 0$ such that $P_{d+1}(z) = 0$. Then

$$zC^d\left(\frac{z}{C} - z_1\right)\cdot\ldots\cdot\left(\frac{z}{C} - z_d\right) + (Cz - z_1)\cdot\ldots\cdot(Cz - z_d) = 0.$$

Therefore

$$\begin{aligned}
\left|zC^d\left(\frac{z}{C} - z_1\right)\cdot\ldots\cdot\left(\frac{z}{C} - z_d\right)\right| &= |z|\left|\left(\frac{z}{C} - z_1\right)\cdot\ldots\cdot\left(\frac{z}{C} - z_d\right)\right| \\
&= |z|\cdot|(z - Cz_1)\cdot\ldots\cdot(z - Cz_d)| \\
&= |(Cz - z_1)\ldots(Cz - z_d)|.
\end{aligned}$$

Since $|z_i| = 1$, we can easily find that

$$\begin{aligned}
|z - Cz_i|^2 - |Cz - z_i|^2 &= (z - Cz_i)(\overline{z} - C\overline{z_i}) - (Cz - z_i)(C\overline{z} - \overline{z_i}) \\
&= (1 - C^2)(|z|^2 - 1).
\end{aligned}$$

So for $|z| > 1$, we have $|z - Cz_i| > |Cz - z_i|$. Therefore

$$\begin{aligned}
|z|\cdot|(z - Cz_1)\cdot\ldots\cdot(z - Cz_d)| &> |(z - Cz_1)\cdot\ldots\cdot(z - Cz_d)| \\
&> |(Cz - z_1)\cdot\ldots\cdot(Cz - z_d)|.
\end{aligned}$$

Furthermore, for $|z| < 1$ we have $|z - Cz_i| < |Cz - z_i|$. Therefore

$$\begin{aligned}
|z|\cdot|(z - Cz_1)\cdot\ldots\cdot(z - Cz_d)| &< |(z - Cz_1)\cdot\ldots\cdot(z - Cz_d)| \\
&< |(Cz - z_1)\cdot\ldots\cdot(Cz - z_d)|.
\end{aligned}$$

Therefore $|z| = 1$. ■

Problem 8.21. Find all nonconstant polynomials $P(z)$ with complex coefficients for which all complex roots of $P(z)$ and $P(z) - 1$ have absolute value 1.

USA Team Selection Test 2021

Solution. Let $d = \deg P(z)$ and $P(z) = C(z - r_1)\cdot\ldots\cdot(z - r_d)$, where $|r_1| = 1$ and C is an arbitrary complex number. Let z_0 be any root of the polynomial[1] $P(z) - 1$. It follows that $|z_0| = 1$ and $P(z_0) = 1$, that is,

$$C(z_0 - r_1)\cdot\ldots\cdot(z_0 - r_d) = 1.$$

[1]The polynomial $P(z) - 1$ only has simple roots. To see this note that since the roots of $P(z)$ lie on the unit circle, according to Gauss-Lucas Theorem, roots of $P'(z)$ lie within the convex hull of roots of $P(z)$, that is inside or on the unit circle. Notice that if some roots of $P'(z)$ lie on the unit circle, they must be in common with roots of $P(z)$, contradiction.

Taking the conjugate of both sides, it follows that

$$\overline{C}\,(\overline{z_0}-\overline{r_1})\ldots(\overline{z_0}-\overline{r_d})=1.$$

Since $\overline{r_i}=\frac{1}{r_i}$ and $\overline{z_0}=\frac{1}{z_0}$, this becomes

$$\frac{(-1)^d\overline{C}}{r_1\ldots r_d z_0^d}\underbrace{(z_0-r_1)\ldots(z_0-r_d)}_{C^{-1}}=1.$$

It follows that

$$z_0^d=\frac{(-1)^d\overline{C}}{Cr_1\ldots r_d}=C_1.$$

Hence any root of $P(z)-1$ is a root of z^d-C_1. Thus $P(z)-1$ divides z^d-C_1, and comparing degrees and leading coefficients, we get $P(z)-1=C\left(z^d-C_1\right)$. Hence we can write $P(z)=\alpha z^d+\beta$ for some complex numbers α, β. The condition that all roots of $P(z)$ have modulus 1 says $|\alpha|=|\beta|$ and the condition that all roots of $P(z)-1$ have modulus 1 says $|\alpha|=|\beta-1|$. Hence $|\beta|=|\beta-1|$, which is equivalent to $\mathrm{Re}(\beta)=\frac{1}{2}$. Thus all such polynomials are of the form

$$P(z)=\alpha z^d+\beta$$

with $|\alpha|=|\beta|$ and $\mathrm{Re}(\beta)=\frac{1}{2}$. ■

Problem 8.22. Let $D=\{z\in\mathbb{C}:\mathrm{Re}(z)<1\}$. Let $d\geq 1$ be a positive integer and let $a_0,\ldots,a_d$ be real numbers such that $0<a_0\leq a_1\leq\ldots\leq a_{d-1}$ and $a_{d-1}>a_d>0$. Prove that all the roots of $P(x)=a_dx^d+a_{d-1}x^{d-1}+\ldots+a_0$ lie in D.

Solution. Observe that

$$(x-1)P(x)=a_dx^{d+1}+(a_{d-1}-a_d)x^d-\Big((a_{d-1}-a_{d-2})x^{d-1}+\ldots$$
$$+(a_1-a_0)x+a_0\Big)=a_dx^{d+1}+(a_{d-1}-a_d)x^d-Q(x).$$

Suppose on the contrary, that $P(x)$ has a root r with $\mathrm{Re}\,r\geq 1$. Then

$$\left|a_dr^{d+1}+(a_{d-1}-a_d)r^d\right|=|ra_d+a_{d-1}-a_d|\left|r^d\right|\geq|a_d+a_{d-1}-a_d|\left|r^d\right|$$
$$=a_{d-1}\left|r^d\right|.$$

Furthermore, since $|r|\geq\mathrm{Re}\,r\geq 1$,

$$|Q(r)|\leq|a_{d-1}-a_{d-2}|\,|r|^{d-1}+\ldots+|a_1-a_0|\,|r|+a_0$$
$$\leq|r|^{d-1}(a_{d-1}-a_{d-2}+\ldots+a_1-a_0+a_0)|r|^{d-1}$$
$$=a_{d-1}|r|^{d-1}.$$

Combining these two inequalities, it follows that

$$|(r-1)P(r)|\geq\left|a_dr^{d+1}+(a_{d-1}-a_d)r^d\right|-|Q(r)|\geq a_{d-1}(|r|-1)\left|r^d\right|\geq 0.$$

Since $P(r)=0$, we must have equality throughout, hence we must have $r=1$. But clearly $P(1)>0$. This is a contradiction and completes our proof. ■

Problem 8.23. The polynomial

$$P(x)=rx^3+qx^2+px+1$$

has positive real coefficients and only one real root. Define the sequence $a_1=1$, $a_2=-p$, $a_3=p^2-q$ and for each $n\geq 1$,

$$a_{n+3}+pa_{n+2}+qa_{n+1}+ra_n=0.$$

Prove that the sequence has infinitely many terms which are negative real numbers.

Vietnamese Team Selection Test 2009

Solution. Let

$$Q(x)=x^3P\left(\frac{1}{x}\right)=x^3+px^2+qx+r.$$

The roots of $Q(x)$ are the reciprocals of the roots of $P(x)$, hence only one of them is real call it α, and the other two are complex conjugate call them β and γ. Look at

$$T_n = \alpha^n(\beta-\gamma) + \beta^n(\gamma-\alpha) + \gamma^n(\alpha-\beta).$$

Then we easily see that $T_0 = T_1 = 0$ and a short computation gives

$$T_2 = -(\alpha-\beta)(\beta-\gamma)(\gamma-\alpha).$$

Furthermore, Newton's Identities imply that

$$T_{n+3} + pT_{n+2} + qT_{n+1} + rT_n = 0.$$

From this we compute that $T_3 = -pT_2$ and $T_4 = (p^2-q)T_2$. Comparing this to the definition of a_n, we see that

$$a_n = \frac{T_{n+1}}{T_2} = \frac{\alpha^{n+1}}{(\alpha-\beta)(\alpha-\gamma)} + \frac{\beta^{n+1}}{(\beta-\gamma)(\beta-\alpha)} + \frac{\gamma^{n+1}}{(\gamma-\alpha)(\gamma-\beta)}.$$

Since $p, q, r > 0$, the real root α of $Q(x)$ must be negative and therefore the first term in this formula, which equals $\dfrac{\alpha^{n+1}}{|\alpha-\beta|^2}$, is negative for all even n. The remaining two terms are complex conjugate. If we define

$$C = \frac{\beta}{(\beta-\gamma)(\beta-\alpha)},$$

then their sum is just $2\,\mathrm{Re}(C\beta^n)$. Now write

$$\beta^2 = r(\cos\theta + i\sin\theta) \text{ and}$$
$$C = s(\cos\phi + i\sin\phi)$$

for some $r, s > 0$ and $-\pi < \theta, \phi < \pi$. Note that since β is not real, $\theta \neq 0$, and since we could always interchange γ and β, we may assume $0 < \theta < \pi$. Then

$$2\,\mathrm{Re}(C\beta^{2m}) = 2sr^m\cos(m\theta+\phi).$$

As we increase t, the angle $t\theta+\phi$ will tend to ∞, which means it will pass through infinitely many intervals $((2k+1/2)\pi, (2k+3/2)\pi)$. Since $\theta < \pi$ and these intervals have width π, there will always be at least one integer choice of t that lands in each of these intervals. Thus there will be infinitely many integers m such that $m\theta+\phi \in ((2k+1/2)\pi, (2k+3/2)\pi)$ for some integer k. But any such m will have $\cos(m\theta+\phi) < 0$. Hence $a_{2m} < 0$ for these m. ■

Problem 8.24. Let $P(x)$ and $Q(x)$ be monic polynomials with complex coefficients such that

$$P(x) - Q(y) = \prod_{j=1}^{n}(a_jx + b_jy + c_j)$$

for some nonzero complex numbers a_j, b_j, c_j. Prove that there are complex numbers a, b, c such that

$$P(x) = (x+a)^n + c, \quad Q(x) = (x+b)^n + c.$$

Solution. It is easy to deduce that $\deg P(x) = \deg Q(x) = n$. Examining the coefficients of x^n and y^n on both sides, we easily find that

$$a_1 \cdot \ldots \cdot a_n = 1, \quad b_1 \cdot \ldots \cdot b_n = -1.$$

Thus if we define $d_j = -\frac{b_j}{a_j}$ and $e_j = \frac{c_j}{a_j}$, we can rewrite the original equality as

$$P(x) - Q(y) = \prod_{j=1}^{n}(x - d_jy + e_j).$$

Now, checking the homogeneous parts of degree n on both sides, we get

$$\prod_{j=1}^{n}(x - d_jy) = x^n - y^n = \prod_{j=1}^{n}(x - \omega^j y),$$

where ω is a primitive n-th root of unity. Thus by reordering the factors, we can assume that $d_j = \omega^j$ for $j = 1, \ldots, n$. Let a and b be the solutions to $a - b = e_n$ and $a - \omega b = e_1$, or equivalently,

$$a = \frac{e_1 - \omega e_n}{1-\omega}, \quad b = \frac{e_1 - e_n}{1-\omega},$$

and define $F(x) = P(x-a)$ and $G(x) = Q(x-b)$. Then we find that

$$F(x) - G(y) = (x-y)(x-\omega y)\prod_{j=2}^{n-1}(x-\omega^j y + f_j),$$

where $f_j = e_j - a + \omega^j b$, $2 \le j \le n-1$. Now, for $x = y$, $x = \omega y$, we get

$$G(y) = F(y) = F(\omega y)$$

for each y. Therefore if r is any root of $F(x)$, we find that ωr, $\omega^2 r$, ..., $\omega^{n-1}r$ are all the roots of $F(x)$. Hence

$$F(x) = G(x) = (x-r)(x-\omega r)\cdot\ldots\cdot(x-\omega^{n-1}r) = x^n - r^n.$$

So $P(x) = F(x+a) = (x+a)^n - r^n$ and $Q(x) = G(x+b) = (x+b)^n - r^n$. ■

Problem 8.25. Find all positive integers n such that the polynomial

$$a^n(b-c) + b^n(c-a) + c^n(a-b)$$

has $a^2+b^2+c^2+ab+ac+bc$ as factor.

American Mathematical Monthly, Problem 10306

Solution. We specialize by putting $b = 2$, $c = 1$. We then ask whether the polynomial $P(a) = a^n - (2^n-1)a + 2^n - 2$ can have $Q(a) = a^2 + 3a + 7$ as a factor. The roots of Q are $\frac{-3\pm i\sqrt{19}}{2}$, with the absolute value of $\sqrt{7}$. Assume now that $n \ge 5$ and let r be one of the roots of Q. Then

$$|P(r)| = |r^n - (2^n-1)r + 2^n - 2| \ge |r|^n - 2^n(1+|r|) - 5 > 7^{\frac{n}{2}} - 4\cdot 2^n > 0.$$

Hence $Q(x)$ cannot divide $P(x)$ for $n \ge 5$. It is easy to check that for $n = 2, 3$, $P(r) \ne 0$. It remains to check the cases $n = 1, 4$, which are the solutions. For $n = 4$, we have

$$a^4(b-c)+b^4(c-a)+c^4(a-b) = (a^2+b^2+c^2+ab+ac+bc)(a-b)(b-c)(c-a).$$ ■

Problem 8.26. Let P and Q be two nonzero polynomials with complex coefficients. Prove that P and Q have the same roots with the same multiplicity for correspondent roots if and only if the function $f : \mathbb{C} \to \mathbb{R}$ defined by $f(x) = |P(x)| - |Q(x)|$ has constant sign on $\mathbb{C}$ (it can also vanish).

Marcel Ţena - Romanian Mathematical Olympiad 1978

Solution. Assume that the nonzero polynomials $P(x), Q(x) \in \mathbb{C}[x]$ have the same roots with the same multiplicity for correspondent roots. Then there exists $\lambda \in \mathbb{C}^*$ such that $P(x) = \lambda Q(x)$. Therefore $f(x) = |Q(x)|(|\lambda| - 1)$, which has constant sign on $\mathbb{C}$.
Now we prove the converse statement, i.e., we prove that if the function $f : \mathbb{C} \to \mathbb{R}$ defined by $f(x) = |P(x)| - |Q(x)|$ has constant sign on $\mathbb{C}$, then the polynomials P and Q have the same roots with the same multiplicity for correspondent roots. Assume without loss of generality that $f(x) \ge 0$ for all $x \in \mathbb{C}$. Then

$$|P(x)| \ge |Q(x)| \quad \forall x \in \mathbb{C}. \tag{8.3}$$

If x_0 is a root of P, then from (8.3) we get $|Q(x_0)| \le 0$, which gives $Q(x_0) = 0$. Then x_0 is a root of Q. This means that each root of P is also a root of Q. Let $x_1, x_2, \ldots, x_k$ be the distinct roots of Q with multiplicities $q_1, q_2, \ldots, q_k$, respectively ($q_i \ge 1$, $i = 1, 2, \ldots, k$). Then P has roots $x_1, x_2, \ldots, x_k$ with multiplicities $p_1, p_2, \ldots, p_k$, respectively ($p_i \ge 0$, $i = 1, 2, \ldots, k$), where we take $p_i = 0$ if x_i is not a root of polynomial P. We have

$$P(x) = a(x-x_1)^{p_1}(x-x_2)^{p_2}\cdot\ldots\cdot(x-x_k)^{p_k},$$

$$Q(x) = b(x-x_1)^{q_1}(x-x_2)^{q_2}\cdot\ldots\cdot(x-x_k)^{q_k},$$

where $a, b \in \mathbb{C}^*$. We will prove that $p_1 = q_1$, $p_2 = q_2$, ..., $p_k = q_k$. Inequality (8.3) can be written as

$$|a||x-x_1|^{p_1}\cdot\ldots\cdot|x-x_k|^{p_k} \ge |b||x-x_1|^{q_1}\cdot\ldots\cdot|x-x_k|^{q_k} \quad \forall x \in \mathbb{C}. \tag{8.4}$$

We first prove that $p_i \le q_i$ for all $i = 1, 2, \ldots, k$. We prove that $p_1 \le q_1$ since the other inequalities can be proved similarly. Assume on the contrary, that $p_1 > q_1$. If $x \in \mathbb{C} \setminus \{x_1, x_2, \ldots, x_k\}$, inequality (8.4) becomes

$$|a||x-x_1|^{p_1-q_1}|x-x_2|^{p_2}\cdot\ldots\cdot|x-x_k|^{p_k} \ge |b||x-x_2|^{q_2}\cdot\ldots\cdot|x-x_k|^{q_k}.$$

As $x \to x_1$ (for example take $x = x_1 + \alpha$, where $\alpha \in \mathbb{R}$ and $\alpha \to 0$), we get

$$|b||x_1 - x_2|^{q_2} \cdot \ldots \cdot |x_1 - x_k|^{q_k} \leq 0,$$

contradiction. Therefore $p_i \leq q_i$ for all $i = 1, 2, \ldots, k$. We now prove that it is not possible that one of these inequalities is strict. So assume without loss of generality that $p_1 < q_1$. If $x \in \mathbb{C} \setminus \{x_1, x_2, \ldots, x_k\}$, inequality (8.4) becomes

$$|a| \geq |b||x - x_1|^{q_1 - p_1}|x - x_2|^{q_2 - p_2} \cdot \ldots \cdot |x - x_k|^{q_k - p_k}.$$

As $|x - x_1| \to \infty$ (for example take $x = x_1 + \beta$, where $\beta \in \mathbb{R}$ and $\beta \to \infty$), we get that the right-hand side of this inequality goes to infinity, while the left-hand side is a constant, a contradiction. We conclude that $p_i = q_i$ for all $i = 1, 2, \ldots, k$. ■

Problem 8.27. Let $f = x^{2n} + a_{2n-1}x^{2n-1} + \ldots + a_1 x + 1 \in \mathbb{C}[x]$ be a polynomial such that $a_{2n-k} = a_k \ \forall k \in \{1, 2, \ldots, n-1\}$ and

$$|a_1| + |a_2| + \ldots + |a_{2n-1}| < 2.$$

If α is a root of f, prove that $\left|\alpha + \frac{1}{\alpha}\right| < 2$.

Alin Pop - Gazeta Matematică B 12/2003, *Problem* C:2694

Solution. Let $z \in \mathbb{C}^*$ such that $\left|z + \frac{1}{z}\right| \geq 2$. We will prove by induction on n that

$$\left|z^{n+1} + \frac{1}{z^{n+1}}\right| \geq \left|z^n + \frac{1}{z^n}\right| \qquad \forall n \geq 0.$$

The base case $n = 0$ is just the hypothesis. For the inductive step, assume that

$$\left|z^n + \frac{1}{z^n}\right| \geq \left|z^{n-1} + \frac{1}{z^{n-1}}\right|.$$

We have

$$\begin{aligned}
\left|z^{n+1} + \frac{1}{z^{n+1}}\right| &= \left|\left(z + \frac{1}{z}\right)\left(z^n + \frac{1}{z^n}\right) - \left(z^{n-1} + \frac{1}{z^{n-1}}\right)\right| \\
&\geq \left|z + \frac{1}{z}\right|\left|z^n + \frac{1}{z^n}\right| - \left|z^{n-1} + \frac{1}{z^{n-1}}\right| \\
&\geq \left|z^n + \frac{1}{z^n}\right|\left(\left|z + \frac{1}{z}\right| - 1\right) \\
&\geq \left|z^n + \frac{1}{z^n}\right|,
\end{aligned}$$

so the statement is true for all $n \geq 1$. Let $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$ and

$$\left|\alpha + \frac{1}{\alpha}\right| \geq 2.$$

We have

$$\left|a_n + a_{n+1}\alpha + a_{n-1}\frac{1}{\alpha} + \ldots + a_{2n-1}\alpha^{n-1} + a_1\frac{1}{\alpha^{n-1}}\right| = \left|\alpha^n + \frac{1}{\alpha^n}\right|,$$

so

$$|a_n| + |a_{n+1}| \cdot \left|\alpha + \frac{1}{\alpha}\right| + \ldots + |a_{2n-1}| \cdot \left|\alpha^{n-1} + \frac{1}{\alpha^{n-1}}\right| \geq \left|\alpha^n + \frac{1}{\alpha^n}\right|.$$

It follows that

$$|a_n| + \left|\alpha^n + \frac{1}{\alpha^n}\right|(|a_{n+1}| + |a_{n+2}| + \ldots + |a_{2n-1}|) \geq \left|\alpha^n + \frac{1}{\alpha^n}\right|,$$

which gives

$$\begin{aligned}
|a_n| &\geq \left|\alpha^n + \frac{1}{\alpha^n}\right|(1 - |a_{n+1}| - |a_{n+2}| - \ldots - |a_{2n-1}|) \\
&\geq 2(1 - |a_{n+1}| - |a_{n+2}| - \ldots - |a_{2n-1}|),
\end{aligned}$$

so $|a_1| + \ldots + |a_{n-1}| + |a_n| + |a_{n+1}| + \ldots + |a_{2n-1}| \geq 2$, a contradiction. ■

Problem 8.28. Let $a, b, c, d > 0$. Prove that

$$\sqrt{\left(a+\sqrt{\frac{bcd}{a}}\right)\left(b+\sqrt{\frac{acd}{b}}\right)\left(c+\sqrt{\frac{abd}{c}}\right)\left(d+\sqrt{\frac{abc}{d}}\right)}+2\sqrt{abcd}$$
$$\geq ab+bc+cd+da+ac+bd.$$

Solution. Let $P(x)=(x^2+a^2)(x^2+b^2)(x^2+c^2)(x^2+d^2)$. Since

$$P(x)=|(x+ai)(x+bi)(x+ci)(x+di)|^2,$$

and

$$(x+ai)(x+bi)(x+ci)(x+di)$$
$$=x^4+i\left(\sum a\right)x^3-\left(\sum ab\right)x^2-i\left(\sum abc\right)x+abcd,$$

we have

$$P(x)=\left(x^4-\left(\sum ab\right)x^2+abcd\right)^2+\left(\left(\sum a\right)x^3-\left(\sum abc\right)x\right)^2.$$

Therefore

$$P(x)\geq\left(x^4-\left(\sum ab\right)x^2+abcd\right)^2.$$

Plugging in $x=\sqrt[4]{abcd}$, we get

$$(a^2+\sqrt{abcd})(b^2+\sqrt{abcd})(c^2+\sqrt{abcd})(d^2+\sqrt{abcd})\geq\left(2abcd-\sqrt{abcd}\sum ab\right)^2.$$

Hence

$$\sqrt{(a^2+\sqrt{abcd})(b^2+\sqrt{abcd})(c^2+\sqrt{abcd})(d^2+\sqrt{abcd})}\geq\sqrt{abcd}\sum ab-2abcd,$$

which rearranges to the desired inequality. ∎

Problem 8.29. Find all positive integers n such that there are n points $P_1,\ldots,P_n$ on the unit circle satisfying the following property: for any point M on the unit circle, $\sum_{i=1}^{n} MP_i^k$ is a fixed value for

(i) $k=2018$;

(ii) $k=2019$.

Solution. (i) Let $m=1009$, and lay down complex coordinates. Let the affixes of the points $M, P_1,\ldots,P_n$ be $z,\omega_1,\ldots,\omega_n$. Since these points are on the unit circle their affixes all have modulus 1. Then

$$MP_i^2=|z-\omega_i|^2=\left|\frac{z}{\omega_i}-1\right|^2=2-\frac{z}{\omega_i}-\frac{\omega_i}{z}.$$

Thus

$$MP_i^{2m}=(2-\frac{z}{\omega_i}-\frac{\omega_i}{z})^m.$$

Let

$$f(x)=\left(2-x-\frac{1}{x}\right)^m=\frac{(-1)^m(x-1)^{2m}}{x^m}=\sum_{k=-m}^{m}a_kx^k,$$

where

$$a_k=\binom{2m}{m+k},\ k=-m,\ldots,m.$$

Let

$$S_k=\sum_{i=1}^{n}\omega_i^k$$

and

$$F(z)=\sum_{i=1}^{n}f\left(\frac{z}{\omega_i}\right)=\sum_{i=1}^{n}\sum_{k=-m}^{m}a_kz^k\omega_i^{-k}.$$

This yields

$$F(z)=\sum_{k=-m}^{m}a_k\left(\sum_{i=1}^{n}\omega_i^{-k}\right)z^k=\sum_{k=-m}^{m}a_kS_{-k}z^k.$$

Since $F(z)=C$ is constant, we can write that

$$z^m(F(z)-C)=\left(\left(\sum_{k=-m}^{m}a_kS_{-k}z^k\right)-C\right)z^m.$$

Therefore $a_k S_{-k} = 0$ for all $k = \pm 1, \ldots, \pm m$. That is, $S_1 = \ldots = S_m = 0$. If $n \leq m$, then by Newton's Identities we can find that $\omega_i = 0$ for all $i = 1, \ldots, m$. Therefore $n \geq m+1$. Now, putting $\omega_l = \cos\frac{2\pi l}{n} + i\sin\frac{2\pi l}{n}$, we have $S_{-k} = 0$ for all $k = \pm 1, \ldots, \pm m$, but $S_0 \neq 0$ and $C = na_0 = n\binom{2m}{m}$. Therefore the integers n for which such points exist are exactly those with $n \geq 1010$.

(ii) Let $C = \{z \in \mathbb{C} : |z| = 1\}$ be the unit circle and let

$$A = \{z \in C : 2\varepsilon < \arg(z) < 2\pi\} \text{ for some } 0 < \varepsilon < \frac{\pi}{n}.$$

We can write $P_l = \omega_l^2$ with $\omega_l \in A_1 = \{z \in C : \varepsilon < \arg(z) < \pi\}$. Define

$$B = C - A = \{z \in C : 0 \leq \arg(z) \leq 2\varepsilon\}$$

and

$$B_1 = C - A_1 = \{z \in C : 0 \leq \arg(z) \leq \varepsilon\}.$$

Take $z \in B_1$. Then $z^2 \in B$. Take z^2 as M. Hence

$$|MP_l|^2 = |z^2 - \omega_l^2| = 2 - \frac{z^2}{\omega_l^2} - \frac{\omega_l^2}{z^2} = \left(\left(\frac{z}{\omega_l} - \frac{\omega_l}{z}\right)i\right)^2.$$

We have that $0 \leq \arg(z) \leq \varepsilon < \arg(\omega_l) < \pi$. Since $\frac{z}{\omega_l}, \frac{\omega_l}{z}$ lie on the unit circle, then they are conjugate. Hence $\operatorname{Re}\left(\frac{z}{\omega_l} - \frac{\omega_l}{z}\right) = 0$. Thus

$$|MP_l| = i\left(\frac{z}{\omega_l} - \frac{\omega_l}{z}\right).$$

That is,

$$|MP_l|^{2m+1} = \left(\frac{z}{\omega_l} - \frac{\omega_l}{z}\right)^{2m+1} i^{2m+1}.$$

Define

$$g(x) = i^{2m+1}\left(x - \frac{1}{x}\right)^{2m+1} = i^{2m+1}\frac{(x^2-1)^{2m+1}}{x^{2m+1}} = \sum_{k=0}^{2m+1} b_k x^{2k-2m-1}$$

with $b_k = i^{2m+1}(-1)^{k+1}\binom{2m+1}{k}$. Thus

$$G(z) = \sum_{i=1}^{n} g\left(\frac{z}{\omega_l}\right) = \sum_{i=1}^{n}\sum_{k=0}^{2m+1} b_k z^{2k-2m-1}\omega_i^{2m+1-2k}$$
$$= \sum_{k=0}^{2m+1} b_k S_{2m+1-2k} z^{2k-2m-1}.$$

Since $G(z) = K$ is constant, we have

$$z^{2m+1}(G(z) - K) = \sum_{k=0}^{2m+1} b_k S_{2m+1-2k} z^{2k} - Kz^{2m+1}.$$

Considering the coefficient of z^{2m}, we find that $S_1 = 0$. Therefore

$$\sum_{i=1}^{n} \operatorname{Re}(\omega_i) = 0.$$

But, by the choice of ω_i this quantity is positive. Thus in this case, there is no n for which such points exist. ∎

Problem 8.30. Polynomials $u_i(x) = a_i x + b_i$ $(a_i, b_i \in \mathbb{R},\ i = 1, 2, 3)$ satisfy

$$(u_1(x))^n + (u_2(x))^n = (u_3(x))^n$$

for some natural number $n > 2$. Prove that there exist real numbers A, B, c_1, c_2, c_3 such that $u_i(x) = c_i(Ax + B)$ for $i = 1, 2, 3$.

Polish Mathematical Olympiad 1972

Solution. If $a_1 = a_2 = 0$, then the polynomials u_1 and u_2 are constant. Therefore the polynomial u_3 is also constant, i.e., $a_3 = 0$. In this case, it's enough to take $c_i = b_i$ for $i = 1, 2, 3$, $A = 0$ and $B = 1$. Assume that at least one of the numbers a_1 and a_2 is different from zero, say $a_1 \neq 0$. Setting $y = a_1 x + b_1$, we get

$$u_j(x) = \frac{a_j}{a_1}y + \frac{b_j a_1 - a_j b_1}{a_1} = A_j y + B_j, \text{ where } A_j = \frac{a_j}{a_1},$$

$$B_j = \frac{b_j a_1 - a_j b_1}{a_1} \text{ for } j = 2, 3.$$

The given equality takes the form

$$y^n + (A_2 y + B_2)^n = (A_3 y + B_3)^n, \qquad y \in \mathbb{R}.$$

By comparing the constant terms and the coefficients of y and y^n on both sides of this equality, we get the system of equations

$$\begin{aligned} B_2^n &= B_3^n \\ nA_2B_2^{n-1} &= nA_3B_3^{n-1} \\ 1 + A_2^n &= A_3^n. \end{aligned}$$

■

We have two cases.

(i) If $B_2 = 0$, then $B_3 = 0$ and therefore $b_j a_1 - a_j b_1 = 0$ for $j = 2, 3$, i.e., $b_j = \frac{a_j}{a_1} b_1$. In this case, just take $c_1 = 1$, $c_j = \frac{a_j}{a_1}$ for $j = 2, 3$, $A = a_1$, $B = b_1$.

(ii) If $B_2 \neq 0$, then $B_3 \neq 0$ and dividing the second equation by the first equation we get $\frac{A_2}{B_2} = \frac{A_3}{B_3}$. Raising both sides of the last equality to n-th power and using the first equation of the system, we get $A_2^n = A_3^n$. This contradicts the third equation of the system. Therefore this case cannot take place.

Problem 8.31. Determine all pairs of polynomials P and Q with complex coefficients such that for all complex numbers x, we have

$$P(P(x)) - Q(Q(x)) = 1 + i, \quad P(Q(x)) - Q(P(x)) = 1 - i.$$

Solution. Note that $P(P(x)) - P(Q(x))$ and $Q(P(x)) - Q(Q(x))$ are divisible by $P(x) - Q(x)$. It follows from this fact that

$$2i = P(P(x)) - P(Q(x)) + Q(P(x)) - Q(Q(x)),$$

is divisible by $P(x) - Q(x)$. Hence $P(x) - Q(x)$ is constant. Assume that $P(x) = Q(x) + C$. Since

$$\underbrace{P(P(x)) - Q(P(x))}_{C} + \underbrace{P(Q(x)) - Q(Q(x))}_{C} = 2,$$

we find that $C = 1$. Hence $P(x) = Q(x) + 1$. Therefore

$$P(P(x)) = 1 + Q(P(x)) = 1 + Q(1 + Q(x)).$$

This yields $Q(1+Q(x)) - Q(Q(x)) = i$. It is obvious that $Q(x)$ is not constant. Therefore $Q(1+x) - Q(x) = i$ and so $Q(x)$ is linear with leading coefficient i. This implies that $Q(x) = ix + a$ and $P(x) = ix + a + 1$ for some a. ■

Problem 8.32. Let $P(x) = a_0 + a_1x + a_2x^2 + a_{10}x^{10} + a_{11}x^{11} + a_{12}x^{12} + a_{13}x^{13}$, $a_{13} \neq 0$ and $Q(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + b_{10}x^{10} + b_{11}x^{11} + b_{12}x^{12} + b_{13}x^{13}$, $b_3 \neq 0$. Let $D(x) = \gcd(P(x), Q(x))$. Find the maximum value of $\deg D(x)$.

Solution. Let $R(x) = a_0 + a_1x + a_2x^2$ and $S(x) = a_{10} + a_{11}x + a_{12}x^2 + a_{13}x^3$. Then $P(x) = R(x) + x^{10}S(x)$. Now, let $T(x) = b_0 + b_1x + b_2x^2 + b_3x^3$ and $U(x) = b_{10} + b_{11}x + b_{12}x^2 + b_{13}x^3$. Then $Q(x) = T(x) + x^{10}U(x)$. Since

$$\begin{aligned} P(x)U(x) - Q(x)S(x) &= R(x)U(x) + x^{10}S(x)U(x) - T(x)S(x) - x^{10}S(x)U(x) \\ &= R(x)U(x) - T(x)S(x), \end{aligned}$$

we have that $D(x)$ divides $R(x)U(x) - T(x)S(x) = -b_3a_{13}x^6 + \ldots$. Since $b_3a_{13} \neq 0$, we find that the degree of $R(x)U(x) - T(x)S(x)$ is 6. Hence $\deg D(x) \leq 6$.

To prove that $\deg D(x) = 6$ is the maximum, we just need to give an example of polynomials $P(x)$ and $Q(x)$ where the gcd has degree 6. To generate such an example we choose 6 roots for $D(x)$. For each chosen root r, the equations $P(r) = Q(r) = 0$ give us two linear equations in the coefficients. If we do this for the roots $\{0, 1, 1, -1, i, -i\}$, where the repeat of 1 means we want a double root there, then we get the polynomials

$$P(x) = 2x^{13} - 3x^{10} + 3x^2 - 2x$$

and

$$Q(x) = x^{11} - x^{10} - x^3 - x^2,$$

which have a gcd of $D(x) = x(x-1)^2(x+1)(x^2+1)$. ■

Problem 8.33. Determine all polynomials P such that for every real number x,

$$(P(x))^2 + P(-x) = P(x^2) + P(x).$$

P. Calábec - Czech-Slovak Mathematical Olympiad 2001

First Solution. If the polynomial P is constant, i.e $P(x) = c$ for some $c \in \mathbb{R}$, then the number c satisfies the condition $c^2 + c = c + c$, i.e., $c = 0$ or $c = 1$. So $P(x) = 0$ or $P(x) = 1$ are solutions to the problem. If $\deg P(x) > 0$, then $P(x) = ax^n + Q(x)$, where $a \in \mathbb{R}$, $a \neq 0$, and Q is a polynomial of degree at most $n-1$. Then

$$(ax^n + Q(x))^2 + a(-x)^n + Q(-x) = ax^{2n} + Q(x^2) + ax^n + Q(x). \quad (8.5)$$

Comparing the coefficients of the x^{2n} term, we get $a^2 = a$, which gives $a = 1$. So equation (8.5) becomes

$$2x^n Q(x) + (Q(x))^2 - Q(x^2) = (1 - (-1)^n)x^n + Q(x) - Q(-x). \quad (8.6)$$

Assume that $\deg Q(x) = k > 0$. Then on the left-hand side of (8.6) there is a polynomial of degree at least $n + k$, but on the right-hand side there is a polynomial of degree at most n. Therefore the polynomial Q is constant, i.e., $Q(x) = b$ for some $b \in \mathbb{R}$. After substituting into (8.6), we get

$$2bx^n + b^2 - b = (1 - (-1)^n)x^n,$$

which is true for every x only when $2b = 1 - (-1)^n$ and $b^2 - b = 0$. So if n is even we get $P(x) = x^n$ and if n is odd we get $P(x) = x^n + 1$. In conclusion, $P(x) \in \{0, 1, x^2, x^4, x^6, \ldots, x+1, x^3+1, x^5+1, \ldots\}$. ■

Second Solution. The given relation can be written as

$$(P(x))^2 + 2P(-x) = P(x^2) + P(x) + P(-x).$$

On the right-hand side there is an even function of the variable x. Thus the function on the left-hand side must be even: for every real number x,

$$(P(-x))^2 + 2P(x) = (P(x))^2 + 2P(-x),$$

i.e.,

$$(P(x) - P(-x))\,(P(x) + P(-x) - 2) = 0.$$

Thus either $P(x) = P(-x)$ and hence $P(x)$ is even, or $P(x) - 1 = 1 - P(-x)$ and hence $P(x) - 1$ is an odd polynomial.
In the first case, we write $P(x) = R(x^2)$ and in the second case we write $P(x) = 1 + xR(x^2)$. In either case, the equation reduces to $R(x^2) = R(x)^2$. As we saw in the solution to Example 3.18, this implies $R(x) = x^n$ for some $n \geq 0$. Hence $P(x) = x^{2n}$ or $1 + x^{2n+1}$ for $n \geq 0$ are the solutions. ■

Problem 8.34. Find all monic polynomials $P(x)$, $Q(x)$ of the same degree such that for all real numbers x,

$$P(x)^2 - P(x^2) = Q(x).$$

Solution. Write $P(x) = x^d + R(x)$, where $\deg R(x) = k < d$.
Then we compute that

$$P(x)^2 - P(x^2) = 2x^d R(x) + R(x)^2 - R(x^2).$$

This is a polynomial of degree $d+k$, and we want it to be equal to $Q(x)$, which has degree d. Thus $k = 0$ and $R(x) = C$ is a constant polynomial. This gives

$$P(x)^2 - P(x^2) = 2Cx^d + C^2 - C = Q(x).$$

Since $Q(x)$ is monic we find $C = \frac{1}{2}$. Thus the solutions are

$$P(x) = x^d + \frac{1}{2}, \quad Q(x) = x^d - \frac{1}{4}.$$ ■

Problem 8.35. Find all monic polynomials $P(x)$, $Q(x)$ such that $P(1) = 1$ and

$$2P(x) = Q\left(\frac{(x+1)^2}{2}\right) - Q\left(\frac{(x-1)^2}{2}\right).$$

Greek Mathematical Olympiad 2016

Solution. Let $Q(x) = x^d + \ldots + b_0$. Then

$$Q\left(\frac{(x+1)^2}{2}\right) - Q\left(\frac{(x-1)^2}{2}\right) = \left(\frac{(x+1)^2}{2}\right)^d - \left(\frac{(x-1)^2}{2}\right)^d + \ldots$$

has degree $2d-1$ and leading coefficient $\frac{d}{2^{d-2}}$. Since $P(x)$ is monic, we find that $d = 2^{d-1}$. Therefore either $d = 1$ or $d = 2$. If $d = 1$, then $Q(x) = x + b$ and we find that $P(x) = x$. If $d = 2$, then

$$Q(x) = x^2 + a_1 x + a_0,$$

and we have

$$P(x) = \frac{1}{2}\left(Q\left(\frac{(x+1)^2}{2}\right) - Q\left(\frac{(x-1)^2}{2}\right)\right) = x^3 + (1+a_1)x.$$

Since $P(1) = 1$, we find that $a_1 = -1$. Whence

$$P(x) = x^3, \quad Q(x) = x^2 - x + a_0.$$

Problem 8.36. Find all polynomials $P(x)$ with real coefficients such that for all $|x| < 1$,

$$P\left(x\sqrt{2}\right) = P\left(x + \sqrt{1-x^2}\right).$$

USA TSTST 2014

Solution. Assume that $0 < x < 1$. Putting $\sqrt{1-x^2}$ instead of x in above equality, we find that

$$P\left(\sqrt{2}\cdot\sqrt{1-x^2}\right) = P\left(\sqrt{1-x^2} + \sqrt{1-\left(\sqrt{1-x^2}\right)^2}\right) = P\left(\sqrt{1-x^2} + x\right)$$

Hence

$$P\left(x\sqrt{2}\right) = P\left(\sqrt{2}\sqrt{1-x^2}\right).$$

Setting $x\sqrt{2} = t$, we get

$$\sqrt{2}\cdot\sqrt{1-x^2} = \sqrt{2-2x^2} = \sqrt{2-t^2}.$$

That is,

$$P(t) = P\left(\sqrt{2-t^2}\right),$$

for all $0 < t < \sqrt{2}$.
Now, write $P(x) = Q(x^2) + xR(x^2)$ for some polynomials $Q(x)$ and $R(x)$.
If $R(x) \neq 0$, then putting $x = \sqrt{2-t^2}$, we get

$$Q(t^2) + tR(t^2) = Q(2-t^2) + \sqrt{2-t^2}R(2-t^2).$$

Thus

$$\sqrt{2-t^2} = \frac{Q(t^2) + tR(t^2) - Q(2-t^2)}{R(2-t^2)}.$$

Cancelling out any common factors, we will get

$$\sqrt{2-t^2} = \frac{f(t)}{g(t)},$$

where $f(t)$ and $g(t)$ are relatively prime polynomials. Squaring we get

$$g(t)^2(2-t^2) = f(t)^2.$$

This holds for all $0 < t < \sqrt{2}$, hence for infinitely many values of t, thus it must hold as an identity between polynomials. This implies $f\left(\pm\sqrt{2}\right) = 0$, so we can write $f(t) = (2-t^2)h(t)$ for some polynomial $h(t)$. Then we get

$$g(t)^2 = (2-t^2)h(t)^2.$$

However, this implies $g(\pm\sqrt{2}) = 0$, and hence $f(t)$ and $g(t)$ have a common factor, a contradiction.
Hence $R(t) = 0$ and so $Q(t^2) = Q(2-t^2)$ for $0 < t < \sqrt{2}$. Since this holds for infinitely many t, it holds as an identity between polynomials and therefore $Q(x) = Q(2-x)$. Thus $Q(x) = A((x-1)^2)$ and

$$P\left(x\sqrt{2}\right) = Q(2x^2) = A((2x^2-1)^2) = A(4x^4 - 4x^2 + 1).$$

Moreover,

$$P\left(x+\sqrt{1-x^2}\right) = Q\left(1+2x\sqrt{1-x^2}\right) = A\left(\left(1+2x\sqrt{1-x^2}-1\right)^2\right)$$
$$= A(4x^2(1-x^2)) = A(4x^2-4x^4).$$

Thus

$$A(4x^4-4x^2+1) = A(4x^2-4x^4).$$

Putting $4x^4-4x^2+1=z$, we find that $A(z)=A(1-z)$ for infinitely many z, and therefore for all z. Thus $A(x)=B(x^2-x)$ for some polynomial $B(x)$. Therefore

$$P(x) = Q(x^2) = A((x^2-1)^2) = B((x^2-1)^4-(x^2-1)^2)$$
$$= B((x^2-1)^2(x^4-2x^2)).$$ ■

Problem 8.37. Find all polynomials $P(x)$ with real coefficients for which there is a unique polynomial $Q(x)$ with $Q(0)=0$ such that

$$x+Q(y+P(x)) = y+Q(x+P(y)) \qquad \forall x,y.$$

Solution. Let $\deg P(x)=p$, $\deg Q(x)=q$. Substituting $y=0$, we find that $x+Q(P(x))=Q(x+P(0))$. The degree condition shows that $\max\{1,pq\}=q$. Hence we find that $p\le 1\le q$, which gives $P(x)=ax+b$ for some real numbers a and b. Thus the original equation becomes

$$x+Q(ax+y+b) = y+Q(x+ay+b).$$

If $q=1$, then from $Q(0)=0$, we find that $Q(x)=cx$ for some real number $c\neq 0$. In this case, the equation reduces to $(1+ac)x+cy+cb=cx+(1+ac)y+cb$. This holds if and only if $1+ca=c$, which means $c=\frac{1}{1-a}$. Thus for $a\neq 1$, we have found one solution $Q(x)=\frac{x}{1-a}$.
Assume now that $q>1$. Writing $Q(x)=a_qx^d+\ldots$ and comparing the leading coefficients, we find that $a^q=1$. Thus either $a=1$, or $a=-1$. In the first

case, we get $x+Q(x+y+b)=y+Q(x+y+b)$ hence $x=y$, a contradiction. In the second case,

$$x+Q(b+y-x) = y+Q(b+x-y).$$

Let $S(x)=Q(b+x)-\frac{x}{2}$. Then this equation just reduces to $S(x)=S(-x)$. Hence $S(x)$ is even, and we can write $S(x)=T(x^2)$ for some polynomial $T(x)$. Thus for $a=-1$, we have found infinitely many solutions $P(x)=-x+b$ and

$$Q(x) = S(x-b)+\frac{x-b}{2} = T((x-b)^2)+\frac{x-b}{2}.$$

Thus in this case the solution is not unique.
Thus the polynomials $P(x)$ for which there is a unique solution are the polynomials $P(x)=ax+b$ with $a\neq\pm 1$. ■

Problem 8.38. Do there exist a polynomial $P(x)$ of degree $d>0$ with rational coefficients such that some of its coefficients are not integers, a polynomial $Q(x)$ with integer coefficients, and a set S of $d+1$ integers such that $P(s)=Q(s)$ for each $s\in S$?

Solution. The answer is no. Assume on the contrary that there exists such polynomials. Further assume that $Q(x)$ has the minimal degree among all such examples. Since $P(s)=Q(s)$ for all $s\in S$, it follows that we can write

$$Q(x) = P(x)+R(x)\prod_{s\in S}(x-s),$$

for some polynomial $R(x)$. Suppose $\deg R(x)=k$ and that $R(x)$ has leading coefficient b_k. Then $Q(x)$ has degree $d+k+1$ and leading coefficient b_k. Therefore b_k must be an integer. But then the polynomial

$$Q_1(x) = Q(x)-b_kx^k\prod_{s\in S}(x-s)$$

has integer coefficients, has $Q_1(s)=Q(s)=P(s)$ for all $s\in S$, and has lower degree than $Q(x)$. This contradicts the minimality of the degree of $Q(x)$. Thus such polynomials cannot exist. ■

Problem 8.39. Find all the polynomials $P(x)$ with real coefficients such that $|P(x)| \leq x$ for all real numbers x.

Romanian Mathematical Olympiad 1974

Solution. If $x = 0$ we have $|P(0)| \leq 0$, so $P(0) = 0$.
It follows that $P(x) = xQ(x)$ for some polynomial $Q(x)$ such that $|Q(x)| \leq 1$ for all $x \in \mathbb{R}$. Since $Q(x)$ is bounded, it must be constant, i.e., $Q(x) = c$ for all $x \in \mathbb{R}$ and $|c| \leq 1$. Therefore $P(x) = cx$, where $|c| \leq 1$. ∎

Problem 8.40. Let $P \in \mathbb{R}[x]$ such that $P(\sin t) = P(\cos t)$ for all $t \in \mathbb{R}$. Prove that there exists a polynomial $Q \in \mathbb{R}[x]$ such that $P(x) = Q(x^4 - x^2)$.

Vladimir Maşek - Romanian IMO Team Selection Test 1983

Solution. Since $P(\sin t) = P(\cos t) = P(\cos(-t)) = P(\sin(-t)) = P(-\sin t)$ and $\sin t$ takes on infinitely many values, it follows that $P(x) = P(-x)$. Since $P(x)$ is an even polynomial, we can write $P(x) = R(x^2)$, for some polynomial $R(x)$. Hence we see that $R(\sin^2 t) = R(\cos^2 t) = R(1 - \sin^2 t)$. Since $\sin^2 t$ takes on infinitely many values, it follows that $R(x) = R(1 - x)$, and hence that we can write $R(x) = Q(x^2 - x)$ for some polynomial $Q(x)$. Thus

$$P(x) = R(x^2) = Q(x^4 - x^2),$$

as desired. ∎

Problem 8.41. Let $P(x)$ be a polynomial with real coefficients satisfying the condition $P(\cos\theta + \sin\theta) = P(\cos\theta - \sin\theta)$ for every real number θ. Prove that $P(x) = Q((1 - x^2)^2)$ for some polynomial $Q(x)$ with real coefficients.

Solution. Since $a = \cos\theta + \sin\theta = \sqrt{2}\sin(\theta + \pi/4)$ and

$$b = \cos\theta - \sin\theta = \sqrt{2}\cos(\theta + \pi/4),$$

we see that the pair (a, b) can take on all real values with $a^2 + b^2 = 2$. Hence the problem is reduced to finding all polynomials $P(x)$ such that $P(a) = P(b)$ whenever $a^2 + b^2 = 2$. This implies that $P(a) = P(-a)$. Hence $P(x)$ is even.

Therefore we can write $P(x) = R(x^2)$ for some polynomial $R(x)$.
The hypothesis becomes $R(a^2) = R(b^2) = R(2 - a^2)$ which implies that $R(x) = R(2 - x)$. Therefore $R(x) = Q((1 - x)^2)$ for some polynomial $Q(x)$. Hence $P(x) = R(x^2) = Q((1 - x^2)^2)$ as desired. ∎

Problem 8.42. Find all the polynomials $P \in \mathbb{R}[x]$ such that

$$P(\sin x) = P(\tan x)P(\cos x) \text{ for any } x \in \left(\frac{\pi}{3}, \frac{\pi}{2}\right).$$

Vladimir Maşek - Romanian Mathematical Olympiad 1986

First Solution. If $P(x) = c$, where $c \in \mathbb{R}$, then $c = c^2$, which gives $P(x) = 0$ or $P(x) = 1$. Now, assume that $P(x)$ is not constant, i.e., assume that $\deg P(x) = n \geq 1$. Let $t = \cos x$. Then $t \in \left(0, \frac{1}{2}\right)$ and

$$P(\sqrt{1 - t^2}) = P(t)P\left(\frac{\sqrt{1 - t^2}}{t}\right) \quad \forall t \in \left(0, \frac{1}{2}\right).$$

Since this equality holds for infinitely many t, it holds for all $t \in (0, 1)$. (Note that this is a slightly subtle point, since the functions involved are not polynomials, or even rational functions. They are algebraic functions, which does suffice. One elementary argument is to substitute $t = \frac{2s}{1+s^2}$, which gives $\sqrt{1 - t^2} = \frac{1-s^2}{1+s^2}$, then invoke fact that rational functions that agree at infinitely many points are identical.) From this equality we get

$$\frac{P(\sqrt{1 - t^2})}{P(t)} = P\left(\frac{\sqrt{1 - t^2}}{t}\right) \qquad \forall t \in (0, 1).$$

Using the substitution $t \mapsto \sqrt{1 - t^2}$, it follows that

$$\frac{P(t)}{P(\sqrt{1 - t^2})} = P\left(\frac{t}{\sqrt{1 - t^2}}\right) \qquad \forall t \in (0, 1).$$

Hence

$$P\left(\frac{t}{\sqrt{1 - t^2}}\right) P\left(\frac{\sqrt{1 - t^2}}{t}\right) = 1 \qquad \forall t \in (0, 1).$$

Setting $y = \dfrac{t}{\sqrt{1-t^2}}$, we obtain that

$$P(y)P\left(\frac{1}{y}\right) = 1 \qquad \forall y \in (0, +\infty).$$

By Problem 3.5, we conclude that $P(x) = x^n$. ∎

Second Solution. Clearly, the zero polynomial $P(x) \equiv 0$ satisfies the given relation. Let $P(x) \in \mathbb{R}[x]$ be a nonzero polynomial of degree $n \in \mathbb{N}$ satisfying the given condition. We will prove by induction on n that $P(x) = x^n$ for all $n \in \mathbb{N}$. If $n = 0$, we have $P(x) = c$ for some $c \in \mathbb{R}^*$ and the given relation can be written as $c = c^2$, which gives $c = 1$. So $P(x) = 1 = x^0$. Assume that the only polynomial of degree n having the given property is x^n. We prove that the only polynomial of degree $n+1$ with the given property is x^{n+1}. Let $P(x) \in \mathbb{R}[x]$, $\deg P(x) = n+1$, such that

$$P(\sin x) = P(\tan x)P(\cos x) \qquad \forall x \in \left(\frac{\pi}{3}, \frac{\pi}{2}\right). \tag{8.7}$$

Then

$$P(\cos x) = \frac{P(\sin x)}{P(\tan x)} \qquad \forall x \in \left(\frac{\pi}{3}, \frac{\pi}{2}\right) \setminus A, \tag{8.8}$$

where A is the finite set for those values of $x \in \left(\frac{\pi}{3}, \frac{\pi}{2}\right)$ for which $P(\tan x) = 0$. Taking the limit $x \to \pi/2$ of both sides in (8.8), we get

$$P(0) = \frac{P(1)}{\lim\limits_{x \to \frac{\pi}{2}} P(\tan x)} = \frac{P(1)}{\lim\limits_{y \to \infty} P(y)} = 0.$$

Consequently, $P(x) = xQ(x)$ for some polynomial $Q(x) \in \mathbb{R}[x]$ with $\deg Q(x) = n$. Equation (8.7) becomes

$$(\sin x)Q(\sin x) = (\tan x)Q(\tan x)(\cos x)Q(\cos x) \qquad \forall x \in \left(\frac{\pi}{3}, \frac{\pi}{2}\right),$$

so

$$Q(\sin x) = Q(\tan x)Q(\cos x) \qquad \forall x \in \left(\frac{\pi}{3}, \frac{\pi}{2}\right).$$

By inductive hypothesis, we have $Q(x) = x^n$, so $P(x) = xQ(x) = x^{n+1}$ and the conclusion follows. ∎

Problem 8.43. Find all quadruples of polynomials $P_1(x)$, $P_2(x)$, $P_3(x)$, $P_4(x)$ with real coefficients such that for each quadruple of integers x, y, z, t such that $xy - zt = 1$, one has

$$P_1(x)P_2(y) - P_3(z)P_4(t) = 1.$$

Alexander Golovanov - Saint Petersburg Mathematical Olympiad 1996

First Solution. If $P_1(1) = 0$, then $P_3(z)P_4(t) = -1$ for each pair of integers z, t, and so P_3 and P_4 are constant functions with product -1. This reduces the condition to $P_1(x)P_2(y) = 0$, so one of P_1 and P_2 is identically zero. Ignoring such cases, which are easily enumerated, we assume $P_i(1) \neq 0$ for all i.

We first note that $P_1(x)P_2(1) = P_1(1)P_2(x)$ for all nonzero integers x, so that P_1 and P_2 are equal up to a scalar factor; similarly, P_3 and P_4 are equal up to a scalar factor. Now, note that $P_1(x)P_2(ay) = P_1(ax)P_2(y)$ for all nonzero a, x, y, so that the difference between the two sides is identically zero as a polynomial in a. In particular, that means no term in $P_1(x)P_2(y)$ has unequal exponent in x and y, and the same is true of $P_1(x)P_1(y)$. On the other hand, if $P_1(x)$ has terms of more than one degree, then $P_1(x)P_1(y)$ contains a term with different degrees in x and y. Hence $P_1(x) = cx^k$ for some integer k and some constant c, and similarly $P_2(x) = dx^k$, $P_3(x) = ex^m$, $P_4(x) = fx^m$.

Thus we must determine when $cdx^k y^k - efz^m t^m = 1$ whenever $xy - zt = 1$ in integers. From $x = y = 1$ and $z = t = 0$, we see that $cd = 1$, and similarly we find $ef = 1$. Looking at $(x, y, z, t) = (n+1, 1, n, 1)$, we see that $(n+1)^k - n^m = 1$. Looking at the degree of this as a polynomial in n, we see that $k = m$. If $k > 1$, we get a contradiction by looking at the coefficient of n^{k-1}. We conclude $P_1(x) = cx$, $P_2(x) = x/c$, $P_3(x) = ex$, $P_4(x) = x/e$ for some nonzero real numbers c, e. ∎

Second Solution. Assume that $\deg P_i = d_i$. Take a large positive integer N with more than $d_1 + d_2$ divisors and set $(x, y, z, t) = (x, \frac{N}{x}, 1, N-1)$. Then

$$P_1(x)\, P_2\left(\frac{N}{x}\right) = 1 + P_3(1)\, P_4(N-1).$$

The above equation has more than $d_1 + d_2$ roots. Hence for all x,

$$P_1(x)\,P_2\left(\frac{N}{x}\right)$$

is constant. This shows that $P_1(x), P_2(x)$ have the same degree. Let

$$P_1(x) = ax^d + \ldots + c, \qquad P_2(x) = bx^d + \cdots + e.$$

Then

$$Kx^d = \left(ax^d + \cdots + c\right)\left(ex^d + \cdots + b\right).$$

This shows that $bc = ea = 0$. Then $c = e = 0$. Taking $P_1(x) = x^r S(x)$, $P_2(x) = x^s T(x)$ with $S(0), T(0) \neq 0$, we find that $r = s$. Then $T(x)S\left(\frac{N}{x}\right)$ is again constant. Hence either, $S(0), T(0) = 0$ or $T(x), S(x)$ are constant. The latter is possible, whence $P_1(x) = ax^d$, $P_2(x) = bx^d$. By the same argument, $P_3(x) = cx^k$, $P_4(x) = ex^k$. Putting $x = y = 1$, $z = t = 0$, we get $ab = 1$. Analogously, $cd = 1$.
Now, putting $x = z = 1$, $t = y - 1$, we find $y^n - (y-1)^m = 1$ for each y. Therefore $m = n = 1$.
Thus $P_1(x) = ax$, $P_2(x) = \frac{x}{a}$, $P_3(x) = cx$, $P_4(x) = \frac{x}{c}$. ■

Problem 8.44. Suppose that F, G, H are polynomials of degree at most $2n+1$ with real coefficients such that:

(i) For all real x we have $F(x) \leq G(x) \leq H(x)$.

(ii) There exist distinct real numbers $x_1, x_2, \ldots, x_n$ such that $F(x_i) = H(x_i)$ for $i = 1, 2, 3, \ldots, n$.

(iii) There exists a real number x_0 different from $x_1, x_2, \ldots, x_n$ such that $F(x_0) + H(x_0) = 2G(x_0)$.

Prove that $F(x) + H(x) = 2G(x)$ for all real numbers x.

Baltic Way 2007

Solution. Let $P(x) = G(x) - F(x)$. Observe that $\deg P(x) \leq 2n + 1$. By condition (i), we have $P(x) \geq 0$ for all real numbers x. By condition (ii), $x_1, x_2, \ldots, x_n$ are roots of $P(x)$. Since $P(x) \geq 0$ for all real numbers x, each of these roots must have even multiplicity. Thus P is divisible by $(x - x_i)^2$ for $i = 1, 2, \ldots, n$, i.e.,

$$P(x) = Q(x)(x - x_1)^2(x - x_2)^2 \cdot \ldots \cdot (x - x_n)^2,$$

where $Q(x)$ is a polynomial with real coefficients. By comparing the degrees, we see that $\deg Q(x) \leq \deg P(x) - 2n \leq 1$. However, $Q(x) \geq 0$ for all real numbers x, and this is impossible if $Q(x)$ is linear. Hence $Q(x)$ is constant. Then

$$G(x) - F(x) = a(x - x_1)^2(x - x_2)^2 \cdot \ldots \cdot (x - x_n)^2$$

for some real number $a \geq 0$. Likewise, we prove that

$$H(x) - F(x) = b(x - x_1)^2(x - x_2)^2 \cdot \ldots \cdot (x - x_n)^2$$

for some real number $b \geq 0$. Now, by condition (iii), there is a real number x_0 different from $x_1, x_2, \ldots, x_n$ such that

$$F(x_0) + H(x_0) - 2G(x_0) = (b - 2a)(x_0 - x_1)^2(x_0 - x_2)^2 \cdot \ldots \cdot (x_0 - x_n)^2 = 0.$$

It follows that $b - 2a = 0$, i.e., the expression becomes identically zero. So $F(x) + H(x) - 2G(x) = 0$ for all real numbers x, as we wanted to prove. ■

Problem 8.45. Consider two polynomials P and Q with real coefficients having the property that the sets

$$\{n \in \mathbb{N} \mid P(n) \leq Q(n)\} \quad \text{and} \quad \{n \in \mathbb{N} \mid Q(n) \leq P(n)\}$$

are infinite. Prove that $P = Q$.

Laurenţiu Panaitopol, Laurenţiu Panaitopol Competition 2010

Solution. From the hypothesis, it follows that there exist sequences $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ such that $a_n < b_n < a_{n+1} < b_{n+1}$ and

$$P(a_n) \geq Q(a_n),\ P(b_n) \leq Q(b_n) \text{ for all } n \in \mathbb{N}.$$

Considering polynomial $F = P - Q$, we have $F(a_n) \leq 0 \leq F(b_n)$ for all $n \in \mathbb{N}$, so F has infinitely many roots and so F is the zero polynomial. ■

Problem 8.46. Prove that there doesn't exist a rational function $R(z)$ such that $R(n) = n!$ for all natural numbers n.

Jacques Marion - Crux Mathematicorum 5/1976

First Solution. Assume on the contrary, that there exists a rational function $R(z)$ such that $R(n) = n!$. Let

$$R(z) = \frac{P(z)}{Q(z)} = \frac{a_r z^r + a_{r-1} z^{r-1} + \ldots + a_0}{b_s z^s + b_{s-1} z^{s-1} + \ldots + b_0},$$

where P and Q are relatively prime polynomials and $a_r, b_s \neq 0$.
Since $\lim_{n\to\infty} \frac{n^{r-s}}{n!} = 0$, we have

$$1 = \lim_{n\to\infty} \frac{P(n)/Q(n)}{R(n)} = \lim_{n\to\infty} \frac{a_r n^{r-s}}{b_s n!} = 0,$$

a contradiction. ■

Second Solution. Since $(n+1)! = R(n+1) = (n+1)R(n)$ for all natural numbers n, we find that $R(x+1) = (x+1)R(x)$ for all x. Therefore, $R(0) = 0$. We also see that if $r \geq 0$ is a root of $R(x)$, then $r+1$ is a root of $R(x)$. Thus $R(x)$ has roots at all nonnegative integers. However this forces $R(x) = 0$, a contradiction. ■

Problem 8.47. Find all polynomials $P(x)$ such that

$$P(x)P(2x^2) = P(x + x^3).$$

Mathematics and Youth Journal

Solution. One easily sees that the constant solutions are $P(x) = 0$ or 1. We will show that these are the only solutions. Suppose $P(x)$ is nonconstant and

let $d = \deg P(x) > 0$. Plugging in $x = 0$, we get $P(0)^2 = P(0)$, hence that $P(0) \in \{0, 1\}$. If $P(0) = 0$, then writing $P(x) = x^k Q(x)$, where $Q(0) \neq 0$, we get $2^k x^{2k} Q(x)Q(2x^2) = (1 + x^2)^k Q(x + x^3)$, which forces $Q(0) = 0$, a contradiction. So we must have $P(0) = 1$. Looking at the coefficient of x^{3d}, we see that the leading coefficient of $P(x)$ is $\frac{1}{2^d}$.
Let r be a root of $P(x)$ with maximum modulus. The product of the moduli of the d roots is equal to 2^d, so this implies $|r| \geq 2$. Plugging in $x = r$, we find that $r + r^3$ is also a root of $P(x)$, and we compute

$$|r + r^3| = |r^2 + 1| \cdot |r| \geq (|r|^2 - 1)|r| \geq 3|r| > |r|.$$

This contradicts the maximality of $|r|$. ■

Problem 8.48. Prove that for each positive integer n, there exists a polynomial of degree n with n distinct real roots such that

$$P(x(4 - x)) = P(x)P(4 - x).$$

Mongolian Mathematical Olympiad

Solution. Let $P(x) = (x - c_1) \cdot \ldots \cdot (x - c_n)$. We have

$$P(4x - x^2) = (-1)^n \prod_{i=1}^{n} (x^2 - 4x - c_i)$$

and

$$P(x)P(4 - x) = (-1)^n \prod_{i=1}^{n} (x - c_i)(x - 4 + c_i) = (-1)^n \prod_{i=1}^{n} (x^2 - 4x - c_i^2 + 4c_i).$$

If we prove that for every n the system of equations

$$\begin{cases} c_2 = 4c_1 - c_1^2, \\ c_3 = 4c_2 - c_2^2, \\ \quad \vdots \\ c_1 = 4c_n - c_n^2 \end{cases}$$

has a solution with the c_i distinct real numbers, then we will have the desired example. We can easily find that $c_i \in [0,4]$. Whence setting $c_1 = 4\sin^2\alpha$, we get

$$c_2 = 16\sin^2\alpha - 16\sin^4\alpha = 16\sin^2\alpha\cos^2\alpha = 4\sin^2 2\alpha$$

and inductively $c_k = 4\sin^2 2^k\alpha$. When this argument cycles around, we get

$$c_1 = 4\sin^2\alpha = 4\sin^2 2^{n+1}\alpha.$$

Then we find that $2^{n+1}\alpha = k\pi \pm \alpha$ for some integer k and hence

$$\alpha = \frac{k\pi}{2^{n+1}\pm 1}.$$

Choosing $k = 1$ and the $+$ sign, we get

$$c_i = 4\sin^2\frac{2^i\pi}{2^{n+1}+1},$$

and since $\frac{2^i\pi}{2^{n+1}+1} < \frac{\pi}{2}$, we see that the c_i increase with i, and hence are distinct real numbers. Therefore our proof is complete. ■

Remark. Compare the previous problem with what you have learned in Chapter 4.

Problem 8.49. Find all polynomials P with real coefficients such that

$$\frac{P(x)}{yz} + \frac{P(y)}{zx} + \frac{P(z)}{xy} = P(x-y) + P(y-z) + P(z-x)$$

holds for all nonzero real numbers x, y, z satisfying $2xyz = x + y + z$.

Titu Andreescu and Gabriel Dospinescu - USA Mathematical Olympiad 2019

Solution. If $P(x) = c$ for a constant c, then

$$\frac{c(x+y+z)}{xyz} = 3c.$$

We have $2c = 3c$. Therefore $c = 0$.
Now consider the case of non-constant polynomials. First we have

$$xP(x) + yP(y) + zP(z) = xyz(P(x-y) + P(y-z) + P(z-x))$$

for all nonzero real numbers x, y, z satisfying $2xyz = x + y + z$. Both sides of the equality are polynomials (of x, y, z). They have the same values on the 2-dimensional surface $2xyz = x + y + z$, except for some 1-dimensional curves in it. By continuity, the equality holds for all points on the surface, including those with $z = 0$. Let $z = 0$, we have $y = -x$ and $x(P(x) - P(-x)) = 0$. Therefore P is an even function.
(Here is a sketch of an elementary proof. Let $z = \frac{x+y}{2xy-1}$. We have

$$xP(x) + yP(y) + \frac{x+y}{2xy-1}P\left(\frac{x+y}{2xy-1}\right)$$

$$= xy\frac{x+y}{2xy-1}\left(P(x-y) + P\left(y - \frac{x+y}{2xy-1}\right) + P\left(\frac{x+y}{2xy-1} - x\right)\right).$$

This is an equality of rational expressions. By multiplying $(2xy-1)^N$ on both sides for a sufficiently large N, they become polynomials, say $A(x,y) = B(x,y)$ for all real x, y with $x \neq 0$, $y \neq 0$, $x+y \neq 0$ and $2xy - 1 \neq 0$. For a fixed x, we have two polynomials (of y) having same values for infinitely many y. They must be identical. Let $y = 0$, we have $x^{N+1}(P(x) - P(-x)) = 0$.)
Notice that if $P(x)$ is a solution, then so is $cP(x)$ for any constant c. For simplicity, we assume the leading coefficient of P is 1:

$$P(x) = x^n + a_{n-2}x^{n-2} + \cdots + a_2x^2 + a_0,$$

where n is a positive even number.
Let $y = \frac{1}{x}$, $z = x + \frac{1}{x}$. We have

$$xP(x) + \frac{1}{x}P\left(\frac{1}{x}\right) + \left(x+\frac{1}{x}\right)P\left(x+\frac{1}{x}\right)$$

$$= \left(x+\frac{1}{x}\right)\left(P\left(x-\frac{1}{x}\right) + P(-x) + P\left(\frac{1}{x}\right)\right).$$

Simplify using $P(x) = P(-x)$,

$$\left(x+\frac{1}{x}\right)\left(P\left(x+\frac{1}{x}\right)-P\left(x-\frac{1}{x}\right)\right)=\frac{1}{x}P(x)+xP\left(\frac{1}{x}\right).$$

Expand and combine like terms, both sides are of the form

$$c_{n-1}x^{n-1}+c_{n-3}x^{n-3}+\cdots+c_1x+c_{-1}x^{-1}+\cdots+c_{-n+1}x^{-n+1}.$$

They have the same values for infinitely many x. They must be identical. We just compare their leading terms. On the left hand side it is $2nx^{n-1}$. There are two cases for the right hand sides: If $n > 2$, it is x^{n-1}. If $n = 2$, it is $(1 + a_0)x$. It does not work for $n > 2$. When $n = 2$, we have $4 = 1 + a_0$, therefore $a_0 = 3$.
The solution is $P(x) = c(x^2 + 3)$ for any constant c. ■

Problem 8.50. Find all polynomials $P(x)$ for which:

$$P(a+b) = 6\left(P(a)+P(b)\right)+15a^2b^2(a+b),$$

for all complex numbers a and b such that $a^2 + b^2 = ab$.

Titu Andreescu and Mircea Becheanu - Mathematical Reflections, Problem U484

Solution. Letting $a = b = 0$ yields $P(0) = 12P(0)$, so $P(0) = 0$. Clearly, $P \not\equiv 0$. Thus $P(x) = c_nx^n + \cdots + c_1x$, with $n \geq 1$ and $c_n \neq 0$.
Suppose that $a^2 + b^2 = ab$. We claim that for each $k \geq 1$, there is a constant f_k such that $a^k + b^k = f_k(a + b)^k$. Indeed, $f_1 = 1$, and since

$$a^2+b^2=(a+b)^2-2ab=(a+b)^2-2\left(a^2+b^2\right),$$

$f_2 = \frac{1}{3}$. Inductively, for $k \geq 2$,

$$\begin{aligned}a^{k+1}+b^{k+1}&=(a^k+b^k)(a+b)-ab(a^{k-1}+b^{k-1})\\&=f_k(a+b)^{k+1}-\frac{1}{3}f_{k-1}(a+b)^{k+1}.\end{aligned}$$

Thus $f_{k+1} = f_k - \frac{1}{3}f_{k-1}$. In particular, $f_3 = 0$ and $f_4 = -\frac{1}{9} = f_5$.
Using a generating function or otherwise, we can also obtain

$$f_k=\left(\frac{\sqrt{3}+i}{2\sqrt{3}}\right)^k+\left(\frac{\sqrt{3}-i}{2\sqrt{3}}\right)^k.$$

Therefore for $k \geq 6$,

$$|6f_k| \leq 12\left|\frac{\sqrt{3}+i}{2\sqrt{3}}\right|^k=12\left(\frac{1}{\sqrt{3}}\right)^k\leq\frac{12}{27}<1.$$

Equating coefficients of $(a + b)^k$ in $P(a + b) = 6(P(a) + P(b)) + \frac{5}{3}(a + b)^5$, we get $(1 - 6f_k)c_k = 0$ for all $k \neq 5$, thus $c_k = 0$ for all $k \neq 5$. Also, $c_5 = 6f_5c_5 + \frac{5}{3} = -\frac{2}{3}c_5 + \frac{5}{3}$, so $c_5 = 1$. In conclusion, $P(x) = x^5$ is the only solution. ■

Remark. Solving the recursion in the previous problem can be done in many ways. The generating function method mentioned means looking at the function

$$F(x)=\sum_{n=0}^{\infty}f_nx^n.$$

The recursion shows that

$$\left(\frac{1}{3}x^2-x+1\right)F(x)=f_0+(f_1-f_0)x+\sum_{n=2}^{\infty}\left(f_n-f_{n-1}+\frac{1}{3}f_{n-2}\right)x^n=2-x,$$

and hence

$$F(x)=\frac{3(2-x)}{x^2-3x+3}.$$

To derive a formula for f_n from this, we note that writing

$$\alpha=\frac{\sqrt{3}+i}{2\sqrt{3}}\quad\text{and}\quad\beta=\frac{\sqrt{3}-i}{2\sqrt{3}},$$

we can check that

$$F(x)=\frac{3(2-x)}{x^2-3x+3}=\frac{1}{1-\alpha x}+\frac{1}{1-\beta x}.$$

So expanding the geometric series

$$\frac{1}{1-\alpha x} = 1 + \alpha x + \alpha^2 x^2 + \dots$$

and analogously for β gives the formula above. One can also check that the sequences α^n and β^n satisfy the recursion, hence so does any sequence of the form $C_1\alpha^n + C_2\beta^n$. Then we use the initial values to solve for the constants C_1 and C_2. An alternate approach is to calculate f_n far enough to notice that $(i\sqrt{3})^n f_n$ is periodic in n with period 6. Since the solution only uses that $f_n \neq \frac{1}{6}$, one could also note that the recursion implies f_n is rational with denominator a power of 3, hence it cannot equal $\frac{1}{6}$.

Problem 8.51. Find all polynomials P with complex coefficients such that

$$P(a) + P(b) = 2P(a+b),$$

whenever a and b are complex numbers satisfying $a^2 + 5ab + b^2 = 0$.

Titu Andreescu and Mircea Becheanu - Mathematical Reflections, Problem U491

Solution. Let (a, b) be a pair of nonzero numbers which satisfy the condition $a^2 + 5ab + b^2 = 0$. Then

$$\frac{a}{b} = \frac{-5 \pm \sqrt{21}}{2} \tag{8.9}$$

Let $\lambda = \frac{-5+\sqrt{21}}{2}$. Then for every real number t, the pair $(\lambda t, t)$ satisfies the given condition.

Let $P(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial which is a solution of the problem. Then we have:

$$\sum_{i=0}^{n} a_i \lambda^i t^i + \sum_{i=0}^{n} a_i t^i = 2\sum_{i=0}^{n} a_i (\lambda+1)^i t^i,$$

for all numbers t, hence as polynomials in t. Taking the coefficient of t^i on both sides shows that whenever $a_i \neq 0$, we have the condition:

$$1 + \lambda^i = 2(1+\lambda)^i \tag{8.10}$$

This is true for $i = 0, 3$ and it fails for $i = 1$ and $i = 2$. We will show that it can not happen for $i > 3$.
Suppose it holds for $i > 0$. We will first show that i is necessarily odd. From (8.10), it follows that λ is a root of the rational polynomial

$$f(x) = 2(x+1)^i - x^i - 1.$$

But λ is a root of $g(x) = x^2+5x+1$, which is therefore its minimal polynomial. So $g(x)$ divides $f(x)$ in $\mathbb{Z}[x]$, that is,

$$2(x+1)^i - x^i - 1 = (x^2 + 5x + 1)h(x),$$

for some polynomial $h(x)$ with integer coefficients. Putting $x = -1$ in this equality, we obtain $-(-1)^i - 1 = -3h(-1)$, showing that $(-1)^i \equiv -1 \pmod 3$, so i is odd.
Now, since $0 < \lambda + 1 < 1$, the function $p(i) = 2(1+\lambda)^i$ decreases as i increases. The function $q(i) = 1 + t^i$ can be written, for i odd, as

$$q(i) = 1 + (-1)^i(-t)^i = 1 - (-t)^i.$$

Since $0 < -\lambda < 1$, it increases as i increases. So the equation (8.10) has at most one solution for i odd. Since we saw that $i = 3$ is a solution, it is the only solution. Thus we have shown that the solutions to this problem are exactly the polynomials $a_0 + a_3 x^3$. ■

Problem 8.52. Let a be a positive integer such that

$$f(x) = x^2 + ax + 2017!,$$

has no real roots. Prove that there is no integer k such that $f(x^k)$ is reducible over $\mathbb{Z}[x]$.

Solution. Assume on the contrary, that there is a number k such that

$$f(x^k) = g(x)h(x),$$

for some nonconstant polynomials g and h with integer coefficients. The polynomial $f(x)$ has two complex roots with modulus $\sqrt{2017!}$. Therefore all roots

of $f(x^k)$ have modulus $\sqrt[2k]{2017!}$. This implies that the modulus of products of the roots of g is $2017!^{(\deg g)/(2k)}$. The polynomial $g(x)$ has integer coefficients, so this must be an integer. However the prime 2017 divides 2017! exactly once, so 2017! is not a power of any integer. Thus $\deg g$ must be a multiple of $2k$. This is a contradiction since the fact that $h(x)$ is nonconstant means $\deg g < 2k$. ■

Problem 8.53. Find all ordered pairs (m, n) of positive integers such that there exist polynomials $P(x)$, $Q(x)$ of degree m, n respectively, and with real coefficients, such that the numbers $1, 2, \ldots, mn$ are roots of $P(Q(x))$.

First Solution. If $m = 1$, a solution is

$$P(x) = x, \quad Q(x) = (x-1)\cdot\ldots\cdot(x-n).$$

If $n = 1$, a solution is

$$P(x) = (x-1)\cdot\ldots\cdot(x-m), \quad Q(x) = x.$$

If $n = 2$, a solution is

$$P(x) = \prod_{k=1}^{m}(x + k(2m+1-k)), \quad Q(x) = x(x-2m-1).$$

Now, assume that $m > 1$ and $n > 2$.
As we saw in the text, the roots of $P(Q(x))$ are the union of the sets of roots of the equations $Q(x) = r_i$, where r_i varies over the roots of $P(x)$. Since $P(Q(x))$ has mn real roots, it follows that $P(x)$ must have m real roots. Let $r_1 < \ldots < r_m$ be root of $P(x)$. By replacing $P(x)$ by $P(-x)$, if necessary, we can assume that $Q(1) = r_1$. Then the argument given in Example 5.20, shows that the sequence $Q(1), Q(2), \ldots, Q(mn)$ will cycle through $r_1, r_2, \ldots, r_m$, then turn, and cycle through $r_m, r_{m-1}, \ldots, r_1$, then turn again and repeat this pattern. Thus

$$Q(1) = r_1,\ Q(2) = r_2,\ \ldots,\ Q(m) = r_m,\ Q(m+1) = r_m,\ Q(m+2) = r_{m-1}, \ldots.$$

Hence the roots of $Q(1) = r_k$ will be

$$\{k, 2m+1-k, 2m+k, 4m+1-k, \ldots\}.$$

In particular, we see that for each integer x with $2m+1 \le x \le mn$, we have

$$Q(x) = Q(x-2m).$$

The degree of the polynomial $Q(x) - Q(x-2m)$ is $n-1$, and we have found $m(n-2)$ roots. Hence $m(n-2) \le n-1$. Since $m \ge 2$ and $n \ge 3$, we see that the only possibility is $(m, n) = (2, 3)$.
The case $(m, n) = (2, 3)$ cannot occur since the roots of $Q(x) - r_1$ would be $\{1, 4, 5\}$ and the roots of $Q(x) = r_2$ would be $\{2, 3, 6\}$. These sets have different sums, but since $\deg Q(x) > 2$, they should have the same sum. ■

Second Solution. We could also finish the argument in a way similar to Example 5.20. After finding that the roots of $Q(1) = r_k$ are

$$\{k, 2m+1-k, 2m+k, 4m+1-k, \ldots\},$$

we argue that since $\deg Q(x) = n > 2$ each of these sets must have the same sum and the same sum of squares. Since the elements of these sets taken two at a time have sums $2m+1, 6m+1, \ldots$, we see that the equal sum condition forces n to be even. However looking at the sums of squares of these pairs, we see that

$$1^2 + (2m)^2 > 2^2 + (2m-1)^2,\ (2m+1)^2 + (4m)^2 > (2m+2)^2 + (4m-1)^2, \ldots.$$

Thus for n even, the set $\{1, 2m, 2m+1, 4m, \ldots\}$ has larger sum of squares than the set $\{2, 2m-1, 2m+2, 4m-1, \ldots\}$, which gives a contradiction. Thus there are no solutions with $m > 1$ and $n > 2$. ■

Problem 8.54. Find all monic polynomials $P(x)$, $Q(x)$ such that

$$P(Q(x)) = x^{2019}.$$

First Solution. Let $P(x) = (x-r_1)^{\alpha_1} \cdot \ldots \cdot (x-r_d)^{\alpha_1}$, where $r_1, \ldots, r_d$ are distinct. Then

$$P(Q(x)) = (Q(x)-r_1)^{\alpha_1} \ldots (Q(x)-r_d)^{\alpha_1} = x^{2019}.$$

Since $Q(x)-r_1, \ldots, Q(x)-r_d$ have no roots in common and the only root on the right-hand side is 0, we deduce that $d = 1$. Thus

$$P(x) = (x-r_1)^{\alpha_1}.$$

Moreover,

$$(Q(x)-r_1)^{\alpha_1} = x^{2019}.$$

Thus $Q(0) = r_1$. In addition, the equation $Q(x) - r_1$ has $x = 0$ as its only root. Whence $Q(x) - r_1 = x^{\beta_1}$. Thus $x^{\alpha_1\beta_1} = x^{2019}$, which gives $\alpha_1\beta_1 = 2019$. We find that

$$(\alpha_1\beta_1) \in \{(1,2019),(3,673),(673,3),(2019,1)\}.$$

Therefore

$$(P(x),Q(x)) = (x-r_1, r_1+x^{2019}), ((x-r_1)^3, r_1+x^{673}),$$
$$((x-r_1)^{673}, r_1+x^3), \text{ or } ((x-r_1)^{2019}, r_1+x).$$

■

Second Solution. We can use differentiation to solve this problem. Differentiating gives

$$P'(Q(x))Q'(x) = 2019x^{2018}.$$

Thus $Q'(x)$ must divide $2019x^{2018}$ and hence

$$Q'(x) = kx^c,$$

for some constant k and integer $c \geq 0$. Integrating we find that

$$Q(x) = \frac{k}{c+1}x^{c+1} + e,$$

for some constant e and since $Q(x)$ is monic, we conclude that $k = c+1$. Thus $Q(x) = x^{c+1} + e$. Plugging this into the original equation, we find that

$$P(x^{c+1} + e) = x^{2019}$$

and hence

$$P(x) = (x-e)^{\frac{2019}{c+1}}.$$

Since $P(x)$ is a polynomial, we have that $(c+1) \mid 2019$.
Hence $c+1 \in \{1,3,673,2019\}$, and we get the same solutions as above. ■

Problem 8.55. Let P, Q, R be nonconstant polynomials with integer coefficients such that for any real number x,

$$P(Q(x)) = Q(R(x)) = R(P(x)).$$

Show that $P = Q = R$.

Polish Mathematical Olympiad 2009

Solution. Substituting $y = P(x)$ in the equality $P(Q(y)) = Q(R(y))$, we get

$$P(Q(P(x))) = Q(R(P(x))).$$

On the other hand, the equality $P(Q(x)) = R(P(x))$ implies the equality $Q(P(Q(x))) = Q(R(P(x)))$. This means that $P(Q(P(x))) = Q(P(Q(x)))$ and consequently

$$P(Q(P(Q(P(Q(x)))))) = Q(P(Q(P(Q(P(x)))))).$$

By Example 5.26 applied to polynomials

$$F(x) = P(Q(x)) \quad \text{and} \quad G(x) = Q(P(x)),$$

we get $P(Q(x)) = Q(P(x))$. Hence $Q(P(x)) = R(P(x))$ and therefore $Q = R$ because P is not constant and for infinitely many y we have $Q(y) = R(y)$. Since this gives $P(Q(x)) = Q(R(x)) = Q(Q(x))$ and $Q(x)$ is nonconstant, we conclude that $P(x) = Q(x)$. ■

Problem 8.56. Find all polynomials $P(x)$, $Q(x)$ with real coefficients such that

$$P(P(x)) = Q(Q(1-x)).$$

Belarusian Mathematical Olympiad 2001

First Solution. Let

$$R(x) = P\left(\frac{1}{2}+x\right) - \frac{1}{2}, \quad S(x) = Q\left(\frac{1}{2}+x\right) - \frac{1}{2}.$$

Then

$$P(P(x)) = R\left(P(x) - \frac{1}{2}\right) + \frac{1}{2} = R\left(R\left(x - \frac{1}{2}\right)\right) + \frac{1}{2},$$

$$Q(Q(x)) = S\left(P(x) - \frac{1}{2}\right) + \frac{1}{2} = S\left(S\left(x - \frac{1}{2}\right)\right) + \frac{1}{2}.$$

Now, the equality $P(P(x)) = Q(Q(1-x))$ is reduced to

$$R\left(R\left(x - \frac{1}{2}\right)\right) = S\left(S\left(\frac{1}{2} - x\right)\right).$$

Thus $R(R(t)) = S(S(-t))$ for each t. It is clear that $R(x)$ and $S(x)$ have the same degree. Let

$$R(x) = a_d x^d + \ldots + a_0, \quad S(x) = b_d x^d + \ldots + b_0.$$

Then

$$R(R(x)) = a_d R(x)^d + a_{d-1} R(x)^{d-1} + \ldots + a_0,$$
$$S(S(-x)) = b_d S(-x)^d + b_{d-1} S(-x)^{d-1} + \ldots + b_0.$$

Examining the leading coefficients, we find that $a_d^{d+1} = (-1)^{d^2} b_d^{d+1}$. If d is odd the left-hand side is positive and the right-hand side is negative, a contradiction. Hence d is even, and we get $a_d^{d+1} = b_d^{d+1}$. Therefore $a_d = b_d$. Now, rewrite the identity $R(R(x)) = S(S(-x))$ as

$$a_d(R(x) - S(-x))(R(x)^{d-1} + \ldots + S(-x)^{d-1})$$
$$= a_{d-1} R(x)^{d-1} + \ldots + a_0 - b_{d-1} S(-x)^{d-1} - \ldots - b_0.$$

As always, $R(x)^{d-1} + \ldots + S(-x)^{d-1}$ is a polynomial of degree $d(d-1)$ and the right-hand side has degree at most $d(d-1)$.
This implies that $R(x) - S(-x)$ is constant, that is, $S(-x) = R(x) + C$. Hence

$$R(R(x)) = S(C + R(x)).$$

If $R(x)$ is not constant, this implies $R(x) = S(C+x)$ (and if $R(x)$ is constant, then $S(x) = R(x)$ is also constant and this still holds). On the other hand $R(x) = S(-x) - C$. Hence

$$S(x + C) + C = S(-x).$$

Putting $x = -\frac{C}{2}$, we deduce that $C = 0$. Therefore $S(x) = S(-x)$. Thus

$$S(x) = R(x) = T(x^2)$$

and

$$P(x) = Q(x) = T\left(\left(x - \frac{1}{2}\right)^2\right) + \frac{1}{2}. \quad \blacksquare$$

Second Solution. We will use long-run behavior lemma.
Since $\deg P(P(x)) = (\deg P(x))^2$ and $\deg Q(Q(1-x)) = (\deg Q(x))^2$, we see that $\deg P(x) = \deg Q(x)$. Let d be the common degree and assume $d > 0$. Let a_d be the leading coefficient of $P(x)$ and b_d the leading coefficient of $Q(x)$. Then we get $a_d^{d+1} = (-1)^d b_d^{d+1}$. As in the previous solution, this implies that d is even and $a_d = b_d$. Now, by using the long-run behavior lemma, we obtain

$$\lim_{x\to\infty} \left(\sqrt[d]{|P(P(x))|} - a|P(x) + b_1|\right) = 0,$$

and

$$\lim_{x\to\infty} \left(\sqrt[d]{|Q(Q(1-x))|} - a|Q(1-x) + b_2|\right) = 0.$$

Hence

$$\lim_{x\to\infty} (|P(x) + b_1| - |Q(1-x)) + b_2|) = 0.$$

Since $P(x)$ and $Q(x)$ have the same (even) degree and leading coefficient, this implies that $P(x) - Q(1-x) = C$, where $C = b_2 - b_1$. Substituting this into the original equation, we obtain that

$$P(P(x)) = Q(P(x) - C).$$

Then $P(x) = Q(x - C)$. Moreover, $P(x) = Q(1-x) + C$. Considering them together, we get

$$P(x) = P(1 - x - C) + C.$$

Thus putting $x = \frac{1-C}{2}$, we find that $C = 0$. Hence

$$P(x) = Q(x), \quad P(x) = P(1-x).$$

From the second equality, we can see that there exist a polynomial $R(x)$ such that

$$P(x) = Q(x) = R\left(\left(x - \frac{1}{2}\right)^2\right). \qquad \blacksquare$$

Problem 8.57. Let k be odd. Let $f_1, \ldots, f_k$ be polynomials with real coefficients such that

$$f_1(f_2(x)) = f_2(f_3(x)) = \ldots = f_k(f_1(x)).$$

Prove that $f_1 = \ldots = f_k$.

Solution. Let $d_i = \deg f_i(x)$.
Then comparing degrees we find $d_1 d_2 = d_2 d_3 = \ldots = d_k d_1$. Hence $d_{i+2} = d_i$, and since k is odd, we conclude that all polynomials $f_i(x)$ are of the same degree, say d. If the leading coefficient of the polynomial f_i is a_i, we find that

$$a_i a_{i+1}^d = a_{i+1} a_{i+2}^d.$$

Thus

$$\frac{a_i}{a_{i+1}} = \left(\frac{a_{i+1}}{a_{i+2}}\right)^d.$$

Iterating this around the cycle, we find

$$\frac{a_i}{a_{i+1}} = \left(\frac{a_i}{a_{i+1}}\right)^{d^k}.$$

Hence $\frac{a_i}{a_{i+1}} = \pm 1$. Now, if the value of -1 ever occurs, then we have d odd, and we find that $\frac{a_i}{a_{i+1}} = -1$ for all i. However, since the product of $\frac{a_1}{a_2} \cdot \ldots \cdot \frac{a_k}{a_1} = 1$ and k is odd, we get a contradiction. So all the leading coefficients are equal. Denote it by a. Now by the long-run behavior lemma, we find that

$$\lim_{x \to \infty} \left(\sqrt[d]{f_{i-1}(f_i(x))} - A \cdot |f_i(x) - b_i|\right) = 0,$$

where $A = \sqrt[d]{a}$. Thus for all i, j, we have

$$\lim_{x \to \infty} (|f_i(x) - b_i| - |f_j(x) - b_j|) = 0.$$

Since the f_i have the same degree and leading coefficient, this implies that

$$f_i(x) - b_i = f_j(x) - b_j.$$

If $d > 1$, then this implies all the f_i have the same coefficient of x^{d-1} and the constants b_i in the long-run behavior lemma are computed from this coefficient (and the leading one). Thus $b_i = b_j$ and $f_i(x) = f_j(x)$ for all x. If $d = 1$, then we can write $f_i(x) = ax + c_i$, and from the original equation, we find that $ac_2 + c_1 = ac_3 + c_2 = \ldots = ac_1 + c_k$. Call this common value B. If $a = -1$, we find $c_i = c_{i+1} + B$. Hence iterating around a cycle we get $c_i = c_i + kB$ and $B = 0$. Thus all the c_i are equal. If $a \neq -1$, we find that $ac_{i+1} + c_i = B$, which we can rewrite as

$$c_i - \frac{B}{a+1} = -a\left(c_{i+1} - \frac{B}{a+1}\right).$$

Hence iterating this around the cycle, we get

$$c_i - \frac{B}{a+1} = (-a)^k \left(c_i - \frac{B}{a+1}\right).$$

Since $a \neq -1$ and k is odd, we conclude that $c_i = \frac{B}{a+1}$ for all i.
Thus $f_1 = \ldots = f_k$. $\blacksquare$

Problem 8.58. Do there exist polynomials $P(x)$ and $Q(x)$ with integer coefficients of degree at least 2018 such that

$$P(Q(x)) - 3Q(P(x)) = 1?$$

Solution. The answer is yes. Assuming that the pair $(P(x), Q(x))$ satisfies the condition of the problem. Then using the substitution $x \mapsto P \circ Q \circ P(x)$, we see that $(P \circ Q \circ P(x), Q \circ P(x))$ also satisfies the condition of the problem. Note that

$$P_0(x) = x^2 + 3x + 1, \quad Q_0(x) = 3x + 3$$

satisfy the condition of the problem. Now, define

$$P_{n+1}(x) = P_n \circ Q_n \circ P_n, \quad Q_{n+1} = Q_n \circ P_n.$$

It is clear that after finitely many steps, the degree of P_n and Q_n will be at least 2018. (In fact, $\deg P_n = 2^{F_{2n}}$ and $\deg Q_n = 2^{F_{2n-1}}$, where F_n denotes the Fibonacci numbers. Hence $\deg P_4(x) > \deg Q_4(x) = 2^{21} > 2018$.) ∎

Problem 8.59. Let $P(x)$ be a nonconstant polynomial with integer coefficients such that for all but finitely many positive integer n, $P(1) + \ldots + P(n)$ divides $nP(n+1)$. Prove that there is a non-negative integer k such that for each positive integer n we have

$$P(n) = \binom{n+k}{n-1} P(1).$$

Solution. Let

$$x_n = \frac{nP(n+1)}{P(1) + \ldots + P(n)}.$$

By the hypotheses, x_n will be an integer for all but finitely many values of n. Suppose $P(x)$ has degree d and leading coefficient a_d. Then we know from the Chapter 3.6, that there is a polynomial $R(x)$ of degree $d+1$, with leading coefficient $\frac{a_d}{d+1}$, and with $R(0) = 0$, such that $R(x) - R(x-1) = P(x)$. Summing this last equation for $x = 1, 2, \ldots, n$, we get

$$P(1) + \ldots + P(n) = R(n) - R(0) = R(n).$$

Note that this implies that $R(x)$ is an integer-valued polynomial.
Since $xP(x+1)$ is a polynomial of degree $d+1$ with leading coefficient a_d, we see that

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} \frac{nP(n+1)}{P(1) + \ldots + P(n)} = \lim_{n\to\infty} \frac{nP(n+1)}{R(n)} = \lim_{n\to\infty} \frac{a_d}{\frac{a_d}{d+1}} = d+1.$$

Since x_n is an integer for all sufficiently large n, we conclude that in fact $x_n = d+1$ for all sufficiently large n. Thus

$$nP(n+1) = (d+1)R(n)$$

for all sufficiently large n. Thus the polynomials $xP(x+1)$ and $(d+1)R(x)$ agree for infinitely many values, hence they are identical. Thus

$$xP(x+1) - xP(x) = (d+1)(R(x) - R(x-1)) = (d+1)P(x),$$

which we can rewrite as

$$\frac{P(x+1)}{P(x)} = \frac{x+d+1}{x}.$$

Multiplying this identity for $x = 1, 2, \ldots, n-1$, we get

$$\frac{P(n)}{P(1)} = \frac{P(n)}{P(n-1)} \cdot \frac{P(n-1)}{P(n-2)} \cdot \ldots \cdot \frac{P(2)}{P(1)} = \frac{n+d-1}{n-1} \cdot \frac{n+d-2}{n-2} \cdot \ldots \cdot \frac{d+1}{1}$$
$$= \frac{(n+d-1)!}{(n-1)!d!} = \binom{n+d-1}{n-1}.$$

Hence $k = d-1$. ∎

Problem 8.60. Find all polynomials $P(x)$ with integer coefficients such that for all positive integers a, b, c that are the side lengths of a right-angled triangle, the numbers $P(a), P(b), P(c)$ are also the side lengths of a right-angled triangle.

First Solution. Since there are right-angles triangles with side lengths $(2n, n^2-1, n^2+1)$, we see that $P(2n) > 0$ for all integers $n \geq 2$. Thus $P(x)$

has positive leading coefficient. Thus after a certain point, $P(x)$ is strictly increasing. Thus for large enough n we will have $P(n^2+1) > P(n^2-1), P(2n)$. Hence $P(n^2+1)$ must be the hypotenuse of the right triangle, and we find that

$$P(n^2+1)^2 = P(2n)^2 + P(n^2-1)^2.$$

Assume now that $\deg P(x) = d$, and let $P(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$ with $a_d \neq 0$. We have

$$P(n^2+1)^2 = a_d^2 n^{4d} + (2da_d^2 + 2a_d a_{d-1})n^{4d-2} + \ldots$$

and

$$P(n^2-1)^2 + P(2n)^2 = a_d^2 n^{4d} + (-2da_d^2 + 2a_d a_{d-1})n^{4d-2} + \ldots + 2^{2d}a_d^2 n^{2d} + \ldots.$$

If $d > 1$, then comparing the coefficients of n^{4d-2}, we get $4da_d^2 = 0$, and a contradiction.
Hence $d = 1$. So $P(x) = a_1 x + a_0$ and the equation

$$P(n^2+1)^2 = P(2n)^2 + P(n^2-1)^2$$

simplifies to $-4a_0 a_1 n + a_0(4a_1 - a_0) = 0$. Hence $a_0 = 0$ and $P(x) = a_1 x$. ■

Second Solution. First, we will establish the following lemma.

Lemma. Let $P(x)$ be a polynomial with $\deg P(x) = d \geq 2$ and positive leading coefficient. Assume that $s < t$. Then $sP(tx) > tP(sx)$ for all sufficiently large x.

Proof. Writing $P(x) = a_d x^d + Q(x)$ with $\deg Q(x) < d$, we have

$$sP(tx) - tP(sx) = a_d ts(t^{d-1} - s^{d-1})x^d + sQ(tx) - tQ(sx).$$

Since $\deg(sQ(tx) - tQ(sx)) < d$, we find that for all sufficiently large x, we have $sP(tx) > tP(sx)$. This completes our proof. □

Now, since $(a, b, c) = (5k, 4k, 3k)$ are side lengths of a right-angled triangle, we find that $P(5k), P(4k), P(3k)$ are the side lengths of a right-angled triangle. By the above lemma, we have for large k

$$3P(5k) > 5P(3k), \quad 4P(5k) > 5P(4k).$$

Hence taking the square and then adding we get

$$25P(5k)^2 > 25(P(3k)^2 + P(4k)^2),$$

that is, $P(5k)^2 > P(3k)^2 + P(4k)^2$. Thus there are no such polynomials with $d \geq 2$. For $d = 1$, writing $P(x) = ax + b$, we find that

$$P(5k)^2 - P(4k)^2 - P(3k)^2 = -4abk - b^2 = 0,$$

hence the only solutions are $P(x) = ax$. ■

Problem 8.61. Find all polynomials P, Q with real coefficients such that

$$P(Q(x)) = P(x)^{2017}.$$

Solution. If $(P(x), Q(x))$ is a solution then $(-P(x), Q(x))$ is also a solution. Hence, without loss of generality, assume that $P(x)$ has positive leading coefficient. Assume that $\deg P(x) = d$ and write

$$P(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0,$$

where $a_d \neq 0$. Since $\sqrt[d]{P(Q(x))} = \sqrt[d]{P(x)^{2017}}$, long-run behavior lemma gives

$$\lim_{x\to\infty}\left(\sqrt[d]{a_d}\left|Q(x) + \frac{a_{d-1}}{da_d}\right| - \sqrt[d]{a_d^{2017}}\left(x + \frac{a_{d-1}}{da_d}\right)^{2017}\right) = 0$$

(where if d is odd, we can drop the absolute value). Hence

$$Q(x) + \frac{a_{d-1}}{da_d} = \pm\sqrt[d]{a_d^{2016}}\left(x + \frac{a_{d-1}}{da_d}\right)^{2017}.$$

Putting $B = \frac{a_{d-1}}{da_d}$, $A = \pm\sqrt[d]{a_d^{2016}}$ (where the minus sign is only allowed for d even), we can write this as

$$Q(x) = A(x+B)^{2017} - B.$$

After plugging $Q(x)$ into the original equation, we find that

$$P(A(x+B)^{2017} - B) = P(x)^{2017}.$$

Then $P(Ax^{2017}-B) = P(x-B)^{2017}$. Let $R(x) = P(x-B) = a_dx^d+a_sx^s+\ldots$. Then $R(Ax^{2017}) = R(x)^{2017}$. Examining the coefficient of the second nonzero term on both sides, we find that the second nonzero monomial on the left-hand side is a_sx^{2017s} and on the right-hand side is $a_d^{2016}a_sx^{2016d+s}$. This contradicts the existence of s. Hence $R(x) = a_dx^d$. That is, $P(x) = a_d(x+B)^d$ and $Q(x) = A(x+B)^{2017} - B$, where $A^d = a_d^{2016}$. ∎

Problem 8.62. Evaluate the sum

$$\sum_{k=1}^{1000} \frac{(2^k-3^1)\cdot\ldots\cdot(2^k-3^{1000})}{(2^k-2^1)\cdot\ldots\cdot(2^k-2^{k-1})(2^k-2^{k+1})\cdot\ldots\cdot(2^k-2^{1000})}.$$

Solution. Let $P(x) = (x-3^1)\cdot\ldots\cdot(x-3^{1000}) - (x-2^1)\cdot\ldots\cdot(x-2^{1000})$. Then $P(x)$ is a polynomial of degree at most 999 and the L.I.F for $P(x)$ at the points $2, 4, \ldots, 2^{1000}$ reads

$$\sum_{k=1}^{1000} \frac{(x-2^1)\cdot\ldots\cdot(x-2^{k-1})(x-2^{k+1})\cdot\ldots\cdot(x-2^{100})(2^k-3^1)\cdot\ldots\cdot(2^k-3^{1000})}{(2^k-2^1)\cdot\ldots\cdot(2^k-2^{k-1})(2^k-2^{k+1})\cdot\ldots\cdot(2^k-2^{1000})}.$$

Hence the requested sum is just the leading coefficient of $P(x)$, which is

$$2^1+\ldots+2^{1000} - (3^1+\ldots+3^{1000}) = 2^{1001} - \frac{3^{1001}+1}{2}.$$ ∎

Problem 8.63. Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$. Prove that

$$\sum_{k=1}^{n} \frac{\prod_{i=1}^{n}(a_k+b_i)}{\prod_{i\neq k}(a_k-a_i)} = \sum_{k=1}^{n} \frac{\prod_{i=1}^{n}(b_k+a_i)}{\prod_{i\neq k}(b_k-b_i)}.$$

Chinese Team Selection Test 2010

Solution. Let $P(x) = (x+a_1)\cdot\ldots\cdot(x+a_n) - (x-b_1)\cdot\ldots\cdot(x-b_n)$. Then

$$P(-a_k) = (-1)^{n+1}\prod_{i=1}^{n}(a_k+b_i), \quad P(b_k) = \prod_{i=1}^{n}(b_k+a_i).$$

Note that $\deg P(x) \leq n-1$. Now, write the L.I.F. once for $-a_1, \ldots, -a_n$ and again for $b_1, \ldots, b_n$. We find that

$$P(x) = (-1)^{n-1}\sum_{k=1}^{n} \frac{\prod_{i\neq k}(x+a_i)}{\prod_{i\neq k}(a_k-a_i)} P(-a_k).$$

On the other hand

$$P(x) = \sum_{k=1}^{n} \frac{\prod_{i\neq k}(x-b_i)}{\prod_{i\neq k}(b_k-b_i)} P(b_k).$$

Now, examining the coefficient of x^{n-1}, we get

$$\sum_{k=1}^{n} \frac{P(b_k)}{\prod_{i\neq k}(b_k-b_i)} = (-1)^{n-1}\sum_{k=1}^{n} \frac{P(-a_k)}{\prod_{i\neq k}(a_k-a_i)}.$$

Substituting the values for $P(b_k)$, $P(-a_k)$, we find that

$$\sum_{k=1}^{n} \frac{\prod_{i=1}^{n}(a_k+b_i)}{\prod_{i\neq k}(a_k-a_i)} = \sum_{k=1}^{n} \frac{\prod_{i=1}^{n}(b_k+a_i)}{\prod_{i\neq k}(b_k-b_i)} = \sum_{k=1}^{n}(a_k+b_k). \qquad \blacksquare$$

Problem 8.64. Let

$$b_i = (a_i-a_1)\cdot\ldots\cdot(a_i-a_{i-1})(a_i-a_{i+1})\cdot\ldots\cdot(a_i-a_n).$$

Prove that $(n-1)!$ divides $\operatorname{lcm}(b_1,\ldots,b_n)$.

Fedor Petrov - Saint Petersburg Mathematical Olympiad 2005

Solution. Let $P(x) = (x-1)\cdot\ldots\cdot(x-n+1)$. Write the L.I.F. for $P(x)$ and $a_1,\ldots,a_n$. Therefore

$$P(x) = \sum_{i=1}^{n} \frac{Q_i(x)}{Q_i(a_i)} P(a_i).$$

Comparing the leading coefficients on both sides, we get

$$1 = \sum_{i=1}^{n} \frac{P(a_i)}{Q_i(a_i)} = \sum_{i=1}^{n} \frac{P(a_i)}{b_i}.$$

Hence $\operatorname{lcm}(b_1,\ldots,b_n) = c_1P(a_1)+\ldots+c_nP(a_n)$ for positive integers

$$c_i = \frac{\operatorname{lcm}(b_1,b_2,\ldots,b_n)}{b_i}.$$

Moreover, for each integer m, we have that $P(m)$ is a product of $n-1$ consecutive integers, hence it is divisible by $(n-1)!$. Thus $(n-1)!$ divides $P(a_1),\ldots,P(a_n)$. Thus $(n-1)!$ divides $c_1P(a_1)+\ldots+c_nP(a_n)$, and so it divides $\operatorname{lcm}(b_1,\ldots,b_n)$. $\blacksquare$

Problem 8.65. Let $P(x)$ be a nonconstant polynomial with real coefficients. For all positive real numbers M, prove that there is a positive integer m such that for any monic polynomial $Q(x)$ of degree greater than or equal to m, the total number of integer solutions of the inequality $|P(Q(x))| \leq M$ does not exceed $\deg Q(x)$.

Navid Safaei - Iranian Mathematical Olympiad 2018

Solution. It is clear that the set of solutions to the inequality $|P(x)| \leq M$ is a subset of an interval of the form $(-a,a)$ for some positive real number a. Now, let $\deg Q(x) = d \geq m$. Consider the integers $x_0 < x_1 < \ldots < x_d$. By the L.I.F, we find that

$$Q(x) = \sum_{i=0}^{d} Q(x_i) \prod_{i\neq j} \frac{x-x_j}{x_i-x_j}.$$

Since $Q(x)$ is monic, we have

$$1 = \sum_{i=0}^{d} Q(x_i) \prod_{i\neq j} \frac{1}{x_i-x_j}.$$

The right-hand side is less than or equal to

$$\max_i |Q(x_i)| \cdot \sum_{i=0}^{d} \frac{1}{i!(d-i)!} = \frac{2^d}{d!} \cdot \max_i |Q(x_i)|.$$

Hence

$$\max_i |Q(x_i)| \geq \frac{d!}{2^d} \geq \frac{m!}{2^m}.$$

Now, choose m such that $(-a,a) \subseteq \left(-\frac{m!}{2^m}, \frac{m!}{2^m}\right)$. We deduce that, from any $d+1$ integers, at least one of them satisfies the inequality

$$|Q(x)| > \frac{m!}{2^m},$$

but all the integer solutions of the inequality $|P(Q(x))| \leq M$ must satisfy the inequality.

$$|Q(x)| \leq \frac{m!}{2^m}.$$

Hence there are at most d integer solutions to $|P(Q(x))| \leq M$. ∎

Problem 8.66. Find all distinct positive integers $a_1, \ldots, a_n$ such that for each positive integer $k = 1, \ldots, n$ the number $a_1 \cdot \ldots \cdot a_n$ divides $(k+a_1) \cdot \ldots \cdot (k+a_n)$.

Solution. Let $P(x) = (x+a_1) \cdot \ldots \cdot (x+a_n)$. Then $P(0), \ldots, P(n)$ are divisible by $a_1 \cdot \ldots \cdot a_n$. Writing the L.I.F. for $P(x)$ and $0, 1, \ldots, n$ and comparing the leading coefficients, we find that

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} P(i) = n!.$$

Since $P(0), \ldots, P(n)$ are divisible by $a_1 \cdot \ldots \cdot a_n$, we find that $a_1 \cdot \ldots \cdot a_n$ divides the left-hand side and hence divides $n!$. Therefore $a_1 \cdot \ldots \cdot a_n \leq n!$. But $a_1, \ldots, a_n$ are distinct positive integers, hence $a_1 \cdot \ldots \cdot a_n \geq 1 \cdot 2 \cdot \ldots \cdot n = n!$, which means that $\{a_1, \ldots, a_n\} = \{1, 2, \ldots, n\}$. ∎

Problem 8.67. Let d be a positive integer. Find the largest value of the constant $C(d)$ such that for any polynomial $P(x) = a_0 + \ldots + a_d x^d$ of degree d with complex coefficients and every permutation $(x_0, \ldots, x_d)$ of $(0, 1, \ldots, d)$, we have

$$\sum_{k=0}^{d} |P(x_k) - P(x_{k+1})| \geq C|a_d|,$$

where $x_{d+1} = x_0$.

Chinese Team Selection Test 2010

Solution. First let's simplify the problem statement. The problem allows $P(x)$ to have complex coefficients. Since we can multiply $P(x)$ by a constant without changing the constant C, we can assume a_d is real. Also, we can let

$Q(x)$ be the real part of $P(x)$, which will therefore be a polynomial with the same degree and leading coefficient. If we find a constant C that works for $Q(x)$, then we will have

$$\sum_{k=0}^{d} |P(x_k) - P(x_{k+1})| \geq \sum_{k=0}^{d} |Q(x_k) - Q(x_{k+1})| \geq C|a_d|.$$

so this same constant will also work for $P(x)$. Thus we may assume $P(x)$ has real coefficients.

Let $m = \min\limits_{0 \leq k \leq d} P(k) = P(x_i)$ and $M = \max\limits_{0 \leq k \leq d} P(k) = P(x_j)$ be the minimum and maximum values of $P(x_k)$. Then (interpretting sums as being cyclic), the Triangle Inequality gives

$$\sum_{k=i}^{j-1} |P(x_k) - P(x_{k+1})| \geq P(x_j) - P(x_i) = M - m,$$

and

$$\sum_{k=j}^{i-1} |P(x_k) - P(x_{k+1})| \geq P(x_j) - P(x_i) = M - m,$$

with equality if and only if

$$P(x_i) \leq P(x_{i+1}) \leq \cdots \leq P(x_j) \quad \text{and} \quad P(x_j) \geq P(x_{j+1}) \geq \cdots \geq P(x_i).$$

Thus the minimum over all permutations of the sum $\sum\limits_{k=0}^{d} |P(x_k) - P(x_{k+1})|$ is just $2(M - m)$.

Thus the problem is reduced to finding the largest constant $C = C(d)$, such that for any polynomial $P(x)$ of degree d with real coefficients and leading coefficient a_d, $m = \min_{0 \leq k \leq d} P(k)$, and $M = \max_{0 \leq k \leq d} P(k)$, we have

$$2(M - m) \geq C|a_d|.$$

Now we further simplify by invoking the L.I.F.. Instead of choosing a polynomial $P(x)$, we choose the values $P(0), P(1), \ldots, P(d) \in [m, M]$. Then we

use the L.I.F. to build the unique polynomial of degree at most d with these values

$$P(x) = \sum_{k=0}^{d} \frac{(-1)^{d-k}}{x-k} \binom{d}{k} \binom{x}{d} P(k).$$

Since the leading coefficient of this polynomial $P(x)$ is given by

$$a_d = \frac{1}{d!} \sum_{k=0}^{d} (-1)^{d-k} \binom{d}{k} P(k),$$

we see that we just need the largest C such that

$$2(M-m) \geq \frac{C}{d!} \sum_{k=0}^{d} (-1)^{d-k} \binom{d}{k} P(k).$$

Since the left-hand side is linear in the values $P(k)$ and we are free to choose any number in $[m, M]$ for these values, finding the maximum of the left-hand side is easy: we just take M for $d-k$ even, and m for $d-k$ odd. This gives

$$2(M-m) \geq \frac{C}{d!} \left(M \sum_{d-k \text{ even}} \binom{d}{k} - m \sum_{d-k \text{ odd}} \binom{d}{k} \right) = \frac{C}{d!} (M-m) 2^{d-1}.$$

Hence the largest constant is $C = \frac{d!}{2^{d-2}}$. ∎

Problem 8.68. Let $d > 1$ be an odd integer and let $P(x)$ be a polynomial of degree d. Suppose that $P(k) = 2^k$ for $k = 0, 1, 2, \ldots, d$. Prove that $P(x)$ is divisible by $x+1$, but it is not divisible by $(x+1)^2$.

Navid Safaei

First Solution. We saw in the text that the polynomial $P(x)$ can be written as

$$P(x) = \binom{x}{0} + \binom{x}{1} + \ldots + \binom{x}{d}.$$

Using the Pascal's triangle recursion

$$\binom{x+1}{k} = \binom{x}{k-1} + \binom{x}{k}$$

and the easy identity

$$\binom{x+1}{k} = \frac{x+1}{k} \binom{x}{k-1},$$

we see that since d is odd, we have

$$\begin{aligned} P(x) &= \binom{x+1}{1} + \binom{x+1}{3} + \ldots + \binom{x+1}{d} \\ &= (x+1) \left(1 + \frac{1}{3} \binom{x}{2} + \ldots + \frac{1}{d} \binom{x}{d-1} \right). \end{aligned}$$

Thus we see that $P(x)$ is divisible by $x+1$. Calling the second factor above $Q(x)$, to show that $(x+1)^2$ does not divide $P(x)$ it suffices to show that $Q(-1) \neq 0$. Since

$$\binom{-1}{2m} = \frac{(-1)(-2) \cdot \ldots \cdot (-2m)}{(2m)!} = 1,$$

we see that

$$Q(-1) = 1 + \frac{1}{3} + \ldots + \frac{1}{d} \neq 0,$$

and we are done. ∎

Second Solution. Since we have seen that

$$P(x) = \binom{x}{0} + \binom{x}{1} + \ldots + \binom{x}{d},$$

the leading coefficient of $P(x)$ is equal to $\frac{1}{d!}$.
Consider the polynomial $Q(x) = P(x+1) - 2P(x)$. It is easy to deduce that $\deg Q(x) = d$, $Q(x)$ has leading coefficient $\frac{1}{d!}$, and

$$Q(0) = Q(1) = \ldots = Q(d-1) = 0.$$

Therefore

$$Q(x) = P(x+1) - 2P(x) = -\frac{1}{d!}x\,(x-1)\cdot\ldots\cdot(x-(d-1))\,.$$

Note that since d is odd,

$$Q(d-1-x) = (-1)^d Q(x) = -Q(x).$$

Thus

$$Q(-1) = -Q(d) = \frac{1}{d!}\cdot d! = 1.$$

Hence

$$1 = Q(-1) = P\,(0) - 2P\,(-1) = 1 - 2P\,(-1)\,.$$

Thus $P(-1) = 0$ as desired.
From the fact that $Q(d-1-x) = -Q(x)$, we find that

$$Q'(d-1-x) = Q'(x).$$

Hence $Q'(d) = Q'(-1) = P'(0) - 2P'(-1)$. Since we can compute that

$$Q'\,(x) = -\frac{1}{d!}x\,(x-1)\cdot\ldots\cdot(x-(d-1))\left(\frac{1}{x}+\cdots+\frac{1}{x-d+1}\right),$$

we get

$$Q'(d) = -\left(1+\frac{1}{2}+\ldots+\frac{1}{d}\right).$$

On the other hand, $P'(0)$ is equal to the coefficient of x in the expression,

$$\binom{x}{0}+\binom{x}{1}+\ldots+\binom{x}{d},$$

which gives

$$P'(0) = 1-\frac{1}{2}+\frac{1}{3}-\ldots+\frac{1}{d}.$$

Thus we get

$$P'(-1) = \frac{1}{2}(P'(0) - Q'(d)) = 1+\frac{1}{3}+\ldots+\frac{1}{d} \neq 0,$$

and we are done. ∎

Problem 8.69. Let $d > 1$ be an odd integer and $P(x)$ be a polynomial of degree d. Suppose that $P(k) = 2^k$ for $k = 0, 1, 2, \ldots, d$. Prove that there exist at most finitely many integers x such that $P(k)$ is some power of 2.

Taiwanese Team Selection Test 2018

Solution. By previous problem, we find that $d!P(x) = (x+1)Q(x)$ for some monic polynomial $Q(x)$ with integer coefficients satisfying $Q(-1) \neq 0$.
Since $d > 1$ is odd, we have $d \geq 3$. Therefore there is some constant M, such that for $x > M$, we have $P(x) > (x+1)^2$. Since $P(x)$ has odd degree and positive leading coefficient, we will only have $P(m) > 0$ for finitely many negative integers m. Thus it suffices to show that there are only finitely integers $m > M$, for which $P(m)$ is a power of 2.
Suppose that $m > M$ is such an integer with $P(m) = 2^n$. Write $m+1 = 2^a \cdot b$ with b odd. Since $(m+1) \mid d!P(m) = d! \cdot 2^n$, we see that $b \mid d!$. Further since $m > M$, we have $P(m) = 2^n > (m+1)^2 \geq 2^{2a}$, hence $n > 2a$. Thus it follows that $(m+1)^2 = 2^{2a} \cdot b^2$ divides $(d!)^2 P(m) = d!(m+1)Q(m)$. Hence $m+1 \mid d!Q(m)$. However, since Q is a polynomial with integer coefficents we also know that $m+1 \mid Q(m) - Q(-1)$. Thus $m+1 \mid d!Q(-1)$. Since $Q(-1) \neq 0$, there are only finitely many integers $m+1$ for which this can occur. ∎

Problem 8.70. A polynomial $P(x)$ of degree d satisfies $P(k) = 2^k$ for all integers $k = 0, 1, \ldots, d$.
Prove that $P(k) \geq 2^{k-1}$ for all integers $k = d+1, d+2, \ldots, 2d+1$.

Solution. We have seen that

$$P(x) = \binom{x}{0}+\binom{x}{1}+\ldots+\binom{x}{d}.$$

Therefore by the symmetry of the binomial coefficients we also have

$$P(x) = \binom{x}{x-d}+\binom{x}{x-d+1}+\ldots+\binom{x}{x}.$$

Adding these we get

$$2P(x) = \binom{x}{0} + \binom{x}{1} + \ldots + \binom{x}{d} + \binom{x}{x-d} + \binom{x}{x-d+1} + \ldots + \binom{x}{x}.$$

If $k = d+1, d+2, \ldots, 2d+1$, then for $x = k$ we get

$$2P(k) \geq \sum_{j=0}^{k} \binom{k}{j} = 2^k,$$

since the right-hand side has every term in the sum at least once. ∎

Remark. Based on the above proof, we see that for $k = 2d+1$, we have equality

$$P(2d+1) = 2^{2d}.$$

Problem 8.71. Let $P(x)$ be a polynomial with complex coefficients of degree d such that $P(0) = 0$. Show that for each complex number α, $|\alpha| < 1$, there are complex numbers $z_1, \ldots, z_{d+2}$ on the unit circle such that

$$P(\alpha) = \sum_{i=1}^{d+2} P(z_i).$$

American Mathematical Monthly, Problem 11432

Solution. We will prove the stronger statement that there exist $d+2$ numbers on the unit circle such that for any α with $|\alpha| < 1$, there are complex numbers $z_1, \ldots, z_{d+2}$ on the unit circle such that for $i = 1, \ldots, d$ we have

$$\sum_{i=1}^{d+2} z_i^k = \alpha^k.$$

To derive the problem statement from our statement, simply multiply these identities by the coefficients of $P(x)$ and sum.

We will find the numbers $z_1, \ldots, z_{d+2}$ by finding the polynomial for which they are the roots. Accordingly, write

$$Q(z) = \prod_{i=1}^{d+2} (z - z_i) = \sum_{j=0}^{d+2} (-1)^j \sigma_j z^{d+2-j}.$$

The desired condition on the roots is that the power sums $S_1, \ldots, S_d$ are the powers of α, $S_k = \alpha^k$. Hence we want $\sigma_1 = S_1 = \alpha$ and from Newton's Identities

$$S_k - S_{k-1}\sigma_1 + \ldots + (-1)^{k-1} S_1 \sigma_{k-1} + k(-1)^k \sigma_k = 0,$$

for $k = 2, \ldots, d$, we see that $\sigma_2 = \cdots = \sigma_d = 0$.
Thus we have

$$Q(z) = z^{d+2} - \alpha z^{d+1} + Az + B$$

for some complex numbers A, B. Now we need to further arrange that the roots of $Q(z)$ lie on the unit circle. This forces $|B| = 1$, and for simplicity we take $B = 1$. Then Vieta's formulas say that

$$A = -\sum_{i=1}^{d+2} \frac{1}{z_i} = -\sum_{i=1}^{d+2} \overline{z_i} = -\overline{\alpha}.$$

Hence we must have

$$Q(z) = z^{d+2} - \alpha z^{d+1} - \overline{\alpha} z + 1.$$

We still need to prove that the roots of $Q(z)$ actually lie on the unit circle. If z is a root of $Q(z)$, we must have

$$z^{d+1} = \frac{\overline{\alpha} z - 1}{z - \alpha}.$$

Let

$$f(z) = \frac{\overline{\alpha} z - 1}{z - \alpha}$$

be the right-hand side, and observe that

$$|f(z)|^2 - 1 = \frac{(1-|\alpha|^2)(1-|z|^2)}{|z-\alpha|^2}.$$

Therefore if $|z| < 1$, we have

$$|z|^{d+1} < 1 < |f(z)|,$$

and a contradiction. If $|z| > 1$, the inequalities both reverse and we still get a contradiction.
Therefore as desired, all roots of $Q(z)$ lie on the unit circle. ■

Problem 8.72. Let a, b, c be integers such that $a+b+c = 0$. Prove that:

(i) $(a^2b^2 + c^2b^2 + a^2c^2) \mid (a^5b^5 + c^5b^5 + a^5c^5)$;

(ii) If $n-1$ is divisible by 3, then $(a^2+b^2+c^2) \mid (a^n+b^n+c^n)$;

(iii) if $n-2$ is divisible by 3, then $(a^2b^2+c^2b^2+a^2c^2) \mid (a^nb^n+c^nb^n+c^na^n)$.

Kvant, Problem M2023

Solution. Let

$$S_n = a^n + b^n + c^n, \quad T_n = a^nb^n + c^nb^n + c^na^n$$

be the power sums and define

$$P_n = \frac{1}{2}\left[a^n + b^n + (-a-b)^n\right] = \frac{1}{2}S_n.$$

Then we see that $P_1 = 0$, $P_2 = -(a^2+ab+b^2)$, and $P_3 = -\frac{3ab(a+b)}{2}$ are all integers (since at least one of a, b, and $a+b$ must be even). From Newton's Identities, we get

$$P_{n+3} = (a^2+ab+b^2)P_{n+1} + ab(a+b)P_n.$$

Hence we conclude that P_n is an integer for all n. Furthermore, since P_1 and P_2 are multiples of a^2+ab+b^2 and Newton's Identities give

$$P_{n+3} \equiv ab(a+b)P_n \pmod{a^2+ab+b^2},$$

we conclude that P_n is divisible by a^2+ab+b^2 if n is not divisible by 3. For $n = 3m+1$, we get

$$P_{3m+4} = (a^2+ab+b^2)P_{3m+2} + ab(a+b)P_{3m+1}.$$

Since P_{3m+2} is divisible by a^2+ab+b^2, we find that

$$P_{3m+4} \equiv ab(a+b)P_{3m+1} \pmod{(a^2+ab+b^2)^2}.$$

Since $P_1 = 0$ is divisible by $(a^2+ab+b^2)^2$, we conclude that P_n is divisible by $(a^2+ab+b^2)^2$ if n is 1 modulo 3.
Now we apply these results to our problem. If n not a multiple of 3, then we have seen that

$$\frac{S_2}{2} = P_2 \mid P_n = \frac{S_n}{2},$$

and hence $S_2 \mid S_n$, which is more than was asked in (ii). Similarly, if n is 1 modulo 3, then we have seen that

$$(a^2+ab+b^2)^2 \mid P_n = \frac{S_n}{2},$$

Hence $2(a^2+ab+b^2)^2 \mid S_n$. Also note that $P_4 = (a^2+ab+b^2)^2$, so

$$S_4 = 2(a^2+ab+b^2)^2.$$

Now note that $2T_n = S_n^2 - S_{2n}$, hence in particular, $T_2 = (a^2+ab+b^2)^2$. If $n = 3m+2$, then $S_2 = 2(a^2+ab+b^2)$ divides S_{3m+2}, so $2(a^2+ab+b^2)^2$ divides S_{3m+2}^2. Since $2n = 6m+4$ is 1 modulo 3, we also have that $2(a^2+ab+b^2)^2$ divides S_{6m+4}. Hence $2(a^2+ab+b^2)^2 = 2T_2$ divides $S_{3m+2}^2 - S_{6m+4} = 2T_{3m+2}$, and thus T_2 divides T_{3m+2} This is (iii) and (i) is a special case. ■

Remark. The following problem is from Kvant M2173, and was proposed for USA TST 2015:
Let $p > 3$ be a prime number such that a^2+ab+b^2 is divisible by p. Prove that $(a+b)^p - a^p - b^p$ is divisible by p^3.

Problem 8.73. Let $x_1, \ldots, x_n \in \mathbb{Z}$ satisfy $\gcd(x_1, \ldots, x_n) = 1$. Define $s_k = x_1^k + \ldots + x_n^k$. Prove that

$$\gcd(s_1, \ldots, s_n) \mid \operatorname{lcm}(1, 2, \ldots, n).$$

Komal

Solution. Let p be a prime dividing $\gcd(s_1, \ldots, s_n)$ and let

$$v_p(\gcd(s_1, \ldots, s_n)) = t.$$

We will prove that $p^t \leq n$. This will solve the problem since it proves that $p^t \mid \operatorname{lcm}(1, 2, \ldots, n)$. Let

$$P(x) = (x - x_1) \cdot \ldots \cdot (x - x_n) = x^n - \sigma_1 x^{n-1} + \ldots + (-1)^n \sigma_n.$$

Then

$$S_{n+r} = \sigma_1 S_{n+r-1} - \sigma_2 S_{n+r-2} + \ldots + (-1)^{n-1} \sigma_n S_r,$$

which implies that S_k is divisible by p^t for each k. Now take $k = tp^{t-1}(p-1)$. Since $\varphi(p^t) = p^{t-1}(p-1)$, the general form of Fermat's Little Theorem implies that if $\gcd(a, p) = 1$, then $a^k \equiv 1 \pmod{p^t}$. Further, since $k \geq t$, if $p \mid a$, then $p^t \mid a^k$ and hence $a^k \equiv 0 \pmod{p^t}$. Thus ${x_1}^k + \ldots + {x_n}^k \equiv s \pmod{p^t}$, where s is the number of $x_1, \ldots, x_n$ which are relatively prime to p. Since $\gcd(x_1, \ldots, x_n) = 1$, we have $1 \leq s \leq n$. However, we have already seen that S_k is a multiple of p^t, hence $p^t \mid s$. Thus $n \geq s \geq p^t$. ∎

Problem 8.74. Let $x_1, \ldots, x_{1000}$ be integers such that

$$\sum_{i=1}^{1000} x_i^k \equiv 0 \pmod{2017} \quad \text{for all} \quad k = 1, 2, \ldots, 672.$$

Prove that $2017 \mid x_i$ for all $i = 1, 2, \ldots, 1000$.

Japanese Mathematical Olympiad 2017

Solution. Let S_k and σ_k be the power sums and elementary symmetric polynomials in $x_1, \ldots, x_{1000}$. The statement of the problem implies that

$$S_1 \equiv \ldots \equiv S_{672} \equiv 0 \pmod{2017}.$$

First, we prove that $\sigma_1 \equiv \ldots \equiv \sigma_{672} \equiv 0 \pmod{2017}$. We proceed the proof by induction on k. For $k = 1$, since $\sigma_1 = S_1$, we are done. Assume that the statement holds for all positive integer less than k. Then since $k \leq 672 < 1000$, by Newton's Identities we find that

$$(-1)^{k+1} k\sigma_k = S_k - \sigma_1 S_{k-1} + \sigma_2 S_{k-2} + \ldots + (-1)^k S_1 \sigma_{k-1}.$$

The right-hand side is divisible by 2017, hence 2017 divides $k\sigma_k$.
Since $\gcd(k, 2017) = 1$, σ_k is divisible by 2017. This completes our proof.
Now, use Newton's Identities for S_{1000+r}, which reads

$$S_{1000+r} = \sigma_1 S_{999+r} - \sigma_2 S_{998+r} + \ldots + (-1)^{n-1} \sigma_{1000} S_r.$$

For $1 \leq r \leq 344$, we can write this as

$$S_{1000+r} = \sum_{i=0}^{328} (-1)^{i+1} \sigma_{1000-i} S_{r+i} + \sum_{i=329}^{999} (-1)^{i+1} \sigma_{1000-i} S_{r+i}.$$

In the first sum S_{r+i} is divisible by 2017 since $i + r \leq 672$. In the second sum σ_{1000-i} is divisible by 2017. Therefore $S_{1001}, \ldots, S_{1344}$ are divisible by 2017. Finally,

$$S_{2016} = \sum_{i=0}^{328} (-1)^{i+1} \sigma_{1000-i} S_{1016+i} + \sum_{i=329}^{999} (-1)^{i+1} \sigma_{1000-i} S_{1016+i}.$$

Again, the first and second sums are divisible by 2017.
Let r be the number of $x_1, \ldots, x_{1000}$ which are not divisible by 2017. If 2017 does not divide a, then Fermat's Little Theorem implies that $a^{2016} \equiv 1 \pmod{2017}$. If 2017 divides a, then of course $a^{2016} \equiv 0 \pmod{2017}$. Hence $S_{2016} \equiv r \pmod{2017}$. The calculation above shows that r must be divisible by 2017, but it is at most 1000. Hence we must have $r = 0$, which says that all of $x_1, \ldots, x_{1000}$ are divisible by 2017. ∎

Remark. Assume that g is a primitive root modulo 2017. Setting

$$x_j \equiv g^{3(j-1)} \pmod{2017}, \quad j = 1, \ldots, 672$$

and $x_j = 0$, $673 \leq j \leq 1000$, we can compute that for each $k = 1, 2, \ldots, 671$, then

$$\sum_{i=1}^{1000} x_i^k \equiv 0 \pmod{2017}.$$

This shows that 672 is the best bound for k.

Problem 8.75. Let n be an integer not divisible by 3. Find all integer solutions of the equation

$$(a^2 - bc)^n + (b^2 - ac)^n + (c^2 - ab)^n = 1.$$

H. Van Der Berg - Mathematical Reflections, Problem O52

First Solution. Let

$$P(a, b, c) = (a^2 - bc)^n + (b^2 - ac)^n + (c^2 - ab)^n.$$

We first prove that for each n not divisible by 3, $P(a, b, c)$ is divisible by $a^2 + b^2 + c^2 - ab - ac - bc$. For $n = 1$ it is obvious. For $n = 2$,

$$(a^2 - bc)^2 + (b^2 - ac)^2 + (c^2 - ab)^2 = (a^2 + b^2 + c^2)^2 - (ab + ac + bc)^2,$$

which is clearly a multiple of $a^2 + b^2 + c^2 - ab - ac - bc$. Now define

$$x = a^2 - bc, \quad y = b^2 - ac, \quad z = c^2 - ab.$$

Then

$$x^2 - yz = a(a^3 + b^3 + c^3 - 3abc) = a(a + b + c)(a^2 + b^2 + c^2 - ab - ac - bc).$$

By the same argument, $y^2 - xz$ and $z^2 - xy$ are divisible by

$$a^2 + b^2 + c^2 - ab - ac - bc.$$

Since

$$x^{n+3} + y^{n+3} + z^{n+3} = (x^2 - yz)x^{n+1} + (y^2 - xz)y^{n+1} + (z^2 - yx)x^{n+1} + xyz(x^n + y^n + z^n),$$

we see that if $x^n + y^n + z^n$ is a multiple of $a^2 + b^2 + c^2 - ab - ac - bc$, then so is $x^{n+3} + y^{n+3} + z^{n+3}$. Iterating this proves the claim.
Now we turn to the problem. Since

$$a^2 + b^2 + c^2 - ab - ac - bc = \frac{1}{2}\left[(a - b)^2 + (b - c)^2 + (c - a)^2\right] \geq 0,$$

divides $P(a, b, c)$, any solution to $P(a, b, c) = 1$ must have

$$a^2 + b^2 + c^2 - ab - ac - bc = 1.$$

Thus two of a, b, c must be equal and the third must differ from them by 1. Since $P(a, b, c) = P(-a, -b, -c)$, we may assume the third value is one more. Thus we need to look for integer solutions to

$$1 = P(k, k, k + 1) = (2k + 1)^n + 2(-k)^n.$$

If $n = 1$, this always holds and we get the solutions $(a, b, c) = (k, k, k \pm 1)$ and its permutations. If n is even, then both terms on the right-hand side are nonnegative, and we see that the only solutions is $k = 0$. This gives $(a, b, c) = (0, 0, \pm 1)$ and its permutations. If $n > 1$ is odd, then the equation becomes $(2k + 1)^n = 2k^n + 1$. It is easy to check that $k = 0, -1$ are solutions. For $k \geq 1$, we have $(2k + 1)^n > 2k^n + 1$, so no solutions. For $k \leq -2$, we let $k = -m$ and write the equation as $1 + (2m - 1)^n = 2m^n$. We have $2m - 1 \geq \frac{3}{2}m$, hence $(2m - 1)^n \geq \frac{27}{8}m^n > 2m^n$, and again we get no solutions. Hence for $n > 1$ odd, the solutions are $(a, b, c) = (0, 0, \pm 1)$, $(1, 1, 0)$, $(-1, -1, 0)$, and their permutations. ■

Second Solution. Let $S_n = (a^2 - bc)^n + (b^2 - ac)^n + (c^2 - ab)^n$ and write

$$(x - a^2 + bc)(x - b^2 + ca)(x - c^2 + ab) = x^3 - px^2 + qx - r.$$

Then we compute $S_1 = p = a^2 + b^2 + c^2 - ab - bc - ca$ and

$$q = -(ab + bc + ca)(a^2 + b^2 + c^2 - ab - bc - ca).$$

Since Newton's Identities give $S_2 = p^2 - 2q$, we see that S_2 is a multiple of $a^2 + b^2 + c^2 - ab - bc - ca$. From the Newton's Identity recursion

$$S_{n+3} = pS_{n+2} - qS_{n+1} + rS_n$$

and these initial values, we see that S_n is a multiple of $a^2+b^2+c^2-ab-bc-ca$ if n is not a multiple of 3. Thus as in the previous solution, we have reduced to looking at the cases where $a^2 + b^2 + c^2 - ab - bc - ca = 1$. ■

Problem 8.76. Let $r > 0$ and $r = r^{\frac{2}{3}} + 1$. Prove that there exists a positive integer N such that

$$4^{100} \left| N - r^{300} \right| < 1.$$

Solution. Consider the polynomial $P(x) = x^3 - x^2 - 1$. For $x \leq 1$, we have $x^2(x-1) < 1$ hence no roots of $P(x)$. For $x > 1$, $x^2(x-1)$ is increasing. Hence $P(x)$ has only one real root r_1 and the other two roots r_2, r_3 are conjugate. Now turning to our problem, we see that $r = r_1^3$. Since the power sums $S_k = r_1^k + r_2^k + r_3^k$ satisfy $S_0 = 3$, $S_1 = S_2 = 1$, and $S_n = S_{n-1} + S_{n-3}$. We see that $N = S_{900} = r_1^{900} + r_2^{900} + r_3^{900}$ is a positive integer. It remains to prove that

$$\left| N - r^{300} \right| = \left| N - r_1^{900} \right| = \left| r_2^{900} + r_3^{900} \right| < 4^{-100}.$$

Observe that $r_2^{900} + r_3^{900} = 2\mathrm{Re}(r_2^{900}) \leq 2|r_2|^{900}$. Finally since

$$P(\sqrt{2}) = 2\sqrt{2} - 3 < 0,$$

we find that $r_1 > \sqrt{2}$. Since $r_1 r_2 r_3 = r_1 |r_2|^2 = 1$, we get $|r_2|^2 = \frac{1}{r_1} < 2^{-\frac{1}{2}}$. Hence

$$2|r_2|^{900} < 2^{-224} < 2^{-200} = 4^{-100}.$$ ■

Problem 8.77. Find all integers n such that for any positive real numbers a, b, c, x, y, z such that

$$\max(a, b, c, x, y, z) = a, \quad a + b + c = x + y + z, \quad abc = xyz,$$

the inequality $a^n + b^n + c^n \geq x^n + y^n + z^n$ holds.

Chinese Team Selection Test 2018

Solution. Plugging $t = a$ into the equation

$$(t - x)(t - y)(t - z) - (t - a)(t - b)(t - c) = (xy + yz + zx - ab - bc - ca)t,$$

we find that $xy + yz + zx > ab + ac + bc$. Define

$$T_n = a^n + b^n + c^n - x^n - y^n - z^n,$$

it follows that

$$\begin{aligned} &T_{n+3} - (x + y + z)T_{n+2} + (xy + yz + zx)T_{n+1} - xyzT_n \\ &= (xy + yz + zx - ab - ac - bc)(a^{n+1} + b^{n+1} + c^{n+1}) > 0. \end{aligned}$$

Rewrite this inequality as

$$T_{n+3} - (x + y)T_{n+2} + xyT_{n+1} > z(T_{n+2} - (x + y)T_{n+1} + xyT_n).$$

We compute that $T_0 = T_1 = 0$, and

$$\begin{aligned} T_2 &= a^2 + b^2 + c^2 - x^2 - y^2 - z^2 \\ &= (a + b + c)^2 - (x + y + z)^2 - 2(ab + ac + bc - xy - yz - zx) \\ &= -2(ab + ac + bc - xy - yz - zx) > 0. \end{aligned}$$

Hence

$$T_2 - (x + y)T_1 + xyT_0 = T_2 > 0.$$

Thus the inequality above implies that for each $n \geq 0$, we have

$$T_{n+2} - (x + y)T_{n+1} + xyT_n > 0.$$

Write this as

$$T_{n+2} - xT_{n+1} > y(T_{n+1} - xT_n).$$

Since $T_2 > 0$ we find that $T_2 - xT_1 = T_2 > 0$. Thus the previous inequality implies that $T_{n+2} - xT_{n+1} > 0$ for all $n > 0$. Iterating this argument one more time gives $T_{n+2} > 0$ for all $n \geq 0$. Hence $T_n \geq 0$ for all $n \geq 0$. Thus the inequality holds for nonnegative n.
Now, define $U_m = T_{-m}$. In this case,

$$\frac{1}{xy} + \frac{1}{yz} + \frac{1}{xz} = \frac{1}{ab} + \frac{1}{ac} + \frac{1}{bc}, \quad \frac{1}{xyz} = \frac{1}{abc},$$

and

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} > \frac{1}{a} + \frac{1}{b} + \frac{1}{c}.$$

Furthermore,

$$U_{m+3} - \left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c}\right) U_{m+2} + \left(\frac{1}{ab} + \frac{1}{ac} + \frac{1}{bc}\right) U_{m+1} - \frac{U_m}{abc}$$
$$= \left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - \frac{1}{x} - \frac{1}{y} - \frac{1}{z}\right)(x^{-m-2} + y^{-m-2} + z^{-m-2}) < 0.$$

In this case we compute $U_0 = U_{-1} = 0$, and $U_1 < 0$. Thus modifying the argument above slightly, we first find that

$$U_{m+2} - \left(\frac{1}{a} + \frac{1}{b}\right) U_{m+1} + \frac{1}{ab} U_m < 0$$

for all $m \geq -1$. Then that $U_{m+2} - \frac{1}{a} U_{m+1} < 0$, and finally that $U_{m+2} < 0$ for all $m \geq -1$. Hence for all $m \geq 1$, $U_m < 0$ and $T_{-m} < 0$. Thus the inequality holds only for nonnegative integers. ■

Alphabetical Index