The IMO Compendium Group
Olympiad Training Materials
www.imo.org.yu
www.imocompendium.com

Polynomials in One Variable

Dušan Djukić

Contents

1 General Properties

A *Monomial* in variable x is an expression of the form cx^k, where c is a constant and k a nonnegative integer. Constant c can be e.g. an integer, rational, real or complex number.

A *Polynomial* in x is a sum of finitely many monomials in x. In other words, it is an expression of the form

$$P(x) = a_n x^n + a_{n-1} + \cdots + a_1 x + a_0. \qquad (*)$$

If only two or three of the above summands are nonzero, P is said to be a *binomial* and *trinomial*, respectively.

The constants $a_0, \ldots, a_n$ in $(*)$ are the *coefficients* of polynomial P. The set of polynomials with the coefficients in set A is denoted by $A[x]$ - for instance, $\mathbb{R}[x]$ is the set of polynomials with real coefficients.

We can assume in $(*)$ w.l.o.g. that $a_n \neq 0$ (if $a_n = 0$, the summand $a_n x^n$ can be erased without changing the polynomial). Then the exponent n is called the *degree* of polynomial P and denoted by $\deg P$. In particular, polynomials of degree one, two and three are called *linear*, *quadratic* and *cubic*. A nonzero constant polynomial has degree 0, while the zero-polynomial $P(x) \equiv 0$ is assigned the degree $-\infty$ for reasons soon to become clear.

Example 1. $P(x) = x^3(x+1) + (1-x^2)^2 = 2x^4 + x^3 - 2x^2 + 1$ *is a polynomial with integer coefficients of degree 4.*
$Q(x) = 0x^2 - \sqrt{2}x + 3$ *is a linear polynomial with real coefficients.*
$R(x) = \sqrt{x^2} = |x|$, $S(x) = \frac{1}{x}$ *and* $T(x) = \sqrt{2x+1}$ *are not polynomials.*

Polynomials can be added, subtracted or multiplied, and the result will be a polynomial too:

$$A(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad B(x) = b_0 + b_1 x + \cdots + b_m x^m$$
$$A(x) \pm B(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots,$$
$$A(x)B(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_n b_m x^{m+n}.$$

The behavior of the degrees of the polynomials under these operations is clear:

Theorem 1. *If A and B are two polynomials then:*

(i) $\deg(A \pm B) \leq \max(\deg A, \deg B)$, *with the equality if* $\deg A \neq \deg B$.

(ii) $\deg(A \cdot B) = \deg A + \deg B$. □

The conventional equality $\deg 0 = -\infty$ actually arose from these properties of degrees, as else the equality (ii) would not be always true.

Unlike a sum, difference and product, a quotient of two polynomials is not necessarily a polynomial. Instead, like integers, they can be divided with a residue.

Theorem 2. *Given polynomials A and $B \neq 0$, there are unique polynomials Q (quotient) and R (residue) such that*

$$A = BQ + R \quad \textit{and} \quad \deg R < \deg B.$$

Proof. Let $A(x) = a_n x^n + \cdots + a_0$ and $B(x) = b_k x^k + \cdots + b_0$, where $a_n b_k \neq 0$. Assume k is fixed and use induction on n. For $n < k$ the statement is trivial. Suppose that $n = N \geq k$ and that the statement is true for $n < N$. Then $A_1(x) = A(x) - \frac{a_n}{b_k} x^{n-k} B(x)$ is a polynomial of degree less than n (for its coefficient at x^n iz zero); hence by the inductive assumption there are unique polynomials Q_1 and R such that $A_1 = BQ_1 + R$ and $\deg R$. But this also implies

$$A = BQ + R, \quad \text{where} \quad Q(x) = \frac{a_n}{b_k} x^{n-k} + Q_1(x)\,. \,\square$$

Example 2. *The quotient upon division of $A(x) = x^3 + x^2 - 1$ by $B(x) = x^2 - x - 3$ is $x + 2$ with the residue $5x + 5$, as*

$$\frac{x^3 + x^2 - 1}{x^2 - x - 3} = x + 2 + \frac{5x + 5}{x^2 - x - 3}\,.$$

We say that polynomial A is *divisible* by polynomial B if the remainder R when A is divided by B equal to 0, i.e. if there is a polynomial Q such that $A = BQ$.

Theorem 3 (Bezout's theorem). *Polynomial $P(x)$ is divisible by binomial $x - a$ if and only if $P(a) = 0$.*

Proof. There exist a polynomial Q and a constant c such that $P(x) = (x - a)Q(x) + c$. Here $P(a) = c$, making the statement obvious. □

Number a is a *zero (root)* of a given polynomial $P(x)$ if $P(a) = 0$, i.e. $(x - a) \mid P(x)$.

To determine a zero of a polynomial f means to solve the equation $f(x) = 0$. This is not always possible. For example, it is known that finding the exact values of zeros is impossible in general when f is of degree at least 5. Nevertheless, the zeros can always be computed with an arbitrary precision. Specifically, $f(a) < 0 < f(b)$ implies that f has a zero between a and b.

Example 3. *Polynomial $x^2 - 2x - 1$ has two real roots: $x_{1,2} = 1 \pm \sqrt{2}$.*

Polynomial $x^2 - 2x + 2$ has no real roots, but it has two complex roots: $x_{1,2} = 1 \pm i$.

Polynomial $x^5 - 5x + 1$ has a zero in the interval $[1.44, 1.441]$ which cannot be exactly computed.

More generally, the following simple statement holds.

Theorem 4. *If a polynomial P is divisible by a polynomial Q, then every zero of Q is also a zero of P.* □

The converse does not hold. Although every zero of x^2 is a zero of x, x^2 does not divide x.

Problem 1. *For which n is the polynomial $x^n + x - 1$ divisible by a) $x^2 - x + 1$, b) $x^3 - x + 1$?*

Solution. a) The zeros of polynomial x^2-x+1 are $\epsilon_{1,2}=\frac{1\pm i\sqrt{3}}{2}$. If x^2-x+1 divides x^n+x-1, then $\epsilon_{1,2}$ are zeros of polynomial x^n+x-1, so $\epsilon_i^n=1-\epsilon_i=\epsilon_i^{-1}$. Since $\epsilon^k=1$ if and only if $6\mid k$, the answer is $n=6i-1$.

b) If $f(x)=x^3-x+1$ divides x^n+x-1, then it also divides x^n+x^3. This means that every zero of $f(x)$ satisfies $x^{n-3}=-1$; in particular, each zero of f has modulus 1. However, $f(x)$ has a zero between -2 and -1 (for $f(-2)<0<f(-1)$) which is obviously not of modulus 1. Hence there is no such n. $\triangle$

Every nonconstant polynomial with complex coefficients has a complex root. We shall prove this statement later; until then we just believe.

The following statement is analogous to the unique factorization theorem in arithmetics.

Theorem 5. *Polynomial $P(x)$ of degree $n>0$ has a unique representation of the form*

$$P(x)=c(x-x_1)(x-x_2)\cdots(x-x_n),$$

not counting the ordering, where $c\neq 0$ and $x_1,\ldots,x_n$ are complex numbers, not necessarily distinct.

Therefore, $P(x)$ has at most $\deg P=n$ different zeros.

Proof. First we show the uniqueness. Suppose that

$$P(x)=c(x-x_1)(x-x_2)\cdots(x-x_n)=d(x-y_1)(x-y_2)\cdots(x-y_n).$$

Comparing the leading coefficients yields $c=d$. We may assume w.l.o.g. that there are no i,j for which $x_i=y_j$ (otherwise the factor $x-x_i$ can be canceled on both sides). Then $P(x_1)=0$. On the other hand, $P(x_1)=d(x_1-y_1)\cdots(x_1-y_n)\neq 0$, a contradiction.

The existence is shown by induction on n. The case $n=1$ is clear. Let $n>1$. The polynomial $P(x)$ has a complex root, say x_1. By Bezout's theorem, $P(x)=(x-x_1)P_1(x)$ for some polynomial P_1 of degree $n-1$. By the inductive assumption there exist complex numbers $x_2,\ldots,x_n$ for which $P_1(x)=c(x-x_2)\cdots(x-x_n)$, which also implies $P(x)=c(x-x_1)\cdots(x-x_n)$. $\square$

Corollary. If polynomials P and Q has degrees not exceeding n and coincide at $n+1$ different points, then they are equal.

Grouping equal factors yields the *canonical representation*:

$$P(x)=c(x-a_1)^{\alpha_1}(x-a_2)^{\alpha_2}\cdots(x-a_k)^{\alpha_k},$$

where α_i are natural numbers with $\alpha_1+\cdots+\alpha_k=n$. The exponent α_i is called the *multiplicity* of the root a_i. It is worth emphasizing that:

Theorem 6. *Polynomial of n-th degree has exactly n complex roots counted with their multiplicities.* $\square$

We say that two polynomials Q and R are *coprime* if they have no roots in common; Equivalently, there is no nonconstant polynomial dividing them both, in analogy with coprimeness of integers. The following statement is a direct consequence of the previous theorem:

Theorem 7. *If a polynomial P is divisible by two coprime polynomials Q and R, then it is divisible by $Q\cdot R$.* $\square$

Remark: This can be shown without using the existence of roots. By the Euclidean algorithm applied on polynomials there exist polynomials K and L such that $KQ+LR=1$. Now if $P=QS=RT$ for some polynomials R,S, then $R(KT-LS)=KQS-LRS=S$, and therefore $R\mid S$ and $QR\mid QS=P$.

If polynomial $P(x)=x^n+\cdots+a_1x+a_0$ with real coefficients has a complex zero ξ, then $P(\overline{\xi})=\overline{\xi^n}+\cdots+a_1\overline{\xi}+a_0=\overline{P(\xi)}=0$. Thus:

Theorem 8. *If ξ is a zero of a real polynomial $P(x)$, then so is $\overline{\xi}$.* □

In the factorization of a real polynomial $P(x)$ into linear factors we can group conjugated complex zeros:

$$P(x) = (x - r_1) \cdots (x - r_k)(x - \xi_1)(x - \overline{\xi_1}) \cdots (x - \xi_l)(x - \overline{\xi_l}),$$

where r_i are the real zeros, ξ complex, and $k + 2l = n = \deg P$. Polynomial $(x - \xi)(x - \overline{\xi}) = x^2 - 2Re\xi + |\xi|^2 = x^2 - p_i x + q_i$ has real coefficients which satisfy $p_i^2 - 4q_i < 0$. This shows that:

Theorem 9. *A real polynomial $P(x)$ has a unique factorization (up to the order) of the form*

$$P(x) = (x - r_1) \cdots (x - r_k)(x^2 - p_1 x + q_1) \cdots (x^2 - p_l x + q_l),$$

where r_i and p_j, q_j are real numbers with $p_i^2 < 4q_i$ and $k + 2l = n$. □

It follows that a real polynomial of an odd degree always has an odd number of zeros (and at least one).

2 Zeros of Polynomials

In the first section we described some basic properties of polynomials. In this section we describe some further properties and at the end we prove that every complex polynomial actually has a root.

As we pointed out, in some cases the zeros of a given polynomial can be exactly determined. The case of polynomials of degree 2 has been known since the old age. The well-known formula gives the solutions of a quadratic equation $ax^2 + bx + c = 0$ ($a \neq 0$) in the form

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

When f has degree 3 or 4, the (fairly impractical) formulas describing the solutions were given by the Italian mathematicians Tartaglia and Ferrari in the 16-th century. We show Tartaglia's method of solving a cubic equation.

At first, substituting $x = y - a/3$ reduces the cubic equation $x^3 + ax^2 + bx + c = 0$ with real coefficients to

$$y^3 + py + q = 0, \quad \text{where} \quad p = b - \frac{a^2}{3}, \quad q = c - \frac{ab}{3} + \frac{2a^3}{27}.$$

Putting $y = u + v$ transforms this equation into $u^3 + v^3 + (3uv + p)y + q = 0$. But, since u and v are variable, we are allowed to bind them by the condition $3uv + p = 0$. Thus the above equation becomes the system

$$uv = -\frac{p}{3}, \quad u^3 + v^3 = -q$$

which is easily solved: u^3 and v^3 are the solutions of the quadratic equation $t^2 + qt - \frac{p^3}{27} = 0$ and $uv = -p/3$ must be real. Thus we come to the solutions:

Theorem 10 (Cardano's formula). *The solutions of the equation $y^3 + py + q = 0$ with $p, q \in \mathbb{R}$ are*

$$y_i = \epsilon^j \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \epsilon^{-j} \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad j = 0, 1, 2,$$

where ϵ is a primitive cubic root of unity. □

A polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0$ is *symmetric* if $a_{n-i} = a_i$ for all i. If $\deg f = n$ is odd, then -1 is a zero of f and the polynomial $f(x)/(x+1)$ is symmetric. If $n = 2k$ is even, then

$$f(x)/x^k = a_0(x^k + x^{-k}) + \cdots + a_{k-1}(x + x^{-1}) + a_k$$

is a polynomial in $y = x + x^{-1}$, for so is each of the expressions $x^i + x^{-i}$ (see problem 3 in section 7). In particular, $x^2 + x^{-2} = y^2 - 2$, $x^3 + x^{-3} = y^3 - 3y$, etc. This reduces the equation $f(x) = 0$ to an equation of degree $n/2$.

Problem 2. *Show that the polynomial $f(x) = x^6 - 2x^5 + x^4 - 2x^3 + x^2 - 2x + 1$ has exactly four zeros of modulus 1.*

Solution. Set $y = x + x^{-1}$. Then

$$\frac{f(x)}{x^3} = g(y) = y^3 - 2y^2 - 2y + 2.$$

Observe that x is of modulus 1 if and only if $x = \cos t + i \sin t$ for some t, in which case $y = 2\cos t$; conversely, $y = 2\cos t$ implies that $x = \cos t \pm i \sin t$. In other words, $|x| = 1$ if and only if y is real with $-2 \le y \le 2$, where to each such y correspond two values of x if $y \ne \pm 2$. Therefore it remains to show that $g(y)$ has exactly two real roots in the interval $(-2, 2)$. To see this, it is enough to note that $g(-2) = -10$, $g(0) = 2$, $g(2) = -2$, and that therefore g has a zero in each of the intervals $(-2, 0)$, $(0, 2)$ and $(2, \infty)$. $\triangle$

How are the roots of a polynomial related to its coefficients? Consider a monic polynomial

$$P(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = (x - x_1)(x - x_2) \cdots (x - x_n)$$

of degree $n > 0$. For example, comparing coefficients at x^{n-1} on both sides gives us $x_1 + x_2 + \cdots + x_n = -a_1$. Similarly, comparing the constant terms gives us $x_1 x_2 \cdots x_n = (-1)^n a_n$. The general relations are given by the Vieta formulas below.

Definition 1. Elementary symmetric polynomials *in $x_1, \ldots, x_n$ are the polynomials $\sigma_1, \sigma_2, \ldots, \sigma_n$, where*

$$\sigma_k = \sigma_k(x_1, x_2, \ldots, x_n) = \sum x_{i_1} x_{i_2} \ldots x_{i_k},$$

the sum being over all k-element subsets $\{i_1, \ldots, i_k\}$ of $\{1, 2, \ldots, n\}$.

In particular, $\sigma_1 = x_1 + x_2 + \cdots + x_n$ and $\sigma_n = x_1 x_2 \cdots x_n$. Also, we usually set $\sigma_0 = 1$ and $\sigma_k = 0$ for $k > n$.

Theorem 11 (Vieta's formulas). *If $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the zeros of polynomial $P(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$, then $a_k = (-1)^k \sigma_k(\alpha_1, \ldots, \alpha_n)$ for $k = 1, 2, \ldots, n$.*

Proof. Induction on n. The case $n = 1$ is trivial. Assume that $n > 1$ and write $P(x) = (x - x_n)Q(x)$, where $Q(x) = (x - x_1) \cdots (x - x_{n-1})$. Let us compute the coefficient a_k of $P(x)$ at x^k. Since the coefficients of $Q(x)$ at x^{k-1} and x^k are $a'_{k-1} = (-1)^{k-1} \sigma_{k-1}(x_1, \ldots, x_{n-1})$ and $a'_k = (-1)^k \sigma_k(x_1, \ldots, x_{n-1})$ respectively, we have

$$a_k = -x_n a'_{k-1} + a'_k = \sigma_k(x_1, \ldots, x_n). \ \square$$

Example 4. *The roots x_1, x_2, x_3 of polynomial $P(x) = x^3 - ax^2 + bx - c$ satisfy $a = x_1 + x_2 + x_3$, $b = x_1 x_2 + x_2 x_3 + x_3 x_1$ and $c = x_1 x_2 x_3$.*

Problem 3. *Prove that not all zeros of a polynomial of the form $x^n + 2nx^{n-1} + 2n^2 x^{n-2} + \cdots$ can be real.*

Solution. Suppose that all its zeros $x_1, x_2, \ldots, x_n$ are real. They satisfy

$$\sum_i x_i = -2n, \quad \sum_{i<j} x_i x_j = 2n^2.$$

However, by the mean inequality we have

$$\sum_{i<j} x_i x_j = \frac{1}{2}\left(\sum_i x_i\right)^2 - \frac{1}{2}\sum_i x_i^2 \leq \frac{n-1}{2n}\left(\sum_i x_i\right)^2 = 2n(n-1),$$

a contradiction. $\triangle$

Problem 4. *Find all polynomials of the form $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_j \in \{-1, 1\}$ $(j = 0, 1, \ldots, n)$, whose all roots are real.*

Solution. Let $x_1, \ldots, x_n$ be the roots of the given polynomial. Then

$$x_1^2 + x_2^2 + \cdots + x_n^2 = (\textstyle\sum_i x_i)^2 - 2(\sum_{i<j} x_i x_j) = a_{n-1}^2 - 2a_{n-2} \leq 3;$$
$$x_1^2 x_2^2 \cdots x_n^2 = 1.$$

By the mean inequality, the second equality implies $x_1^2 + \cdots + x_n^2 \geq n$; hence $n \leq 3$. The case $n = 3$ is only possible if $x_1, x_2, x_3 = \pm 1$. Now we can easily find all solutions: $x \pm 1$, $x^2 \pm x - 1$, $x^3 - x \pm (x^2 - 1)$. $\triangle$

One contradiction is enough to show that not all zeros of a given polynomial are real. On the other hand, if the task is to show that all zeros of a polynomial *are* real, but not all are computable, the situation often gets more complicated.

Problem 5. *Show that all zeros of a polynomial $f(x) = x(x-2)(x-4)(x-6) + (x-1)(x-3)(x-5)(x-7)$ are real.*

Solution. Since $f(-\infty) = f(\infty) = +\infty$, $f(1) < 0$, $f(3) > 0$ and $f(5) < 0$, polynomial f has a real zero in each of the intervals $(-\infty, 1)$, $(1, 3)$, $(3, 5)$, $(5, \infty)$, that is four in total. $\triangle$

We now give the announced proof of the fact that every polynomial has a complex root. This fundamental theorem has many different proofs. The proof we present is, although more difficult than all the previous ones, still next to elementary. All imperfections in the proof are made on purpose.

Theorem 12 (The Fundamental Theorem of Algebra). *Every nonconstant complex polynomial $P(x)$ has a complex zero.*

Proof. Write $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Suppose that $P(0) = a_0 \neq 0$. For each $r > 0$, let C_r be the circle in the complex plane with the center at point 0 and radius r. Consider the continuous curve $\gamma_r = P(C_r) = \{P(x) \mid |x| = r\}$. The curve described by the monomial x^n, i.e. $\{x^n \mid x \in C_r\}$ rounds point 0 n times. If r is large enough, for example $r > 1 + |a_0| + \cdots + |a_{n-1}|$, we have $|x^n| > |a_{n-1}x^{n-1} + \cdots + a_0| = |P(x) - x^n|$, which means that the rest $P(x) - x^n$ in the expression of $P(x)$ can not "reach" point 0. Thus for such r the curve γ_r also rounds point 0 n times; hence, it contains point 0 in its interior.

For very small r the curve γ_r is close to point $P(0) = a_0$ and leaves point 0 in its exterior. Thus, there exists a minimum $r = r_0$ for which point 0 is *not* in the exterior of γ_r. Since the curve γ_r changes continuously as a function of r, it cannot jump over the point 0, so point 0 must lie on the curve γ_{r_0}. Therefore, there is a zero of polynomial $P(x)$ of modulus r_0. $\square$

3 Polynomials with Integer Coefficients

Consider a polynomial $P(x) = a_n x^n + \cdots + a_1 x + a_0$ with integer coefficients. The difference $P(x) - P(y)$ can be written in the form

$$a_n(x^n - y^n) + \cdots + a_2(x^2 - y^2) + a_1(x - y),$$

in which all summands are multiples of polynomial $x - y$. This leads to the simple though important arithmetic property of polynomials from $\mathbb{Z}[x]$:

Theorem 13. *If P is a polynomial with integer coefficients, then $P(a) - P(b)$ is divisible by $a - b$ for any distinct integers a and b.*

In particular, all integer roots of P divide $P(0)$. □

There is a similar statement about rational roots of polynomial $P(x) \in \mathbb{Z}[x]$.

Theorem 14. *If a rational number p/q ($p, q \in \mathbb{Z}$, $q \neq 0$, nzd$(p, q) = 1$) is a root of polynomial $P(x) = a_n x^n + \cdots + a_0$ with integer coefficients, then $p \mid a_0$ and $q \mid a_n$.*

Proof. We have

$$q^n P\left(\frac{p}{q}\right) = a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_0 q^n.$$

All summands but possibly the first are multiples of q, and all but possibly the last are multiples of p. Hence $q \mid a_n p^n$ and $p \mid a_0 q^n$ and the claim follows. □

Problem 6. *Polynomial $P(x) \in \mathbb{Z}[x]$ takes values ± 1 at three different integer points. Prove that it has no integer zeros.*

Solution. Suppose to the contrary, that a, b, c, d are integers with $P(a), P(b), P(c) \in \{-1, 1\}$ and $P(d) = 0$. Then by the previous statement the integers $a - d, b - d$ and $c - d$ all divide 1, a contradiction. △

Problem 7. *Let $P(x)$ be a polynomial with integer coefficients. Prove that if $P(P(\cdots P(x) \cdots)) = x$ for some integer x (where P is iterated n times), then $P(P(x)) = x$.*

Solution. Consider the sequence given by $x_0 = x$ and $x_{k+1} = P(x_k)$ for $k \geq 0$. Assume $x_k = x_0$. We know that

$$d_i = x_{i+1} - x_i \mid P(x_{i+1}) - P(x_i) = x_{i+2} - x_{i+1} = d_{i+1}$$

for all i, which together with $d_k = d_0$ implies $|d_0| = |d_1| = \cdots = |d_k|$.

Suppose that $d_1 = d_0 = d \neq 0$. Then $d_2 = d$ (otherwise $x_3 = x_1$ and x_0 will never occur in the sequence again). Similarly, $d_3 = d$ etc, and hence $x_k = x_0 + kd \neq x_0$ for all k, a contradiction. It follows that $d_1 = -d_0$, so $x_2 = x_0$. △

Note that a polynomial that takes integer values at all integer points does not necessarily have integer coefficients, as seen on the polynomial $\frac{x(x-1)}{2}$.

Theorem 15. *If the value of the polynomial $P(x)$ is integral for every integer x, then there exist integers $c_0, \ldots, c_n$ such that*

$$P(x) = c_n \binom{x}{n} + c_{n-1} \binom{x}{n-1} + \cdots + c_0 \binom{x}{0}.$$

The converse is true, also.

Proof. We use induction on n. The case $n = 1$ is trivial; Now assume that $n > 1$. Polynomial $Q(x) = P(x+1) - P(x)$ is of degree $n-1$ and takes integer values at all integer points, so by the inductive hypothesis there exist $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ such that

$$Q(x) = a_{n-1}\binom{x}{n-1} + \cdots + a_0\binom{x}{0}.$$

For every integer $x > 0$ we have $P(x) = P(0) + Q(0) + Q(1) + \cdots + Q(x-1)$. Using the identity $\binom{0}{k} + \binom{1}{k} + \cdots + \binom{x-1}{k} = \binom{x}{k+1}$ for every integer k we obtain the desired representation of $P(x)$:

$$P(x) = a_{n-1}\binom{x}{n} + \cdots + a_0\binom{x}{1} + P(0). \ \square$$

Problem 8. *Suppose that a natural number m and a real polynomial $R(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ are such that $R(x)$ is an integer divisible by m whenever x is an integer. Prove that $n!a_n$ is divisible by m.*

Solution. Apply the previous theorem on polynomial $\frac{1}{m}R(x)$ (with the same notation). The leading coefficient of this polynomial equals $c_n + nc_{n-1} + \cdots + n!c_0$, and the statement follows immediately. $\triangle$

4 Irreducibility

Polynomial $P(x)$ with integer coefficients is said to be *irreducible* over $\mathbb{Z}[x]$ if it cannot be written as a product of two nonconstant polynomials with integer coefficients.

Example 5. *Every quadratic or cubic polynomial with no rational roots is irreducible over $\mathbb{Z}$. Such are e.g. $x^2 - x - 1$ and $2x^3 - 4x + 1$.*

One analogously defines (ir)reducibility over the sets of polynomials with e.g. rational, real or complex coefficients. However, of the mentioned, only reducibility over $\mathbb{Z}[x]$ is of interest. Gauss' Lemma below claims that the reducibility over $\mathbb{Q}[x]$ is equivalent to the reducibility over $\mathbb{Z}[x]$. In addition, we have already shown that a real polynomial is always reducible into linear and quadratic factors over $\mathbb{R}[x]$, while a complex polynomial is always reducible into linear factors over $\mathbb{C}[x]$.

Theorem 16 (Gauss' Lema). *If a polynomial $P(x)$ with integer coefficients is reducible over $\mathbb{Q}[x]$, then it is reducible over $\mathbb{Z}[x]$, also.*

Proof. Suppose that $P(x) = a_n x^n + \cdots + a_0 = Q(x)R(x) \in \mathbb{Z}[x]$, where $Q(x)$ and $R(x)$ nonconstant polynomials with rational coefficients. Let q and r be the smallest natural numbers such that the polynomials $qQ(x) = q_k x^k + \cdots + q_0$ and $rR(x) = r_m x^m + \cdots + r_0$ have integer coefficients. Then $qrP(x) = qQ(x) \cdot rR(x)$ is a factorization of the polynomial $qrP(x)$ into two polynomials from $\mathbb{Z}[x]$. Based on this, we shall construct such a factorization for $P(x)$.

Let p be an arbitrary prime divisor of q. All coefficients of $P(x)$ are divisible by p. Let i be such that $p \mid q_0, q_1, \ldots, q_{i-1}$, but $p \nmid q_i$. We have $p \mid a_i = q_0 r_i + \cdots + q_i r_0 \equiv q_i r_0 \pmod{p}$, which implies that $p \mid r_0$. Furthermore, $p \mid a_{i+1} = q_0 r_{i+1} + \cdots + q_i r_1 + q_{i+1} r_0 \equiv q_i r_1 \pmod{p}$, so $p \mid r_1$. Continuing in this way, we deduce that $p \mid r_j$ for all j. Hence $rR(x)/p$ has integer coefficients. We have thus obtained a factorization of $\frac{rq}{p}P(x)$ into two polynomials from $\mathbb{Z}[x]$. Continuing this procedure and taking other values for p we shall eventually end up with a factorization of $P(x)$ itself. $\square$

From now on, unless otherwise specified, by "irreducibility" we mean irreducibility over $\mathbb{Z}[x]$.

Problem 9. *If $a_1, a_2, \ldots, a_n$ are integers, prove that the polynomial $P(x) = (x - a_1)(x - a_2)\cdots(x - a_n) - 1$ is irreducible.*

Solution. Suppose that $P(x) = Q(x)R(x)$ for some nonconstant polynomials $Q, R \in \mathbb{Z}[x]$. Since $Q(a_i)R(a_i) = -1$ for $i = 1, \ldots, n$, we have $Q(a_i) = 1$ and $R(a_i) = -1$ or $Q(a_i) = -1$ and $R(a_i) = 1$; either way, we have $Q(a_i) + R(a_i) = 0$. It follows that the polynomial $Q(x) + R(x)$ (which is obviously nonzero) has n zeros $a_1, \ldots, a_n$ which is impossible for its degree is less than n. $\triangle$

Theorem 17 (Extended Eisenstein's Criterion). *Let $P(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. If there exist a prime number p and an integer $k \in \{0, 1, \ldots, n-1\}$ such that*

$$p \mid a_0, a_1, \ldots, a_k, \quad p \nmid a_{k+1} \quad \text{and} \quad p^2 \nmid a_0,$$

then $P(x)$ has an irreducible factor of a degree greater than k.

In particular, if p can be taken so that $k = n - 1$, then $P(x)$ is irreducible.

Proof. Like in the proof of Gauss's lemma, suppose that $P(x) = Q(x)R(x)$, where $Q(x) = q_k x^k + \cdots + q_0$ and $R(x) = r_m x^m + \cdots + r_0$ are polynomials from $\mathbb{Z}[x]$. Since $a_0 = q_0 r_0$ is divisible by p and not by p^2, exactly one of q_0, r_0 is a multiple of p. Assume that $p \mid q_0$ and $p \nmid r_0$. Further, $p \mid a_1 = q_0 r_1 + q_1 r_0$, implying that $p \mid q_1 r_0$, i.e. $p \mid q_1$, and so on. We conclude that all coefficients $q_0, q_1, \ldots, q_k$ are divisible by p, but $p \nmid q_{k+1}$. It follows that $\deg Q \geq k + 1$. $\square$

Problem 10. *Given an integer $n > 1$, consider the polynomial $f(x) = x^n + 5x^{n-1} + 3$. Prove that there are no nonconstant polynomials $g(x), h(x)$ with integer coefficients such that $f(x) = g(x)h(x)$. (IMO93-1)*

Solution. By the (extended) Eisenstein criterion, f has an irreducible factor of degree at least $n - 1$. Since f has no integer zeros, it must be irreducible. $\triangle$

Problem 11. *If p is a prime number, prove that the polynomial $\Phi_p(x) = x^{p-1} + \cdots + x + 1$ is irreducible.*

Solution. Instead of $\Phi_p(x)$, we shall consider $\Phi_p(x + 1)$ and show that it is irreducible, which will clearly imply that so is Φ_p. We have

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{p-1} x^{p-2} + \cdots + \binom{p}{2} x + p.$$

This polynomial satisfies all the assumptions of Eisenstein's criterion, based on which it is irreducible. $\triangle$

In investigating reducibility of a polynomial, it can be useful to investigate its zeros and their modules. The following problems provide us an illustration.

Problem 12. *Prove that the polynomial $P(x) = x^n + 4$ is irreducible over $\mathbb{Z}[x]$ if and only if n is a multiple of 4.*

Solution. All zeros of polynomial P have the modulus equal to $2^{2/n}$. If Q and R are polynomials from $\mathbb{Z}[x]$ and $\deg Q = k$, then $|Q(0)|$ is the product of the modules of the zeros of Q and equals $2^{2k/n}$; since this should be an integer, we deduce that $n = 2k$.

If k is odd, polynomial Q has a real zero, which is impossible since $P(x)$ has none. Therefore, $2 \mid k$ and $4 \mid n$. $\triangle$

If the zeros cannot be exactly determined, one should find a good enough bound. Estimating complex zeros of a polynomial is not always simple. Our main tool is the triangle inequality for complex numbers:

$$|x| - |y| \leq |x + y| \leq |x| + |y|.$$

Consider a polynomial $P(x) = a_n x^n + a_{n-k} xn - k + \cdots + a_1 x + a_0$ with complex coefficients ($a_n \neq 0$). Let α be its zero. If M is a real number such that $|a_i| < M|a_n|$ for all i, it holds that

$$0 = |P(\alpha)| \geq |a_n||\alpha|^n - M|a_n|(|\alpha|^{n-k} + \cdots + |\alpha| + 1) > |a_n||\alpha|^n \left(1 - \frac{M}{|\alpha|^{k-1}(|\alpha| - 1)}\right),$$

which yields $|\alpha|^{k-1}(|\alpha| - 1) < M$. We thus come to the following estimate:

Theorem 18. *Let $P(x) = a_n x^n + \cdots + a_0$ be a complex polynomial with $a_n \neq 0$ and $M = \max\limits_{0 \leq k < n} \left|\frac{a_k}{a_n}\right|$. If $a_{n-1} = \cdots = a_{n-k+1} = 0$, then all roots of the polynomial P are less than $1 + \sqrt[k]{M}$ in modulus.*

In particular, for $k = 1$, each zero of $P(x)$ is of modulus less than $M + 1$. □

Problem 13. *If $\overline{a_n \ldots a_1 a_0}$ is a decimal representation of a prime number and $a_n > 1$, prove that the polynomial $P(x) = a_n x^n + \cdots + a_1 x + a_0$ is irreducible. (*BMO 1989.2*)*

Solution. Suppose that Q and R are nonconstant polynomials from $\mathbb{Z}[x]$ with $Q(x)R(x) = P(x)$. Let $x_1, \ldots, x_k$ be the zeros of Q and $x_{k+1}, \ldots, x_n$ be the zeros of R. The condition of the problem means that $P(10) = Q(10)R(10)$ is a prime, so we can assume w.l.o.g. that

$$|Q(10)| = (10 - x_1)(10 - x_2) \cdots (10 - x_k) = 1.$$

On the other hand, by the estimate in 18, each zero x_i has a modulus less than $1 + 9/2 = 11/2 < 9$; hence $|10 - x_i| > 1$ for all i, contradicting the above inequality. △

Problem 14. *Let $p > 2$ be a prime number and $P(x) = x^p - x + p$.*

1. *Prove that all zeros of polynomial P are less than $p^{\frac{1}{p-1}}$ in modulus.*
2. *Prove that the polynomial $P(x)$ is irreducible.*

Solution.

1. Let y be a zero of P. Then $|y|^p - |y| \leq |y^p - y| = p$. If we assume that $|y| \geq p^{\frac{1}{p-1}}$, we obtain

   $$|y|^p - |y| \geq (p-1)p^{\frac{1}{p-1}} > p,$$

   a contradiction. Here we used the inequality $p^{\frac{1}{p-1}} > \frac{p}{p-1}$ which follows for example from the binomial expansion of $p^{p-1} = ((p-1)+1)^{p-1}$.

2. Suppose that $P(x)$ is the product of two nonconstant polynomials $Q(x)$ and $R(x)$ with integer coefficients. One of these two polynomials, say Q, has the constant term equal to $\pm p$. On the other hand, the zeros $x_1, \ldots, x_k$ of Q satisfy $|x_1|, \ldots, |x_k| < p^{\frac{1}{p-1}}$ by part (a), and $x_1 \cdots x_k = \pm p$, so we conclude that $k \geq p$, which is impossible. △

5 Interpolating polynomials

A polynomial of n-th degree is uniquely determined, given its values at $n + 1$ points. So, suppose that P is an n-th degree polynomial and that $P(x_i) = y_i$ in different points $x_0, x_1, \ldots, x_n$. There exist unique polynomials $E_0, E_1, \ldots, E_n$ of n-th degree such that $E_i(x_i) = 1$ and $E_i(x_j) = 0$ for $j \neq i$. Then the polynomial

$$P(x) = y_0 E_0(x) + y_1 E_1(x) + \cdots + y_n E_n(x)$$

has the desired properties: indeed, $P(x_i) = \sum_j y_j E_j(x_i) = y_i E_i(x_i) = y_i$. It remains to find the polynomials $E_0, \ldots, E_n$. A polynomial that vanishes at the n points x_j, $j \neq i$, is divisible by $\prod_{j \neq i}(x - x_j)$, from which we easily obtain $E_i(x) = \prod_{j \neq i} \frac{(x - x_j)}{(x_i - x_j)}$. This shows that:

Theorem 19 (Newton's interpolating polynomial). *For given numbers $y_0, \dots, y_n$ and distinct $x_0, \dots, x_n$ there is a unique polynomial $P(x)$ of n-th degree such that $P(x_i) = y_i$ for $i = 0, 1, \dots, n$. This polynomial is given by the formula*

$$P(x) = \sum_{i=0}^{n} y_i \prod_{j \neq i} \frac{(x - x_j)}{(x_i - x_j)}. \quad \square$$

Example 6. *Find the cubic polynomial Q such that $Q(i) = 2^i$ for $i = 0, 1, 2, 3$.*

Solution. $Q(x) = \frac{(x-1)(x-2)(x-3)}{-6} + \frac{2x(x-2)(x-3)}{2} + \frac{4x(x-1)(x-3)}{-2} + \frac{8x(x-1)(x-2)}{6} = \frac{x^3+5x+6}{6}$. $\triangle$

In order to compute the value of a polynomial given in this way in some point, sometimes we do not need to determine its Newton's polynomial. In fact, Newton's polynomial has an unpleasant property of giving the answer in a complicated form.

Example 7. *If the polynomial P of n-th degree takes the value 1 in points $0, 2, 4, \dots, 2n$, compute $P(-1)$.*

Solution. $P(x)$ is of course identically equal to 1, so $P(-1) = 1$. But if we apply the Newton polynomial, here is what we get:

$$P(1) = \sum_{i=0}^{n} \prod_{j \neq i} \frac{1 - 2i}{(2j - 2i)} = \sum_{i=0}^{n} \prod_{j \neq i} \frac{-1 - 2j}{(2i - 2j)} = \frac{(2n+1)!!}{2^n} \sum_{i=1}^{n+1} \frac{(-1)^{n-i}}{(2i+1)i!(n-i)!}. \quad \triangle$$

Instead, it is often useful to consider the *finite difference* of polynomial P, defined by $P^{[1]}(x) = P(x+1) - P(x)$, which has the degree by 1 less than that of P. Further, we define the k-th finite difference, $P^{[k]} = (P^{[k-1]})^{[1]}$, which is of degree $n - k$ (where $\deg P = n$). A simple induction gives a general formula

$$P^{[k]} = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} P(x+i).$$

In particular, $P^{[n]}$ is constant and $P^{[n+1]} = 0$, which leads to

Theorem 20. $P(x+n+1) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n+1}{i} P(x+i)$. $\square$

Problem 15. *Polynomial P of degree n satisfies $P(i) = \binom{n+1}{i}^{-1}$ for $i = 0, 1, \dots, n$. Evaluate $P(n+1)$.*

Solution. We have

$$0 = \sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} P(i) = (-1)^{n+1} P(n+1) + \begin{cases} 1, & 2 \mid n; \\ 0, & 2 \nmid n. \end{cases}$$

It follows that $P(n+1) = \begin{cases} 1, & 2 \mid n; \\ 0, & 2 \nmid n. \end{cases}$ $\triangle$

Problem 16. *If $P(x)$ is a polynomial of an even degree n with $P(0) = 1$ and $P(i) = 2^{i-1}$ for $i = 1, \dots, n$, prove that $P(n+2) = 2P(n+1) - 1$.*

Solution. We observe that $P^{[1]}(0) = 0$ i $P^{[1]}(i) = 2^{i-1}$ for $i = 1, \dots, n-1$; furthermore, $P^{[2]}(0) = 1$ i $P^{[2]}(i) = 2^{i-1}$ for $i = 1, \dots, n-2$, etc. In general, it is easily seen that $P^{[k]}(i) = 2^{i-1}$ for $i = 1, \dots, n-k$, and $P^{[k]}(0)$ is 0 for k odd and 1 for k even. Now

$$P(n+1) = P(n) + P^{[1]}(n) = \dots = P(n) + P^{[1]}(n-1) + \dots + P^{[n]}(0) = \begin{cases} 2^n, & 2 \mid n; \\ 2^n - 1, & 2 \nmid n. \end{cases}$$

Similarly, $P(n+2) = 2^{2n+1} - 1$. $\triangle$

6 Applications of Calculus

The derivative of a polynomial $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is given by

$$P'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1.$$

The inverse operation, the indefinite integral, is given by

$$\int P(x)dx = \frac{a_n}{n+1}x^{n+1} + \frac{a_{n-1}}{n}x^n + \cdots + a_0 x + C.$$

If the polynomial P is not given by its coefficients but rather by its canonical factorization, as $P(x) = (x-x_1)^{k_1}\cdots(x-x_n)^{k_n}$, a more suitable expression for the derivative is obtained by using the logarithmic derivative rule or product rule:

$$P'(x) = P(x)\left(\frac{k_1}{x-x_1} + \cdots + \frac{k_n}{x-x_n}\right).$$

A similar formula can be obtained for the second derivative.

Problem 17. *Suppose that real numbers* $0 = x_0 < x_1 < \cdots < x_n < x_{n+1} = 1$ *satisfy*

$$\sum_{j=0,\, j\neq i}^{n+1} \frac{1}{x_i - x_j} = 0 \quad \textit{za } i = 1, 2, \ldots, n. \tag{1}$$

Prove that $x_{n+1-i} = 1 - x_i$ *for* $i = 1, 2, \ldots, n$.

Solution. Let $P(x) = (x-x_0)(x-x_1)\cdots(x-x_n)(x-x_{n+1})$. We have

$$P'(x) = \sum_{j=0}^{n+1} \frac{P(x)}{x-x_j} \quad \text{i} \quad P''(x) = \sum_{j=0}^{n+1}\sum_{k\neq j} \frac{P(x)}{(x-x_j)(x-x_k)}\,.$$

Therefore

$$P''(x_i) = 2P'(x_i)\sum_{j\neq i}\frac{1}{(x_i - x_j)}$$

for $i = 0, 1, \ldots, n+1$. Thus the condition of the problem is equivalent to $P''(x_i) = 0$ for $i = 1, 2, \ldots, n$. Therefore

$$x(x-1)P''(x) = (n+2)(n+1)P(x).$$

It is easy to see that there is a unique monic polynomial of degree $n+2$ satisfying the above differential equation. On the other hand, the monic polynomial $Q(x) = (-1)^n P(1-x)$ satisfies the same equation and has degree $n+2$, so we must have $(-1)^n P(1-x) = P(x)$, which implies the statement. $\triangle$

What makes derivatives of polynomials especially suitable is their property of preserving multiple zeros.

Theorem 21. *If* $(x-\alpha)^k \mid P(x)$, *then* $(x-\alpha)^{k-1} \mid P'(x)$.

Proof. If $P(x) = (x-\alpha)^k Q(x)$, then $P'(x) = (x-\alpha)^k Q'(x) + k(x-\alpha)^{k-1}Q(x)$. $\square$

Problem 18. *Determine a real polynomial* $P(x)$ *of degree at most 5 which leaves remainders* -1 *and 1 upon division by* $(x-1)^3$ *and* $(x+1)^3$, *respectively.*

Solution. If $P(x)+1$ has a triple zero at point 1, then its derivative $P'(x)$ has a double zero at that point. Similarly, $P'(x)$ has a double zero at point -1 too. It follows that $P'(x)$ is divisible by the polynomial $(x-1)^2(x+1)^2$. Since $P'(x)$ is of degree at most 4, it follows that

$$P'(x) = c(x-1)^2(x+1)^2 = c(x^4-2x^2+1)$$

for some constant c. Now $P(x) = c(\frac{1}{5}x^5 - \frac{2}{3}x^3 + x) + d$ for some real numbers c and d. The conditions $P(-1)=1$ and $P(1)=-1$ now give us $c=-15/8$, $d=0$ and

$$P(x) = -\frac{3}{8}x^5 + \frac{5}{4}x^3 - \frac{15}{8}x. \ \triangle$$

Problem 19. *For polynomials $P(x)$ and $Q(x)$ and an arbitrary $k \in \mathbb{C}$, denote*

$$P_k = \{z \in \mathbb{C} \mid P(z) = k\} \quad \textit{and} \quad Q_k = \{z \in \mathbb{C} \mid Q(z) = k\}.$$

Prove that $P_0 = Q_0$ and $P_1 = Q_1$ imply that $P(x) = Q(x)$.

Solution. Let us assume w.l.o.g. that $n = \deg P \geq \deg Q$. Let $P_0 = \{z_1, z_2, \ldots, z_k\}$ and $P_1 = \{z_{k+1}, z_{k+2}, \ldots, z_{k+m}\}$. Polynomials P and Q coincide at $k+m$ points $z_1, z_2, \ldots, z_{k+m}$. The result will follow if we show that $k+m > n$.

We have

$$P(x) = (x-z_1)^{\alpha_1}\cdots(x-z_k)^{\alpha_k} = (x-z_{k+1})^{\alpha_{k+1}}\cdots(x-z_{k+m})^{\alpha_{k+m}} + 1$$

for some natural numbers $\alpha_1, \ldots, \alpha_{k+m}$. Let us consider $P'(x)$. We know that it is divisible by $(x-z_i)^{\alpha_i - 1}$ for $i = 1, 2, \ldots, k+m$; hence,

$$\prod_{i=1}^{k+m} (x-z_i)^{\alpha_i - 1} \mid P'(x).$$

Therefore, $2n-k-m = \deg \prod_{i=1}^{k+m}(x-z_i)^{\alpha_i-1} \leq \deg P' = n-1$, i.e. $k+m \geq n+1$, as desired. $\triangle$

Even if P has no multiple zeros, certain relations between zeros of P and P' still hold. For example, the following statement holds for all differentiable functions.

Theorem 22 (Rolle's Theorem). *Between every two zeros of a polynomial $P(x)$ there is a zero of $P'(x)$.*

Corollary. If all zeros of $P(x)$ are real, then so are all zeros of $P'(x)$.)

Proof. Let $a < b$ be two zeros of polynomial P. Assume w.l.o.g. that $P'(a) > 0$ and consider the point c in the interval $[a,b]$ in which P attains a local maximum (such a point exists since the interval $[a,b]$ is compact). We know that $P(x) = P(c) + (x-c)[P'(c) + o(1)]$. If for example $P'(c) > 0$ (the case $P'(c) < 0$ leads to a similar contradiction), then $P(x) > P(c)$ would hold in a small neighborhood of c, a contradiction. It is only possible that $P'(c) = 0$, so c is a root of $P'(x)$ between a and b. □

7 Symmetric polynomials

A symmetric polynomial in variables $x_1, \ldots, x_n$ is every polynomial that is not varied by permuting the indices of the variables. For instance, polynomial x_1^2 is symmetric as a polynomial in x_1 (no wonder), but is not symmetric as a polynomial in x_1, x_2 as changing places of the indices 1 and 2 changes it to the polynomial x_2^2.

Definition 2. *The polynomial $P(x_1, x_2, \ldots, x_n)$ is* symmetric *if, for every permutation π of $\{1, 2, \ldots, n\}$, $P(x_1, x_2, \ldots, x_n) \equiv P(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$.*

An obvious property of a symmetric polynomial is that its coefficients at two terms of the forms $x_1^{i_1}\cdots x_n^{i_n}$ and $x_1^{j_1}\cdots x_n^{j_n}$, where $(j_1,\ldots,j_n)$ is a permutation $(i_1,\ldots,i_n)$, always coincide. For example, if the expansion of a symmetric polynomial in x,y,z contains the terms x^2y, then it also contains x^2z, xy^2, etc, with the same coefficient.

Thus, the polynomials σ_k $(1\le k\le n)$ introduced in section 2 are symmetric. Also symmetric is e.g. the polynomial $x_1^2+x_2^2$.

A symmetric polynomial is said to be *homogenous* if all its terms are of the same degree. Equivalently, polynomial T is homogenous of degree d if $T(tx_1,\ldots,tx_n)=t^dT(x_1,\ldots,x_n)$ holds for all x and t. For instance, $x_1^2+x_2^2$ is homogenous of degree $d=2$, but $x_1^2+x_2^2+1$, although symmetric, is not homogenous.

Every symmetric polynomial in $x_1,\ldots,x_n$ can be written as a sum of homogenous polynomials. Moreover, it can also be represented as a linear combination of certain "bricks". These bricks are the polynomials

$$T_a=\sum x_1^{a_{i_1}}\cdots x_n^{a_{i_n}} \qquad (*)$$

for each n-tuple $a=(a_1,\ldots,a_n)$ of nonnegative integers with $a_1\ge\cdots\ge a_n$, where the summation goes over all permutations $(i_1,\ldots,i_n)$ of the indices $1,\ldots,n$. In the expression for T_a the same summand can occur more than once, so we define S_a as the sum of the *different* terms in $(*)$. The polynomial T_a is always an integral multiple of S_a. For instance,

$$T_{(2,2,0)}=2(x_1^2x_2^2+x_2^2x_3^2+x_3^2x_1^2)=2S_{(2,2,0)}.$$

All the n-tuples a of degree $d=a_1+\cdots+a_n$ can be ordered in a lexicographic order so that

$$a>a' \quad\text{if}\quad s_1=s_1',\ldots,s_k=s_k' \text{ and } s_{k+1}>s_{k+1}' \text{ for some } k\ge 1,$$

where $s_i=a_1+\cdots+a_i$. In this ordering, the least n-tuple is $m=(x+1,\ldots,x+1,x,\ldots,x)$, where $x=[d/n]$ and $x+1$ occurs $d-n[d/n]$ times.

The polynomials T_a can be multiplies according to the following simple formula:

Theorem 23. *If $a=(a_1,\ldots,a_n)$ and $b=(b_1,\ldots,b_n)$ are n-tuples of nonnegative integers, it holds that*

$$T_a\cdot T_b=\sum_{\pi} T_{a+\pi(b)},$$

where the sum goes over all permutations $\pi(b)$ of the n-tuple b. (We define $(x_i)_{i=1}^n+(y_i)_{i=1}^n=(x_i+y_i)_{i=1}^n$.)

Proof. It suffices to observe that

$$x_1^{\pi_1(b)}\cdots x_n^{\pi_n(b)}T_a=\sum x_{i_1}^{a_1+\pi_{i_1}(b)}\cdots x_{i_n}^{a_n+\pi_{i_n}(b)},$$

and to sum up over all permutations π. □

There are infinitely many mentioned bricks, and these are obviously not mutually independent. We need simpler elements which are independent and using which one can express every symmetric polynomial by basic operations. It turns out that these atoms are $\sigma_1,\ldots,\sigma_n$.

Example 8. *The following polynomials in x,y,z can be written in terms of $\sigma_1,\sigma_2,\sigma_3$:*
$xy+yz+zx+x+y+z=\sigma_2+\sigma_1$;
$x^2y+x^2z+y^2x+y^2z+z^2x+z^2y=\sigma_1\sigma_2-3\sigma_3$;
$x^2y^2+y^2z^2+z^2x^2=\sigma_2^2-2\sigma_1\sigma_3$.

Theorem 24. *Every symmetric polynomial in $x_1,\ldots,x_n$ can be represented in the form of a polynomial in $\sigma_1,\ldots,\sigma_n$. Moreover, a symmetric polynomial with integer coefficients is also a polynomial in $\sigma_1,\ldots,\sigma_n$ with integer coefficients.*

Proof. It is enough to prove the statement for the polynomials S_a of degree d (for each d). Assuming that it holds for the degrees less than d, we use induction on n-tuples a. The statement is true for the smallest n-tuple m: Indeed, $S_m = \sigma_n^q \sigma_r$, where $d = nq + r$, $0 \le r < n$. Now suppose that the statement is true for all S_b with $b < a$; we show that it also holds for S_a.

Suppose that $a = (a_1, \ldots, a_n)$ with $a_1 = \cdots = a_k > a_{k+1}$ ($k \ge 1$). Consider the polynomial $S_a - \sigma_k S_{a'}$, where $a' = (a_1 - 1, \ldots, a_k - 1, a_{k+1}, \ldots, a_n)$. According to theorem 23 it is easy to see that this polynomial is of the form $\sum_{b<a} c_b S_b$, where c_b are integers, and is therefore by the inductive hypothesis representable in the form of a polynomial in σ_i with integer coefficients. □

The proof of the previous theorem also gives us an algorithm for expressing each symmetric polynomial in terms of the σ_i. Nevertheless, for some particular symmetric polynomials there are simpler formulas.

Theorem 25 (Newton's Theorem on Symmetric Polynomials). *If we denote $s_k = x_1^k + x_2^k + \cdots + x_n^k$, then:*

$$\begin{aligned} k\sigma_k &= s_1\sigma_{k-1} - s_2\sigma_{k-2} + \cdots + (-1)^k s_{k-1}\sigma_1 + (-1)^{k+1} s_k; \\ s_m &= \sigma_1 s_{m-1} - \sigma_2 s_{m-2} + \cdots + (-1)^{n-1}\sigma_n s_{m-n} \quad \textit{za } m \ge n. \end{aligned}$$

(All the polynomials are in n variables.)

Proof. Direct, for example by using the formula 23. □

Problem 20. *Suppose that complex numbers $x_1, x_2, \ldots, x_k$ satisfy*

$$x_1^j + x_2^j + \cdots + x_k^j = n, \qquad \textit{for } j = 1, 2, \ldots, k,$$

where n, k are given positive integers. Prove that

$$(x - x_1)(x - x_2)\ldots(x - x_k) = x^k - \binom{n}{1}x^{k-1} + \binom{n}{2}x^{k-2} - \cdots + (-1)^k\binom{n}{k}.$$

Solution. We are given $s_k = n$ for $k = 1, \ldots, n$. The Newton's theorem gives us $\sigma_1 = n$, $\sigma_2 = \frac{1}{2}(n\sigma_1 - n) = \binom{n}{2}$, $\sigma_3 = \frac{1}{3}(n\sigma_2 - n\sigma_1 + n) = \binom{n}{3}$, etc. We prove by induction on k that $\sigma_k = \binom{n}{k}$. If this holds for $1, \ldots, k-1$, we have

$$\sigma_k = \frac{n}{k}\left[\binom{n}{k-1} - \binom{n}{k-2} + \binom{n}{k-3} - \cdots\right].$$

Since $\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$, the above equality telescopes to $\sigma_k = \frac{n}{k}\binom{n-1}{k-1}$, which is exactly equal to $\binom{n}{k}$. △

8 Problems

1. A monic polynomial $f(x)$ of fourth degree satisfies $f(1) = 10$, $f(2) = 20$ and $f(3) = 30$. Determine $f(12) + f(-8)$.

2. Consider complex polynomials $P(x) = x^n + a_1x^{n-1} + \cdots + a_n$ with the zeros $x_1, \ldots, x_n$, and $Q(x) = x^n + b_1x^{n-1} + \cdots + b_n$ with the zeros $x_1^2, \ldots, x_n^2$. Prove that if $a_1 + a_3 + a_5 + \cdots$ and $a_2 + a_4 + a_6 + \cdots$ are real numbers, then $b_1 + b_2 + \cdots + b_n$ is also real.

3. If a polynomial P with real coefficients satisfies for all x

$$P(\cos x) = P(\sin x),$$

show that there exists a polynomial Q such that $P(x) = Q(x^4 - x^2)$ for each x.

4. (a) Prove that for each $n \in \mathbb{N}$ there is a polynomial T_n with integer coefficients and the leading coefficient 2^{n-1} such that $T_n(\cos x) = \cos nx$ for all x.
   (b) Prove that the polynomials T_n satisfy $T_{m+n}+T_{m-n} = 2T_mT_n$ for all $m, n \in \mathbb{N}$, $m \geq n$.
   (c) Prove that the polynomial U_n given by $U_n(2x) = 2T_n(x)$ also has integer coefficients and satisfies $U_n(x + x^{-1}) = x^n + x^{-n}$.

   The polynomials $T_n(x)$ are known as the *Chebyshev polynomials*.

5. Prove that if $\cos \frac{p}{q}\pi = a$ is a rational number for some $p, q \in \mathbb{Z}$, then $a \in \{0, \pm\frac{1}{2}, \pm 1\}$.

6. Prove that the maximum in absolute value of any monic real polynomial of n-th degree on $[-1, 1]$ is not less than $\frac{1}{2^{n-1}}$.

7. The polynomial P of n-th degree is such that, for each $i = 0, 1, \ldots, n$, $P(i)$ equals the remainder of i modulo 2. Evaluate $P(n + 1)$.

8. A polynomial $P(x)$ of n-th degree satisfies $P(i) = \frac{1}{i}$ for $i = 1, 2, \ldots, n + 1$. Find $P(n + 2)$.

9. Let $P(x)$ be a real polynomial.
   (a) If $P(x) \geq 0$ for all x, show that there exist real polynomials $A(x)$ and $B(x)$ such that $P(x) = A(x)^2 + B(x)^2$.
   (b) If $P(x) \geq 0$ for all $x \geq 0$, show that there exist real polynomials $A(x)$ and $B(x)$ such that $P(x) = A(x)^2 + xB(x)^2$.

10. Prove that if the equation $Q(x) = ax^2 + (c - b)x + (e - d) = 0$ has real roots greater than 1, where $a, b, c, d, e \in \mathbb{R}$, then the equation $P(x) = ax^4 + bx^3 + cx^2 + dx + e = 0$ has at least one real root.

11. A monic polynomial P with real coefficients satisfies $|P(i)| < 1$. Prove that there is a root $z = a + bi$ of P such that $(a^2 + b^2 + 1)^2 < 4b^2 + 1$.

12. For what real values of a does there exist a rational function $f(x)$ that satisfies $f(x^2) = f(x)^2 - a$? (A rational function is a quotient of two polynomials.)

13. Find all polynomials P satisfying $P(x^2 + 1) = P(x)^2 + 1$ for all x.

14. Find all P for which $P(x)^2 - 2 = 2P(2x^2 - 1)$.

15. If the polynomials P and Q each have a real root and

$$P(1 + x + Q(x)^2) = Q(1 + x + P(x)^2),$$

    prove that $P \equiv Q$.

16. Find all polynomials $P(x)$ with real coefficients satisfying the equality

$$P(a - b) + P(b - c) + P(c - a) = 2P(a + b + c)$$

    for all triples (a, b, c) of real numbers such that $ab + bc + ca = 0$. *(IMO04-2)*

17. A sequence of integers $(a_n)_{n=1}^{\infty}$ has the property that $m - n \mid a_m - a_n$ for any distinct $m, n \in \mathbb{N}$. Suppose that there is a polynomial $P(x)$ such that $|a_n| < P(n)$ for all n. Show that there exists a polynomial $Q(x)$ such that $a_n = Q(n)$ for all n.

18. Let $P(x)$ be a polynomial of degree $n > 1$ with integer coefficients and let k be a natural number. Consider the polynomial $Q(x) = P(P(\ldots P(P(x))\ldots))$, where P is applied k times. Prove that there exist at most n integers t such that $Q(t) = t$. *(IMO06-5)*

19. If P and Q are monic polynomials such that $P(P(x)) = Q(Q(x))$, prove that $P \equiv Q$.

20. Let m, n and a be natural numbers and $p < a - 1$ a prime number. Prove that the polynomial $f(x) = x^m(x-a)^n + p$ is irreducible.

21. Prove that the polynomial $F(x) = (x^2+x)^{2^n} + 1$ is irreducible for all $n \in \mathbb{N}$.

22. A polynomial $P(x)$ has the property that for every $y \in \mathbb{Q}$ there exists $x \in \mathbb{Q}$ such that $P(x) = y$. Prove that P is a linear polynomial.

23. Let $P(x)$ be a monic polynomial of degree n whose zeros are $i-1, i-2, \ldots, i-n$ (where $i^2 = -1$) and let $R(x)$ and $S(x)$ be the real polynomials such that $P(x) = R(x) + iS(x)$. Prove that the polynomial $R(x)$ has n real zeros.

24. Let a, b, c be natural numbers. Prove that if there exist coprime polynomials P, Q, R with complex coefficients such that
$$P^a + Q^b = R^c,$$
then $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} > 1$.
Corollary: The Last Fermat Theorem for polynomials.

25. Suppose that all zeros of a monic polynomial $P(x)$ with integer coefficients are of module 1. Prove that there are only finitely many such polynomials of any given degree; hence show that all its zeros are actually roots of unity, i.e. $P(x) \mid (x^n - 1)^k$ for some natural n, k.

9 Solutions

1. The polynomial $f(x) - 10x$ vanishes at points $x = 1, 2, 3$, so it is divisible by polynomial $(x-1)(x-2)(x-3)$. The monicity implies that $f(x) - 10x = (x-1)(x-2)(x-3)(x-c)$ for some c. Now
$$f(12) + f(-8) = 11 \cdot 10 \cdot 9 \cdot (12-c) + 120 + (-9)(-10)(-11)(-8-c) - 80 = 19840.$$

2. Note that $Q(x^2) = \prod(x^2 - x_i^2) = \prod(x - x_i) \cdot \prod(x + x_i) = (-1)^n P(x)P(-x)$. We now have
$$b_1 + b_2 + \cdots + b_n = Q(1) - 1 = (-1)^n P(1)P(-1) - 1 = (-1)^n(1 + B - A)(1 + B + A),$$
where $A = a_1 + a_3 + a_5 + \cdots$ and $B = a_2 + a_4 + \cdots$.

3. It follows from the conditions that $P(-\sin x) = P(\sin x)$, i.e. $P(-t) = P(t)$ for infinitely many t, so the polynomials $P(x)$ and $P(-x)$ coincide. Therefore, $P(x) = S(x^2)$ for some polynomial S. Now $S(\cos^2 x) = S(\sin^2 x)$ for all x, i.e. $S(1-t) = S(t)$ for infinitely many t, which implies $S(x) \equiv S(1-x)$. This is equivalent to $R(x - \frac{1}{2}) = R(\frac{1}{2} - x)$, i.e. $R(y) \equiv R(-y)$, where R is a polynomial such that $S(x) = R(x - \frac{1}{2})$. Now $R(x) = T(x^2)$ for some polynomial T, and therefore $P(x) = S(x^2) = R(x^2 - \frac{1}{2}) = T(x^4 - x^2 + \frac{1}{4}) = Q(x^4 - x^2)$ for some polynomial Q.

4. (a) Clearly, $T_0(x) = 1$ and $T_1(x) = x$ satisfy the requirements. For $n > 1$ we use induction on n. Since $\cos(n+1)x = 2\cos x \cos nx - \cos(n-1)x$, we can define $T_{n+1} = 2T_1T_n - T_{n-1}$. Since T_1T_n and T_{n-1} are of degrees $n+1$ and $n-1$ respectively, T_{n+1} is of degree $n+1$ and has the leading coefficient $2 \cdot 2^n = 2^{n+1}$. It also follows from the construction that all its coefficients are integers.

   (b) The relation follows from the identity $\cos(m+n)x + \cos(m-n)x = 2\cos mx \cos nx$.

(c) The sequence of polynomials (U_n) satisfies $U_0(x) = 2$, $U_1(x) = x$ and $U_{n+1} = U_1U_n - U_{n-1}$, implying that each U_n has integer coefficients. The equality $U_n(x + x^{-1}) = x^n + x^{-n}$ holds for each $x = \cos t + i \sin t$, and therefore it holds for all x.

5. Suppose that $\cos \frac{p}{q}\pi = a$. It follows from the previous problem that $U_q(2a) = 2\cos p\pi = \pm 2$, where U_q is monic with integer coefficients, so $2a$ is an integer by theorem 14.

6. Note that equality holds for a multiple of the n-th Chebyshev polynomial $T_n(x)$. The leading coefficient of T_n equals 2^{n-1}, so $C_n(x) = \frac{1}{2^{n-1}}T_n(x)$ is a monic polynomial and

$$|T_n(x)| = \frac{1}{2^{n-1}}\,|\cos(n \arccos x)| \le \frac{1}{2^{n-1}} \quad \text{za } x \in [-1, 1].$$

Moreover, the values of T_n at points $1, \cos\frac{\pi}{n}, \cos\frac{2\pi}{n}, \cdots, \cos\frac{(n-1)\pi}{n}, -1$ are alternately $\frac{1}{2^{n-1}}$ and $-\frac{1}{2^{n-1}}$.

Now suppose that $P \neq T_n$ is a monic polynomial such that $\max_{-1\le x\le 1} |P(x)| < \frac{1}{2^{n-1}}$. Then $P(x) - C_n(x)$ at points $1, \cos\frac{\pi}{n}, \cdots, \cos\frac{(n-1)\pi}{n}, -1$ alternately takes positive and negative values. Therefore the polynomial $P - C_n$ has at least n zeros, namely, at least one in every interval between two adjacent points. However, $P - C_n$ is a polynomial of degree $n - 1$ as the monomial x^n is canceled, so we have arrived at a contradiction.

7. Since $P^{[i]}(x) = (-2)^{i-1}(-1)^x$ for $x = 0, 1, \ldots, n - i$, we have

$$P(n+1) = P(n) + P^{[1]}(n-1) + \cdots + P^{[n]}(0) = \begin{cases} 2^n, & 2 \nmid n; \\ 1 - 2^n, & 2 \mid n. \end{cases}$$

8. By theorem 20 we have

$$P(n+2) = \sum_{i=0}^{n}(-1)^{n-i}\frac{1}{i+1}\binom{n+1}{i} = \frac{1}{n+2}\sum_{i=0}^{n}(-1)^{n-i}\binom{n+2}{i+1} = \begin{cases} 0, & 2 \nmid n; \\ \frac{2}{n+2}, & 2 \mid n. \end{cases}$$

9. By theorem 9, the polynomial $P(x)$ can be factorized as

$$P(x) = (x - a_1)^{\alpha_1} \cdots (x - a_k)^{\alpha_k} \cdot (x^2 - b_1x + c_1) \cdots (x^2 - b_mx + c_m), \qquad (*)$$

where a_i, b_j, c_j are real numbers such that the a_i are different and the polynomials $x^2 - b_ix + c_i$ has no real zeros.

The condition $P(x) \ge 0$ for all x implies that the α_i are even, whereas the condition $P(x) \ge 0$ for $x \ge 0$ implies that $(\forall i)$ α_i is even or $a_i < 0$. It is now easy to write each factor in $(*)$ in the form $A^2 + B^2$, respectively $A^2 + xB^2$, so by the known formula $(a^2 + \gamma b^2)(c^2 + \gamma d^2) = (ac + \gamma bd)^2 + \gamma(ad - bc)^2$ one can express their product $P(x)$ in the desired form.

10. Write

$$P(-x) = ax^4 + (c - b)x^2 + (e - d) - b(x^3 - x^2) - d(x - 1).$$

If r is a root of the polynomial Q, we have $P(\sqrt{r}) = -(\sqrt{r} - 1)(br + d)$ and $P(-\sqrt{r}) = (\sqrt{r}+1)(br+d)$. Note that one of the two numbers $P(\pm\sqrt{r})$ positive and the other is negative (or both are zero). Hence there must be a zero of P between $-\sqrt{r}$ and $\sqrt{r}$.

11. Let us write $P(x) = (x - x_1) \cdots (x - x_m)(x^2 - p_1x + q_1) \cdots (x^2 - p_nx + q_n)$, where the polynomials $x^2 - p_kx + q_k$ have no real zeros. We have

$$1 > |P(i)| = \prod_{j=1}^{m} |i - x_j| \prod_{k=1}^{n} |-1 - p_ki + q_k|,$$

and since $|i-x_j|^2 = 1+x_j^2 > 1$ for all j, we must have $|-1-p_ki+q_k| < 1$ for some k, i.e.

$$p_k^2 + (q_k-1)^2 < 1. \qquad (*)$$

Let $a \pm bi$ be the zeros of the polynomial $x^2 - p_kx + q_k$ (and also of the polynomial P). Then $p_k = 2a$ and $q_k = a^2+b^2$, so the inequality $(*)$ becomes $4a^2 + (a^2+b^2-1)^2 < 1$, which is equivalent to the desired inequality.

12. Write f in the form $f = P/Q$, where P and Q are coprime polynomials and Q is monic. Comparing the leading coefficients we conclude that P is also monic. The condition of the problem becomes $P(x^2)/Q(x^2) = P(x)^2/Q(x)^2 - a$. Since $P(x^2)$ and $Q(x^2)$ are coprime (if they have a common zero, so do P and Q), it follows that $Q(x^2) = Q(x)^2$ and hence $Q(x) = x^n$ for some $n \in \mathbb{N}$. Therefore, $P(x^2) = P(x)^2 - ax^{2n}$.

    Let $P(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} + x^m$. Comparing the coefficients of $P(x)^2$ and $P(x^2)$ we find that $a_{n-1} = \cdots = a_{2m-n+1} = 0$, $a_{2m-n} = a/2$, $a_1 = \cdots = a_{m-1} = 0$ and $a_0 = 1$. Clearly, this is only possible if $a = 0$, or $a = 2$ and $2m - n = 0$.

13. Since P is symmetric with respect to point 0, it is easy to show that P is also a polynomial in x^2, so there is a polynomial Q such that $P(x) = Q(x^2+1)$ or $P(x) = xQ(x^2+1)$. Then $Q((x^2+1)^2+1) = Q(x^2+1)^2 - 1$, respectively $(x^2+1)Q((x^2+1)^2+1) = x^2Q(x^2+1)^2 + 1$. The substitution $x^2+1 = y$ yields $Q(y^2+1) = Q(y)^2 + 1$, resp. $yQ(y^2+1) = (y-1)Q(y)^2 + 1$.

    Suppose that $yQ(y^2+1) = (y-1)Q(y)^2 + 1$. Setting $y = 1$ gives us $Q(2) = 1$. Note that if $a \neq 0$ and $Q(a) = 1$ then $aQ(a^2+1) = (a-1)+1$, so $Q(a^2+1) = 1$ as well. This leads to an infinite sequence (a_n) of points at which Q takes the value 1, given by $a_0 = 2$ and $a_{n+1} = a_n^2 + 1$. We conclude that $Q \equiv 1$.

    We have shown that if $Q \not\equiv 1$, then $P(x) = Q(x^2+1)$. Now we easily come to all solutions: these are the polynomials of the form $T(T(\cdots(T(x))\cdots))$, where $T(x) = x^2+1$.

14. Let us denote $P(1) = a$. We have $a^2 - 2a - 2 = 0$. Since $P(x) = (x-1)P_1(x) + a$, substituting in the original equation and simplifying yields $(x-1)P_1(x)^2 + 2aP_1(x) = 4(x+1)P_1(2x^2-1)$. For $x = 1$ we have $2aP_1(1) = 8P_1(1)$, which together with $a \neq 4$ implies $P_1(1) = 0$, i.e. $P_1(x) = (x-1)P_2(x)$, so $P(x) = (x-1)^2P_2(x) + a$. Assume that $P(x) = (x-1)^nQ(x) + a$, where $Q(1) \neq 0$. Again substituting in the original equation and simplifying yields $(x-1)^nQ(x)^2 + 2aQ(x) = 2(2x+2)^nQ(2x^2-1)$, which implies that $Q(1) = 0$, a contradiction. We conclude that $P(x) = a$.

15. At first, note that there exists $x = a$ for which $P(a)^2 = Q(a)^2$. This follows from the fact that, if p and q are real roots of P and Q respectively, then $P(p)^2 - Q(p)^2 \leq 0 \leq P(q)^2 - Q(q)^2$, whereby $P^2 - Q^2$ is a continuous function. Then we also have $P(b) = Q(b)$ for $b = 1 + a + P(a)^2$. Assuming that a is the largest real number with $P(a) = Q(a)$, we come to an immediate contradiction.

16. Let $P(x) = a_0 + a_1x + \cdots + a_nx^n$. For every x the triple $(a,b,c) = (6x, 3x, -2x)$ satisfies the condition $ab + bc + ca = 0$. The condition in P gives us $P(3x) + P(5x) + P(-8x) = 2P(7x)$ for all x, so by comparing the coefficients on both sides we obtain $K(i) = \left(3^i + 5^i + (-8)^i - 2\cdot 7^i\right) = 0$ whenever $a_i \neq 0$. Since $K(i)$ is negative for odd i and positive for $i = 0$ and even $i \geq 6$, $a_i = 0$ is only possible for $i = 2$ and $i = 4$. Therefore, $P(x) = a_2x^2 + a_4x^4$ for some real numbers a_2, a_4. It is easily verified that all such $P(x)$ satisfy the conditions.

17. Let d be the degree of P. There is a unique polynomial Q of degree at most d such that $Q(k) = a_k$ for $k = 1, 2, \ldots, d+1$. Let us show that $Q(n) = a_n$ for all n.

Let $n > d+1$. Polynomial Q might not have integral coefficients, so we cannot deduce that $n-m \mid Q(n)-Q(m)$, but it certainly has rational coefficients, i.e. there is a natural number M for which $R(x) = MQ(x)$ has integral coefficients. By the condition of the problem, $M(a_n - Q(n)) = M(a_n - a_k) - (R(n) - R(k))$ is divisible by $n-k$ for each $k = 1, 2, \ldots, d+1$. Therefore, for each n we either have $a_n = Q(n)$ or

$$L_n = \text{lcm}(n-1, n-2, \ldots, n-d-1) \leq M(a_n - Q(n)) < Cn^d$$

for some constant C independent of n.

Suppose that $a_n \neq Q(n)$ for some n. note that L_n is not less than the product $(n-1)\cdots(n-d-1)$ divided by the product P of numbers $\gcd(n-i, n-j)$ over all pairs (i,j) of different numbers from $\{1, 2, \ldots, d+1\}$. Since $\gcd(n-i, n-j) \leq i-j$, we have $P \leq 1^d 2^{d-1} \cdots d$. It follows that

$$(n-1)(n-2)\cdots(n-d-1) \leq PL_n < CPn^d,$$

which is false for large enough n as the left hand side is of degree $d+1$. Thus, $a_n = Q(n)$ for each sufficiently large n, say $n > N$.

What happens for $n \leq N$? By the condition of the problem, $M(a_n - Q(n)) = M(a_n - a_k) - (R(n) - R(k))$ is divisible by $m-n$ for every $m > N$, so it must be equal to zero. Hence $a_n = Q(n)$ for all n.

18. We have shown in 7 from the text that every such t satisfies $P(P(t)) = t$. If every such t also satisfies $P(t) = t$, the number of solutions is clearly at most $\deg P = n$. Suppose that $P(t_1) = t_2$, $P(t_2) = t_1$, $P(t_3) = t_4$ i $P(t_4) = t_3$, where $t_1 \neq t_{2,3,4}$. By theorem 10, $t_1 - t_3$ divides $t_2 - t_4$ and vice versa, from which we deduce that $t_1 - t_3 = \pm(t_2 - t_4)$. Assume that $t_1 - t_3 = t_2 - t_4$, i.e. $t_1 - t_2 = t_3 - t_4 = k \neq 0$. Since the relation $t_1 - t_4 = \pm(t_2 - t_3)$ similarly holds, we obtain $t_1 - t_3 + k = \pm(t_1 - t_3 - k)$ which is impossible. Therefore, we must have $t_1 - t_3 = t_4 - t_2$, which gives us $P(t_1) + t_1 = P(t_3) + t_3 = c$ for some c. It follows that all integral solutions t of the equation $P(P(t)) = t$ satisfy $P(t) + t = c$, and hence their number does not exceed n.

19. Suppose that $R = P - Q \neq 0$ and that $0 < k \leq n-1$ is the degree of $R(x)$. Then

$$P(P(x)) - Q(Q(x)) = [Q(P(x)) - Q(Q(x))] + R(P(x)).$$

Writing $Q(x) = x^n + \cdots + a_1 x + a_0$ yields

$$Q(P(x)) - Q(Q(x)) = [P(x)^n - Q(x)^n] + \cdots + a_1[P(x) - Q(x)],$$

where all the summands but the first have a degree at most $n^2 - n$, while the first summand equals $R(x) \cdot \left(P(x)^{n-1} + P(x)^{n-2}Q(x) + \cdots + Q(x)^{n-1}\right)$ and has the degree $n^2 - n + k$ with the leading coefficient n. Therefore the degree of $Q(P(x)) - Q(Q(x))$ is $n^2 - n + k$. On the other hand, the degree of the polynomial $R(P(x))$ equals $kn < n^2 - n + k$, from which we conclude that the difference $P(P(x)) - Q(Q(x))$ has the degree $n^2 - n + k$, a contradiction.

It remains to check the case of a constant $R \equiv c$. Then the condition $P(P(x)) = Q(Q(x))$ yields $Q(Q(x) + c) = Q(Q(x)) - c$, so the equality $Q(y + c) = Q(y) - c$ holds for infinitely many values of y; hence $Q(y + c) \equiv Q(y) - c$ which is only possible for $c = 0$ (to see this, just compare the coefficients).

20. Suppose that $f(x) = g(x)h(x)$ for some nonconstant polynomials with integer coefficients. Since $|f(0)| = p$, either $|g(0)| = 1$ or $|h(0)| = 1$ holds. Assume w.l.o.g. that $|g(0)| = 1$. Write $g(x) = (x - \alpha_1)\cdots(x - \alpha_k)$. Then $|\alpha_1 \cdots \alpha_k| = 1$. Since $f(\alpha_i) - p = \alpha_i^m(\alpha_i - a)^n = -p$, taking the product over $i = 1, 2, \ldots, k$ yields $|g(a)|^n = |(\alpha_1 - a)\cdots(\alpha_k - a)|^n = p^k$. Since $g(a)$ divides $|g(a)h(a)| = p$, we must have $|g(a)| = p$ and $n = k$. However, a must divide $|g(a) - g(0)| = p \pm 1$, which is impossible.

21. Suppose that $F = G \cdot H$ for some polynomials G, H with integer coefficients. Let us consider this equality modulo 2. Since $(x^2+x+1)^{2^n} \equiv F(x) \pmod 2$, we obtain $(x^2+x+1)^{2^n} = g(x)h(x)$, where $g \equiv G$ and $h \equiv H$ are polynomials over $\mathbb{Z}_2$. The polynomial x^2+x+1 is irreducible over $\mathbb{Z}_2[x]$, so there exists a natural number k for which $g(x) = (x^2+x+1)^k$ and $h(x) = (x^2+x+1)^{2^n-k}$; of course, these equalities hold in $\mathbb{Z}_2[x]$ only.

    Back in $\mathbb{Z}[x]$, these equalities become $H(x) = (x^2+x+1)^{2^n-k} + 2V(x)$ and $G(x) = (x^2+x+1)^k + 2U(x)$ for some polynomials U and V with integer coefficients. Thus,

$$[(x^2+x+1)^k + 2U(x)][(x^2+x+1)^{2^n-k} + 2V(x)] = F(x).$$

    Now if we set $x = \epsilon = \frac{-1+i\sqrt{3}}{2}$ in this equality, we obtain $U(\epsilon)V(\epsilon) = \frac{1}{4}F(\epsilon) = \frac{1}{2}$. However, this is impossible as the polynomial $U(x)V(x)$ has integer coefficients, so $U(\epsilon)V(\epsilon)$ must be of the form $a + b\epsilon$ for some $a, b \in \mathbb{Z}$ (since $\epsilon^2 = -1 - \epsilon$), which is not the case with $\frac{1}{2}$.

22. It is clear, for example by theorem 16, that P must have rational coefficients. For some $m \in \mathbb{N}$ the coefficients of the polynomial $mP(x)$ are integral. Let p be a prime number not dividing m. We claim that, if P is not linear, there is no rational number x for which $P(x) = \frac{1}{mp}$. Namely, such an x would also satisfy $Q(x) = mpP(x) - 1 = 0$. On the other hand, the polynomial $Q(x)$ is irreducible because so is the polynomial $x^nQ(1/x)$ by the Eisenstain criterion; indeed, all the coefficients of $x^nQ(1/x)$ but the first are divisible by p and the constant term is not divisible by p^2. This proves our claim.

23. Denote $P(x) = P_n(x) = R_n(x) + iS_n(x)$. We prove by induction on n that all zeros of P_n are real; moreover, if $x_1 > x_2 > \cdots > x_n$ are the zeros of R_n and $y_1 > y_2 > \cdots > y_{n-1}$ the zeros of R_{n-1}, then

$$x_1 > y_1 > x_2 > y_2 > \cdots > x_{n-1} > y_{n-1} > x_n.$$

    This statement is trivially true for $n = 1$. Suppose that it is true for $n-1$.

    Since $R_n + iS_n = (x - i + n)(R_{n-1} + iS_{n-1})$, the polynomials R_n and S_n satisfy the recurrent relations $R_n = (x+n)R_{n-1} + S_{n-1}$ and $S_n = (x+n)S_{n-1} - R_{n-1}$. This gives us

$$R_n - (2x + 2n - 1)R_{n-1} + [(x+n-1)^2 + 1]R_{n-2} = 0.$$

    If $z_1 > \cdots > z_{n-2}$ are the (real) zeros R_{n-2}, by the inductive hypothesis we have $z_{i-1} > y_i > z_i$. Since the value of R_{n-2} is alternately positive and negative on the intervals $(z_1, +\infty)$, (z_2, z_1), etc, it follows that $\operatorname{sgn} R_{n-2}(y_i) = (-1)^{i-1}$. Now we conclude from the relation $R_n(y_i) = -[(x+n-1)^2 + 1]R_{n-2}(y_i)$ that

$$\operatorname{sgn} R_n(y_i) = (-1)^i,$$

    which means that the polynomial R_n has a zero on each of the n intervals $(y_1, +\infty)$, (y_2, y_1), $\ldots$, $(-\infty, y_{n-1})$. This finishes the induction.

24. We first prove the following auxiliary statement.

    Lemma. If A, B and C are coprime polynomials with $A + B = C$, then the degree of each of the polynomials A, B, C is less than the number of different zeros of the polynomial ABC.

    Proof. Let

$$A(x) = \prod_{i=1}^{k} (x - p_i)^{a_i}, \quad B(x) = \prod_{i=1}^{l} (x - q_i)^{b_i}, \quad C(x) = \prod_{i=1}^{m} (x - r_i)^{c_i}.$$

Let us rewrite the given equality as $A(x)/C(x) + B(x)/C(x) = 1$ and differentiate it with respect to x. We obtain

$$\frac{A(x)}{C(x)}\left(\sum_{i=1}^{k}\frac{a_i}{x-p_i}-\sum_{i=1}^{m}\frac{c_i}{x-r_i}\right)=-\frac{B(x)}{C(x)}\left(\sum_{i=1}^{l}\frac{b_i}{x-q_i}-\sum_{i=1}^{m}\frac{c_i}{x-r_i}\right),$$

from which we see that $A(x)/B(x)$ can be expressed as a quotient of two polynomials of degree not exceeding $k+l+m-1$. The statement follows from the coprimeness of A and B.

Now we apply the Lemma on the polynomials P^a, Q^b, R^c. We obtain that each of the numbers $a\deg P$, $b\deg Q$, $c\deg R$ is less than $\deg P + \deg Q + \deg R$, and therefore

$$\frac{1}{a} > \frac{\deg P}{\deg P + \deg Q + \deg R},$$

etc. Adding these yields the desired inequality.

25. Let us fix $\deg P = n$. Let $P(x) = (x-z_1)\cdots(x-z_n) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where $|z_i| = 1$ for $i = 1, \ldots, n$. By the Vieta formulas, $a_{n-i} = \pm\sigma_i(z_1, \ldots, z_n)$, which is a sum of $\binom{n}{i}$ summands of modulus 1, and hence $|a_{n-i}| \le \binom{n}{i}$. Therefore, there are at most $2\binom{m}{i}+1$ possible values of the coefficient of $P(x)$ at x^{n-i} for each i. Thus the number of possible polynomials P of degree n is finite.

Now consider the polynomial $P_r(x) = (x-z_1^r)\cdots(x-z_n^r)$ for each natural number r. All coefficients of polynomial P_r are symmetric polynomials in z_i with integral coefficients, so by the theorem 24 they must be integers. Therefore, every polynomial P_r satisfies the conditions of the problem, but there are infinitely many r's and only finitely many such polynomials. We conclude that $P_r(x) = P_s(x)$ for some distinct $r, s \in \mathbb{N}$, and the main statement of the problem follows.