IMOTC 2025

Jyoti Prakash Saha

17 May 2025

List of problems and examples

Contents

§1 Warm up

Exercise 1.1 (Tournament of Towns Spring 2020, Junior O Level P4, by Alexandr Yuran)**.** For some integer n, the equation $x^2+y^2+z^2-xy-yz-zx = n$

has an integer solution x, y, z. Prove that the equation $x^2 + y^2 - xy = n$ also has an integer solution x, y.

Walkthrough —

(a) Note that the identity

$$x^2 + y^2 + z^2 - xy - yz - zx = (x - y)^2 - (x - y)(z - y) + (z - y)^2$$

holds.

Solution 1. ■

§2 Polynomials

For further problems, we refer to [Goy21].

§2.1 Warm up

Exercise 2.1 (MMO 2015 Grade 9 P6)**.** Do there exist two polynomials with integer coefficients such that each of them has a coefficient with absolute value exceeding 2015, but no coefficient of their product has absolute value exceeding 1?

Summary — Try to come up with enough polynomials $g_1(x), g_2(x), g_3(x), \dots$ and $h_1(x), h_2(x), h_3(x), \dots$ such that each of the products $g_1g_2g_3\dots$ and $h_1h_2h_3\dots$ have at least one coefficient which is **large in absolute value**, and all the coefficients of the product $(g_1g_2g_3\dots)(h_1h_2h_3\dots)$ are at most 1 in absolute value.

Walkthrough —

(a) Try to come up with a polynomial $P(x)$ whose coefficients are at most 1 in absolute value, and it can be written as a product of enough factors (say $f_1(x), f_2(x), \dots$) such that each of such factor $f_i(x)$ admits a decomposition into the product of two polynomials $g_i(x)$ and $h_i(x)$.

(b) Can you make sure that the product of the g_i's, and the product of the h_i's have to have at least one large coefficient?

(c) For instance, would taking $g_1(x) = g_2(x) = g_3(x) = \dots = 1 - x$ work for some suitable choice of $h_1(x), h_2(x), \dots$?

(d) Does taking

$$h_1(x) = 1 + x,$$
$$h_2(x) = 1 + x + x^2,$$

$$h_3(x) = 1 + x + x^2 + x^3,$$

etc. work?

(e) Note that the product of enough g_i's would have a large coefficient (namely, the coefficient of the second largest power of x). On the other hand, the product of enough h_i's would have a large coefficient (namely, the coefficient of the power of x).

(f) What can be said about the absolute value of the coefficients of the product of these two products?

The above seems to work except that having a control on the coefficients of the product $(g_1g_2g_3\dots)(h_1h_2h_3\dots)$ seems hard[1].

Solution 2. Consider the polynomial

$$P(x) = (1-x)(1-x^2)(1-x^4)(1-x^8)\cdots(1-x^{2^{2016}}).$$

Since

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} < 2^n,$$

it follows that the coefficients of $P(x)$ are at most 1 in absolute value. Note that

$$P(x) = Q(x)R(x)$$

holds where

$$Q(x) = (1-x)^{2017},$$
$$R(x) = (1+x)(1+x+x^2+x^3)\cdots(1+x+x^2+\cdots+x^{2^{2016}-1}).$$

The coefficient of x^{2016} in $Q(x)$ is equal to 2017, and the coefficient of x in $R(x)$ is equal to 2016. This completes the proof. ■

§2.2 Even and odd polynomials

Exercise 2.2 (MMO 1946 Grades 7-8 P5)**.** Prove that after completing the multiplication and collecting the terms

$$(1 - x + x^2 - x^3 + \cdots - x^{99} + x^{100})(1 + x + x^2 + \cdots + x^{99} + x^{100})$$

has no monomials of odd degree.

Summary — What happens if x is replaced by $-x$?

[1] Is it because it fails?

Walkthrough —
(a)

Solution 3. Let $P(x)$ denote the polynomial

$$(1 - x + x^2 - x^3 + \cdots - x^{99} + x^{100})(1 + x + x^2 + \cdots + x^{99} + x^{100}).$$

Note that $P(x) = P(-x)$. By the Claim below, it follows that $P(x)$ has no monomials of odd degree.

Claim — Let $Q(x)$ be a polynomial satisfying $Q(x) = Q(-x)$. Then $Q(x)$ has no monomials of odd degree.

Proof of the Claim. Note that

$$Q(x) = \frac{Q(x) + Q(-x)}{2} + \frac{Q(x) - Q(-x)}{2}$$

holds. Using $Q(x) = Q(-x)$, it follows that $Q(x) = \frac{Q(x)+Q(-x)}{2}$. Consequently, $Q(x)$ has no monomials of odd degree. □

■

Remark. The above decomposition of $Q(x)$ is a special case of general phenomena[a].

[a] Can you think of a few? Which **general phenomena** is referred to?!

Remark. The above solution is more elegant, and less cumbersome. Moreover, it also highlights the underlying reason, whereas the solution below obscures the conceptual viewpoint.

Solution 4. One can multiply the polynomials to note that

$$\begin{aligned}
&1 - x + x^2 - x^3 + \cdots - x^{99} + x^{100} \\
&= 1 - x + x^2(1 - x) + x^4(1 - x) + x^6(1 - x) + \cdots + x^{98}(1 - x) + x^{100} \\
&= (1 - x)(1 + x^2 + x^4 + x^6 + \cdots + x^{98}) + x^{100}.
\end{aligned}$$

Using this, we obtain

$$\begin{aligned}
&(1 - x + x^2 - x^3 + \cdots - x^{99} + x^{100})(1 + x + x^2 + \cdots + x^{99} + x^{100}) \\
&= \big((1 - x)(1 + x^2 + x^4 + x^6 + \cdots + x^{98}) + x^{100}\big)(1 + x + x^2 + \cdots + x^{99} + x^{100}) \\
&= (1 - x)(1 + x^2 + x^4 + x^6 + \cdots + x^{98})(1 + x + x^2 + \cdots + x^{99} + x^{100}) \\
&\quad + x^{100}(1 + x + x^2 + \cdots + x^{99} + x^{100}) \\
&= (1 + x^2 + x^4 + x^6 + \cdots + x^{98})(1 - x^{101})
\end{aligned}$$

$$
\begin{aligned}
&\quad + x^{100}(1 + x + x^2 + \cdots + x^{99} + x^{100}) \\
&= (1 + x^2 + x^4 + x^6 + \cdots + x^{98})(1 - x^{101}) \\
&\quad + x^{100}(x + x^3 + x^5 + \cdots + x^{99}) \\
&\quad + x^{100}(1 + x^2 + x^4 + \cdots + x^{98} + x^{100}) \\
&= (1 + x^2 + x^4 + x^6 + \cdots + x^{98})(1 - x^{101}) \\
&\quad + x^{101}(1 + x^2 + x^4 + x^6 + \cdots + x^{98}) \\
&\quad + x^{100}(1 + x^2 + x^4 + \cdots + x^{98} + x^{100}) \\
&= 1 + x^2 + x^4 + x^6 + \cdots + x^{98} + x^{100}(1 + x^2 + x^4 + \cdots + x^{98} + x^{100}),
\end{aligned}
$$

which has no monomial of odd degree. ■

Example 2.3. Let n be an even positive integer, and let $p(x)$ be a polynomial of degree n such that $p(k) = p(-k)$ for $k = 1, 2, \ldots, n$. Prove that there is a polynomial $q(x)$ such that $p(x) = q(x^2)$.

Walkthrough —

(a) Note that the polynomial $p(x) - p(-x)$ has degree $< n$ because n is even. Observe that it has at least n roots.

Remark. What would happen if n is not assumed to be even?

Solution 5. Note that the polynomial $p(x) - p(-x)$ has degree at most n, and it vanishes at the integers $-n, \ldots, -2, 1, 0, 1, 2, \ldots, n$. Thus, it has at least $2n + 1$ roots. It follows that the polynomial is identically zero, that is, the polynomials $p(x), p(-x)$ are equal. This implies that $p(x)$ is equal to $q(x^2)$ for some polynomial $q(x)$. ■

Exercise 2.4 (Tournament of Towns Spring 2014, Senior A Level P7, by D. A. Zvonkin)**.** Consider a polynomial $P(x)$ such that

$$P(0) = 1, \quad (P(x))^2 = 1 + x + x^{100}Q(x),$$

where $Q(x)$ is also a polynomial. Prove that in the polynomial $(P(x) + 1)^{100}$, the coefficient of x^{99} is zero.

Walkthrough —

(a) Since $P(x)^2$ is congruent to $1 + x$ modulo x^{100}, show that $(P(x) + 1)^{100} + (1 - P(x))^{100}$ is congruent to a polynomial of degree 50 in $1 + x$ modulo x^{100}.

> **(b)** Prove that $(P(x)+1)^{100}$ is congruent to a polynomial of degree 50 in $1+x$ modulo x^{100}.

Solution 6. Note that

$$(P(x)+1)^{100}+(1-P(x))^{100}$$

is a polynomial in $P(x)^2$ of degree 50. Given three polynomials $f(x), g(x), h(x)$ having complex coefficients, with $h(x) \neq 0$, we say that $f(x)$ **is congruent to** $g(x)$ **modulo** $h(x)$ if $h(x)$ divides $f(x)-g(x)$, that is, $f(x)-g(x)$ is the product of $h(x)$ and a polynomial in x with complex coefficients. Since $P(x)^2$ is congruent to $1+x$ modulo x^{100}, it follows that $(P(x)+1)^{100}+(1-P(x))^{100}$ is congruent to a polynomial of degree 50 in $1+x$ modulo x^{100}. Using that $P(x) \equiv 1 \bmod x$, we obtain that $(P(x)+1)^{100}$ is congruent to a polynomial of degree 50 in $1+x$ modulo x^{100}. This shows that the coefficient of x^{99} in $(P(x)+1)^{100}$ is zero. ■

§2.3 Factorization and roots

Example 2.5. Let a, b, c be three distinct real numbers. Show that

$$\frac{(a-x)(b-x)}{(a-c)(b-c)}+\frac{(b-x)(c-x)}{(b-a)(c-a)}+\frac{(c-x)(a-x)}{(c-b)(a-b)}=1.$$

> **Walkthrough** — Can a polynomial having degree at most two admit more than two distinct roots?

Exercise 2.6 (USAMO 1975 P3, AoPS)**.** [**GA17**, Problem 151] A polynomial $P(x)$ of degree n satisfies

$$P(k)=\frac{k}{k+1} \quad \text{for } k=0,1,2,\ldots,n.$$

Find $P(n+1)$.

> **Walkthrough** —
>
> **(a)** Consider the polynomial $(x+1)P(x)-x$.

Solution 7. Note that $xP(x+1)-x$ is a polynomial of degree $n+1$, and it vanishes at the $n+1$ integers $0,1,2,\ldots,n$. It follows that

$$(x+1)P(x)-x=cx(x-1)(x-2)\ldots(x-n)$$

for some nonzero real number c. Substituting $x = -1$ yields

$$-1 = (-1)^{n+1}c(n+1)!,$$

which gives $c = \frac{(-1)^n}{(n+1)!}$. This implies that

$$(n+2)P(n+1) = n + 1 + (-1)^n,$$

and consequently,

$$P(n+1) = \frac{n+1+(-1)^n}{n+2}.$$

■

Example 2.7. Determine the remainder when $x + x^9 + x^{25} + x^{49} + x^{81} + x^{121}$ is divided by $x^3 - x$.

Example 2.8. Let $g(x)$ and $h(x)$ be polynomials with real coefficients such that

$$g(x)(x^2 - 3x + 2) = h(x)(x^2 + 3x + 2)$$

and $f(x) = g(x)h(x) + (x^4 - 5x^2 + 4)$. Prove that $f(x)$ has at least four real roots.

Example 2.9. Let $P(x)$ be a polynomial of degree $\leq n$ having rational coefficients. Suppose $P(k) = \frac{1}{k}$ holds for $1 \leq k \leq n+1$. Determine $P(0)$.

Example 2.10. Let $P(x)$ be a polynomial with real coefficients such that $P(\sin\alpha) = P(\cos\alpha)$ for all $\alpha \in \mathbb{R}$. Show that $P(x) = Q(x^2 - x^4)$ for some polynomial $Q(x)$ with real coefficients.

Walkthrough —

(a) Show that $P(x) = P(-x)$ for any $-1 \leq x \leq 1$, and hence $P(x) = f(x^2)$.

(b) Deduce that $f(x) = f(1-x)$ for any $0 \leq x \leq 1$.

(c) Using induction or otherwise, prove that $f(x) = g(x - x^2)$ for some polynomial $g(x)$ with real coefficients.

Example 2.11. Let $p_1, \ldots, p_n$ denote $n \geq 1$ distinct integers. Show that the polynomial

$$(x-p_1)^2(x-p_2)^2\cdots(x-p_n)^2 + 1$$

cannot be expressed as the product of two non-constant polynomials with integral coefficients.

Example 2.12. Show that any odd degree polynomial with real coefficients has at least one real root.

Exercise 2.13 (Putnam 1999 A2, AoPS)**.** Show that for some fixed positive integer n, we can always express a polynomial with real coefficients which is nowhere negative as a sum of the squares of n polynomials.

Walkthrough —

(a) Show that the real roots of P have even multiplicity.

(b) Conclude that P can be expressed as a product of monic quadratic polynomials with real coefficients having nonreal roots, and even powers of linear polynomials with real coefficients.

(c) Show that a monic quadratic polynomial with real coefficients having nonreal roots is the sum of the squares of two polynomials with real coefficients.

Solution 8. Note that if P is a constant polynomial, then it is clear. Henceforth, let us assume that P is a nonconstant polynomial.

Claim — The polynomial P can be written as the product of polynomials, each of which can be expressed as the sum of the squares of two polynomials with real coefficients.

Proof of the Claim. Since P has real coefficients, it follows that if $\alpha \in \mathbb{C} \setminus \mathbb{R}$ is a root of P, then so is $\overline{\alpha}$. Thus, the nonreal complex roots of P form pairs of complex conjugates. Note that

$$(x-\alpha)(x-\overline{\alpha}) = (x-\mathrm{Re}(\alpha))^2 + \mathrm{Im}(\alpha)^2.$$

Decomposing P over the pairs of nonreal complex conjugate roots, and the real roots, it follows that P can be expressed as the product

$$cf(x)\prod_{a\in A}(x-a)^{m_a},$$

where c denote the leading coefficient of P, $f(x)$ denotes the product of (possibly no) quadratic polynomials of the form $(x-a)^2+b^2$ with $a \in \mathbb{R}, b \in \mathbb{R}\setminus\{0\}$, and A denotes the set of real roots of P, and for an element $a \in A$, the multiplicity of a is denoted by m_a.

Evaluating P at a suitable real number (for instance, at $1+\sum_{a\in A} a$ (resp. 1) if A is nonempty (resp. empty)), it follows that $c > 0$.

Let a be an element of A. Since A is finite, there exists a real number $\varepsilon > 0$ such that the interval $(a-\varepsilon, a+\varepsilon)$ contains no real roots of P other than a. If m_a were odd, then the sign of $P(x)$ would not remain constant as x ranges over in $(a-\varepsilon, a+\varepsilon)\setminus\{a\}$. Hence, it follows that m_a is even.

Since $c > 0$ amd m_a is even for any $a \in A$, the Claim follows. □

Claim — Let $f_1(x), g_1(x), f_2(x), g_2(x)$ be polynomials with real coefficients. Then the following holds.

$$(f_1(x)^2+g_1(x)^2)(f_2(x)^2+g_2(x)^2)$$

$$= (f_1(x)f_2(x) - g_1(x)g_2(x))^2 + (f_1(x)g_2(x) - f_2(x)g_1(x))^2$$

Proof of the Claim. Note that

$$\begin{aligned}
&(f_1(x)^2 + g_1(x)^2)(f_2(x)^2 + g_2(x)^2) \\
&= f_1(x)^2 f_2(x)^2 + g_1(x)^2 g_2(x)^2 - 2f_1(x)f_2(x)g_1(x)g_2(x) \\
&\quad + f_1(x)^2 g_2(x)^2 + f_2(x)^2 g_1(x)^2 + 2f_1(x)g_2(x)f_2(x)g_1(x) \\
&= (f_1(x)f_2(x) - g_1(x)g_2(x))^2 + (f_1(x)g_2(x) + f_2(x)g_1(x))^2.
\end{aligned}$$

□

Combining the above Claims, and using induction, the result follows. ■

§3 Differentiation and double roots

Lemma 1

Let $P(x)$ be a polynomial with complex coefficients, and α be a complex number. Then α is a root of $P(x)$ having multiplicity at least $r \geq 2$ (i.e., $(x-\alpha)^r$ divides $P(x)$) if and only if it is a root of $P(x), P'(x), \ldots, P^{(r)}(x)$, where $P^{(r)}(x)$ denotes the r-fold derivative of $P(x)$.

Solution 9. ■

To solve the problem below, it suffices to have following weaker version.

Lemma 2

Let $P(x)$ be a polynomial with complex coefficients, and α be a complex number. Then α is a double root of $P(x)$ (i.e., $(x-\alpha)^2$ divides $P(x)$) if and only if it is a root of $P(x)$ and $P'(x)$.

Example 3.1 (Putnam 1956 B7, IMOSL 1981 Cuba)**.** The polynomials $P(z)$ and $Q(z)$ with complex coefficients have the same set of numbers for their zeroes but possibly different multiplicities. The same is true of the polynomials $P(z)+1$ and $Q(z)+1$. **Assume that at least one of $P(z), Q(z)$ is nonconstant.** Prove that $P(z) = Q(z)$.

Walkthrough —

(a) Assume that $\deg P \geq \deg Q$.

(b) Denote these two set of roots by S_1, S_2. Considering multiplicities, show

that

$$2\deg P - |S_1| - |S_2| \le \deg P' = \deg P - 1,$$

which yields

$$|S_1| + |S_2| > \deg P.$$

(c) Note that $P - Q$ vanishes at the elements of $S_1 \cup S_2$, which has size larger than the degree of $P - Q$.

Solution 10. On the contrary, let us assume that $P \neq Q$. Without loss of generality, let us assume that $\deg P \ge \deg Q$. Let S_1 (resp. S_2) denote the common set of zeroes of P, Q (resp. $P+1, Q+1$). For a polynomial $f(x)$, let us denote its multiset of zeroes by $\mathcal{Z}(f)$.

Note that $\mathcal{Z}(P')$ contains $\mathcal{Z}(P) \setminus S_1$, and $\mathcal{Z}(P')$ also contains $\mathcal{Z}(P+1) \setminus S_2$. Since $\mathcal{Z}(P)$ and $\mathcal{Z}(P+1)$ are disjoint, it follows that

$$2\deg P - |S_1| - |S_2| \le \deg P' < \deg P - 1,$$

where the final step holds since $\deg P \ge \deg Q$, and one of P, Q is nonconstant. This gives that $|S_1| + |S_2| > \deg P$.

Note that S_1, S_2 are disjoint, and

$$P(z) - Q(z) = (P(z) + 1) - (Q(z) + 1)$$

holds. It follows that $P - Q$ vanishes at $S_1 \cup S_2$, and hence $\deg P \ge |S_1| + |S_2|$. This contradicts the inequality $|S_1| + |S_2| > \deg P$. Consequently, we obtain $P = Q$. ■

§4 Finite differences

Example 4.1 (India RMO 2013b P3)**.** Consider the expression

$$2013^2 + 2014^2 + 2015^2 + \cdots + n^2.$$

Prove that there exists a natural number $n > 2013$ for which one can change a suitable number of plus signs to minus signs in the above expression to make the resulting expression equal 9999.

Summary — "Differentiating" a polynomial enough times makes it linear.

Walkthrough —

(a) Consider the polynomial $P(k) = k^2$, and the polynomial $Q(k) := P(k) - (k-1)$.

(b) Since $Q(k)$ is a linear polynomial in k, the difference $R(k) := Q(k) - Q(k-2)$ is a constant, that is, it does not depend on k.

(c) Note that $R(k)$ is a ± 1-**linear combination**[a] of four consecutive squares.

[a] The content posted here and at this blog by Evan Chen are quite useful.

(d) Does this help?

[a]What does it mean?

Solution 11. Consider the polynomial $P(k) = k^2$, and the polynomial $Q(k) := P(k) - (k-1)$. Since $Q(k)$ is a linear polynomial in k, the difference $R(k) := Q(k) - Q(k-2)$ is a constant, that is, it does not depend on k. Indeed, $Q(k) = 2k-1$, and $R(k) = 4$. Note that $R(k) = k^2-(k-1)^2-(k-2)^2+(k-3)^2$.

Note that

$$2013^2 + 2014^2 + 2015^2 + 2016^2 + 2017^2 > 9999$$

holds, and the integers $2013^2+2014^2+2015^2+2016^2+2017^2, 9999$ are congruent modulo 4, that is, they differ by a multiple of 4. Let $m \geq 1$ be an integer such that

$$9999 = 2013^2 + 2014^2 + 2015^2 + 2016^2 + 2017^2 - 4m$$

holds. Since

$$-k^2 + (k+1)^2 + (k+2)^2 - (k+3)^2 = -4,$$

it follows that

$$\begin{aligned}
&9999\\
&= 2013^2 + 2014^2 + 2015^2 + 2016^2 + 2017^2\\
&- 2018^2 + 2019^2 + 2020^2 - 2021^2\\
&- \dots\\
&- \big((2018 + 4(m-1))^2 + (2019 + 4(m-1))^2\\
&\qquad + (2020 + 4(m-1))^2 - (2021 + 4(m-1))^2\big).
\end{aligned}$$

It follows that there exists a natural number $n = 2021 + 4(m-1) > 2013$, for which one can change a suitable number of plus signs to minus signs in the expression

$$2013^2 + 2014^2 + 2015^2 + \dots + n^2$$

to make the resulting expression equal to 9999. ■

Exercise 4.2 (Bay Area MO 12 2016 P4)**.** Find a positive integer N and $a_1, a_2, \dots, a_N$, where $a_k = 1$ or $a_k = -1$ for each $k = 1, 2, \dots, N$, such that

$$a_1 \cdot 1^3 + a_2 \cdot 2^3 + a_3 \cdot 3^3 + \dots + a_N \cdot N^3 = 20162016,$$

or show that this is impossible.

Summary — "Differentiating" a polynomial enough times makes it linear.

Walkthrough —

(a) Consider the polynomial $P(k) := k^3$. Note that $R(k) := P(k) - P(k-1)$ is a quadratic polynomial in k.

(b) Also note that $S(k) := R(k) - R(k-2)$ is a linear polynomial in k.

Solution 12. Consider the polynomial $P(k) := k^3$. Note that $R(k) := P(k) - P(k-1)$ is equal to $3k^2 - 3k + 1$. Also note that $S(k) := R(k) - R(k-2)$ is equal to $6(2k-2) - 6$. This gives $S(k) - S(k-4) = 48$. It follows that **some ± 1-linear combination** of any given eight consecutive cubes is equal to 48. More specifically,

$$k^3 - (k-1)^3 - (k-2)^3 + (k-3)^3 - (k-4)^3 + (k-5)^5 + (k-6)^3 - (k-7)^3 = 48,$$

or equivalently,

$$-k^3 + (k+1)^3 + (k+2)^3 - (k+3)^3 - (k+4)^3 + (k+5)^3 + (k+6)^3 - (k+7)^3 = 48.$$

Note that 20162016 is divisible by 3 and 16. Since $3, 16$ do not have any common prime factor, it follows that 20162016 is a multiple of 48. Write

$$f(k) = -k^3 + (k+1)^3 + (k+2)^3 - (k+3)^3 - (k+4)^3 + (k+5)^3 + (k+6)^3 - (k+7)^3.$$

Note that

$$f(1) + f(9) + f(17) + \cdots + f(8m-7) = 20162016,$$

where m denotes the integer $20162016/48$. We conclude that one may take $N = 8m = 20162016/6 = 3360336$ so that the given condition holds. ■

§5 Growth of polynomials

Example 5.1. Does there exist a polynomial $P(x)$ with rational coefficients such that $\sin x = P(x)$ for all $x \geq 100$?

Example 5.2 (India RMO 2015b P3)**.** Find all integers a, b, c such that $a^2 = bc + 4$ and $b^2 = ca + 4$.

Summary — In absolute value, a higher degree polynomial dominates a smaller degree polynomial at arguments which are large enough in absolute value.

Solution 13. Let a, b, c be integers satisfying the given equations.

Let us first consider the case that $a = b$. Note that $a(a-c) = 4$ holds, which shows that $(a, a-c)$ is equal to one of the elements of

$$\{(d, d - 4/d) \mid d \text{ is a divisor of } 4\},$$

and hence (a, b, c) is equal to one of

$$(1, 1, -3), (-1, -1, 3), (2, 2, 0), (-2, -2, 0), (4, 4, 3), (-4, -4, -3).$$

Now, let us consider the case that $a \neq b$. Note that

$$a^3 - b^3 = a(bc + 4) - b(ca + 4) = 4(a - b)$$

holds, which yields

$$a^2 + ab + b^2 = 4.$$

It follows that at least one of a, b is even, and hence, both of them are even. Observe that

$$\left(a + \frac{b}{2}\right)^2 + 3\left(\frac{b}{2}\right)^2 = 4$$

holds, which shows that $(a + b/2, b/2)$ is equal to one of

$$(2, 0), (-2, 0), (1, 1), (1, -1), (-1, 1), (-1, -1),$$

and hence (a, b) is equal to one of

$$(2, 0), (-2, 0), (0, 2), (2, -2), (-2, 2), (0, -2).$$

This implies that (a, b, c) is equal to one of

$$(2, 0, -2), (-2, 0, 2), (0, 2, -2), (2, -2, 0), (-2, 2, 0), (0, -2, 2).$$

Considering the above cases, it follows that (a, b, c) is equal to one of

$$(1, 1, -3), (-1, -1, 3), (2, 2, 0), (-2, -2, 0), (4, 4, 3), (-4, -4, -3),$$

$$(2, 0, -2), (-2, 0, 2), (0, 2, -2), (2, -2, 0), (-2, 2, 0), (0, -2, 2).$$

Note that any of the above pairs satisfy the given equations. This proves that the above tuples are precisely all the solutions of the given equation over the integers. ■

§6 Rational and irrational numbers

Example 6.1. Show that for any $n \geq 2$, the rational number

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

is not an integer.

Example 6.2 (Moscow Math Circles)**.** Does there exist irrational numbers x, y with $x > 0$ such that x^y is rational?

Summary — Consider $\sqrt{2}^{\sqrt{2}}$.

Walkthrough —

(a) Consider $\sqrt{2}^{\sqrt{2}}$.

(b) If $\sqrt{2}^{\sqrt{2}}$ is rational, then we are done by taking $x = y = \sqrt{2}$.

(c) If $\sqrt{2}^{\sqrt{2}}$ is irrational, then can you find out suitable x, y?

Example 6.3 (Junior Balkan MO TST 1999)**.** Let S be a set of rational numbers with the following properties:

1. $\frac{1}{2} \in S$,
2. If $x \in S$, then both $\frac{x}{2} \in S$ and $\frac{1}{x+1} \in S$.

Prove that S contains all the rational numbers from the interval $(0, 1)$.

Exercise 6.4 (British Mathematical Olympiad Round 1 2004/5 P5)**.** Let S be a set of rational numbers with the following properties:

1. $\frac{1}{2} \in S$,
2. If $x \in S$, then both $\frac{1}{x+1} \in S$ and $\frac{x}{x+1} \in S$.

Prove that S contains all rational numbers in the interval $0 < x < 1$.

Walkthrough —

(a) Since $\frac{1}{2}$ lies in S, by the second condition, it follows that $\frac{2}{3}$ lies in S and so does $\frac{1}{3}$.

(b) Taking $x = \frac{1}{3}$, it follows that

$$\frac{3}{4}, \frac{1}{4}$$

lie in S. **Note that we have showed that S contains all the rationals between 0 and 1 with denominator at most 4.**

(c) Taking $x = \frac{2}{3}$, it follows that

$$\frac{2}{5}, \frac{3}{5}$$

lie in S. We are **not in a position** to conclude that S contains all the rationals between 0 and 1 with denominator at most 5.

(d) Taking $x = \frac{1}{4}$, it follows that

$$\frac{1}{5}, \frac{4}{5}$$

lie in S. It follows that S contains all the rationals between 0 and 1 with denominator at most 5.

(e) Does the above provide any insight to conclude that S contains all the rationals between 0 and 1? For instance, can one expect the following (and then prove, or realize that it is false, or argue along different lines)?

> For a rational number x lying in S, the rationals
>
> $$\frac{1}{x+1}, \frac{x}{x+1}$$
>
> have denominators larger[a] than that of x.
>
> [a] Often, while being naive, one takes the liberty to write **larger** to mean **no smaller**, that is, **greater than or equal to**. But this is **NOT allowed** while writing down a solution.

Or, stated in a different way,

> A rational number lying in $(0,1)$ can be obtained from a rational number lying in $(0,1)$ with smaller denominator by applying one of the maps
>
> $$x \mapsto \frac{1}{x+1}, x \mapsto \frac{x}{x+1}.$$

Solution 14. It suffices to establish the following.

> **Claim —** For any integer $k \geq 2$, all the rationals lying in $(0,1)$ with denominators not exceeding k lie in S, that is, we have
>
> $$\left\{\frac{1}{\ell}, \frac{2}{\ell}, \ldots, \frac{\ell-2}{\ell}, \frac{\ell-1}{\ell}\right\} \subseteq S \quad \text{for all } 2 \leq \ell \leq k. \tag{1}$$

Proof of the Claim. Eq. (1) holds for $k = 2$ from condition (1). Suppose Eq. (1) holds for $k = n-1$ for some integer $n \geq 3$. Let m be an integer satisfying $1 \leq m < n$. Using the induction hypothesis, we will show that $\frac{m}{n}$ lies in S. Note that for $0 < x < 1$, the inequalities

$$0 < \frac{x}{x+1} < \frac{1}{2}, \frac{1}{2} < \frac{1}{x+1} < 1$$

hold. Using Condition (1), it follows that $\frac{m}{n}$ lies in S if $\frac{m}{n} = \frac{1}{2}$. If $0 < \frac{m}{n} < \frac{1}{2}$, then

$$\frac{x}{x+1} = \frac{m}{n}$$

holds for $x = \frac{m}{n-m}$, which is a rational number lying in $(0,1)$ with denominator $\leq n-1$, and by induction hypothesis, the set S contains $\frac{m}{n}$. Moreover, if $\frac{1}{2} < \frac{m}{n} < 1$, then

$$\frac{1}{x+1} = \frac{m}{n}$$

holds for $x = \frac{n-m}{m}$, which is a rational number lying in $(0, 1)$ with denominator $\leq n-1$, and by induction hypothesis, the set S contains $\frac{m}{n}$. We conclude that for any integer $n \geq 3$, Eq. (1) holds for $k = n$ if it holds for $k = n-1$. □

■

§7 Size of the roots

Example 7.1. Let $f(x)$ and $g(x)$ be nonconstant polynomials with real coefficients such that $f(x^2 + x + 1) = f(x)g(x)$. Show that $f(x)$ has even degree.

Walkthrough — If the polynomial $f(x)$ admits a real root α, then note that $\alpha^2 + \alpha + 1$ is also a real root of $f(x)$ and $\alpha^2 + \alpha + 1 > \alpha$.

Example 7.2. Find all polynomials $P(x)$ (with complex coefficients) satisfying

$$P(x)P(x+2) = P(x^2).$$

Summary — Note that if α is a root of P, then so are α^2 and $(\alpha-2)^2$. Considering absolute values, show that P cannot have a root other than 1. Conclude that $P(x) = c(x-1)^n$.

Walkthrough —

(a)

Solution 15. Let $P(x)$ be a polynomial with complex coefficients satisfying the given condition.

Claim — If P has a root $\alpha \neq 1$, then P has a root which has absolute larger than the absolute value of α.

Proof of the Claim. Note that if $|\alpha| \leq 1$, then

$$\begin{aligned} |(\alpha-2)^2| &\geq (2 - |\alpha|)^2 \\ &\geq 1 \\ &\geq |\alpha|. \end{aligned}$$

Moreover, if $|(\alpha-2)^2| = |\alpha|$ holds, then $|\alpha| = 1$ and $\alpha = 2r$ for some real number $r \geq 0$, and hence, $\alpha = 1$. This shows that if $\alpha \neq 1$, and $|\alpha| \leq 1$, then $|(\alpha-2)^2| > |\alpha|$ holds. Also note that if $|\alpha| > 1$, then $|\alpha^2| > |\alpha|$ holds. Since $\alpha^2, (\alpha-2)^2$ are also roots of P, the Claim follows. □

If P has a root other than 1, then applying the above Claim to a root of P having the largest absolute value yields a contradiction. Hence, P is a constant polynomial, or the only root of P is equal to 1.

If P is a constant, then P is equal to 0 or 1. If P is a nonconstant polynomial, then P is equal to $c(x-1)^n$ for some $c \in \mathbb{C} \setminus \{0\}$, and an integer $n \geq 1$. Using the hypothesis, it follows that $c = 1$.

Observing that the polynomials $0, 1, (x-1)^n$ satisfy the given condition, we conclude that there are all the required polynomials. ■

Exercise 7.3 (Problem 4.12, Putnam training problems by Miguel A. Lerma)**.** Does there exist a polynomial $f(x)$ satisfying

$$xf(x-1) = (x+1)f(x)?$$

Walkthrough —

(a)

Solution 16. Note that the zero polynomial is the only constant polynomial which satisfies the given condition.

Suppose there exists a nonconstant polynomial $f(x)$ satisfying the given condition.

Claim — Any root of $f(x)$ is an integer.

Proof of the Claim. On the contrary, let us assume that α is root of $f(x)$, and that α is not an integer. Note that for any root of β of $f(x)$ in $\mathbb{C} \setminus \mathbb{Z}$, the element $\beta - 1$ is also a root of $f(x)$ lying in $\mathbb{C} \setminus \mathbb{Z}$. It follows that for any integer $k \geq 1$, the element $\alpha - k$ is also a root of $f(x)$. Taking k to be an integer larger than $|\alpha| + \sum_{\gamma \in \mathbb{C}, f(\gamma)=0} |\gamma|$, we obtain

$$|\alpha - k| \geq k - |\alpha| > |\gamma|,$$

and hence $f(x)$ has a root having absolute value larger than that of any of its roots, which is impossible. □

A similar argument can be used to prove that $f(x)$ does not vanish at any negative integer. Moreover, noting that if $f(x)$ vanishes at an integer $n \geq -1$, then $f(x)$ also vanishes at $n+1 \geq -1$, it can be proved using a similar argument that the roots of $f(x)$ are ≤ -2. This contradicts the assumption that there exists a nonconstant polynomial satisfying the given condition. Consequently, the zero polynomial is the only polynomial that satisfies the given condition. ■

Example 7.4 (Problem 2 of the Problem session for October 28, Fall 2020, Putnam Club)**.** Find all polynomials $P(x)$ satisfying

$$xP(x-1) = (x-20)P(x).$$

Example 7.5 (India INMO 2018 P4)**.** Find all polynomials $P(x)$ with real coefficients such that $P(x^2+x+1)$ divides $P(x^3-1)$.

Walkthrough —

(a) Show that if α is a root of $P(x)$, then $P(x)$ vanishes at $(\beta_1-1)\alpha$ and $(\beta_2-1)\alpha$, where β_1, β_2 are the roots of $x^2+x+1=\alpha$.

(b) If α is nonzero, then show that one of $(\beta_1-1)\alpha$ and $(\beta_2-1)\alpha$ is larger than α in absolute value.

Solution 17. Let us establish the following claim.

Claim — Let α denote a nonzero root of $P(x)$ in $\mathbb{C}$. Then for some $\beta \in \mathbb{C}$ satisfying $\beta^2+\beta+1=\alpha$, the element $(\beta-1)\alpha$ is a root of $P(x)$ and is larger than α in absolute value.

Proof of the Claim. Let β_1, β_2 denote the roots of $x^2+x+1=\alpha$ in $\mathbb{C}$. Since $P(x^2+x+1)$ divides the polynomial $P(x^3-1)$, it follows that for any $1 \le i \le 2$,

$$\beta_i^3 - 1 = (\beta_i - 1)(\beta_i^2 + \beta_i + 1) = (\beta_i - 1)\alpha$$

is a root of $P(x)$. Noting that

$$\begin{aligned} |\beta_1 - 1| + |\beta_2 - 1| &\ge |\beta_1 + \beta_2 - 2| \\ &= |-1-2| \\ &> 2, \end{aligned}$$

we obtain that at least one of $\beta_1 - 1, \beta_2 - 1$ has absolute value larger than 1. Consequently, $|(\beta_i-1)\alpha| > |\alpha|$ holds for some $1 \le i \le 2$. This proves the Claim. □

If $P(x)$ has a nonzero root in $\mathbb{C}$, then applying the above Claim to a root of $P(x)$ of largest absolute value, we would obtain a contradiction. Hence, $P(x)$ is equal to cx^n for some $c \in \mathbb{R}$ and an integer $n \ge 0$. Moreover, any polynomial of this form satisfies the given condition. Consequently, these are all the polynomials satisfying the given condition. ■

Remark. Note that proving $|(\beta_1-1)(\beta_2-1)| > 1$, in order to conclude that at least one of $\beta_1 - 1, \beta_2 - 1$ has absolute value larger than 1, does not seem to work. Moreover, $|(\beta_1-1)(\beta_2-1)|$ is smaller than $\frac{1}{2}(|\beta_1-1| + |\beta_2-1|)$. **Unsurprisingly**, a lower bound for the bigger quantity can easily be obtained.

Exercise 7.6 (IMOSL 1979, AoPS, Bulgaria)**.** Find all polynomials $f(x)$ with real coefficients satisfying

$$f(x)f(2x^2) = f(2x^3+x).$$

Walkthrough —
(a)

Solution 18. Note that $0, 1$ are the only constant polynomials satisfying the given condition.

Let $f(x)$ be a nonconstant polynomial with real coefficients satisfying the given condition.

Claim — The roots of $f(x)$ in $\mathbb{C}$ are of absolute value at most 1.

Proof of the Claim. If α is a root of $f(x)$ in $\mathbb{C}$, then $2\alpha^3 + \alpha$ is a root of $f(x)$. If $|\alpha| > 1$, then

$$|2\alpha^3 + \alpha| \geq 2|\alpha|^3 - |\alpha| > |\alpha|$$

holds. If some root of $f(x)$ has absolute value larger than 1, then taking α to be a root of $f(x)$ with largest absolute value, we would obtain a contradiction. This proves the Claim. □

Claim — The equality $f(0) = 1$ holds.

Proof of the Claim. Substituting $x = 0$, it follows that $f(0)^2 = f(0)$, and hence $f(0) = 0$ or $f(0) = 1$.

On the contrary, suppose $f(0) = 0$ holds. Write $f(x) = x^k g(x)$ where k is a positive integer, and $g(x)$ is a polynomial with real coefficients with $g(0) \neq 0$. The given condition translates to

$$x^k(2x^2)^k g(x)g(2x^2) = (2x^3 + x)^k g(2x^3 + x),$$

which yields

$$(2x^2)^k g(x)g(2x^2) = (2x^2 + 1)^k g(2x^3 + x).$$

Substituting $x = 0$, we obtain $g(0) = 0$, which is impossible. This proves the Claim. □

By the above Claim, the product of the absolute values of the roots of $f(x)$ is equal to 1. By the first Claim, these absolute values are at most 1. It follows that the roots of $f(x)$ are of absolute value 1.

Let α be a root of $f(x)$. Note that $2\alpha^3 + \alpha$ is also a root of $f(x)$, and we have that

$$|\alpha| = |2\alpha^3 + \alpha| = 1,$$

which yields $|2\alpha^2 + 1| = |\alpha| = 1$. This gives

$$(2\alpha^2 + 1)(2\overline{\alpha}^2 + 1) = 1.$$

Combining it with $|\alpha| = 1$, we obtain

$$\alpha^2 + \overline{\alpha}^2 = -2.$$

Since $|\alpha| = 1$, it follows that $\alpha^2 = -1$, and hence, $\alpha = i$ or $\alpha = -i$. So, the polynomial $f(x)$ is equal to $c(x+i)^a(x-i)^b$ for some $c \in \mathbb{C} \setminus \{0\}$, and some nonnegative integers a, b. Since $f(x)$ has real coefficients, it follows that $a = b$, and c lies in $\mathbb{R}$. This gives that $f(x) = c(x^2+1)^a$. Using $f(0) = 1$, we obtain $c = 1$, and hence $f(x) = (x^2+1)^a$.

Note that if $g(x)$ denotes the polynomial $(x^2+1)^k$, where k is a positive integer, then

$$\begin{aligned} g(x)g(2x^2) &= \left((x^2+1)((2x^2)^2+1)\right)^k \\ &= \left((4x^6+4x^4+x^2+1)\right)^k \\ &= \left(((2x^3+x)^2+1)\right)^k \\ &= g(2x^3+x). \end{aligned}$$

We conclude that the polynomials satisfying the given condition are precisely the constant polynomial $0, 1$, and the polynomials of the form $(x^2+1)^k$ for some positive integer k. ■

§8 Roots of unity

Example 8.1 (India Pre-RMO 2012 P17)**.** Let x_1, x_2, x_3 be the roots of the equation $x^3 + 3x + 5 = 0$. What is the value of the expression

$$\left(x_1 + \frac{1}{x_1}\right)\left(x_2 + \frac{1}{x_2}\right)\left(x_3 + \frac{1}{x_3}\right)?$$

See also **??**, USAMO 2014 P1.

Solution 19. Let $P(x)$ denote the polynomial $x^3 + 3x + 5$. Note that

$$\begin{aligned} &\left(x_1 + \frac{1}{x_1}\right)\left(x_2 + \frac{1}{x_2}\right)\left(x_3 + \frac{1}{x_3}\right) \\ &= \frac{1}{x_1x_2x_3}(x_1^2+1)(x_2^2+1)(x_3^2+1) \\ &= \frac{1}{x_1x_2x_3}(x_1+i)(x_2+i)(x_3+i)(x_1-i)(x_2-i)(x_3-i) \\ &= \frac{1}{x_1x_2x_3}P(-i)P(i) \\ &= \frac{1}{-5}\,|P(i)|^2 \end{aligned}$$

$$= \frac{1}{-5} |5 - 2i|^2$$
$$= -\frac{29}{5}.$$

■

Remark. The above argument is elegant and quite useful. One could have also argued that

$$\left(x_1 + \frac{1}{x_1}\right)\left(x_2 + \frac{1}{x_2}\right)\left(x_3 + \frac{1}{x_3}\right)$$
$$= \left(x_1x_2 + \frac{x_1}{x_2} + \frac{x_2}{x_1} + \frac{1}{x_1x_2}\right)\left(x_3 + \frac{1}{x_3}\right)$$
$$= x_1x_2x_3 + \frac{x_1x_3}{x_2} + \frac{x_2x_3}{x_1} + \frac{x_3}{x_1x_2} + \frac{x_1x_2}{x_3} + \frac{x_1}{x_2x_3} + \frac{x_2}{x_3x_1} + \frac{1}{x_1x_2x_3}$$
$$= x_1x_2x_3 + + \frac{1}{x_1x_2x_3} + \frac{x_1x_2}{x_3} + \frac{x_2x_3}{x_1} + \frac{x_3x_1}{x_2} + \frac{x_1}{x_2x_3} + \frac{x_2}{x_3x_1} + \frac{x_3}{x_1x_2}$$
$$= -5 - \frac{1}{5} + \frac{1}{x_1x_2x_3}\left(x_1^2x_2^2 + x_2^2x_3^3 + x_3^2x_1^2\right) + \frac{1}{x_1x_2x_3}\left(x_1^2 + x_2^2 + x_3^2\right)$$
$$= -5 - \frac{1}{5} - \frac{1}{5}\left((x_1x_2 + x_2x_3 + x_3x_1)^2 - 2x_1x_2x_3(x_1 + x_2 + x_3)\right)$$
$$- \frac{1}{5}\left((x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1)\right)$$
$$= -5 - \frac{1}{5} - \frac{1}{5}\left(3^2\right) - \frac{1}{5}\left(-2 \cdot 3\right)$$
$$= -5 - \frac{1}{5} - \frac{9}{5} + \frac{6}{5}$$
$$= -5 - \frac{4}{5}$$
$$= -\frac{29}{5}.$$

Note that this way of arguing would get complication if we had a higher degree polynomial to start with.

Exercise 8.2 (USAMO 2014 P1, AoPS)**.** Let a, b, c, d be real numbers such that $b - d \geq 5$ and all zeros x_1, x_2, x_3, 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.

See also Example 8.1, India Pre-RMO 2012 P17.

Walkthrough —

(a)

Solution 20. Note that

$$\begin{aligned}(x_1^2+1)(x_2^2+1)(x_3^2+1)(x_4^2+1) &= P(i)P(-i)\\ &= (1-b+d)^2+(a-c)^2\\ &= (b-d-1)^2+(a-c)^2\\ &\geq 16.\end{aligned}$$

Taking $a=c$ and $b=5, d=0$, we obtain

$$(x_1^2+1)(x_2^2+1)(x_3^2+1)(x_4^2+1)=16.$$

Hence, the smallest value the product $(x_1^2+1)(x_2^2+1)(x_3^2+1)(x_4^2+1)$ can take is equal to 16. ■

Exercise 8.3 (USAMO 1976 P5, AoPS)**.** If $P(x)$, $Q(x)$, $R(x)$, and $S(x)$ are all polynomials such that

$$P(x^5)+xQ(x^5)+x^2R(x^5)=(x^4+x^3+x^2+x+1)S(x),$$

prove that $x-1$ is a factor of $P(x)$.

Summary — The primitive 5-th roots of unity can be used to show that $P(1)=0$.

Walkthrough —

(a) Substituting primitive 5-th roots of unity (that is, the 5-th roots of unity other than 1) for x, yields several linear equations in $P(1), Q(1), R(1)$.

(b) Can $Q(1)$ and $R(1)$ be eliminated to obtain that $P(1)=0$?

Solution 21. Denote the 5-th root of unity $\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}$ by ζ. Substituting $x=\zeta,\zeta^2,\zeta^3$, we obtain

$$\begin{aligned}P(1)+\zeta Q(1)+\zeta^2R(1)&=0,\\ P(1)+\zeta^2Q(1)+\zeta^4R(1)&=0,\\ P(1)+\zeta^3Q(1)+\zeta^6R(1)&=0.\end{aligned}$$

Eliminating $R(1)$ from the first two equations yields

$$(1-\zeta^2)P(1)+\zeta^2(1-\zeta)Q(1)=0,$$

and eliminating $R(1)$ from the last two equations yields

$$(1-\zeta^2)P(1)+\zeta^3(1-\zeta)Q(1)=0.$$

Eliminating $Q(1)$ from the above two equations, we obtain $(1-\zeta)P(1)=0$, which gives $P(1)=0$. This shows that $x-1$ is a factor of $P(x)$. ■

Exercise 8.4 (Leningrad Math Olympiad 1991)**.** A finite sequence $a_1, a_2, \ldots, a_n$ is called p-balanced if any sum of the form

$$a_k + a_{k+p} + a_{k+2p} + \ldots$$

is the same for any $k = 1, 2, 3, \ldots, p$. For instance the sequence

$$a_1 = 1, a_2 = 2, a_3 = 3, a_4 = 4, a_5 = 3, a_6 = 2$$

is a 3-balanced. Prove that if a sequence with 50 members is p-balanced for $p = 3, 5, 7, 11, 13, 17$, then all its members are equal zero.

Summary — Consider the polynomial $\sum_{i=1}^{50} a_i x^i$.

Walkthrough —

(a) Show that the polynomial vanishes at any p-th root of unity, other than 1, for $p \in \{3, 5, 7, 11, 13, 17\}$.

(b) How many such roots of unity are there in total?

Solution 22. Let $a_1, a_2, \ldots, a_{50}$ be a sequence of complex numbers. Assume that it is p-balanced for $p \in \{3, 5, 7, 11, 13, 17\}$. For an integer $n \geq 1$, denote the root of unity $\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ by ζ_n. Let $P(x)$ denote the polynomial $\sum_{i=1}^{n} a_i x^i$.

Let $3 \leq p \leq 17$ be a prime. Since $a_1, a_2, \ldots, a_{50}$ is p-balanced, for any $1 \leq \ell < p$, we obtain

$$\begin{aligned} P(\zeta_p^\ell) &= \sum_{k=1}^{p} (a_k + a_{k+p} + \ldots)\zeta_p^{k\ell} \\ &= (a_1 + a_{1+p} + \ldots)\sum_{k=1}^{p} \zeta_p^{k\ell} \\ &= 0, \end{aligned}$$

where the final equality follows since $\zeta_p^\ell \neq 1$. This shows that the polynomial $P(x)$ vanishes at the elements of the set

$$\cup_{p\in\{3,5,7,11,13,17\}} \{\zeta_p^\ell \mid 1 \leq \ell < p\},$$

which contains

$$\sum_{p\in\{3,5,7,11,13,17\}} (p-1) = 2+4+6+10+12+16 = 50$$

elements. Moreover, $P(x)$ also vanishes at 0. Note that $P(x)$ is a polynomial of degree 50, and it has at least 51 zeroes. This gives that $P(x) = 0$, and hence, the terms of the sequence $a_1, a_2, \ldots, a_{50}$ are all equal to zero. ■

Example 8.5. Let $P(x)$ be a monic polynomial with integer coefficients such that all its zeroes lie on the unit circle. Show that all the zeroes of $P(x)$ are roots of unity, that is, $P(x)$ divides $(x^n - 1)^k$ for some positive integers n, k.

The author has learnt the following argument from Mainak Ghosh, during the INMO Training Camp 2025, held at IISER Bhopal.

Walkthrough —

(a) Use the fundamental theorem of symmetric polynomials, to prove the following claim.

> **Claim** — Let $f(x)$ be a monic polynomial of degree n with integer coefficients. Let $\alpha_1, \ldots, \alpha_n$ denote its roots, counting multiplicities. Then for any integer $k \geq 1$, there is a monic polynomial of degree n with integer coefficients, having $\alpha_1^k, \alpha_2^k, \ldots, \alpha_n^k$ as its roots.

(b) Applying the Claim, for each integer $k \geq 1$, obtain a monic polynomial $P_k(x)$ with integer coefficients, having degree same as that of $P(x)$, whose roots, counted with multiplicities, are the k-th powers of the roots of $P(x)$.

(c) Note that the polynomials $P_1(x), P_2(x), \ldots$ are of the same degree, and the absolute values of the coefficients of any of them are bounded from the above by suitable binomial coefficients, which is smaller than 2^n, where n denotes the degree of $P(x)$. Since these polynomials have integer coefficients, by the pigeonhole principle, it follows that there is a positive integer k_0 such that $P_k(x) = P_{k_0}(x)$ holds for infinitely many positive integers k.

(d) Enumerate the roots of $P(x)$, and matching the roots of $P_k(x)$ with those of $P_{k_0}(x)$ (for suitable k's), we obtain a permutation of n letters. By the pigeonhole principle, infinitely many k's yield the same permutation, which implies that there are positive integers $k \neq \ell$ such that for any root of $P(x)$, its k-th and the ℓ-th powers are equal.

Solution 23. ■

§9 Crossing the x-axis

Here are a few problems from this notes, and this one.

Example 9.1. Suppose $P(x)$ is a polynomial with real coefficients such that $P(x) = x$ has no real solution. Show that $P(P(x)) = x$ has no real solutions.

Walkthrough —

(a)

Solution 24. Since $x \mapsto P(x)$ defines a continuous map from $\mathbb{R} \to \mathbb{R}$, by the intermediate value theorem, it follows that $P(x) > x$ holds for all $x \in \mathbb{R}$ or $P(x) < x$ holds for all $x \in \mathbb{R}$. If $P(x) > x$ holds for all $x \in \mathbb{R}$, then $P(P(x)) > P(x) > x$ holds for all $x \in \mathbb{R}$, and hence $P(P(x)) = x$ has no real solutions. Similarly, if $P(x) < x$ holds for all $x \in \mathbb{R}$, then $P(P(x)) = x$ has no real solutions. ■

Example 9.2. Show that any polynomial of odd degree with real coefficients has a real root.

Example 9.3. Let $P(x)$ and $Q(x)$ be monic polynomials of degree 10 having real coefficients. Assume that the equation $P(x) = Q(x)$ has no real roots. Prove that the equation $P(x+1) = Q(x-1)$ has at least one real root.

Walkthrough —

(a) Consider the difference $P(x) - Q(x)$ to show that the coefficient of x^9 in these polynomials are equal.

(b) Prove that the polynomial $P(x+1) - Q(x-1)$ is of degree 9.

Solution 25. Note that $P(x) - Q(x)$ is a polynomial of degree at most 9 having real coefficients. Since $P(x) - Q(x)$ has no real root, it follows that it has degree at most 8. In other words, the coefficients of x^9 in $P(x), Q(x)$ are the same. Note that $P(x+1) - Q(x-1)$ is of degree ≤ 9, and the coefficient of x^9 in $P(x+1) - Q(x-1)$ is equal to the coefficient of x^9 in $(x+1)^{10} - (x-1)^{10}$, which is equal to 20. This shows that $P(x+1) - Q(x-1)$ is a polynomial of degree 9 with real coefficients. Consequently, it has at least one real root. ■

Example 9.4. Let $P(x)$ be a nonconstant polynomial with real coefficients having a real root. Suppose it does not vanish at 0. Show that the monomial terms appearing in $P(x)$ can be erased one by one to obtain its constant term such that the intermediate polynomial have at least one real root.

Exercise 9.5 (China TST 1995 Day 2 P2, AoPS)**.** Alice and Bob play a game with a polynomial of degree at least 4:

$$x^{2n} + \square x^{2n-1} + \square x^{2n-2} + \cdots + \square x + 1.$$

They take turns to fill the empty boxes. If the resulting polynomial has no real root, Alice wins, otherwise, Bob wins. If Alice goes first, who has a winning strategy?

Walkthrough —

(a) There are more odds than evens among the integers $1, 2, \ldots, 2n-1$.

(b) Can Bob have a winning strategy using the odds in his favour?

Solution 26. Bob has a winning strategy, as described below.

Bob makes sure that at the end of each of his turns except the last one, the number of even powers of x whose coefficients have been provided by some of them is equal to the number of odd powers of x whose coefficients have been provided by some of them. This can be done, for instance, if during a turn of Bob, other than the last turn, Bob provides the coefficient of an odd (resp. even) power of x if Alice has provided the coefficient of an even (resp. odd) power of x in the preceeding turn.

Since $n \geq 2$, it follows that Bob gets at least one turn. At the beginning of the final turn of Bob, there are two powers of x whose coefficients are to be determined, denote them by x^i, x^j, their coefficients by c_i, c_j respectively. Let $Q(x)$ denote the polynomial, obtained by the erasing the terms corresponding to x^i, x^j from the polynomial that Bob had at the beginning of his final turn. Note that

$$P(x) = Q(x) + c_i x^i + c_j x^j.$$

Note that at least of i, j is odd. Interchanging i, j if necessary, let us assume that i is odd. We descrie the strategy that Bob follows in the two cases below.

Let us consider the case that j is even. Bob determines c_j in such a way that for any choice of c_i, the completed polynomial $P(x)$ is guaranteed to have at least one real root. This can be done, for instance, by taking c_j satisfying

$$Q(1) + Q(-1) + 2c_j = 0.$$

For any choice of c_i, the above choice of c_j shows that $P(1) + P(-1) = 0$, which implies that $P(x)$ has a root in the interval $[-1, 1]$.

Let us consider the case that j is odd. Bob determines c_j in such a way that for any choice of c_i by Alice in the next turn, the completed polynomial $P(x)$ is guaranteed to have at least one real root. This can be done, for instance, by taking c_j satisfying

$$Q(2) + c_j 2^j + 2^i Q(-1) - c_j 2^i = 0.$$

Since $i \neq j$, the above holds for some $c_j \in \mathbb{R}$. For any choice of c_i, note that

$$P(2) + 2^i P(-1) = 0$$

holds, which implies that $P(x)$ has a root in $[-1, 2]$. ■

§10 Lagrange interpolation

Lemma 3

Let $x_1, \ldots, x_n$ be pairwise distinct real numbers, and $y_1, \ldots, y_n$ be real numbers. Then there exists a unique polynomial $P(x)$ of **degree at most** $n-1$ having real coefficients such that $P(x_i) = y_i$ for all $1 \leq i \leq n$. Moreover, this statement also holds if the reals are replaced by rationals or complex numbers all throughout.

Proof. Note that there is at most one polynomial satisfying the required condition. Observe that the polynomial $P(x)$, defined by

$$P(x) = \sum_{i=1}^{n} y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j},$$

satisfies the required condition. □

Exercise 10.1. If a polynomial of degree n takes rationals to rationals on $n+1$ points, then show that it is a rational polynomial.

Lemma 4

Let $x_1, \ldots, x_n$ be pairwise distinct real numbers, and $y_1, \ldots, y_n$ be real numbers. Then there exists a unique **monic** polynomial $P(x)$ of **degree** n having real coefficients such that $P(x_i) = y_i$ for all $1 \leq i \leq n$. Moreover, this statement also holds if the reals are replaced by rationals or complex numbers all throughout.

Proof. Note that such a polynomial is unique if it exists. By the above lemma, there exists a polynomial $Q(x)$ of degree at most $n-1$ with real coefficients such that $Q(x_i) = y_i - x_i^n$ for all $1 \leq i \leq n$. Write $P(x) = x^n + Q(x)$. Note that $P(x)$ is a monic polynomial of degree n with real coefficients and $P(x_i) = y_i$ for all $1 \leq i \leq n$. □

Here is an alternate argument.

Proof. Note that such a polynomial is unique if it exists. By the above lemma, there exists a polynomial $Q(x)$ of degree at most $n-1$ such that $Q(x_i) = y_i$ for any $1 \leq i \leq n$. Consider the polynomial

$$(x - x_1)(x - x_2) \ldots (x - x_n) + Q(x),$$

which a monic polynomial of degree n, and sends x_i to y_i for all $1 \leq i \leq n$. □

Example 10.2. Suppose $P(x)$ is a monic polynomial of degree $n-1$ with real coefficients. Let $a_1, a_2, \ldots, a_n$ be distinct real numbers. Show that

$$\sum_{i=1}^{n} \frac{P(a_i)}{\prod_{j\neq i}(a_j - a_i)} = 1.$$

Solution 27. For $1 \leq i \leq n$, write $y_i = P(a_i)$. Note that

$$P(x) = \sum_{i=1}^{n} y_i \prod_{j\neq i} \frac{x - a_i}{a_i - a_j}.$$

Comparing the leading coefficients, the result follows. ■

Example 10.3. Let $P(x)$ be a monic polynomial of degree n. Show that

$$\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} P(i) = n!.$$

Walkthrough — Is the above of some use?

Exercise 10.4 (USAMO 2002 P3, AoPS)**.** Prove that any monic polynomial (a polynomial with leading coefficient 1) of degree n with real coefficients is the average of two monic polynomials of degree n with n real roots.

Walkthrough —

(a) Let $F(x)$ be a monic polynomial of degree n with real coefficients. We would like to write

$$2F(x) = P(x) + Q(x),$$

where $P(x), Q(x)$ are polynomials with certain properties.

(b) Let us take $P(x)$ to be a polynomial which changes sign very often, so that it is likely to have n real roots. To do so, choose n real numbers satisfying

$$x_1 < x_2 < \cdots < x_n,$$

and let $y_1, \ldots, y_n$ be real numbers (to be specified later). Apply the Lagrange interpolation formula to obtain a monic polynomial $P(x)$ satisfying $P(x_i) = y_i$ for all i.

(c) Define the polynomial $Q(x)$ using

$$2F(x) = P(x) + Q(x).$$

Note that $Q(x)$ is a monic polynomial with real coefficients.

(d) Can one impose suitable conditions on $y_1, \ldots, y_n$ such that $Q(x)$ changes sign often?

Solution 28. Let $F(x)$ be a monic polynomial od degree n with real coefficients. Let $x_1 < \cdots < x_n$ be real numbers. Note that there exist real numbers $y_1, \ldots, y_n$ satisfying

$$(-1)^i y_i > 0, \quad (-1)^{i-1}(2F(x_i) - y_i) > 0$$

for any $1 \leq i \leq n$. Indeed, y_i's can be taken satisfying $(-1)^i y_i > |F(x_i)|$. Let $P(x)$ be a monic polynomial of degree n with real coefficients such that $P(x_i) = y_i$ for all $1 \leq i \leq n$. Let $Q(x)$ denote the polynomial such that $F(x)$ is the average of $P(x)$ and $Q(x)$. Since $F(x), P(x)$ are monic, it follows that so is $Q(x)$. For any $1 \leq i \leq n$, note that $Q(x_i) = 2F(x_i) - P(x_i) = 2F(x_i) - y_i$ holds, and hence $Q(x_i)$ has sign as that of $(-1)^i$. It follows that each of the polynomials $P(x), Q(x)$ has at least one root in each of the intervals

$$(x_1, x_2), (x_2, x_3), \ldots, (x_{n-1}, x_n).$$

Since these polynomials are of degree n with real coefficients and each of them has at least $n-1$ real roots, all of their roots are real. ■

Exercise 10.5 (Putnam 1968 A6, AoPS)**.** Find all polynomials whose coefficients are all ± 1 and whose roots are all real.

Walkthrough —

(a) Consider the average of the squares of the roots, and show that it is small (and consequently, smaller than their geometric mean) if the polynomial has degree ≥ 4.

(b) Repeat the argument for degree three polynomials.

(c) Finding the degree one and degree two polynomials is easy.

Solution 29. Let $P(x)$ be a polynomial of degree n having real roots. Assume that its coefficients are equal to ± 1. Denote its roots by $\alpha_1, \ldots, \alpha_n$, counting multiplicities. Noting

$$\alpha_1^2 + \cdots + \alpha_n^2 = (\alpha_1 + \cdots + \alpha_n)^2 - 2 \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j,$$

it follows that

$$\alpha_1^2 + \cdots + \alpha_n^2 = 3.$$

Applying the AM-GM inequality, we obtain

$$\alpha_1^2 + \cdots + \alpha_n^2 \geq n,$$

which implies that $n \leq 3$.

If $P(x)$ is a monic linear polynomial, then it is equal to one of $x-1, x+1$.

If $P(x)$ is a monic quadratic polynomial, then considering discriminants, it follows that its constant term is equal to 1, and hence $P(x)$ is equal to one of x^2+x-1, x^2-x-1.

Let us consider the case that $P(x)$ is a monic cubic polynomial, and the coefficient of x^2 in $P(x)$ is equal to 1. Note that x^3+x^2+x-1 vanishes at $x=0$. For any real number $\alpha \leq 0$,

$$\alpha^3+\alpha^2+\alpha-1 = \alpha(\alpha+1)^2-1-\alpha^2 \leq -1$$

holds, which implies that any real root of x^3+x^2+x-1 is positive. Since x^3+x^2+x-1 is of odd degree, it has a real root, and since $x \mapsto x^3+x^2+x-1$ is an increasing function on the set of positive reals, it follows that x^3+x^2+x-1 has only one real root. This gives $P(x) \neq x^3+x^2+x-1$.

Let us consider the case that $P(x) = x^3+x^2-x+1$ Using

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

it follows that $P(x)$ has no root in $[-1,\infty)$. Note that for $-1 \geq a \geq b$, we have

$$\begin{aligned} P(a)-P(b) &= (a-b)(a^2+ab+b^2+a+b-1) \\ &= (a-b)((a^2+a)+(b^2+b)+(ab-1)) \\ &\geq 0. \end{aligned}$$

This shows that x^3+x^2-x+1 has no real root, and hence $P(x) \neq x^3+x^2-x+1$.

Note that not all the roots of

$$x^3+x^2+x+1 = (x+1)(x^2+1)$$

are real. Consequently, if $P(x)$ is a monic cubic polynomial and the coefficient of x^2 in $P(x)$ is equal to 1, then $P(x)$ is equal to x^3+x^2-x-1.

If $P(x)$ is a monic cubic polynomial and the coefficient of x^2 in $P(x)$ is -1, then $-P(-x)$ is equal to x^3+x^2-x-1, and hence $P(x)$ is equal to x^3-x^2-x+1.

This shows that $P(x)$ is equal to one of

$$x-1, x+1, x^2+x-1, x^2-x-1, x^3+x^2-x-1, x^3-x^2-x+1.$$

Note that the discriminants of the quadratic polynomial x^2+x-1, x^2-x-1 are nonnegative, and also note that

$$\begin{aligned} x^3+x^2-x-1 &= (x-1)(x+1)^2, \\ x^3-x^2-x+1 &= (x-1)^2(x+1). \end{aligned}$$

Consequently, the roots of the polynomials

$$x-1, x+1, x^2+x-1, x^2-x-1, x^3+x^2-x-1, x^3-x^2-x+1$$

are all real. Hence, the required polynomials are

$$x-1, x+1, x^2+x-1, x^2-x-1, x^3+x^2-x-1, x^3-x^2-x+1,$$

$$-(x-1), -(x+1), -(x^2+x-1), -(x^2-x-1), -(x^3+x^2-x-1), -(x^3-x^2-x+1).$$

■

§11 Integer divisibility

Example 11.1. If P is a polynomial with integer coefficients and a, b are integers, then $P(a) - P(b)$ is a multiple of $a - b$.

> **Walkthrough** —
>
> **(a)** Show that it suffices to prove it for monomials.

Solution 30. ■

Example 11.2. Let $P(x)$ be a polynomial with integer coefficients such that $P(0), P(1)$ are odd. Show that $P(x)$ does not have any integer root.

Example 11.3 (India RMO 2016g P8)**.** At some integer points a polynomial with integer coefficients take values $1, 2$ and 3. Prove that there exist not more than one integer at which the polynomial is equal to 5.

Solution 31. Denote the polynomial by $P(x)$. On the contrary, let us assume that there are at least two distinct integers where $P(x)$ takes the value 5.

Let a, b, c be integers such that

$$P(a) = 1, P(b) = 2, P(c) = 3.$$

Note that $a - b$ divides $P(a) - P(b)$, $b - c$ divides $P(b) - P(c)$. It follows that $a - b = \pm 1, b - c = \pm 1$. Since a, b are of opposite parity, and so are the integers b, c, we obtain that a, c are of the same parity. Noting that $c - a$ divides $P(c) - P(a) = 2$, it follows that $c - a = \pm 2$. Combining this with $a - b = \pm 1, b - c = \pm 1$, we get $a - b = b - c = 1$ or $a - b = b - c = -1$.

This shows that $P(b-1) = 1, P(b) = 2, P(b+1) = 3$ holds or $P(b+1) = 1, P(b) = 2, P(b-1) = 3$ holds. Note that in the first case, the polynomial $R(x) := P(x - b)$ takes the values $1, 2, 3$ at the integers $-1, 0, 1$ respectively. In the second case, the polynomial $S(x) = P(-x + b)$ takes the values $1, 2, 3$ at

the integers $-1, 0, 1$ respectively. This proves that there is a polynomial $Q(x)$ with integer coefficients which takes the values $1, 2, 3$ at $-1, 0, 1$ respectively.

From the hypothesis, it follows that there are distinct integers i, j such that $Q(i) = Q(j) = 5$. Note that $i - 1$ divides $Q(i) - Q(1) = 2$, i divides $Q(i) - Q(0) = 3$, $i + 1$ divides $Q(i) - Q(-1) = 4$. Since i divdes 3, we obtain $i = \pm 1, \pm 3$. Using $Q(-1) = 1, Q(1) = 3$, we get $i \neq -1, i \neq 1$. This gives $i = \pm 3$. Noting that $i - 1$ divides 2, we obtain $i \neq -3$, and hence $i = 3$. Similarly, it follows that $j = 3$. ■

Example 11.4. Let $P(x)$ be a polynomial with integer coefficients such that $P(20), P(25)$ are of absolute value equal to 1. Show that $P(x)$ does not vanish at any integer.

> **Walkthrough** —
>
> **(a)** If $P(x)$ vanishes at an integer α, then $\alpha - 20$ divides $P(20)$ and $\alpha - 25$ divides $P(25)$.

Solution 32. On the contrary, let us assume that $P(x)$ vanishes at an integer α. Note that $\alpha - 20$ divides 1, and so does $\alpha - 25$. This shows that $\alpha - 20, \alpha - 25$ are of absolute value equal to 1. Applying triangle inequality, we obtain

$$5 \leq |\alpha - 20| + |\alpha - 5| \leq 2,$$

which is impossible. ■

Exercise 11.5 (USAMO 1974 P1, AoPS)**.** Let a, b, and c denote three distinct integers, and let P denote a polynomial having all integral coefficients. Show that it is impossible that $P(a) = b$, $P(b) = c$, and $P(c) = a$.

> **Walkthrough** —
>
> **(a)** Show that each of the integers $a - b, b - c, c - a$ is a multiple of the remaining two integers.
>
> **(b)** Prove that this implies that a, b, c are equal.

Solution 33. Note that

$$a - b \mid P(a) - P(b) = b - c \mid P(b) - P(c) \mid c - a \mid P(c) - P(a) = a - b.$$

Consequently, the integers $a - b, b - c, c - a$ are of the same absolute value. Denote their absolute value by k. Note that their sum is zero. However, the sum is equal to mk, for some $m \in \{\pm 1, \pm 3\}$. Hence, k is equal to zero. This yields that $a = b = c$. ■

Here is a more general result.

Example 11.6. Let $P(x)$ be a polynomial with integer coefficients, and let n be an odd positive integer. Suppose that $x_1, x_2, \ldots, x_n$ is a sequence of integers such that $x_2 = P(x_1), x_3 = P(x_2), \ldots, x_n = P(x_{n-1})$, and $x_1 = P(x_n)$. Prove that all the x_i's are equal.

Walkthrough — Show that

$$a_1 - a_2 \mid a_2 - a_3 \mid a_3 - a_4 \mid \cdots \mid a_n - a_1 \mid a_1 - a_2.$$

Note that sum of these differences is an odd multiple of their absolute value.

Exercise 11.7 (Tournament of Towns Spring 2014, Senior A Level P4, by G.K. Zhukov)**.** In the plane, the points with integer coordinates (x, y) satisfying $0 \leq y \leq 10$ are marked. Consider a polynomial of degree 20 with integer coefficients. Determine the maximum possible number of marked points which can lie on its graph.

Walkthrough —

(a)

Solution 34. Note that the polynomial

$$(x-1)(x-2)(x-3)\ldots(x-20)$$

of degree 20 has integer roots. Let us prove that the graph of no polynomial of degree 20 with integer coefficients passes through more than 20 marked points.

Claim — Let $P(x)$ be a polynomial of degree 20 with integer coefficients. No more than 20 marked points lie on the graph of $P(x)$.

Proof of the Claim. On the contrary, let us assume that there are integers $x_1 < x_2 < \cdots < x_{21}$ such that

$$0 \leq P(x_i) \leq 10$$

holds for all $1 \leq i \leq 21$. For any integer $1 \leq i \leq 10$, the inequality $x_{21} - x_i \geq 11$ holds, and using that $x_{21} - x_i$ divides the integer $P(x_{21}) - P(x_i)$, which lies in $[-10, 10]$, it follows that $P(x_{21}) = P(x_i)$. Similarly, for any integer $12 \leq i \leq 21$, it follows that $P(x_1) = P(x_i)$. This shows that $P(x_i) = P(x_1)$ for any integer $i \in \{1, 2, \ldots, 10\} \cup \{12, 13, \ldots, 21\}$. Since $P(x)$ is a polynomial of degree 20, it follows that

$$P(x) - P(x_1) = c(x - x_1)(x - x_2)\ldots(x - x_{10})(x - x_{12})(x - x_{13})\ldots(x - x_{21})$$

holds for some nonzero integer a. This yields that

$$|P(x_{11}) - P(x_1)| \geq (10!)^2,$$

which is impossible. □

This proves that the maximum possible number of marked points which can lie on the graph of a polynomial of degree 20 with integer coefficients is equal to 20. ■

Lemma 5

Let P be a polynomial with integer coefficients. Suppose a is an integer and k is a positive integer such that $P^k(a) = a$, where P^k denotes the k-fold composite map from $\mathbb{Z} \to \mathbb{Z}$. Show that $P^2(a) = a$.

Proof. Let ℓ denote the smallest positive integer such that $P^\ell(a) = a$. If $\ell = 1$ or $\ell = 2$, then we are done. Henceforth, we assume that $\ell \geq 3$.

Note that

$$P(a) - a \mid P^2(a) - P(a) \mid \cdots \mid P^\ell(a) - P^{\ell-1}(a) = a - P^{\ell-1}(a) \mid P(a) - a.$$

Since $a - P^{\ell-1}(a)$ is nonzero, it follows that the above differences are nonzero. Consequently, for any $1 \leq i \leq \ell$,

$$P^{i+1}(a) - P^i(a) = \pm(P^i(a) - P^{i-1}(a)).$$

If $P^{i+1}(a) = P^{i-1}(a)$ holds for some $1 \leq i \leq \ell$, then applying $P^{\ell-i+1}$ to both sides, we obtain $P^2(a) = a$, which contradicts the assumption that $\ell \geq 3$. It follows that for any $1 \leq i \leq \ell$,

$$P^{i+1}(a) - P^i(a) = P(a) - a$$

holds, which implies that

$$\sum_{i=0}^{\ell-1} (P^{i+1}(a) - P^i(a)) = \ell(P(a) - a).$$

This gives $P(a) = a$, which contradicts the assumption that $\ell \geq 3$. This completes the proof. □

Exercise 11.8 (IMO 2006 P5, AoPS, by Dan Schwarz, Romania)**.** Let $P(x)$ be a polynomial of degree $n > 1$ with integer coefficients, and let k be a positive integer. Consider the polynomial $Q(x) = P(P(\ldots P(P(x))\ldots))$, where P occurs k times. Prove that there are at most n integers t such that $Q(t) = t$.

Walkthrough —

(a) Does the above lemma help?

Solution 35. By the above lemma, it reduces to considering the case $Q(x) = P^2(x)$.

Suppose Q has more than n fixed points. Since P is not linear, it follows that P cannot have n fixed points, and hence not all the fixed points of Q are fixed points of P. Let b be a non-fixed point of P, and $Q(b) = b$. Suppose a be a fixed point of Q, other than b.

Let us first consider the case that $P(a) \neq a$. Note that

$$P(b) - a \mid P(a) - b \mid P(b) - a$$

holds, and

$$a - b \mid P(a) - P(b) \mid a - b$$

holds too. This yields that

$$|P(a) - b| = |P(b) - a|, \quad |P(a) - P(b)| = |a - b|.$$

If

$$P(a) - b = a - P(b), \text{ and } P(a) - P(b) = a - b$$

hold, then b would be a fixed point of P. It follows that at least one of

$$P(a) - b = -(a - P(b)), P(a) - P(b) = -(a - b)$$

holds. Consequently, we obtain

$$P(a) + a = P(b) + b.$$

Next, let us consider the case that $P(a) = a$. Note that

$$P(b) - a \mid b - a \mid P(b) - a.$$

Since b is not a fixed point for P, it follows that

$$P(b) - a = a - b,$$

which yields

$$P(a) + a = P(b) + b.$$

This proves that all the roots of $Q(x) = x$ are the roots of $P(x) + x = P(b) + b$. Since $P(x)$ has degree $n > 1$, it follows that the polynomial $P(x) + x - P(b) - b$ is of degree n, and it has more than n roots, which is impossible.

Hence, there are at most n integers t such that $Q(t) = t$ holds. ■

§12 Primes, divisors, and congruences

Example 12.1 (Infinitude of primes). [Sai06] Let $a_1 = 2$ and $a_{n+1} = a_n(a_n+1)$. Show that a_n has at least n distinct prime factors.

Exercise 12.2 (Tournament of Towns Fall 2019, Junior, O Level P4, by Boris Frenkin). There are given 1000 integers $a_1, \ldots, a_{1000}$. Their squares $a_1^2, \ldots, a_{1000}^2$ are written along the circumference of a circle. It so happened that the sum of any 41 consecutive numbers on this circle is a multiple of 41^2. Is it necessarily true that every integer $a_1, \ldots, a_{1000}$ is a multiple of 41?

> **Remark.** Replace 1000 by 10 and 41 by 7, and try to work on the problem.

Solution 36. For any integer m, let $\overline{m}$ denote the integer lying between 1 and 1000, which is congruent to m modulo 1000. Note that

$$a_i^2 \equiv a_j^2 \bmod 41^2$$

holds for any integers i, j lying between 1 and 1000, and satisfying $i \equiv j \bmod 41$. It follows that

$$a_1^2 \equiv a_{\overline{41k+1}}^2 \bmod 41^2$$

for any integer k. Since the integers $41, 1000$ are relatively prime, it follows that the integers

$$41, 41 \cdot 2, 41 \cdot 3, \ldots, 41 \cdot 1000$$

are pairwise distinct modulo 1000, that is, these integers are congruent to $1, 2, \ldots, 1000$ modulo 1000 in some order. This shows that a_1^2 is congruent to a_i^2 modulo 41^2 for any integer $1 \le i \le 1000$. It follows that

$$41a_1^2 \equiv a_1^2 + a_2^2 + \cdots + a_{41}^2 \bmod 41^2$$

Since the sum $a_1^2 + a_2^2 + \cdots + a_{41}^2$ is divisible by 41^2, this shows that 41 divides a_1. For any integer $1 \le i \le 1000$, 41^2 divides $a_1^2 - a_i^2$, and using that 41 divides a_1, we obtain 41 divides a_i.

This proves that it is necessary that every integer $a_1, \ldots, a_{1000}$ is a multiple of 41. ■

Example 12.3 (Tournament of Towns, India RMO 1995 P3). [Tao06, Problem 2.1] Prove that among any 18 consecutive three digit numbers there is at least one number which is divisible by the sum of its digits.

> **Walkthrough** —
>
> **(a)** Show that one among any such consecutive integers is divisible by 18.
>
> **(b)** Prove that its sum of digits, is a multiple of 9, and conclude that it is

equal to one of $9, 18, 27$.

(c) Show that the sum of its digits is not 27.

Solution 37. Note that among 18 consecutive three digit numbers, there is an integer divisible by 18. Denote it by $n = 100a + 10b + c$ with a, b, c denoting integers lying between 0 and 9. It follows that 9 divides n, and hence 9 divides $a + b + c$. This shows that $a + b + c$ is equal to one of $9, 18, 27$. Note that $a + b + c = 27$ holds only if $n = 999$. Since 18 divides n, it follows that $a + b + c \neq 27$, and hence, $a + b + c$ is equal to one of $9, 18$. This proves that $a + b + c$ divides n. ■

Exercise 12.4 (China TST 1995 Day 1 P1, AoPS)**.** Find the smallest prime number p that cannot be represented in the form $|3^a - 2^b|$, where a and b are non-negative integers.

Walkthrough —

(a) Any prime smaller than 41 can be expressed as the absolute value of the difference of a nonnegative power of 3 and a nonnegative power of 2.

(b) If $41 = 2^b - 3^a$, then $b \geq 3$ and hence $3^a \equiv -1 \bmod 8$, which is impossible.

(c) Assume that $41 = 3^a - 2^b$. Considering congruence modulo 3, show that b is an even positive integer. Reduce modulo 4 to show that a is even.

(d) Write $a = 2x, b = 2y$, and factorize 41.

(e) Conclude by obtaining a contradiction.

Solution 38. Note that any prime smaller than 41 can be expressed as the absolute value of the difference of a nonnegative power of 3 and a nonnegative power of 2, as shown below.

$$\begin{aligned} 2 &= 3 - 1, \\ 3 &= 4 - 1, \\ 5 &= 9 - 4, \\ 7 &= 8 - 1, \\ 11 &= 27 - 16, \\ 13 &= 16 - 3, \\ 17 &= 81 - 64, \\ 19 &= 27 - 8, \\ 23 &= 32 - 9, \\ 29 &= 32 - 3, \\ 31 &= 32 - 1, \\ 37 &= 64 - 27. \end{aligned}$$

Let us prove the following claim.

Claim — The prime number 41 cannot be expressed as the absolute value of the difference of a nonnegative power of 3 and a nonnegative power of 2.

Proof of the Claim. On the contrary, let us assume that

$$41 = |3^a - 2^b|$$

holds for some nonnegative integers a, b.

First, let us consider the case that $41 = 2^b - 3^a$. Note that $b \geq 3$ holds, and reducing the above modulo 8, it follows that $3^a \equiv -1 \pmod 8$, which is impossible.

Now, let us consider the case that $41 = 3^a - 2^b$. Reducing modulo 3, it follows that $2^b \equiv 1 \pmod 3$, which shows that b is even. Note that b is nonzero. Next, reducing modulo 4, we obtain $3^a \equiv 1 \pmod 4$, which implies that a is even. Writing $a = 2x, b = 2y$ for some positive integers x, y, we obtain

$$41 = 3^{2x} - 2^{2y} = (3^x - 2^y)(3^x + 2^y)$$

with $1 \leq 3^x - 2^y < 3^x + 2^y$, which yields

$$3^x - 2^y = 1, 3^x + 2^y = 41,$$

which is impossible.

Considering the above cases, the claim follows. □

This proves that 41 is smallest prime that cannot be expressed in the given form. ■

Example 12.5 (Bay Area MO 2000 P1)**.** Prove that any integer greater than or equal to 7 can be written as a sum of two relatively prime integers, both greater than 1.

Walkthrough — Consider the case of an odd integer, the case of a multiple of 4, and the case of an even integer, which is not a multiple of 4.

Solution 39. Note that any odd integer can be expressed as the sum of two relatively prime integers. Indeed, for any integer n, the integer $2n + 1$ is the sum of the relatively prime integers $n, n + 1$.

For any integer k, note that

$$4k = (2k - 1) + (2k + 1)$$

holds, and the integers $2k - 1, 2k + 1$ are relatively prime since any of their common divisors is odd and divides $(2k + 1) - (2k - 1) = 2$.

For any integer ℓ, note that

$$4\ell + 2 = (2\ell - 1) + (2\ell + 3)$$

holds, and the integers $2\ell - 1, 2\ell + 3$ are relatively prime since any of their common divisors is odd and divides $(2\ell + 3) - (2\ell - 1) = 4$. ■

§13 Gauss's lemma

Exercise 13.1 (ELMO 2009, AoPS, proposed by Evan O'Dorney)**.** Let a, b, c be positive integers such that $a^2 - bc$ is a square. Prove that $2a + b + c$ is not prime.

Walkthrough —

(a) Consider the quadratic polynomial $p(x) = bx^2 + 2ax + c$.

(b) Show that its discriminant is a perfect square.

(c) Use Gauss's lemma to show that $p(x)$ can be factored into linear polynomials with integer coefficients.

(d) Note that the roots of $p(x)$ are negative rationals.

(e) Conclude that $p(x)$ can be factored into linear polynomials with positive integer coefficients.

(f) Conclude that $p(1) = 2a + b + c$ is not a prime

Solution 40. Consider the quadratic polynomial $p(x) = bx^2 + 2ax + c$ with integer coefficients. Since its discriminant is a perfect square, it follows that its roots are rational, that is, it can be factored over the rationals. By Gauss's lemma, $p(x)$ can be factored into linear polynomials with integer coefficients. Since the leading coefficient of $p(x)$ is positive, it follows that it can be factored into linear polynomials with integer coefficients and having positive leading coefficients. Note that the roots of $p(x)$ are negative rationals. This proves that $p(x)$ can be factored into linear polynomials with positive integer coefficients. Noting that $p(1) = 2a + b + c$, it follows that $2a + b + c$ is not a prime. ■

Remark. Note that in the above, one may prove that $p(x)$ can be factored into linear polynomials with integer coefficients without using Gauss's lemma, possibly by establishing the lemma in this specific case. In fact, the above problem could serve as an introduction to Gauss's lemma.

§14 Irreducibility

Theorem 6 (Eisenstein's criterion)

Let

$$f(x) = a_n x^n + \cdots + a_1 + a_0$$

be a polynomial with integer coefficients. Let p be a prime number and assume that

$$\begin{aligned} a_n &\not\equiv 0 \bmod p, \\ a_{n-1}, \ldots, a_0 &\equiv 0 \bmod p, \\ a_0 &\not\equiv 0 \bmod p^2 \end{aligned}$$

holds. Then $f(x)$ cannot be expressed as a product of two non-constant polynomials with rational coefficients.

Example 14.1. [Art91, Chapter 11, Exercise 4.10, p. 444] Let

$$f(x) = a_{2n+1}x^{2n+1} + a_{2n}x^{2n} + \cdots + a_1 x + a_0$$

be a polynomial of degree $2n+1$ with integer coefficients. Let p be a prime number and assume that

$$\begin{aligned} a_{2n+1} &\not\equiv 0 \bmod p, \\ a_0, a_1, \ldots, a_n &\equiv 0 \bmod p^2, \\ a_{n+1}, \ldots, a_{2n} &\equiv 0 \bmod p, \\ a_0 &\not\equiv 0 \bmod p^3. \end{aligned}$$

Show that $f(x)$ cannot be expressed as a product of two non-constant polynomials with rational coefficients.

Example 14.2. For any prime p, show that there exist non-constant monic polynomials $f_p(x), g_p(x)$ with integer coefficients such that

$$x^4 - 10x^2 + 1 \equiv f_p(x)g_p(x) \bmod p$$

holds. Can the polynomial $x^4 - 10x^2 + 1$ be expressed as the product of two non-constant polynomials with rational coefficients?

§15 Order

Let p be a prime, and a be an integer, not divisible by p. The *order of a modulo p*, denoted by $\mathrm{ord}_p(a)$, is defined to be the smallest positive integer such that $a^{\mathrm{ord}_p(a)} \equiv 1 \bmod p$.

Example 15.1 (Tournament of Towns, India RMO 2014a P3)**.** [**Tao06**, Problem 2.2] [**AE11**, Problem 3.81] Suppose for some positive integers r and s, 2^r is obtained by permuting the digits of 2^s in decimal expansion and $2^r, 2^s$ have same number of digits. Prove that $r = s$.

Solution 41. Since a positive integer is congruent to the sum of its digits modulo 9, it follows that 2^r and 2^s are congruent modulo 9.

Let us consider the case that $r < s$. Note that 9 divides $2^{s-r} - 1$. Since the order of 2 modulo 9 is equal to 6, it follows that 6 divides $s - r$, and hence $2^s \geq 64 \cdot 2^r$, which is impossible. This shows that $r \geq s$ holds. Similarly, it also follows that $s \geq r$ holds. This proves that $s = r$, as required. ■

Example 15.2 (Mathematical Ashes 2011 P2)**.** Find all pairs (m, n) of nonnegative integers for which

$$m^2 + 2 \cdot 3^n = m(2^{n+1} - 1).$$

Walkthrough —

(a) Let m, n be nonnegative integers satisfying the given equation. Considering the roots of $x^2 - x(2^{n+1} - 1) + 2 \cdot 3^n$, it follows that

$$3^k + 2 \cdot 3^\ell = 2^{n+1} - 1$$

holds, for some nonnegative integers k, ℓ satisfying $k + \ell = n$.

(b) Show that if $n \geq 6$, then $\min\{k, \ell\} \geq 2$ holds. Note that

$$3^k < 2^{n+1} < 9^{(n+1)/3}$$

holds, implying $k < 2(n+1)/3$. Also note that

$$2 \cdot 3^\ell < 2^{n+1} < 2 \cdot 3^{2n/3}$$

holds, implying $\ell < 2n/3$. Using $k + \ell = n$, it follows that

$$k > \frac{n-2}{3}, \ell > \frac{n-2}{3}.$$

(c) Let us consider the case[a] that $n \geq 6$. Note that $m := \min\{k, \ell\} \geq 2$ holds.

(i) Note that 9 divides $2^{n+1} - 1$, and show that 6 divides $n+1$. Writing $n + 1 = 6j$ yields

$$2^{n+1} - 1 = (4^j - 1)(4^{2j} + 4^j + 1) = (2^j - 1)(2^j + 1)((4^j - 1)^2 + 3 \cdot 4^j).$$

(ii) Noting that $(4^j - 1)^2 + 3 \cdot 4^j$ is divisible by 3, but not by 9, and that the integers $2^j - 1, 2^j + 1$ are coprime, conclude that 3^{m-1} divides one of $2^j - 1, 2^j + 1$.

(iii) Prove that

$$3^{m-1} \le 2^j + 1 \le 3^j = 3^{\frac{n+1}{6}},$$

implying

$$m - 1 \le \frac{n+1}{6}.$$

(iv) Conclude that

$$\frac{n-2}{3} - 1 < m - 1 \le \frac{n+1}{6}.$$

holds.

(v) This yields $n < 11$, contradicting $n \ge 6$ and 6 divides $n+1$.

(d) It remains to consider the case $n \le 5$.

[a] It also suffices to assume that $n \ge 5$ holds to obtain $m \ge 2$.

§16 Primitive roots

Given a prime p, and an integer a, define the *Legendre symbol* $\left(\frac{a}{p}\right)$ by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \text{ divides } a, \\ 1 & \text{if } p \text{ does not divide } a, \text{ and } a \equiv m^2 \bmod p \text{ for } \textbf{some} \text{ integer } m, \\ -1 & \text{if } p \not\equiv m^2 \bmod p \text{ for } \textbf{every} \text{ integer } m. \end{cases}$$

Exercise 16.1. Show that

$$\left(\frac{-3}{p}\right) = 1 \quad \text{if } p \equiv 1 \bmod 3.$$

Walkthrough — Show that

$$(2\xi + 1)^2 \equiv -3 \bmod p$$

holds for any integer ξ, which is of order 3 modulo p. Does such an integer exist?

Exercise 16.2. Show that

$$\left(\frac{5}{p}\right) = 1 \quad \text{if } p \equiv 1 \bmod 5.$$

Walkthrough — Show that

$$(\xi + \xi^4)^2 + (\xi + \xi^4) \equiv 1 \bmod p$$

holds for any integer ξ, which is of order 5 modulo p. Does such an integer exist?

§17 Quadratic residues

Henceforth, p denotes an odd prime.

Exercise 17.1. Show that the number of solutions of $x^2 \equiv a \bmod p$ is given by

$$1 + \left(\frac{a}{p}\right).$$

Exercise 17.2 (Counting squares and non-squares)**.** Show that

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Exercise 17.3. Prove that

$$\sum_{x=0}^{p-1} \left(\frac{ax+b}{p}\right) = 0$$

holds for any integers a, b with $p \nmid a$.

Note that the sums in the above problems are over different sets.

Exercise 17.4. Let a be an integer. Show that the number of solutions to $x^2 - y^2 \equiv a \bmod p$ is given by

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2+a}{p}\right)\right).$$

Exercise 17.5. Let a be an integer. Prove that the number of solutions to $x^2 - y^2 \equiv a \bmod p$ is equal to

$$\begin{cases} p-1 & \text{if } p \nmid a, \\ 2p-1 & \text{if } p \mid a. \end{cases}$$

Corollary 7

Prove that

$$\sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right) = \begin{cases} -1 & \text{if } p \nmid a, \\ p-1 & \text{if } p \mid a, \end{cases}$$

$$\sum_{y=0}^{p-1} \left(\frac{a-y^2}{p}\right) = \begin{cases} -\left(\frac{-1}{p}\right) & \text{if } p \nmid a, \\ (p-1)\left(\frac{-1}{p}\right) & \text{if } p \mid a. \end{cases}$$

Lemma 8

Let p be an odd prime. Then for any integer a, the congruence

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$$

holds.

Walkthrough — Count the squares! Does Exercise 17.2 help?

Exercise 17.6 (China TST 2009 P6, AoPS)**.** Determine whether there exists an arithmetic progression consisting of 40 terms and each of whose terms can be written in the form $2^m + 3^n$ or not, where m, n are nonnegative integers.

Here is an argument by AoPS user iceillusion.

Walkthrough —

(a) On the contrary, let us assume that there exists such a progression of length 23.

(b) Put $p = 23$. Note that

$$\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1, \quad \left(\frac{-1}{p}\right) = -1.$$

It follows that the terms of the progression are nonzero modulo p, and hence at two of those 23 term progression are congruence modulo p. This shows that their common difference is divisible by p, and hence the 23 terms are congruent to a nonzero residue a modulo p.

(c) Prove the following.

> **Claim** — For any integer a with $p \nmid a$, the number of pairs (x, y) of nonzero quadratic residues modulo p, satisfying $x + y \equiv a \bmod p$ is equal to
>
> $$\begin{aligned} &= \frac{1}{4}\sum_{y=1}^{p-1}\left(1 + \left(\frac{a-y^2}{p}\right)\right) - \frac{1}{4}\left(1 + \left(\frac{a}{p}\right)\right) \\ &= \frac{1}{4}\left(p - 1 - \left(\frac{-1}{p}\right) - \left(\frac{a}{p}\right) - \left(1 + \left(\frac{a}{p}\right)\right)\right) \\ &= \frac{1}{4}\left(p - 2 - \left(\frac{-1}{p}\right) - 2\left(\frac{a}{p}\right)\right). \end{aligned}$$

(d) Consider the 23 pairs $(2^m, 3^n)$ corresponding to the 23 terms of the progression. Note that these pairs, when reduced modulo p, can take at

most

$$\frac{1}{4}\left(p-2-\left(\frac{-1}{p}\right)-2\left(\frac{a}{p}\right)\right) \leq \frac{p-3}{4} = 5$$

values. By the pigeonhole principle, it follows that at least five pairs among these 23 pairs, are congruent to each other modulo p.

(e) Note that the integers $2, 3$ are of order 11 modulo 23. It follows that the pairs of the exponents (m, n), corresponding to these five congruent pairs, are congruent to each other modulo 11.

(f) This produces three suitable positive integers of the form $x + k_1 d, x + k_2 d, x + k_3 d$, with $1 \leq k_1 < k_2 < k_3 \leq 22$.

(g) Obtain a contradiction!

Solution 42. ■

Lemma 9

Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Proof. Let $\mathbb{Z}[i]$ denote the set of complex numbers whose real and imaginary parts are integers. For two elements z_1, z_2 of $\mathbb{Z}[i]$, we write

$$z_1 \equiv z_2 \bmod p$$

if the real part and the imaginary part of $z_1 - z_2$ are multiples of p.

Note that

$$(1+i)^p = (1+i)(2i)^{(p-1)/2} = (1+i)i^{(p-1)/2}2^{(p-1)/2}$$

holds, which yields

$$\left(\frac{2}{p}\right)(1+i)i^{(p-1)/2} \equiv 1 + i(-1)^{(p-1)/2} \bmod p.$$

This shows that

$$\left(\frac{2}{p}\right) = \begin{cases} (-1)^{(p-1)/4} & \text{if } \frac{p-1}{2} \text{ is even,} \\ (-1)^{(p+1)/4} & \text{if } \frac{p-1}{2} \text{ is odd.} \end{cases}$$

□

References

[**AE11**] Titu Andreescu and Bogdan Enescu. *Mathematical Olympiad treasures*. Second. Birkhäuser/Springer, New York, 2011, pp. viii+253. ISBN: 978-0-8176-8252-1; 978-0-8176-8253-8 (cited p. 43)

[**Art91**] Michael Artin. *Algebra*. Englewood Cliffs, NJ: Prentice Hall Inc., 1991, pp. xviii+618. ISBN: 0-13-004763-5 (cited p. 42)

[**GA17**] Răzvan Gelca and Titu Andreescu. *Putnam and beyond*. Second. Springer, Cham, 2017, pp. xviii+850. ISBN: 978-3-319-58986-2; 978-3-319-58988-6. DOI: 10.1007/978-3-319-58988-6. URL: https://doi.org/10.1007/978-3-319-58988-6

[**Goy21**] Rohan Goyal. "Polynomials". Available at https://www.dropbox.com/s/yo31nat6z5ggaue/Polynomials.pdf?dl=0. 2021 (cited p. 4)

[**Sai06**] Filip Saidak. A new proof of Euclid's theorem. In: *Amer. Math. Monthly*, **113**:10 (2006), pp. 937–938. ISSN: 0002-9890. DOI: 10.2307/27642094. URL: http://dx.doi.org/10.2307/27642094 (cited p. 38)

[**Tao06**] Terence Tao. *Solving mathematical problems*. A personal perspective. Oxford University Press, Oxford, 2006, pp. xii+103. ISBN: 978-0-19-920560-8; 0-19-920560-4 (cited pp. 38, 43)