IMOTC 2025

Jyoti Prakash Saha

17 May 2025

List of problems and examples

Contents

§1 Warm up

Example 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.

Summary — Note that

$$x^2+y^2+z^2-xy-yz-zx=(x-y)^2+(z-*)^2-\dots.$$

§2 Polynomials

For further problems, we refer to [Goy21].

§2.1 Warm up

Example 2.1 (Moscow MO 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.

§2.2 Even and odd polynomials

Example 2.2 (Moscow MO 1946 Grades 7–8 P5)**.** Prove that after completing the multiplication and collecting the terms

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

has no monomials of odd degree.

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

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 $k=1,2,\dots,n$. Prove that there is a polynomial $q(x)$ such that $p(x)=q(x^2)$.

Walkthrough — 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?

Example 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.

§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?

Example 2.6 (USAMO 1975 P3)**.** A polynomial $P(x)$ of degree n satisfies

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

Find $P(n+1)$.

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 $-1 \le x \le 1$, and hence $P(x) = f(x^2)$.

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

(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 $n \ge 1$ 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.

Example 2.13 (Putnam 1999 A2)**.** 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.

§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 $r \ge 2$ (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 $P(x)$.

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

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

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 $P-Q$.

§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.

(d) Does this help?

[a]What does it mean?

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

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

or show that this is impossible.

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

§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)**.** Let $P(x)$ be a nonconstant polynomial whose coefficients are positive integers. If $P(n)$ divides $P(P(n) - 2015)$ for all natural numbers n, then prove that $P(-2015) = 0$.

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

§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 $(0, 1)$.

Example 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 $0 < x < 1$.

§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 (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 $P(x) = c(x - 1)^n$.

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

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

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 (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.

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

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

§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

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

Example 8.2 (USAMO 2014 P1)**.** 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.

Example 8.3 (USAMO 1976 P5)**.** 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 $P(x)$.

Example 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 $\sum_{i=1}^{50} a_i x^i$.

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.

§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.

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.

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.

Example 9.5 (China TST 1995 Day 2 P2)**.** 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?

§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 1. 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?

Example 10.4 (USAMO 2002 P3)**.** 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?

Example 10.5 (Putnam 1968 A6)**.** 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.

§11 Integer divisibility

Lemma 5

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

Example 11.1. 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 11.2 (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.

Example 11.3. 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.

Example 11.4 (USAMO 1974 P1)**.** 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 $P(c) = a$.

Here is a more general result.

Example 11.5. 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.

Example 11.6 (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.

Lemma 6

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 $P^2(a) = a$.

Example 11.7 (IMO 2006 P5)**.** (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 $Q(t) = t$.

§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.

Example 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?

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.

Example 12.4 (China TST 1995 Day 1 P1)**.** 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.

Solution 2. 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.

§13 Gauss's lemma

Example 13.1 (ELMO 2009 P1, 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.

Solution 3. 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.

The following is an argument from Mandar Kasulkar.

Solution 4. Let x be a nonnegative integer such that $a^2 - bc = x^2$. Note that

$$\begin{aligned}(2a + b + c)(2a - b - c) &= 4a^2 - (b + c)^2 \\ &= 4a^2 - 4bc + (b - c)^2 \\ &= 4x^2 - (b - c)^2 \\ &= (2x - b + c)(2x + b - c)\end{aligned}$$

holds. Also note that

$$\begin{aligned}-(2a + b + c) &< 2x - b + c \\ &< 2a - b + c \\ &< 2a + b + c, \\ -(2a + b + c) &< 2x + b - c \\ &< 2a + b - c \\ &< 2a + b + c.\end{aligned}$$

If $2a = b + c$, then $2a + b + c$ is not a prime. It remains to consider the case $2a \neq b + c$, which we assume from now on. It follows that the integers $2x - b + c, 2x + b - c$ are nonzero, and lies strictly between $-p$ and p. Since their product is a multiple of $2a + b + c$, we conclude that $2a + b + c$ is not a prime. ■

§14 Irreducibility

Theorem 7 (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 5. 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 8

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 9

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?

Example 17.6 (China TST 2009 P6)**.** 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!

Lemma 10

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. 19)

[**Art91**] Michael Artin. *Algebra*. Englewood Cliffs, NJ: Prentice Hall Inc., 1991, pp. xviii+618. ISBN: 0-13-004763-5 (cited p. 18)

[**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. 15)

[**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. 15, 19)