IMOTC 2026

Jyoti Prakash Saha

§1 Warm up

Exercise 1 (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?

Exercise 2 ()**.** Provide a bijection between the set of positive integers and the set of pairs of positive integers.

Walkthrough —

(a) Does decomposing a positive integer as a product of a power of 2 and an odd integer help?

(b) Show that the map

$$(m, n) \mapsto 2^{m-1}(2n - 1)$$

defines a bijection from $\mathbb{Z}_{\geq 1} \times \mathbb{Z}_{\geq 1}$ to $\mathbb{Z}_{\geq 1}$.

Does

$$(p, q) \mapsto \binom{p+q}{2} + q$$

work?

Exercise 3 (Danube Mathematical Competition, Junior 2019 P2,)**.** Prove that for any real numbers $a_1, a_2, \ldots, a_n$ with $n \in \mathbb{N}$, there exists a real number x such that the numbers $x + a_1, x + a_2, \ldots, x + a_n$ are all irrational.

Walkthrough —

(a) Under what condition on x, it is false that all of the numbers $x + a_1, x + a_2, \ldots, x + a_n$ are irrational?

(b) What can be said about the set of real numbers x such that at least one of the numbers $x + a_1, x + a_2, \ldots, x + a_n$ is rational?

Exercise 4 (Brazil National Olympiad 2020 Level 3 P1,). Prove that there are positive integers $a_1, a_2, \ldots, a_{2020}$ such that

$$\frac{1}{a_1} + \frac{1}{2a_2} + \frac{1}{3a_3} + \cdots + \frac{1}{2020a_{2020}} = 1.$$

Walkthrough —

(a) Show that for any positive integer n, there exist positive integers $a_1, a_2, \ldots, a_n$ such that

$$\frac{1}{a_1} + \frac{1}{2a_2} + \frac{1}{3a_3} + \cdots + \frac{1}{na_n} = 1.$$

(b) Observe that $1 = \frac{1}{2} + \frac{1}{2}$, $1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6}$, $1 = \frac{1}{2} + \frac{1}{6} + \frac{1}{4} + \frac{1}{12}$ etc. hold.

(c) Also note that

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

Exercise 5 (Romania JBMO TST 1999 Day 1 P3,). 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 $(0, 1)$.

Walkthrough —

(a) Taking $x = \frac{1}{2}$, it follows that S contains $\frac{2}{3}$, and hence it also contains $\frac{1}{3}$.

(b) Taking $x = \frac{1}{2}$, it follows that S contains $\frac{1}{4}$. Next, taking $x = \frac{1}{3}$, we obtain that S contains $\frac{3}{4}$.

(c) Applying the map $x \mapsto \frac{1}{x+1}$ to $x = \frac{2}{3}, \frac{1}{4}$, it follows that S contains $\frac{3}{5}, \frac{4}{5}$. Since S contains $\frac{4}{5}$, the set S also contains $\frac{2}{5}, \frac{1}{5}$.

(d) Applying $x \mapsto \frac{1}{x+1}$ to $x = \frac{1}{5}$, it follows that S contains $\frac{5}{6}$. Note that S contains $\frac{4}{6} = \frac{2}{3}, \frac{3}{6} = \frac{1}{2}, \frac{2}{6} = \frac{1}{3}$. It also follows that S contains $\frac{1}{6}$.

(e) Does the above provide any insight into the problem? Can one expect the following?

The rationals lying in $(\frac{1}{2}, 1)$ can be obtained by applying the map $x \mapsto \frac{1}{x+1}$ to the rationals lying in $(0, 1)$ with small denominators. Moreover, a rational number r lying in $(0, \frac{1}{2})$ can be obtained by applying the map $x \mapsto \frac{x}{2}$ to the rationals lying in $(\frac{1}{2}, 1)$, more specifically, to those rationals with denominators at most the denominator of r.

Exercise 6 (IMOSL 2006 N2, , proposed by J. P. Grossman, Canada,). For $x \in (0, 1)$, let $y \in (0, 1)$ be the number whose n-th digit after the decimal point is the 2^n-th digit after the decimal point of x. Show that if x is rational then so is y.

Walkthrough —

(a) Assume that x is a rational number. Let k be the period of the decimal expansion of x.

(b) To show that y is rational, or equivalently, to show that the decimal expansion of y is eventually periodic, it suffices to prove that there exists a positive integer α such that

$$2^{n+\alpha} \equiv 2^n \pmod{k}$$

holds for all sufficiently large positive integers n.

§2 Induction

Here is a proof of Euclid's theorem on the infinitude of primes by Filip Saidak.

Exercise 7 (Infinitude of primes). Let $a_1 = 2$ and $a_{n+1} = a_n(a_n + 1)$ for any positive integer n. Show that a_n has at least n distinct prime factors for any positive integer n.

Walkthrough —

(a) Show that $a_n \geq 2$ for any integer $n \geq 1$.

(b) Note that the integers $a_n, a_n + 1$ have no common prime factor.

(c) Conclude using induction.

Exercise 8 (Infinitude of primes). Show that there are infinitely many primes of the form $4n + 3$.

Walkthrough —

(a) Can Saidak's proof be adapted to show that there are infinitely many primes of the form $4n + 3$?

(b) Does taking $a_1 = 3$ and $a_{n+1} = a_n(4a_n - 1)$ work?

§3 Infinite descent

Exercise 9 (Moscow Mathematical Olympiad First Round 1949 Grades 7–8 P3)**.** Show that the only solution of the equation

$$x^2 + y^2 + z^2 = 2xyz$$

for x, y, z in the integers is $x = y = z = 0$.

Walkthrough —

(a) Let x, y, z be integers satisfying $x^2 + y^2 + z^2 = 2xyz$. Show that at least one of the integers x, y, z is even.

(b) Show that the sum of the squares of some two of the integers x, y, z is divisible by 4.

(c) Prove that x, y, z are all divisible by 2, and satisfy a similar equation.

(d) Prove that 2^n divides x, y, z for all $n \geq 1$, and conclude that $x = y = z = 0$.

Exercise 10 (Kürschák Competition 1983 P1,)**.** Let x, y and z be rational numbers satisfying the equation

$$x^3 + 3y^3 + 9z^3 - 9xyz = 0.$$

Prove that $x = y = z = 0$.

Walkthrough —

(a) Show that if a, b, c are integers satisfying

$$a^3 + 3b^3 + 9c^3 = 9abc,$$

then 3 divides a, and $(b, c, a/3)$ also satisfies the above equation.

(b) If (x, y, z) is a non-trivial integer solution to the given equation with $|x| + |y| + |z|$ minimum, show that x is nonzero, and that $y, z, x/3$ is also a solution to the given equation.

Remark. The method used in the above solution is known as *infinite descent*. The idea is to show that if there is a non-trivial solution to the given equation, then there is a **smaller** non-trivial solution. This leads to an infinite sequence of smaller and smaller non-trivial solutions, which is impossible for positive integers.

Remark. One may also observe that a solution (a, b, c) to the given equation yields a solution $(a/3, b/3, c/3)$ to the same equation. Indeed, if (a, b, c) is a solution, then $(b, c, a/3)$ is also a solution by the above claim. Applying the claim again, we obtain that $(c, a/3, b/3)$ is also a solution. Applying the claim once more, we obtain that $(a/3, b/3, c/3)$ is also a solution. Hence, if there is a non-trivial solution to the given equation, then there is a "**smaller**" non-trivial solution, which is impossible.

Exercise 11 (BStat-BMath 2012 P5)**.** Let m be a natural number with digits consisting entirely of 6's and 0's. Prove that m is not the square of a natural number.

Walkthrough —

(a) Note that if any such number is a perfect square, then its last digit cannot be 6, that is, it is not congruent to 6 modulo 10, because no square is congruent to any of $6, 66$ modulo 100.

(b) It follows that if any such number is perfect square, then it is divisible by 100.

(c) Apply induction (on what?). A crucial step would be to frame an inductive statement appropriately.

Exercise 12 (Saudi Arabia JBMO TST 2025 Day 2 P3, ,)**.** Determine all triples (a, b, c) of integers such that

$$a^3 + b^3 + c^3 = 25(abc + a^2b + b^2c + c^2a).$$

§4 Games

Exercise 13 (Chip-firing game)**.** Assume that on the Cartesian plane, four chips are placed at the origin. In each step, you may choose a lattice point (x, y) having at least a chip on it, remove one chip from (x, y), and place one chip each at $(x + 1, y)$ and one at $(x, y + 1)$. Show that after a finite number of steps, there are at least two chips at some lattice point.

Remark. The problem seems to ask that after any number of finitely many moves, there will exist two coins placed at the same point.

Walkthrough —

(a)

Exercise 14 (Serbia IMO TST 2024 Day 1 P1,). Three coins are placed at the origin of a Cartesian coordinate system. On one move one removes a coin placed at some position (x, y) and places three new coins at $(x + 1, y)$, $(x, y + 1)$ and $(x + 1, y + 1)$. Prove that after finitely many moves, there will exist two coins placed at the same point.

Remark. The problem seems to ask that after any number of finitely many moves, there will exist two coins placed at the same point.

Walkthrough —

(a)

§5 Primes, divisors, and congruences

Exercise 15 (). Show that the square of no rational number is equal to 2.

Walkthrough —

(a) On the contrary, suppose there exist positive integers a, b such that $(a/b)^2 = 2$ and $\gcd(a, b) = 1$.

(b) This gives $a^2 - 2b^2 = 0$.

(c) Read it modulo 3, and conclude.

Exercise 16 (Japan Mathematical Olympiad 1992 P1). Let x, y be coprime positive integers with $xy > 1$, and let n be an even positive integer. Prove that $x^n + y^n$ is not divisible by $x + y$.

Walkthrough —

(a) Assume that $x + y$ divides $x^n + y^n$.

(b) Since x is congruent to $-y$ modulo $x + y$, and n is even, it follows that $x^n + y^n \equiv 2y^n \pmod{x + y}$.

(c) Conclude that $x + y$ divides 2.

Exercise 17 (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.

Walkthrough —

(a) Show that if $1 \leq i, j \leq 1000$ are integers satisfying $i \equiv j \bmod 41$, then $a_i^2 \equiv a_j^2 \bmod 41^2$.

(b) In particular, show that $a_1^2 \equiv a_{41k+1}^2 \bmod 41^2$ for any integer k.

(c) Does it follow that a_1^2 is congruent to a_i^2 modulo 41^2 for any integer $1 \leq i \leq 1000$?

(d) Show that $41a_1^2$ is congruent to $a_1^2 + a_2^2 + \cdots + a_{41}^2$ modulo 41^2, and conclude.

Exercise 18 (Dutch BxMO/EGMO TST 2025 P1,)**.** For a five-digit number $n = abcde$, we define the *twisted sum* of n as $bcdea + cdeab + deabc + eabcd$. For example, the twisted sum of 20253 is $02532 + 25320 + 53202 + 32025 = 113079$. Let m and n be two five-digit numbers with the same twisted sums. Prove that $m = n$.

Walkthrough —

(a) Consider the sum of all the integers obtained by cyclically permuting the digits of n, and denote it by $S(n)$.

(b) For a five-digit number $n = abcde$, express $S(n)$ in terms of a, b, c, d, e.

(c) Show that $S(n) = 11111 \cdot s(n)$, where $s(n)$ denotes the sum of the digits of n.

(d) Assume that m and n are two five-digit numbers with the same twisted sums. Show that $11111 \cdot (s(m) - s(n)) = m - n$.

(e) Read it modulo 9 to obtain that $m - n$ is divisible by 9.

(f) Conclude that $m = n$.

Exercise 19 (Singapore Junior Mathematical Olympiad 2024 P4, ,)**.** Suppose p is a prime number and x, y, z are integers satisfying $0 < x < y < z < p$. If x^3, y^3, z^3 have equal remainders when divided by p, prove that $x^2 + y^2 + z^2$ is divisible by $x + y + z$.

Walkthrough —

(a)

Exercise 20 (RMO 2017a P2,). Show that the equation

$$a^3 + (a+1)^3 + \cdots + (a+6)^3 = b^4 + (b+1)^4$$

has no solutions in integers a, b.

Walkthrough — Read it modulo a suitable integer ★. Are there any intuitions about the choice of ★?

Exercise 21 (Mongolian Mathematical Olympiad 2025 Grades 9-10 E2,). Show that the equation $x^4 + x^3 + x^2 + x = y^6 + 61$ has no integer solutions.

Walkthrough —

(a) Read it modulo 7.

(b) For any integer y, show that $y^6 + 61$ is congruent to one of $5, 6$ modulo 7.

(c) For any integer x, determine the possible values of $x^4 + x^3 + x^2 + x$ modulo 7.

Exercise 22 (Dutch IMO TST 2025 Day 2 P5,). Is it possible for an integer of the form $44\ldots41$ — consisting of an odd number of fours followed by a 1 — to be a square?

Exercise 23 (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.

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.

Exercise 24 (All-Russian Mathematical Olympiad 2025 Grade 11 Day 1 P3, , proposed by A. D. Tereshin,). A pair of polynomials $F(x,y)$, $G(x,y)$ with integer coefficients is called *important*, if the following condition holds: if for some integers a,b,c,d both $F(a,b)-F(c,d)$ and $G(a,b)-G(c,d)$ are divisible by 100, then both $a-c$ and $b-d$ are divisible by 100. Determine if there exist an important pair of polynomials $P(x,y)$, $Q(x,y)$ such that the pair $P(x,y)-xy$, $Q(x,y)+xy$ is also important.

Walkthrough —

(a) Assume that $(F(x,y),G(x,y))$ is an important pair of polynomials.

(b) Show that as k and ℓ range over the integers between 0 and 99, the pair $(F(k,\ell),G(k,\ell))$ takes all the 100^2 possible values modulo 100.

(c) Conclude that the pair $(F(x,y),G(x,y))$ takes the values $(0,0)$, $(1,0)$, $(0,1)$ and $(1,1)$ modulo 100, and the same statement also holds modulo 2.

(d) Does it follow that at the points $(0,0)$, $(1,0)$, $(0,1)$ and $(1,1)$, the pair $(F(x,y),G(x,y))$ takes the values $(0,0)$, $(1,0)$, $(0,1)$ and $(1,1)$ modulo 2 in some order?

(e) What can be said about the existence of an important pair $(P(x,y),Q(x,y))$ of polynomials such that the pair $(P(x,y)-xy,Q(x,y)+xy)$ is also important?

Exercise 25 (Turkey TST 2022 Day 1 P1, ,). Find all pairs (p,q) of prime numbers satisfying

$$2^p = 2^{q-2}+q!$$

Exercise 26 (French Mathematical Olympiad Preparation 2023,). Determine all the non-negative integers n such that 21 divides $2^{2^n}+2^n+1$.

Exercise 27 (Romania JBMO TST 2011 Day 4 P4, ,). Show that there is an infinite number of positive integers t such that none of the equations

$$\begin{cases} x^2+y^6=t \\ x^2+y^6=t+1 \\ x^2-y^6=t \\ x^2-y^6=t+1 \end{cases}$$

has solutions $(x,y)\in\mathbb{Z}\times\mathbb{Z}$.

Exercise 28 (Turkey TST 2014 Day 3 P2, ,). Let $(a_n)_{n=1}^{\infty}$ be a sequence of integers such that $a_1=-5$, $a_2=-6$ and

$$a_{n+1}=a_n+(a_1+1)(2a_2+1)(3a_3+1)\cdots((n-1)a_{n-1}+1)((n^2+n)a_n+2n+1)$$

for all integers $n\geq 2$. Prove that if a prime number p divides na_n+1 for some positive integer n, then there exists an integer m such that $m^2\equiv 5 \pmod p$.

Exercise 29 (Singapore Mathematical Olympiad Open Round 2 2023 P3,). Let $n \geq 2$ be a positive integer. For any integer a, let $Q_a(x)$ denote the polynomial $x^n + ax$. Let p be a prime number and S_a be the set

$$S_a = \{b \mid 0 \leq b \leq p-1, \text{ and } Q_a(c) \equiv b \bmod p \text{ holds for some integer } c\}.$$

Show that the expression $\frac{1}{p-1}\sum_{a=1}^{p-1} |S_a|$ is an integer.

Walkthrough —

(a) Note that $\sum_{a=1}^{p-1} |S_a|$ is equal to the number of ordered pairs (a, b) of integers such that $1 \leq a \leq p-1$, $0 \leq b \leq p-1$ and there exists an integer c satisfying $c^n + ac \equiv b \pmod p$.

(b) Let (a, b) be such an ordered pair. For an integer $1 \leq \lambda \leq p-1$, what can be said about the ordered pair $(\lambda^{n-1}a, \lambda^n b)$ (where the product is taken modulo p, in the sense that any integer is identified with its residue modulo p lying in $\{0, 1, \ldots, p-1\}$)?

§6 More on congruences

Exercise 30 (Estonia Math Olympiad 2025 Open Contest O14,). Is there a positive integer n such that 88 divides $2^n + n^3$?

Walkthrough — Consider congruences modulo 11.

Exercise 31 (USAJMO 2013 P1, proposed by Titu Andreescu). Are there integers a, b such that $a^5b + 3$ and $ab^5 + 3$ are both perfect cubes of integers?

Summary — Consider the integer ab modulo 3, and read $a^5b + 3, ab^5 + 3$ modulo 9.

Walkthrough —

(a) If 3 divides ab, then consider one of the integers $a^5b + 3, ab^5 + 3$ modulo 9.

(b) If 3 does not divide ab, then assuming the integers $a^5b + 3, ab^5 + 3$ to be perfect cubes, determine the integers a^5b, ab^5 modulo 9.

(c) Consider the integer $(ab)^6$ modulo 9.

Exercise 32 (Austrian Mathematical Olympiad, Regional Competition 2024 P4, , proposed by Walther Janous,). Let n be a positive integer. Prove that $a(n) = n^5 + 5^n$ is divisible by 11 if and only if $b(n) = n^5 \cdot 5^n + 1$ is divisible by 11.

Walkthrough — Does $n^5 \cdot a(n)$ agree with $b(n)$ modulo 11 under some conditions on n?

§7 Chinese remainder theorem

Exercise 33 (Canadian Mathematical Olympiad 1991 P1)**.** Show that the equation $x^2 + y^5 = z^3$ has infinitely many solutions in integers x, y, z for which $xyz \neq 0$.

Walkthrough — Note that

$$2^{10} + 2^{10} = 2^{11}$$

holds. But this does not seem to be of any help! What about $2^{20} + 2^{20}$? Also note that if (x, y, z) is a solution, then another solution can be obtained by multiplying $x^2 + y^5 = z^3$ by k^{30}, namely, $(k^{15}x, k^6y, k^{10}z)$ is also a solution.

Exercise 34 ()**.** There are infinitely many triples (x, y, z) of positive integers such that $x^2 + y^3 = z^7$.

Walkthrough —

(a) Note that $2^6 + 2^6 = 2^7$

$$(2^3)^2 + (2^2)^3 = 2^7$$

holds.

(b) Conclude that $(2^3k^{3\cdot7}, 2^2k^{2\cdot7}, 2k^{2\cdot3})$ is a solution to the above equation for any positive integer k.

Here is another argument from .

Walkthrough —

(a) Let a, b, c be positive integers satisfying $a + b = c$.

(b) Multiply the above equation by $a^pb^qc^r$ for some positive integers p, q, r to be determined later, to obtain

$$a^{p+1}b^qc^r + a^pb^{q+1}c^r = a^pb^qc^{r+1}.$$

(c) Can p, q, r be chosen such that the above equation leads to a solution of $x^2 + y^3 = z^7$? More precisely, can the above equation be rewritten as

$$(a^xb^yc^z)^2 + (a^{x'}b^{y'}c^{z'})^3 = (a^{x''}b^{y''}c^{z''})^7$$

for some integers $x, y, z, x', y', z', x'', y'', z''$?

Remark. The following is a result due to Poonen–Schaefer–Stoll , determining the primitive solutions to $x^2 + y^3 = z^7$, that is, the triples of integers having no prime factor in common and satisfying this equation. Its proof uses techniques from Arithmetic Geometry, and lies beyond the scope of this modest notes, for obvious reasons! The **only purpose** of stating the following result is to indicate that finding all solutions of prescribed nature to some equation (say, the primitive solutions to the above equation) often turns out to be a problem of considerable interest, and may require modern techniques to solve them.

Theorem 1 (Poonen, Schaefer, Stoll)
The primitive solutions to $x^2 + y^3 = z^7$ are the 16 tuples

$$(\pm 1, -1, 0), (\pm 1, 0, 1), \pm(0, 1, 1), (\pm 3, -2, 1), (\pm 71, -17, 2),$$

$$(\pm 2213459, 1414, 65), (\pm 15312283, 9262, 113), (\pm 21063928, -76271, 17).$$

Exercise 35 (RMO 2015a P3, , Canadian Mathematical Olympiad 1991 P1, Exercise 33)**.** Show that there are infinitely many triples (x, y, z) of integers, such that $x^3 + y^4 = z^{31}$.

Walkthrough —

(a) Note that

$$2^{12k} + 2^{12k} = 2^{12k+1}$$

holds.

(b) It suffices to find an positive integer k such that $12k + 1 = 31\ell$ holds for some positive integer ℓ. This shows that any such integer ℓ satisfies $\ell \equiv 1 \bmod 3$, and $\ell \equiv -1 \bmod 4$, which implies that $\ell \equiv 7 \bmod 12$. Moreover, if ℓ is congruent to 7 modulo 12, then

$$31\ell - 1 \equiv 31 * 7 - 1 \bmod 12 \equiv 7^2 - 1 \bmod 12 \equiv 0 \bmod 12$$

holds, or equivalently, there exists an integer k_ℓ such that

$$12k_\ell + 1 = 31\ell$$

holds.

(c) Note that

$$(2^{4k_\ell}, 2^{3k_\ell}, 2^\ell)$$

satisfies the given equation, for any positive integer $\ell \equiv 7 \bmod 12$.

Remark. Alternatively, one may argue as follows, motivated by the solution of ??.

Exercise 36 (RMO 2018b P3,). Show that there are infinitely many tuples (a, b, c, d) of natural numbers such that $a^3 + b^4 + c^5 = d^7$.

Walkthrough —

(a) Let x, y, z, w be positive integers satisfying $x + y + z = w$.

(b) Multiply the equation $x + y + z = w$ by $x^\alpha y^\beta z^\gamma w^\delta$ where $\alpha, \beta, \gamma, \delta$ are positive integers.

(c) Can one choose $\alpha, \beta, \gamma, \delta$ such that the resulting equation is of the form $a^3 + b^4 + c^5 = d^7$ for some positive integers a, b, c, d?

Exercise 37 (Dutch IMO TST 2021 Day 2 P3, ,). Show that for every positive integer n there exist positive integers a and b such that n divides $4a^2 + 9b^2 - 1$.

Walkthrough —

(a) Show that it suffices to consider the case that n is a prime power.

(b) Conclude the problem when n is a prime power.

Remark. If 3 does not divide n, then we can take $a = n$ and $b = \frac{n^2-1}{3}$.

§8 Order

Definition 2 (Order of an integer modulo a prime). 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 $a^{\mathrm{ord}_p(a)} \equiv 1 \bmod p$.

Lemma 3

Let p be a prime, and a be an integer, not divisible by p. Let k be an integer such that $a^k \equiv 1 \bmod p$. Then, $\mathrm{ord}_p(a)$ divides k. In particular, $\mathrm{ord}_p(a)$ divides $p - 1$. Moreover, if $a^k \equiv 1 \bmod p$, then $a^{\gcd(k, \mathrm{ord}_p(a))} \equiv 1 \bmod p$.

Exercise 38 (RMO 2014a P3, , cf. Tournament of Towns, Fall 1988, Training). Suppose for some positive integers r and s, the integer 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 $r = s$.

Walkthrough —

(a) On the contrary, assume that $r \neq s$. Without loss of generality, we may assume that $r > s$ holds.

(b) Show that $2^{r-s} - 1$ is divisible by 9.

(c) Prove that 6 divides $r - s$.

(d) Conclude that $2^r \geq 64 \cdot 2^s$ holds, contradicting the fact that 2^r and 2^s have the same number of digits.

Exercise 39 (IMO Shortlist 2010 N2, , proposed by Angelo Di Pasquale, Australia, cf. India IMOTC 2011, Mathematical Ashes 2011 P2)**.** Find all pairs (m, n) of non-negative 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) 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 $k + \ell = n$, show 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 $m \ge 2$.

Exercise 40 (Dutch BxMO/EGMO TST 2025 P5, cf. Korea Final Round 2023 P4,). Determine all positive integers n for which all prime factors of $2^n - 1$ are at most 7.

Walkthrough —

(a)

Exercise 41 (Germany TST 2010 Day 1 P3, ,). Determine all (m, n) of positive integers satisfying $3^m - 7^n = 2$.

Exercise 42 (Romania JBMO TST 2025 Day 2 P4, ,). Determine all natural numbers n such that $2^n - n^2 + 1$ is a perfect square.

§9 Primitive roots

Exercise 43. 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 44. 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?

Exercise 45 (Dutch IMO TST 2021 Day 3 P4,). Let $p>10$ be a prime number. Show that there exist positive integers m and n with $m+n<p$ for which p is a divisor of 5^m7^n-1.

Walkthrough —

(a) Express 5 and 7 as powers of a primitive root modulo p.

(b) Choose m,n suitably so that $5^m7^n\equiv 1 \bmod p$ and $m+n<p$.

§10 Quadratic residues

Definition 4 (Legendre symbol). 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 46. If p is a prime and a,b are integers congruent modulo p, then

$$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right).$$

Exercise 47. For an odd prime p, show that the number of solutions of $x^2\equiv a \bmod p$ is given by

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

Lemma 5

Let p be an odd prime. Then

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

Proof. It suffices to shows that -1 is a square modulo p if and only if $p \equiv 1 \bmod 4$ holds. Using Wilson's theorem, we obtain that

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

If $p \equiv 1 \bmod 4$, then $(p-1)/2$ is even, and hence, -1 is a square modulo p. If -1 is a square modulo p, then $(-1)^{(p-1)/2}$ is congruent to 1 modulo p by Fermat's little theorem, and using that p is odd, we obtain that $p \equiv 1 \bmod 4$. □

Lemma 6

If p is an odd prime, then there exists a non-square modulo p.

Proof. Consider all the non-zero residue classes modulo p. For each non-zero residue class a, consider the pair $\{a, -a\}$. Since p is odd, there are $(p-1)/2$ such pairs. Hence, there are at most $(p-1)/2$ nonzero squares modulo p. Since there are $p-1$ non-zero residue classes modulo p, there must be a non-square modulo p. □

Remark. Indeed, the squares modulo p are precisely the residue classes of the form a^2 with $1 \leq a \leq (p-1)/2$.

Corollary 7

For an odd prime p, there are $p-1$ non-zero residue classes modulo p, among which there are exactly $(p-1)/2$ squares, and consequently, there are exactly $(p-1)/2$ non-squares.

Lemma 8 (Counting squares and non-squares)

Show that

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

Proof. Let $1 \leq r \leq p-1$ be an integer such that r is a non-square modulo p. Note that the prior lemma guarantees the existence of such an integer. Note that the map

$$\{1, 2, \ldots, p-1\} \to \{1, 2, \ldots, p-1\}$$

defined by $a \mapsto \overline{ra}$ is a bijection, where $\overline{ra}$ denotes the smallest positive integer congruent to ra modulo p. This yields

$$\begin{aligned}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) &= \sum_{a=1}^{p-1}\left(\frac{\overline{ra}}{p}\right)\\ &= \sum_{a=1}^{p-1}\left(\frac{ra}{p}\right)\\ &= \sum_{a=1}^{p-1}\left(\frac{r}{p}\right)\left(\frac{a}{p}\right)\\ &= -\sum_{a=1}^{p-1}\left(\frac{a}{p}\right),\end{aligned}$$

and hence, we obtain

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

□

Corollary 9

For any odd prime p, among the nonzero residue classes modulo p, there are as many squares as non-squares.

Lemma 10

Let p be an odd prime. For some integer a not divisible by p, the congruence

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

holds. Moreover, for any integer a, which is not a square modulo p, the above congruence holds.

Walkthrough — Count the squares! Does Lemma 8 help?

Proof. Note that there are exactly $(p-1)/2$ squares modulo p. Indeed, the squares modulo p are precisely the residue classes of the form a^2 with $1 \leq a \leq (p-1)/2$. Observe that these squares are precisely all the solutions of the equation $x^{(p-1)/2} \equiv 1 \bmod p$. By Fermat's little theorem, the remaining $(p-1)/2$ non-squares modulo p are precisely all the solutions of the equation $x^{(p-1)/2} \equiv -1 \bmod p$. □

Corollary 11

Let p be an odd prime. For any integer a not divisible by p, the following holds:

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

Moreover, if a, b are integers, then

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Walkthrough — It suffices to show that if a is a non-square modulo an odd prime p, then $a^{(p-1)/2} \equiv -1 \bmod p$ holds.

Exercise 48. Prove that

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

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

Exercise 49 (Hong Kong TST 1 2023 P2, ,). Let n be a positive integer. Show that if p is a prime dividing $5^{4n} - 5^{3n} + 5^{2n} - 5^n + 1$, then $p \equiv 1 \pmod 4$.

Walkthrough —

(a) Show that $p \geq 3$.

(b) Prove that

$$(2 \cdot 5^{2n} - 5^n + 2)^2 - 5 \cdot 5^{2n} = 4m \equiv 0 \pmod p,$$

and conclude that 5 is a quadratic residue modulo p.

(c) Prove that

$$(5^{2n} - 5^n + 1)^2 + 5^n(5^n - 1)^2 = m \equiv 0 \pmod p,$$

and conclude that -5^n is a quadratic residue modulo p.

(d) Conclude that $p \equiv 1 \pmod 4$.

Lemma 12

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 integer 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

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

If $(p-1)/2$ is even, then the above congruence implies that

$$\left(\frac{2}{p}\right)(1+i)(-1)^{(p-1)/4} \equiv 1 + i \bmod p,$$

and multiplying both sides by $\frac{(p+1)(1-i)}{2}$ yields that

$$\left(\frac{2}{p}\right) \equiv (-1)^{(p-1)/4} \bmod p.$$

If $(p-1)/2$ is odd, then we obtain that

$$-\left(\frac{2}{p}\right)(1+i)(-1)^{(p+1)/4}i \equiv 1 - i \bmod p,$$

and multiplying both sides by $\frac{(p+1)(1-i)i}{2}$ yields that

$$\left(\frac{2}{p}\right) \equiv (-1)^{(p+1)/4} \bmod p.$$

This shows that

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

□

Remark. In the above proof, we have used some properties of the notion of modulo p congruence for elements of $\mathbb{Z}[i]$. The following are some of its properties.

1. If z_1 is an element of $\mathbb{Z}[i]$, then $z_1 \equiv z_1 \bmod p$ holds.
2. If z_1, z_2 are elements of $\mathbb{Z}[i]$ such that $z_1 \equiv z_2 \bmod p$, then $z_2 \equiv z_1 \bmod p$ holds.
3. If z_1, z_2, z_3 are elements of $\mathbb{Z}[i]$ such that $z_1 \equiv z_2 \bmod p$ and $z_2 \equiv z_3 \bmod p$, then $z_1 \equiv z_3 \bmod p$ holds.

4. If z_1, z_2, z_3, z_4 are elements of $\mathbb{Z}[i]$ such that $z_1 \equiv z_2 \bmod p$ and $z_3 \equiv z_4 \bmod p$, then $z_1 + z_3 \equiv z_2 + z_4 \bmod p$ and $z_1 z_3 \equiv z_2 z_4 \bmod p$ hold.
5. If z_1, z_2 are elements of $\mathbb{Z}[i]$, then $(z_1 + z_2)^p \equiv z_1^p + z_2^p \bmod p$ holds.

Exercise 50. Let a be an integer. Show that the number of solutions to $x^2 - y^2 \equiv a \bmod p$ is given by

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

Walkthrough — Use the definition of the Legendre symbol.

Exercise 51. Let a be an integer. Prove that the number of solutions to $x^2 - y^2 \equiv a \bmod p$ is equal to

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

Walkthrough — Change of variables.

Corollary 13

Prove that

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

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

Exercise 52 (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!

Theorem 14 (Quadratic reciprocity)

Let p, ℓ be distinct odd primes. Then the following holds:

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

Proof. Let ζ be a **primitive** ℓ-th root of unity, that is, ζ is a complex number

such that $\zeta^\ell = 1$ and $\zeta^k \neq 1$ for any positive integer $k < \ell$. Consider the Gauss sum

$$\tau = \sum_{a=1}^{\ell-1} \left(\frac{a}{\ell}\right) \zeta^a.$$

Claim — We have

$$\left(\frac{-1}{\ell}\right) \tau^2 = \ell.$$

Proof of the claim. Note that

$$\begin{aligned}
\tau^2 &= \left(\sum_{a=1}^{\ell-1} \left(\frac{a}{\ell}\right) \zeta^a\right) \left(\sum_{b=1}^{\ell-1} \left(\frac{b}{\ell}\right) \zeta^b\right) \\
&= \sum_{1\leq a\leq \ell-1} \left(\sum_{1\leq b\leq \ell-1} \left(\frac{ab}{\ell}\right) \zeta^{a+b}\right) \\
&= \sum_{1\leq a\leq \ell-1} \left(\sum_{1\leq c\leq \ell-1} \left(\frac{c}{\ell}\right) \zeta^{a+ac}\right) \\
&= \sum_{1\leq a\leq \ell-1} \left(\sum_{1\leq c< \ell-1} \left(\frac{c}{\ell}\right) \zeta^{a+ac}\right) + \sum_{1\leq a\leq \ell-1} \left(\frac{-1}{\ell}\right) \\
&= \sum_{1\leq c< \ell-1} \left(\frac{c}{\ell}\right) \sum_{1\leq a\leq \ell-1} \left(\zeta^{c+1}\right)^a + \left(\frac{-1}{\ell}\right) (\ell-1) \\
&= -\sum_{1\leq c< \ell-1} \left(\frac{c}{\ell}\right) + \left(\frac{-1}{\ell}\right) (\ell-1) \\
&= \left(\frac{-1}{\ell}\right) \ell.
\end{aligned}$$

□

Denote the set of all polynomials in ζ with integer coefficients by $\mathbb{Z}[\zeta]$. Note that τ is an element of $\mathbb{Z}[\zeta]$. Two elements z_1, z_2 of $\mathbb{Z}[\zeta]$ are called **congruent modulo** p if their difference is an element of $p\mathbb{Z}[\zeta]$, that is, their difference can be written as $pf(\zeta)$ for some polynomial f with integer coefficients. Using the prior claim, it follows that

$$\tau^p \equiv \tau \left((-1)^{(p-1)(\ell-1)/4} \left(\frac{\ell}{p}\right)\right) \bmod p.$$

Note that

$$\tau^p \equiv \sum_a \left(\frac{a}{\ell}\right) \zeta^{ap} \bmod p$$

$$\equiv \left(\frac{p}{\ell}\right) \sum_a \left(\frac{ap}{\ell}\right) \zeta^{ap} \bmod p$$
$$\equiv \left(\frac{p}{\ell}\right) \tau \bmod p.$$

This implies that

$$\left(\frac{p}{\ell}\right) \tau \equiv \tau \left((-1)^{(p-1)(\ell-1)/4} \left(\frac{\ell}{p}\right)\right) \bmod p.$$

Multiplying both sides by τ, and then by the inverse of ℓ modulo p, we get that

$$\left(\frac{p}{\ell}\right) \equiv (-1)^{(p-1)(\ell-1)/4} \left(\frac{\ell}{p}\right) \bmod p,$$

and the desired result follows. □

Remark. In the above proof, we have used some properties of the notion of modulo p congruence for elements of $\mathbb{Z}[\zeta]$. The following are some of its properties.

1. If z_1 is an element of $\mathbb{Z}[\zeta]$, then $z_1 \equiv z_1 \bmod p$ holds.
2. If z_1, z_2 are elements of $\mathbb{Z}[\zeta]$ such that $z_1 \equiv z_2 \bmod p$, then $z_2 \equiv z_1 \bmod p$ holds.
3. If z_1, z_2, z_3 are elements of $\mathbb{Z}[\zeta]$ such that $z_1 \equiv z_2 \bmod p$ and $z_2 \equiv z_3 \bmod p$, then $z_1 \equiv z_3 \bmod p$ holds.
4. If z_1, z_2, z_3, z_4 are elements of $\mathbb{Z}[\zeta]$ such that $z_1 \equiv z_2 \bmod p$ and $z_3 \equiv z_4 \bmod p$, then $z_1 + z_3 \equiv z_2 + z_4 \bmod p$ and $z_1 z_3 \equiv z_2 z_4 \bmod p$ hold.
5. If z_1, z_2 are elements of $\mathbb{Z}[\zeta]$, then $(z_1 + z_2)^p \equiv z_1^p + z_2^p \bmod p$ holds.

Exercise 53 (Belarus TST 2025 P19, , proposed by V. Kamianetski and Y. Sheshukou)**.** Find all prime numbers p such that $4p + 1$ divides $3^p - 1$.

Walkthrough —

(a) Check that $p = 3$ works.

(b) Assume that $p > 3$ is a prime number such that $4p + 1$ divides $3^p - 1$. Show that any prime divisor of $4p + 1$ is at least as large as $p + 2$. Using this, show that $4p + 1$ is a prime number.

(c) Prove that 3 is a quadratic residue modulo $4p + 1$.

(d) Use the law of quadratic reciprocity to obtain a contradiction.

Remark. Note that if p is a prime and some prime divisor of $4p+1$ is at least as large as $p+2$, then it is not necessary that $4p+1$ is a prime. In fact, for $p=5$, note that $4p+1$ is composite and it admits $p+2$ as a prime factor.

Exercise 54 (Romania TST 2019 Day 4 P2, , cf. Turkish TST 2013 P4,). Find all pairs of positive integers (m,n) such that $m^6 = n^{n+1} + n - 1$.

Walkthrough —

(a) Note that $n=1$ works.

(b) Let $n>1$ be an integer such that $n^{n+1}+n-1$ is a perfect sixth power.

(c) If $n>1$ is odd, then show that $n^{n+1}+n-1$ lies strictly between two consecutive squares.

(d) If $n \equiv 2 \pmod 3$, then show that $n^{n+1}+n-1$ lies strictly between two consecutive cubes.

(e) If $n \equiv 0 \pmod 3$, then show that $n^{n+1}+n-1$ is not a perfect square.

(f) Prove that $n \equiv 4 \bmod 6$ holds.

(g) Show that $n+1$ has a prime divisor $p \equiv 2 \bmod 3$ with $p>3$.

(h) Prove that -3 is a quadratic residue modulo p.

(i) Use the law of quadratic reciprocity to conclude.

Exercise 55 (Turkey TST 2024 P4, ,). Find all pairs of positive integers (a,b) such that

$$\frac{10^a - 3^b + 1}{2^a}$$

is a perfect square.

Exercise 56 (Hong Kong TST 2 2022 P3, ,). Let S be the set of all integers of the form $x^2+3xy+8y^2$ where x and y are integers.

1. Show that if u and v are in S, then so is uv.
2. Can an integer of the form $23k+7$, with k an integer, belong to S?

Exercise 57 (Saudi Arabia TST 2025 Day 2 P6, ,). Prove that there are infinitely many primes p such that each of them divides an integer of the form 3^n-2, but does not divide any integer of the form 2^m-3, where m and n are positive integers.

§11 Rational root theorem

Exercise 58 (Bay Area MO 2004 P5,). Find (with proof) all monic polynomials $f(x)$ with integer coefficients that satisfy the following two conditions.

(i) $f(0) = 2004$.

(ii) If x is irrational, then $f(x)$ is also irrational.

Walkthrough —

(a) First, consider the case when $f(x)$ is a monic polynomial with integer coefficients having degree ≥ 2,

(b) Take a positive integer n and a prime p such that $f(0) - n = -p$.

(c) If p is sufficiently large, then show that $f(x) - n$ does not vanish at any of $1, -1, p, -p$.

(d) If n is sufficiently large, then show that $f(x) - n$ admits a real root, which is necessarily rational (why?), and by the rational root theorem, is equal to 1 or -1 or p or $-p$.

(e) Conclude that the polynomials to be found are linear, and determine them.

Exercise 59 (Balkan Mathematical Olympiad 2018 P2, , proposed by Jeremy King, UK)**.** Let q be a positive rational number. Two ants are initially at the same point X in the plane. In the n-th minute ($n = 1, 2, \dots$) each of them chooses whether to walk due north, east, south or west and then walks the distance of q^n metres. After a whole number of minutes, they are at the same point in the plane (not necessarily X), but have not taken exactly the same route within that time. Determine all possible values of q.

Walkthrough —

(a) Let q be a positive rational number such that the two ants can be at the same point in the plane after a whole number of minutes, without taking the same route.

(b) Let r be a positive integer such that the two ants are at the same point in the plane after r minutes, without taking the same route.

(c) Prove that

$$\varepsilon_1 q + \varepsilon_2 q^2 + \cdots + \varepsilon_r q^r = \varepsilon'_1 q + \varepsilon'_2 q^2 + \cdots + \varepsilon'_r q^r,$$

for some $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r$, $\varepsilon'_1, \varepsilon'_2, \dots, \varepsilon'_r$ are elements of $\{1, -1, i, -i\}$, and the tuples $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r)$ and $(\varepsilon'_1, \varepsilon'_2, \dots, \varepsilon'_r)$ are not equal.

(d) Prove that there exists a nonzero polynomial P of degree at most $r - 1$, which vanishes at q, and has coefficients in $\{0, 2, 1 + i\}$ up to a factor of $\pm 1, \pm i$.

(e) Further, prove that there exists a nonzero polynomial Q of degree at most $r - 1$, which vanishes at q, and has coefficients in $\{0, 1, 1 + i\}$ up to a factor of $\pm 1, \pm i$.

(f) Write $q = \frac{a}{b}$ where a, b are relatively prime positive integers, and show that b divides the leading coefficient of Q in $\mathbb{Z}[i]$, and a divides the constant term of Q in $\mathbb{Z}[i]$, where

$$\mathbb{Z}[i] = \{x + yi : x, y \in \mathbb{Z}\}$$

is the ring of Gaussian integers.

(g) Prove further that a divides the constant term of Q in $\mathbb{Z}[i]$.

(h) Conclude that $q = 1$ is the only possible value of q.

§12 Gauss's lemma

Definition 15. A polynomial with integer coefficients is called *primitive* if the greatest common divisor of its coefficients is 1, and its leading coefficient is positive.

Lemma 16 (Gauss)

A product of primitive polynomials with integer coefficients is primitive.

We refer to for a proof of the above lemma.

Exercise 60 (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.

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.

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.

§13 Irreducible polynomials

Exercise 61 (Korea National Olympiad 1995 Day 2 P2,). Let a, b be integers and p be a prime number such that:

1. p is the greatest common divisor of a and b,
2. p^2 divides a.

Prove that the polynomial $x^{n+2} + ax^{n+1} + bx^n + a + b$ cannot be decomposed into the product of two polynomials with integer coefficients and degree greater than 1.

Exercise 62 (IMO 1993 P1,). Let $n > 1$ be an integer and let $f(x) = x^n + 5 \cdot x^{n-1} + 3$. Prove that there do not exist polynomials $g(x), h(x)$, each having integer coefficients and degree at least one, such that $f(x) = g(x) \cdot h(x)$.

Walkthrough — Reduce the polynomial $f(x)$ modulo 3.

Remark. It also follows from the irreducibility criterion of Perron.

§14 Lifting of the exponents

Theorem 17 (Lifting the exponent)

Let a, b be integers and p be a prime such that p divides $a - b$ and p does not divide ab. Let n be a positive integer.

(i) If $p \geq 3$, then

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n).$$

(ii) If $p = 2$ and n is odd, then

$$v_2(a^n - b^n) = v_2(a - b).$$

(iii) If $p = 2$, n is even, and $v_2(a - b) \geq 2$, then

$$v_2(a^n - b^n) = v_2(a - b) + v_2(a + b) + v_2(n) - 1.$$

Exercise 63 (Hong Kong TST 2 2024 P3, ,). Let n be a positive integer. Prove that there exists a positive integer $m > 1$ such that 7^n divides $3^m + 5^m - 1$.

Walkthrough —

(a) Consider the integer $m = 7^{n-1}$.

(b) Apply lifting-the-exponent lemma to find the highest power of 7 dividing $3^m + 4^m$ and $5^m + 2^m$.

(c) Use the above to show that $3^m + 5^m - 1$ is divisible by 7^n.

(d) Apply lifting-the-exponent lemma again to find the highest power of 7 dividing $8^m - 1$.

(e) Show that 7 does not divide $2^m - 1$.

(f) Conclude that $3^m + 5^m - 1$ is divisible by 7^n.

Exercise 64 (Kürschák Competition 2020 P2,). Find all functions $f\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ such that for any two rational numbers x and y, the conditions

$$f(x+y) \leq f(x) + f(y), f(xy) = f(x)f(y)$$

hold, and $f(2) = \frac{1}{2}$.

Walkthrough — Let $f\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ be a function satisfying the given conditions.

(a) Show that $f(0) = 0$ and $f(1) = f(-1) = 1$.

(b) Show that for any integer n, $f(n)$ is nonzero.

(c) Using the fact that any positive integer can be written as a sum of distinct powers of 2, show that for any positive integer n, the inequality $f(n) \leq 2$ holds.

(d) Prove that for any positive integer n, the inequality $f(n) \leq 1$ holds.

(e) For any odd positive integer n and for any positive integer m, show that the inequality $1 - f(n)^{2^m} \leq f(n^{2^m} - 1)$ holds, and using divisibility properties by powers of 2, prove that $1 - f(n)^{2^m} \leq \frac{1}{2^m}$ holds.

(f) Deduce that for any odd positive integer n, $f(n) = 1$ holds.

(g) Prove that for any rational number r,

$$f(r) = \begin{cases} 0 & \text{if } r = 0, \\ 2^{-v_2(r)} & \text{if } r \neq 0. \end{cases}$$

Let $f\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ be the function defined above. Show that f satisfies the given conditions.

Example 65. Find the solutions of the equation

$$x^{2025} + y^{2025} = 5^z$$

in positive integers x, y, z.

Exercise 66 (Switzerland TST 2022 Day 2 P6,). Let $n \geq 2$ be an integer. Prove that if

$$\frac{n^2 + 4^n + 7^n}{n}$$

is an integer, then it is divisible by 11.

Exercise 67 (China TST 1 2025 Day 4 P11,). Given a positive integer $n \geq 4$, prove that the equation

$$(2^x - 1)(5^x - 1) = y^n$$

has no positive integer solutions (x, y).

Exercise 68 (Romania JBMO TST 2025 Day 2 P4,). Determine all natural numbers n such that $2^n - n^2 + 1$ is a perfect square.

§15 Zsigmondy's theorem

Exercise 69 (INMO 2026 P4,). Two integers a and b are called *companions* if every prime number p either divides both or none of a, b. Determine all functions $f : \mathbb{N}_0 \to \mathbb{N}_0$ such that $f(0) = 0$ and the numbers $f(m) + n$ and $f(n) + m$ are companions for all $m, n \in \mathbb{N}_0$. (Here $\mathbb{N}_0$ denotes the set of all non-negative integers.)

It is worth having a look at IMOSL 2007 N5.

> **Walkthrough** —
>
> **(a)**

Exercise 70 (Saudi Arabia TST 2023 Day 2 P2,). Denote by $\mathbb{N}$ the set of positive integers. Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that $x - y$ divides $x^{f(x)} - y^{f(y)}$ for every two coprime integers x and y.

> **Walkthrough** —
>
> **(a)**

Exercise 71 (RMO 2012e P3,). Find all natural numbers x, y, z such that

$$(2^x - 1)(2^y - 1) = 2^{2^z} + 1.$$