EGMO 2025 training camp

Geometry

Euler line and nine point circle

25.01.2025

Definition 1
Euler line is the line that passes through the following three distinguished points in a triangle: the orthocenter, the circumcenter, and the centroid of the triangle.

Definition 2
The intersection of the three altitudes in a triangle is called the *orthocenter* of the triangle. The center of the circle circumscribed about a triangle is called the *circumcenter* of the triangle. The intersection of the three medians in a triangle is called the *centroid* (or the medicenter) of the triangle.

Definition 3
The midpoints of the segments joining the orthocenter of a triangle to its vertices are called the *Euler points* of the triangle. The three Euler points determines the *Euler triangle* of the given triangle.

Theorem 1
The orthocenter H, circumcenter O, and centroid M of a triangle are always collinear, with point M between H and O, twice as close to O as to H, i.e., $|MH| = 2|MO|$. The line OMH is called *Euler's line*.

Theorem 2
If O and I are the circumcenter and incenter of ABC, then $OI^2 = R(R - 2r)$, where R and r are respectively the circumradius and the inradius of AC. Consequently, $R \geq 2r$.

Theorem 3
The incenter of a triangle lies on the Euler line exactly when the triangle is isosceles. In such a case, the Euler line is the altitude (also simultaneously, median, perpendicular bisector, and angle bisector) towards the base of the isosceles triangle.

Definition 4
The nine-point circle of a triangle is the circle passing through the following 9 points:

- 3 midpoints of the sides of the triangle,
- 3 feet of the altitudes,
- 3 Euler points.

The center of this circle is called the *nine-point center*.

Theorem 4
The radius of the nine-point circle is equal to half of the circumradius of the triangle.

Theorem 5
The nine-point center lies on the Euler line in the middle between the circumcenter and the orthocenter.

Problem 1

The altitudes of $\triangle ABC$ meet at the orthocenter H.
a) Prove that $\triangle ABC$, $\triangle HBC$, $\triangle AHC$, and $\triangle ABH$ share the same nine-point circle.
b) Prove that the Euler lines of $\triangle ABC$,$\triangle HBC$,$\triangle AHC$, and $\triangle ABH$ intersect at one point.

Solution:
a) Let us prove, that, for example, $\triangle ABC$ and $\triangle HBC$ share the same circle of nine points. Indeed, the circle of nine points of these triangles pass through the midpoint of side BC and the midpoint of the segments BH and CH.

b) Euler line passes through the center of the circle of nine points and these triangles share one circle of nine points.

Problem 2

Let G be the centroid and O the circumcenter of $\triangle ABC$. Let X be a point on the circumcircle of $\triangle ABC$, and X' the reflection of X across O.
Prove that XG bisects the segment HX'.

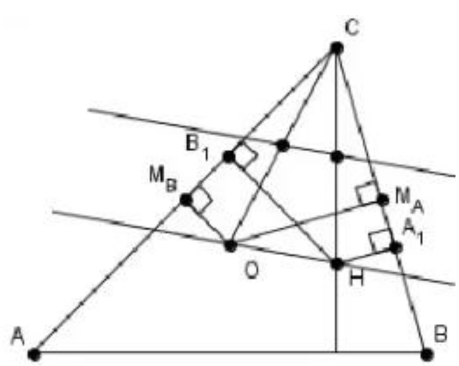
Solution:

HO is median in $\triangle XX'H$, but $HG = 2GO$ (according to Theorem 1), so G is centroid of $\triangle XX'H$. Thus XG is a median of $\triangle XX'H$, and so bisects HX'.

Problem 3

Let H be the orthocenter of $\triangle ABC$. The feet of altitudes from A, B and C respectively are A_1, B_1 and C_1. Let M_A and M_B be the midpoints of BC and AC, respectively.
Prove that the line joining the circumcenter of $\triangle A_1B_1C$ and $\triangle M_AM_BC$ is parallel to the Euler line of $\triangle ABC$.

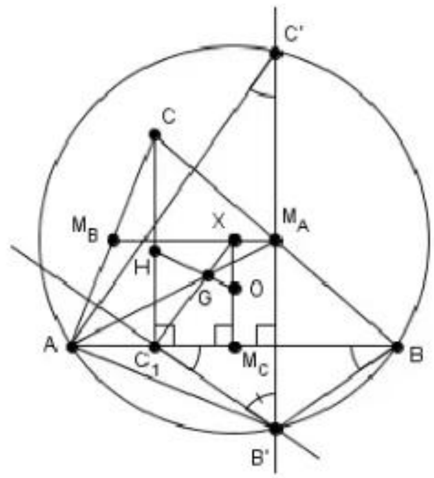
Solution:



CA_1HB_1 and CM_AOM_B are cyclic with $< CA_1H = 90° =< HB_1C$ and $< CM_AO = 90° =< OM_BC$. Thus CH and CO are the respective diameters, and so the circumcenters of $\triangle A_1B_1C$ and $\triangle M_AM_BC$ are the midpoints of OH and CH, respectively. The line joining these midpoints is a midline in $\triangle CHO$, so it is parallel to HO, the Euler line.

Problem 4

Let G be the centroid of $\triangle ABC$, and let C_1 be the foot of the altitude from C to AB. Let X be the intersection of the midline of $\triangle ABC$, parallel to AB, and the perpendicular bisector of AB.
Prove that C_1, G and X are collinear and $C_1G = 2GX$.



Solution 1:

Lets prove that C_1, G and X is, respectively, the orthocenter, the centroid and the circumcenter of some triangle. Let w be the circle with center X and the radius XA. Let B' and C' be the intersections of w and the perpendicular from M_A to AB. X lies on the perpendicular bisector of AB, so B lies on w and thus $< AC^{'}B^{'} =< ABB'$. But $< ABB^{'} =< B^{'}C_1B$ since $B^{'}$ lies on the perpendicular bisector of BC_1. Thus $< C_1B^{'}C^{'} = 90° - < AC'B'$, and so $B'C_1$ is an altitude in $\triangle AB'C'$. But AC_1 is also an altitude, which means C_1D is the orthocenter of $\triangle AB'C'$.

Furthermore, AM_A is median with $AG = 2GM_A$, so G is a centroid in $\triangle AB'C'$. Lastly, X is the circumcenter, and so C_1, G and X is a Euler triangle of $\triangle AB'C'$.

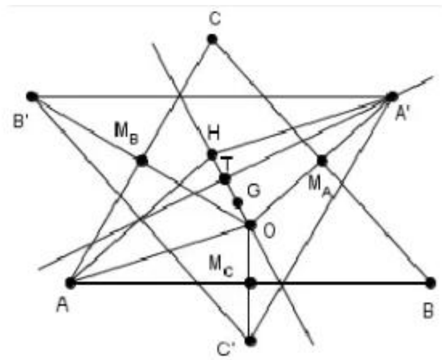
Solution 2:

We have $CC_1 = 2XM_c$ and $CH = 2OM_c$, so $C_1H = 2XO$. At the same time, $HG = 2GO$ and $< C_1HC =< XOG$, so $\triangle HFG \sim \triangle OXG$. This implies$C_1G$ and X lie on a single line with $C_1G = 2GX$.

Problem 5

Let O be the circumcenter of $\triangle ABC$. In $\triangle ABC$, let A' be the reflection of O over BC, B' be the reflection of O over AC, and C' be the reflection of O over AB. Let H be the orthocenter of $\triangle ABC$. Let G be the centroid of $\triangle ABC$. Let T be the midpoint of HG.
Prove that the line $A'T$ bisects both $B'C'$ and AH at the same point.

Solution:



$M_A M_C$ is a midline in $\triangle C'A'O$, so $C'A' || M_C M_A || AC$. Thus $B'O$ and, analogically, $C'O$ are altitudes in $\triangle A'B'C'$, so O is the orthocenter. $AH || A'O$ and, since $\triangle ABC \cong \triangle A'B'C'$, $AH = A'O$(both are distances from the orthocenter to a corresponding vertex). Thus $AOA'H$ is a parallelogram, so $OA = R = HA'$. Analogically, $HB' = R$ and $HC' = R$, so H is the circumcenter of $\triangle A'B'C'$.

Because of $AB' = AO = R$, $AC' = AO = R$, $BH' = R$ and $CH' = R$, $AC'OC$ is a parallelogram. This implies that $B'C'$ and AH bisect each other. By Euler theorem, T is the centroid of $\triangle A'B'C'$, so $A'T$ is a median, and so goes through the midpoint of $B'C'$ and AH.

Functional equations and inequalities

Birgit Veldi

January 26, 2025

1 Some useful definitions

Definition 1. A function f is called *odd* if for every x in its domain $f(-x) = -f(x)$.

Definition 2. A function f is called *even* if for every x in its domain $f(x) = f(-x)$.

Definition 3. A function f is called *monotone* if $x \leq y$ implies that $f(x) \leq f(y)$.

2 Some ideas to start with

- Plug things into
- Add/subtract/multiply equations
- Is there symmetry somewhere?
- Does the function have some nice properties?
- Interchange variables
- Try to guess the solution

3 Introduction

Problem 1. (Estonia TST 2018 P4) Find all functions $f\colon \mathbb{R} \to \mathbb{R}$ such that for all real numbers x and y the following holds:

$$f(xy + f(xy)) = 2xf(y)$$

Problem 2. (Nordic 2022 P1) Find all functions $f : \mathbb{R} \to \mathbb{R}$ such that $f(f(x)f(1-x)) = f(x)$ and $f(f(x)) = 1 - f(x)$, for all real x.

Problem 3. (Estonia TST 2022 P1) Find all functions $f\colon \mathbb{R} \to \mathbb{R}$ such that for all real x and y the following holds

$$f(x) + f(x+y) \leq f(xy) + f(y).$$

4 Injectivity and surjectivity

Definition 4. Injectivive function. A function $f\colon X \to Z$ is called injective (or one-to-one) if for all different $x, y \in X$ we have $f(x) \neq f(y)$. In order words, if we have $f(x) = f(y)$, then it follows that $x = y$.

Definition 5. Surjective function. A function $f : X \to Y$ is called surjective (or onto) if for every $y \in Y$ there exists $x \in X$ such that $f(x) = y$.

Definition 6. Bijective function. A function f is called bijective if it's both injective and surjetive.

Exercise 1. Show that if $f(f(x)) = x$ for every x, then f is bijective.

Problem 4. (2005 Swiss MO Final Round P9) Find all functions $f : \mathbb{R}^+ \to \mathbb{R}^+$ such that for all $x, y > 0$

$$f(yf(x))(x+y) = x^2(f(x) + f(y)).$$

Problem 5. (**Estonia EGMO TST 2025 P7**) Does there exist a surjetive function $f\colon \mathbb{R} \to \mathbb{R}$ such that

$$f(f(x)) = (x-1)f(x) + 2$$

holds for every real number x?

Remark. Function f is called surjective if for all $y \in \mathbb{R}$ there exists $x \in \mathbb{R}$ such that $f(x) = y$.

Problem 6. (Nordic P3 2024) Find all functions $f : \mathbb{R} \to \mathbb{R}$

$$f(f(x)f(y) + y) = f(x)y + f(y - x + 1)$$

For all $x, y \in \mathbb{R}$

5 Introducing new functions

Problem 7. (BW 2007 P5) A function f is defined on the set of all real numbers except 0 and takes all real values except 1. It is also known that

$$f(xy) = f(x)f(-y) - f(x) + f(y)$$

for any $x, y \neq 0$ and that

$$f(f(x)) = \frac{1}{f(\frac{1}{x})}$$

for any $x \notin \{0, 1\}$. Determine all such functions f.

6 Point-wise trap

What happens if we get an equation like this $(f(x) - a)(f(x) - b) = 0$?

Problem 8. (Kyrgyzstan 2012 P4) Find all functions $f : \mathbb{R} \to \mathbb{R}$ such that $f(f(x)^2 + f(y)) = xf(x) + y$, for all $x, y \in \mathbb{R}$.

Problem 9. (IMO SL 2008 A1) Find all functions $f : (0, \infty) \mapsto (0, \infty)$ (so f is a function from the positive real numbers) such that

$$\frac{(f(w))^2 + (f(x))^2}{f(y^2) + f(z^2)} = \frac{w^2 + x^2}{y^2 + z^2}$$

for all positive real numbers w, x, y, z, satisfying $wx = yz$.

Problem 10. (MEMO 2021 P1) Find all functions $f : \mathbb{R} \to \mathbb{R}$ such that

$$f(x^2) - f(y^2) \leq (f(x) + y)(x - f(y))$$

holds for all real x and y.

EGMO 2025 training camp
Division

Deividas Morkūnas

Introduction

1. If $x \mid a$, then there exists an integer n such that $a = xn$.
2. If $x \mid a$ and $x \mid b$, then $x \mid a + b$ and $x \mid a - b$ and $x \mid ab$.
3. If $xa \mid xb$, then $a \mid b$.
4. If $x \mid y$ and $y \mid z$, then $x \mid z$.
5. If $x \mid a$ and $y \mid b$, then $xy \mid ab$.
6. If $x \mid a$ and $x \mid a + b$, then $x \mid b$.
7. If $x \mid a$ and $y \mid a$ and $\gcd(x, y) = 1$, then $xy \mid a$.
8. If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Problems

Problem 1. Prove that for every integer n, $81 \nmid n^3 - 9n + 27$.

Problem 2. For natural numbers a, bc it holds that $(a + b + c)^2 \mid ab(a + b) + bc(b + c) + ca(c + a) + 3abc$. Prove that

$$a + b + c \mid (a - b)^2 + (b - c)^2 + (c - a)^2$$

Problem 3. Determine all integers n such that $n^2 + 2014 \mid n^4 + 2014$ and $n^2 + 2015 \mid n^4 + 2015$.

Problem 4. Let p be a prime number, $p \neq 3$ and let a and b be positive integers such that $p \mid a + b$ and $p^2 \mid a^3 + b^3$. Show that $p^2 \mid a + b$ or $p^3 \mid a^3 + b^3$

Problem 5. Determine all positive integers n such that $\lfloor \sqrt{n} \rfloor - 1 \mid n + 1$ and $\lfloor \sqrt{n} \rfloor + 2 \mid n + 4$.

Problem 6. Let n be a positive integer and let a, b, c, d be integers such that $n \mid a + b + c + d$ and $n \mid a^2 + b^2 + c^2 + d^2$. Show that

$$n \mid a^4 + b^4 + c^4 + d^4 + 4abcd.$$

Problem 7. Find all functions $f \colon \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ such that

$$f(a) + b \mid a^2 + f(a)f(b)$$

for all positive integers a, b.

Problem 8. Prove that for every natural number $n > 1$ there exists a permutation a_1,a_2, ..., a_n of the numbers $1, 2, ..., n$ such that for each $k \in \{1, 2, ..., n - 1\}$ the number $a_{k+1} \mid a_1 + a_2 + ... + a_k$.

Problem 9. Show that there exists infinitely many n such that: $2^n - 1 \mid 2^{2^n} - 1$

Problem 10. Find all functions $f \colon \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ such that

$$n + f(m) \mid f(n) + nf(m)$$

for all $m, n \in \mathbb{Z}^+$

Problem 11. Find all triples (x, y, z) of positive integers, with $z > 1$, such that $x \mid y + 1$, $y \mid z - 1$ and $z \mid x^2 + 1$.

Problem 12. Find all polynomials with integer coefficients, $P(n)$ such that $P(n) \mid 2^n - 1$ for all positive integers n.

Games

Greta Morkūnė, EGMO training camp

2025.01.27

Problem 1. Let n be a positive integer and $M = \{1, 2, 3, 4, 5, 6\}$. A starts with any digit from M. Then B appends to it a digit from M, and so on, until they get a number with $2n$ digits. If the result is a multiple of 9, then B wins; otherwise A wins. Who wins, depending on n?

Problem 2. Start with two piles of p and q chips, respectively. A and B move alternately. A move consists in taking a chip from any pile, taking a chip from each pile, or moving a chip from one pile to the other. The winner is the one to take the last chip. Who wins, depending on the initial conditions?

Problem 3. The number N is the product of k different primes ($k \geq 3$). A and B take turns writing composite divisors of N on a board, according to the following rules. One may not write N. Also, there may never appear two coprime numbers or two numbers, one of which divides the other. The first player unable to move loses. If A starts, who has the winning strategy?

Problem 4. Alice and Bob play a game on a 6 by 6 grid. On his or her turn, a player chooses a rational number not yet appearing on the grid and writes it in an empty square of the grid. Alice goes first, and then the players alternate. When all squares have numbers written in them, in each row, the square with the greatest number in that row is colored black. Alice wins if she can then draw a line from the top of the grid to the bottom of the grid that stays in black squares, and Bob wins if she can't. (If two squares share a vertex, Alice can draw a line from one to the other that stays in those two squares.) Find, with proof, a winning strategy for one of the players.

Problem 5. The SOS Game is played on a 1×2000 grid as follows. Two players in turn write either an S or an O in an empty square. The first player who produces three consecutive boxes that spell SOS wins. If all boxes are filled without producing SOS then the game is a draw. Prove that the second player has a winning strategy.

Problem 6. Alice and Bob play the following game. First, Alice writes a permutation of the numbers from 1 to n, where n is some fixed positive integer such that $n > 1$. In each player's turn, he or she must write a sequence of numbers that has not been written yet such that either:

- The sequence is a permutation of the sequence written by the previous player, or
- The sequence is obtained by deleting one number from the previous player's sequence.

The player who cannot write down a sequence loses. Determine who has a winning strategy.

Problem 7. For positive integers t, a, b, a (t, a, b)-game is a two player game defined by the following rules. Initially, the number t is written on a blackboard. At his first move, the 1st player replaces t with either $t - a$ or $t - b$. Then, the 2nd player subtracts either a or b from this number, and writes the result on the blackboard, erasing the old number. After this, the first player once again subtracts either a or b from the number written on the blackboard, and so on. The player who first reaches a negative number loses the game. Prove that there exist infinitely many values of t for which the first player has a winning strategy for all pairs (a, b) with $a + b = 2005$.

Problem 8. Let $k \geq 2$ Alice and Bob play the following game. To start, Alice arranges the numbers $1, 2, \ldots, n$ in some order in a row and then Bob chooses one of the numbers and places a pebble on it. A player's turn consists of picking up and placing the pebble on an adjacent number under the restriction that the pebble can be placed on the number k at most k times. The two players alternate taking turns beginning with Alice. The first player who cannot make a move loses. For each positive integer n, determine who has a winning strategy.

Problem 9. Five identical empty buckets of 2-liter capacity stand at the vertices of a regular pentagon. Cinderella and her wicked Stepmother go through a sequence of rounds: At the beginning of every round, the Stepmother takes one liter of water from the nearby river and distributes it arbitrarily over the five buckets. Then Cinderella chooses a pair of neighbouring buckets, empties them to the river and puts them back. Then the next round begins. The Stepmother goal's is to make one of these buckets overflow. Cinderella's goal is to prevent this. Can the wicked Stepmother enforce a bucket overflow?

Problem 10. A and B play a game, given an integer N, A writes down 1 first, then every player sees the last number written and if it is n then in his turn he writes $n + 1$ or $2n$, but his number cannot be bigger than N. The player who writes N wins. For which values of N does B win?

Numbers modulo p, arithmetic functions, induction

Aleksei Ganyukov

January 27, 2025

1 Theory

Unless stated otherwise, we denote by n a natural number, or, equivalently, positive integer, $\mathbb{N} = \mathbb{Z}^+ = \{1, 2, 3, \dots\}$, and by p a prime number, $\mathbb{P} = \{2, 3, 5, 7, 11, \dots\}$. We know that every $n \geq 2$ can be expressed in a unique way in the form $p_1^{k_1} \dots p_m^{k_m}$.

Definition 1.1. (Division and congruences) We say integer a divides b and write $a \mid b$ if there exists an integer c such that $b = a \cdot c$. We say two integers a, b are congruent modulo positive integer n and write $a \equiv b \pmod{n}$ if these numbers give the same remainder upon division by n, that is, $n \mid a - b$.

For example, $45 \mid 2025$, $0 \mid 0$, $1 \mid -1$, $2025 \equiv 0 \pmod{45}$, $2026 \equiv 1 \pmod{45}$, $2028 \cdot 2023 \equiv -6 \pmod{45}$.

Observation 1.2. If $a \mid b$, then either $b = 0$ or $|a| \leq |b|$.

Theorem 1.3. (Wilson's theorem) Let p be a prime, then $(p-1)! \equiv -1 \pmod{p}$. For example, $7 \mid 6! + 1$.

Theorem 1.4. (Fermat's little theorem, FLT) Let p be a prime and let a be a positive integer coprime to p (we write $\gcd(a, p) = 1$ or $(a, p) = 1$), then $a^{p-1} \equiv 1 \pmod{p}$ (or $p \mid a^{p-1} - 1$). Consequently, $p \mid a^{(p-1)k} - 1$ for $k \in \mathbb{N}$.

Definition 1.5. It's easy to check that if $(a, p) > 1$, then there's no $k \in \mathbb{N}$ with $a^k \equiv 1 \pmod{p}$. For $(a, p) = 1$, we call $k \in \mathbb{N}$ the order of a modulo p and write $k = \text{ord}_p(a)$ if k is the least positive integer for which $a^k \equiv 1$.

For example, $\text{ord}_{37}(10) = 3$, $\text{ord}_{13}(2025) = \text{ord}_{13}(10) = 6$. By FLT, $10^{36} \equiv 1 \pmod{37}$, $2025^{12} \equiv 1 \pmod{13}$.

Proposition 1.6. $a^n \equiv 1 \pmod{p} \Rightarrow \text{ord}_p(a) \mid n$. In particular, for $(a, p) = 1$, $\text{ord}_p(a) \mid p - 1$.

Definition 1.7. Let p be a prime and let n be a positive integer. We denote by $v_p(n)$ the largest $k \in \mathbb{N}$ for which $p^k \mid n$. In this case we also write $p^k || n$ or $p^k \mid n$ & $p^{k+1} \nmid n$. For example, $v_2(3072) = 10$, $v_{37}(75!) = 2$.

Exercise 1.1. Find in how many zeroes the number 150! ends by evaluating $v_p(150!)$ for some $p \mid 10$.

Exercise 1.2. Positive integers a, b satisfy the chain of divisibilities $a \mid b^2 \mid a^3 \mid b^4 \mid \dots$. Show that $a = b$.

Theorem 1.8. (LTE lemma) For an odd prime p, assume $p \mid x - y$, $p \nmid x, y$. Then $v_p(x^n - y^n) = v_p(x - y) + v_p(n)$. For example, $p \mid \dfrac{x^p - y^p}{x - y}$ (if the stated conditions hold!). Lemma also covers $v_p(x^n + y^n)$ and $v_2(x^n \pm y^n)$.

Exercise 1.3. (Estonia TST 2023) Let $p \in \mathbb{P}, x, y \in \mathbb{Z}$. Find $x^0 y^{p-1} + x^1 y^{p-2} + \dots + x^{p-2} y^1 + x^{p-1} y^0 \pmod{p}$.

In addition to the theory above, one could extend FLT from the prime case p to any $n \in \mathbb{N}$ with the help of the Euler function $\varphi(n)$, obtaining Euler's theorem. Other useful results include Chinese remainder theorem (CRT), Bertrand's postulate and many others. Below we shortly list the common arithmetic functions.

Definition 1.9. For a positive integer n, denote by $d(n), \sigma(n)$ the count and the sum of the positive divisors of n, respectively. Denote by $\varphi(n)$ the count of positive integers $a \leq n$ with $(a, n) = 1$.

When $n = p^k$ for some $k \in \mathbb{N}$, $d(n) = k + 1$, $\sigma(n) = 1 + \dots + p^k = \frac{p^{k+1} - 1}{p - 1}$ and $\varphi(n) = p^{k-1}(p - 1) = p^k \cdot \left(1 - \frac{1}{p}\right)$.

Observation 1.10. $d(n)$ is odd $\Leftrightarrow$ n is a perfect square. If n and $\sigma(n)$ are odd, then n is a perfect square. For $n \geq 3$, $\varphi(n)$ is even.

Theorem 1.11. (Bézout's lemma) Let a, b be positive integers and let $d = (a, b)$ be their greatest common factor. Then there exist integers x, y such that $ax + by = d$.

Theorem 1.12. (Mihăilescu) The only solution of $x^a - y^b = 1$ for $a, b > 1$ and $x, y > 0$ is $(x, a, y, b) = (3, 2, 2, 3)$.

2 Problems

1. (APMO 1998) Show that there doesn't exist positive integers a, b such that $(36a+b)(36b+a)$ is a power of two.

2. Prove that $\sigma(n-1)\sigma(n)\sigma(n+1)$ is even for all $n \geq 2$.

3. Let a, b, n be positive integers with $n \geq 2$. Show that $\sigma(n)^a = n^b$ is not possible.

4.

a) Prove that there exist 100 distinct positive integers $a_1, a_2, \ldots, a_{100}$ such that a_i divides the total sum $s = a_1 + a_2 + \cdots + a_{100}$ for each $i = 1, \ldots, 100$.

b) Prove that there exist 99 distinct positive integers $b_1, \ldots, b_{99}$ such that the sum of their cubes is a cube.

5. An integer larger than 1 is written on the board. Each move consists of substituting the number n on the board with the number $n + \frac{n}{p}$, where p is any prime divisor of n.

a) (Estonia,Ukraine 2021) Prove that as this process continues, 3 is chosen as p infinitely many times.

b) (Swiss 2022) Now assume the prime p chosen at each step is the smallest possible. Prove that after a finite number of moves a multiple of 3^{2025} will appear.

6. (IZhO 2020) Let p be a prime such that for any $a, b \in \mathbb{N}$ the number $2^a 3^b + 1$ is not divisible by p. Prove that for any $c, d \in \mathbb{N}$ the number $2^c + 3^d$ is also not divisible by p.

7.

a) Prove that if $n \mid 2^n - 1$, then $n = 1$. *Hint:* use $\text{ord}_m(2)$

b) Let $k \geq 2$ and let $n_1, \ldots, n_k$ be positive integers such that $n_1 \mid 2^{n_2} - 1$, $n_2 \mid 2^{n_3} - 1, \ldots, n_k \mid 2^{n_1} - 1$. Prove that $n_1 = n_2 = \cdots = n_k = 1$.

8.

a) Let $n > 1$ be an integer. Prove that for each $d \mid n!$ with $d \neq n!$ there exists $d' \mid n!$ such that $d + d' \mid n!$.

b) (IOM 2018) Let $1 = d_0 < d_1 < \cdots < d_m = 4n$ be all positive divisors of $4n$, where n is a positive integer. Prove that there exists $i \in \{1, \ldots, m\}$ such that $d_i - d_{i-1} = 2$.

9. (Peru 2009) Let a, b, c be positive integers with $\gcd(a, b, c) = 1$. Prove that there exists $n \in \mathbb{N}$ such that $a^k + b^k + c^k$ is not divisible by 2^n for all $k \in \mathbb{N}$.

10. (IZhO 2021) Prove that there exists a positive integer n, such that the remainder of 3^n when divided by 2^n is greater than 10^{2025}.

11. (ARO 2018) For $n \geq 3$. denote by s_n the sum of all primes less than n. Prove that there exists a number $m > 10^{2025}$ such that $(s_m, m) = 1$.

12. Let $n \geq 2$ and let $a_1, \ldots, a_n$ be distinct integers.

a) (Ukraine 2023) Call a pair (a_i, a_j) *elegant* if the sum $a_i + a_j$ is a power of 2. Find the largest possible number of elegant pairs.

b) (EMC 2024) Call a pair (a_i, a_j) *binary* if $a_i a_j + 1$ is a power of 2. Find the largest possible number of binary pairs.

Numbers modulo p, arithmetic functions, induction

Aleksei Ganyukov

January 27, 2025

1 Theory

Unless stated otherwise, we denote by n a natural number, or, equivalently, positive integer, $\mathbb{N} = \mathbb{Z}^+ = \{1, 2, 3, \dots\}$, and by p a prime number, $\mathbb{P} = \{2, 3, 5, 7, 11, \dots\}$. We know that every $n \geq 2$ can be expressed in a unique way in the form $p_1^{k_1} \dots p_m^{k_m}$.

Definition 1.1. (Division and congruences) We say integer a divides b and write $a \mid b$ if there exists an integer c such that $b = a \cdot c$. We say two integers a, b are congruent modulo positive integer n and write $a \equiv b \pmod{n}$ if these numbers give the same remainder upon division by n, that is, $n \mid a - b$.

For example, $45 \mid 2025$, $0 \mid 0$, $1 \mid -1$, $2025 \equiv 0 \pmod{45}$, $2026 \equiv 1 \pmod{45}$, $2028 \cdot 2023 \equiv -6 \pmod{45}$.

Observation 1.2. If $a \mid b$, then either $b = 0$ or $|a| \leq |b|$.

Theorem 1.3. (Wilson's theorem) Let p be a prime, then $(p-1)! \equiv -1 \pmod{p}$. For example, $7 \mid 6! + 1$.

Theorem 1.4. (Fermat's little theorem, FLT) Let p be a prime and let a be a positive integer coprime to p (we write $\gcd(a, p) = 1$ or $(a, p) = 1$), then $a^{p-1} \equiv 1 \pmod{p}$ (or $p \mid a^{p-1} - 1$). Consequently, $p \mid a^{(p-1)k} - 1$ for $k \in \mathbb{N}$.

Definition 1.5. It's easy to check that if $(a, p) > 1$, then there's no $k \in \mathbb{N}$ with $a^k \equiv 1 \pmod{p}$. For $(a, p) = 1$, we call $k \in \mathbb{N}$ the order of a modulo p and write $k = \operatorname{ord}_p(a)$ if k is the least positive integer for which $a^k \equiv 1$.

For example, $\operatorname{ord}_{37}(10) = 3$, $\operatorname{ord}_{13}(2025) = \operatorname{ord}_{13}(10) = 6$. By FLT, $10^{36} \equiv 1 \pmod{37}$, $2025^{12} \equiv 1 \pmod{13}$.

Proposition 1.6. $a^n \equiv 1 \pmod{p} \Rightarrow \operatorname{ord}_p(a) \mid n$. In particular, for $(a, p) = 1$, $\operatorname{ord}_p(a) \mid p - 1$.

Definition 1.7. Let p be a prime and let n be a positive integer. We denote by $v_p(n)$ the largest $k \in \mathbb{N}$ for which $p^k \mid n$. In this case we also write $p^k || n$ or $p^k \mid n$ & $p^{k+1} \nmid n$. For example, $v_2(3072) = 10$, $v_{37}(75!) = 2$.

Exercise 1.1. Find in how many zeroes the number 150! ends by evaluating $v_p(150!)$ for some $p \mid 10$.

Exercise 1.2. Positive integers a, b satisfy the chain of divisibilities $a \mid b^2 \mid a^3 \mid b^4 \mid \dots$. Show that $a = b$.

Theorem 1.8. (LTE lemma) For an odd prime p, assume $p \mid x - y$, $p \nmid x, y$. Then $v_p(x^n - y^n) = v_p(x - y) + v_p(n)$. For example, $p \mid \dfrac{x^p - y^p}{x - y}$ (if the stated conditions hold!). Lemma also covers $v_p(x^n + y^n)$ and $v_2(x^n \pm y^n)$.

Exercise 1.3. (Estonia TST 2023) Let $p \in \mathbb{P}, x, y \in \mathbb{Z}$. Find $x^0 y^{p-1} + x^1 y^{p-2} + \dots + x^{p-2} y^1 + x^{p-1} y^0 \pmod{p}$.

In addition to the theory above, one could extend FLT from the prime case p to any $n \in \mathbb{N}$ with the help of the Euler function $\varphi(n)$, obtaining Euler's theorem. Other useful results include Chinese remainder theorem (CRT), Bertrand's postulate and many others. Below we shortly list the common arithmetic functions.

Definition 1.9. For a positive integer n, denote by $d(n), \sigma(n)$ the count and the sum of the positive divisors of n, respectively. Denote by $\varphi(n)$ the count of positive integers $a \leq n$ with $(a, n) = 1$.

When $n = p^k$ for some $k \in \mathbb{N}$, $d(n) = k + 1$, $\sigma(n) = 1 + \dots + p^k = \frac{p^{k+1} - 1}{p - 1}$ and $\varphi(n) = p^{k-1}(p - 1) = p^k \cdot \left(1 - \frac{1}{p}\right)$.

Observation 1.10. $d(n)$ is odd $\Leftrightarrow$ n is a perfect square. If n and $\sigma(n)$ are odd, then n is a perfect square. For $n \geq 3$, $\varphi(n)$ is even.

Theorem 1.11. (Bézout's lemma) Let a, b be positive integers and let $d = (a, b)$ be their greatest common factor. Then there exist integers x, y such that $ax + by = d$.

Theorem 1.12. (Mihăilescu) The only solution of $x^a - y^b = 1$ for $a, b > 1$ and $x, y > 0$ is $(x, a, y, b) = (3, 2, 2, 3)$.

2 Problems

1. (APMO 1998) Show that there doesn't exist positive integers a, b such that $(36a+b)(36b+a)$ is a power of two.

Solution. Assume $(36a+b)(36b+a) = 2^n$ and $d = (a,b)$, $a = dx, b = dy$, then $(x,y) = 1$ and $d^2(36x+y)(36y+x) = 2^n$. Then $36x+y, 36y+x$ are both powers of two, but if $2 \mid 36x+y, 36y+x$, then $2 \mid x, y$ and $(x,y) > 1$, a contradiction. Hence WLOG (without loss of generality) $36x + y = 1 \geq 37$, a contradiction ■

2. Prove that $\sigma(n-1)\sigma(n)\sigma(n+1)$ is even for all $n \geq 2$.

Solution. Assume that all three divisor sums are odd. If n is even, then $n-1, n+1$ are odd perfect squares, i.e. $x^2 - y^2 = 2$, which is impossible. If n is odd, then it's an odd square. Let $n-1 = 2^i x^2, n+1 = 2^j y^2$. Since there are no consecutive perfect squares, i, j are odd. But $2^i x^2 + 2 = 2^k y^2$, so $1 = 2^{k-1}y^2 - 2^{i-1}x^2$, the same contradiction ■

3. Let a, b, n be positive integers with $n \geq 2$. Show that $\sigma(n)^a = n^b$ is not possible.

Solution. Assume it holds, then $\sigma(n), n$ have the same set of divisors. Let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $\sigma(n) = p_1^{\beta_1} \dots p_k^{\beta_k}$. Note that $\sigma(n) > n$, so $a < b$. Furthermore, for all $i \in \{1, \dots, k\}$, $\alpha_i b = \beta_i a$, from where $\beta_i > \alpha_i$ i.e. $\beta_i \geq \alpha_i + 1$.

$$\sigma(n) = \prod_{i=1}^{k} \frac{{p_i}^{\alpha_i+1} - 1}{p_i - 1} \leq \prod_{i=1}^{k} \frac{{p_i}^{\beta_i} - 1}{p_i - 1} = \prod_{i=1}^{k} (1 + \dots + p^{\beta_i - 1}) < \prod_{i=1}^{k} {p_i}^{\beta_i} = \sigma(n),$$

which is a contradiction ■

4.

a) Prove that there exist 100 distinct positive integers $a_1, a_2, \dots, a_{100}$ such that a_i divides the total sum $s = a_1 + a_2 + \dots + a_{100}$ for each $i = 1, \dots, 100$.

b) Prove that there exist 99 distinct positive integers $b_1, \dots, b_{99}$ such that the sum of their cubes is a cube.

Solution. (a) We'll prove the statement by induction. Note that numbers $1, 2, 3$ satisfy this property, and whenever numbers $a_1, \dots, a_k$ satisfy the property (i.e. for each $i = 1, \dots, k$ we have $a_i \mid s_k = a_1 + \dots + a_k$), we can consider adding another number $a_{k+1} = s_k$. Indeed, $a_{k+1} \mid 2a_{k+1} = s_k + a_{k+1} = s_{k+1}$ and for each $i = 1, \dots, k$, $a_i \mid 2s_k = s_k + a_{k+1} = s_{k+1}$ (where s_{k+1} denotes $a_1 + \dots + a_{k+1}$). Hence $a_i \mid s_{k+1}$ holds for all $i = 1, \dots, k+1$ and the property holds for $k+1$ numbers. The base $k = 3$ and the step $k \to k+1$ of the induction hold, hence the statement is also true for $k = 100$ ■

Note 1: Don't forget to mention why a_{k+1} is distinct from $a_1, \dots, a_k$.

Note 2: The statement is obviously true for $k = 1$, but is false for $k = 2$: from $a_1, a_2 \mid a_1 + a_2$ follows $a_1 \mid a_2 \mid a_1$, so $a_1 = a_2$, a contradiction.

Solution. (b) Note that $3^3 + 4^3 + 5^3 = 6^3$. We'll use this identity to solve the problem by induction over the odd positive integers k. The base of $k = 3$ summands is clear. Assume that the cubes of distinct numbers $a_1, \dots, a_k$ sum to a cube s_k^3. Multiply the equality by 6^3, then

$$6^3 s_k^3 = 6^3 a_1^3 + \dots + 6^3 a_k^3 = 6^3 a_1^3 + 6^3 a_{k-1}^3 + (3^3 + 4^3 + 5^3) a_k^3.$$

Hence we have a construction for $k + 2$:

$$(6s_k)^3 = (6a_1)^3 + \dots + (6a_{k-1})^3 + (3a_k)^3 + (4a_k)^3 + (5a_k)^3$$

To ensure that the newly added terms are distinct from the rest ones, note that all three of them are smaller than $6a_k$. Consider a_k, the number that is broken down into three, to be the smallest out of $a_1, \dots, a_k$. Easy to check that this works. Now, both base $k = 3$ and the induction step $k \to k+2$ hold, hence the statement is also true for $k = 99$ ■

Note 1. We can also start the induction from the trivial $k = 1$.

Note 2. The statement is not true for $k = 2$ by Fermat's Last Theorem.

5. An integer larger than 1 is written on the board. Each move consists of substituting the number n on the board with the number $n + \frac{n}{p}$, where p is any prime divisor of n.

a) (Estonia,Ukraine 2021) Prove that as this process continues, 3 is chosen as p infinitely many times.

b) (Swiss 2022) Now assume the prime p chosen at each step is the smallest possible. Prove that after a finite number of moves a multiple of 3^{2025} will appear.

Solution. (a) Let q be the largest prime divisor of n. Observe that any chosen prime divisor inductively satisfies $p \leq \max\{q, n\}$, since $n + \frac{n}{p} = n\frac{p+1}{p}$, so finitely many distinct primes could be chosen. By Infinite Pigeonhole Principle, some prime is then chosen infinitely often. Assume $r > 3$ is the largest prime chosen infinitely often, then, since with every choice of r, $v_r(n)$ decreases, it should also increase infinitely often, hence some larger prime is chosen infinitely many times, contradicting the maximality of r. Therefore only 2 and 3 could be chosen infinitely often, but not only 2. The conclusion follows ■

Solution. (b) Denote by a_n the number obtained on the n-th term (with a_n being the initial number). We'll show by induction that for each $k \in \mathbb{N}$ there exists $m \in \mathbb{Z}^+$ such that $3^k \mid a_m$. The base case is clear: if a_1 is odd, then $a_2 = a_1 + \frac{a_1}{p}$ is even and $a_3 = a_2 + \frac{a_2}{2} = \frac{3a_2}{2}$, from where $3 \mid a_3$; if a_1 is even, then $a_2 = \frac{3a_1}{2}$, from where $3 \mid a_2$.

Assume that $3^k \mid a_m$ for $k \geq 1$. If a_m is even, then $a_{m+1} = \frac{3a_m}{2}$ and $3^{k+1} \mid a_{m+1}$. Now assume a_m is odd, then $a_{m+1} = a_m + \frac{a_m}{3} = \frac{4a_m}{3}$. Then $a_{m+2} = \frac{3a_{m+1}}{2} = 2a_m$ and $a_{m+3} = 3a_m$, from where $3^{k+1} \mid a_{m+3}$. Now, both the base $k = 1$ and the induction step $k \to k+1$ hold, hence the statement is true for $k = 2025$ ■

6. (IZhO 2020) Let p be a prime such that for any $a, b \in \mathbb{N}$ the number $2^a3^b + 1$ is not divisible by p. Prove that for any $c, d \in \mathbb{N}$ the number $2^c + 3^d$ is also not divisible by p.

Solution. We'll solve the problem for general n, using Euler's theorem (note that for a prime p, $\varphi(p) = p - 1$). Assume that $n \mid 2^c + 3^d$, then $(n, 2) = (n, 3) = 1$. Hence $2^{\varphi(n)} \equiv 3^{\varphi(n)} \equiv 1 \pmod{n}$. Let a be a sufficiently large integer such that $x\varphi(n) > c$, then

$$0 \equiv 2^c + 3^d \equiv 2^c + 3^d 2^{x\varphi(n)} \equiv 2^{x\varphi(n)-c}3^d + 1 \pmod{n},$$

so $a = x\varphi(n) - c$ and $b = d$ work, a contradiction ■

7.

a) Prove that if $n \mid 2^n - 1$, then $n = 1$. *Hint:* use $\text{ord}_m(2)$

b) Let $k \geq 2$ and let $n_1, \ldots, n_k$ be positive integers such that $n_1 \mid 2^{n_2} - 1$, $n_2 \mid 2^{n_3} - 1, \ldots, n_k \mid 2^{n_1} - 1$. Prove that $n_1 = n_2 = \cdots = n_k = 1$.

Solution. (a) Assume that $n > 1$ and let $p \mid n$. Then $p \neq 2$ (so $(p, 2) = 1$) and $2^n \equiv 1 \pmod{p}$. It follows that $\text{ord}_p(2) \mid n$. By FLT, $2^{p-1} \equiv 1 \pmod{p}$, hence also $\text{ord}_p(2) \mid p - 1$. It follows that $\text{ord}_p(2) \mid (n, p-1)$, whereas $(n, p-1) \leq \min\{n, p-1\}$. If $\text{ord}_p(2) = 1$, then $p \mid 2^1 - 1 = 1$, which is not possible. Hence $\text{ord}_p(2) > 1$ and there exists a prime q dividing $\text{ord}_p(2)$. Then $q \mid n$ and $q \mid p - 1$, so $q \leq p - 1 < p$. We see that from a prime divisor of n we obtained a smaller prime divisor of n. Assuming that p is the smallest prime divisor of n, $q < p$ should not exist, which gives a contradiction. Hence $n = 1$ ■

Solution. (b) Denote $M := \text{lcm}(n_1, \ldots, n_k)$ (least common multiple). Then for all $i = 1, \ldots, k$ $n_i \mid M$ and $2^{n_i} - 1 \mid 2^M - 1$ (show that $a \mid b \Rightarrow 2^a - 1 \mid 2^b - 1$). Consequently, for all $i \in \{1, \ldots, k\}$ $n_i \mid 2^M - 1$, hence $M \mid 2^M - 1$. It follows by part a) that $M = 1$, so $n_i \mid 1$ for all $i = 1, \ldots, k$, yielding $n_1 = \cdots = n_k = 1$ ■

8.

a) Let $n > 1$ be an integer. Prove that for each $d \mid n!$ with $d \neq n!$ there exists $d' \mid n!$ such that $d + d' \mid n!$.

b) (IOM 2018) Let $1 = d_0 < d_1 < \cdots < d_m = 4n$ be all positive divisors of $4n$, where n is a positive integer. Prove that there exists $i \in \{1, \ldots, m\}$ such that $d_i - d_{i-1} = 2$.

Solution. (a) We'll prove the statement by induction on n. The base case is clear: if $n = 2$, then $1 \mid 2!$, $1+1 = 2 \mid 2!$. Assume the statement works for $n = m$ and consider $n = m + 1$. Consider $d \mid (m+1)!$. If $d \mid m!$, then we are done by induction hypothesis. Otherwise $(d, m+1) > 1$. Let $d = ab$, where $a \mid m!$ and $(b, m!) = 1$. Then $b \mid m + 1$. By induction hypothesis, there exists $a' \mid m!$ such that $a + a' \mid m!$. Then $a'b \mid m!(m+1) = (m+1)!$, and, analogously, $d + a'b = (a + a')b \mid (m+1)!$. Hence choosing $d' = a'b$ works. Since the base and the induction step $n \to n+1$ hold, the statement is true for all $n > 1$ ■

Solution. (b) Assume the statement is false. Let d be the largest even integer with $d, d+2 \mid n$ $(d \geq 2)$, then $d + 1 \mid n$. Consider $2d, 2d+2, 2d+4$, it's easy to show that either the first two or the last two are also divisors, contradicting the maximality of d. Hence the statement is true ■

9. (Peru 2009) Let a, b, c be positive integers with $\gcd(a, b, c) = 1$. Prove that there exists $n \in \mathbb{N}$ such that $a^k + b^k + c^k$ is not divisible by 2^n for all $k \in \mathbb{N}$.

Solution. Note that at least one of a, b, c is odd. If one or all are odd, then the sum $s_k := a^k + b^k + c^k$ is odd for any k, hence taking $n = 1$ works. Next, WLOG consider that a, b are odd and c is even. If k is even, then $a^k + b^k \equiv 2 \pmod 4$ and $v_2(a^k + b^k) = 1$ (meaning $2^1 \mid a^k + b^k$, but $2^2 \nmid a^k + b^k$), so for all even k $4 \mid c^k$ and $4 \nmid s_k$.

If k is odd, then $a^k + b^k = (a+b)(a^{k-1} - a^{k-2}b + \cdots - ab^{k-2} + b^{k-1})$. Note that

$$\frac{a^k + b^k}{a+b} = a^{k-1} - a^{k-2}b + \cdots - ab^{k-2} + b^{k-1} \equiv \underbrace{1^{k-1} + \cdots + 1^{k-1}}_{k \text{ times}} \equiv k \equiv 1 \pmod 2.$$

Therefore $v_2(a^k + b^k) = v_2(a+b)$. Denote $x := v_2(a+b)$. Note that if $k > x$, then $2^{x+1} \mid c^k$, but $2^{x+1} \nmid a^k + b^k$, so $2^{x+1} \nmid s_k$. We aim to choose n such that

1. $n \geq 2$ (to satisfy $2^n \nmid s_k$ for even k);
2. $n \geq x + 1$ (to satisfy $2^n \nmid s_k$ for all odd $k > x$);
3. 2^n does not divide any s_k for $k \leq x$ and k odd.

Denote $y_k := v_2(a^k + b^k + c^k)$ for $k = 1, \ldots, x$, and let $y = \max\{y_1, \ldots, y_x\}$. Then choosing $n = \max\{x, y\} + 1$ works ■

Note: We could only consider y_k for $k \leq x$ and k odd.

10. (IZhO 2021) Prove that there exists a positive integer n, such that the remainder of 3^n when divided by 2^n is greater than 10^{2025}.

Solution. We'll solve the problem for general $A \in \mathbb{N}$ (in this problem $A = 10^{2025}$). Let $3^n = 2^n q_n + r_n$, where $0 < r_n < 2^n$ is the remainder. Assume the statement is false, then $r_n < A$ for all $n \in \mathbb{N}$. Let N be a sufficiently large integer such that $2^N > A$. Consider all integers $n \geq N+2$ and let $m \geq N+2$ be the one with the maximum possible value of r_m, i.e. for all $n \geq N$, $r_n \leq r_m < A$. Then $3^m \equiv r_m \pmod{2^m}$. Note that if $2^m \mid 3^m - r_m$, then $2^m \mid 3(3^m - r_m) = 3^{m+1} - 3r_m$ and $2^m \mid 3^{m+1} - 3r_m - 2^m$. Since one of the two consecutive integers $\dfrac{3^{m+1} - 3r_m}{2^m}$ and $\dfrac{3^{m+1} - 3r_m}{2^m} - 1 = \dfrac{3^{m+1} - 3r_m - 2^m}{2^m}$ is even, either $2^{m+1} \mid 3^{m+1} - 3r_m$ or $2^{m+1} \mid 3^{m+1} - 3r_m - 2^m$. Then $3^{m+1} \equiv 3r_m \pmod{2^{m+1}}$ or $3^{m+1} \equiv 3r_m + 2^m \pmod{2^{m+1}}$.

Note that $3^{m+1} \equiv r_{m+1} \pmod{2^{m+1}}$ and r_{m+1} is the unique integer $0 < r_{m+1} < 2^{m+1}$ with this property. Since

$$3r_m + 2^m < 3A + 2^m < 3 \cdot 2^N + 2^m < 4 \cdot 2^N + 2^m = 2^{N+2} + 2^m \leq 2^m + 2^m = 2^{m+1},$$

we have $0 < 3r_m < 2^{m+1}$ and $0 < 3r_m + 2^m < 2^{m+1}$. Then $r_{m+1} = 3r_m > r_m$ or $r_{m+1} = 3r_m + 2^m > r_m$. In both cases we construct r_{m+1} with the value greater than r_m, contradicting the maximality of r_m. Hence the statement is true ■

Note: Two related problems:

1. (China TST 2009) Let $a > b > 1, b$ is an odd number, let n be a positive integer. If $b^n | a^n - 1$, then $a^b > \frac{3^n}{n}$.
2. (RMM 2024) Fix integers a and b greater than 1. For any positive integer n, let r_n be the (non-negative) remainder that b^n leaves upon division by a^n. Assume there exists a positive integer N such that $r_n < \frac{2^n}{n}$ for all integers $n \geq N$. Prove that a divides b.

11. (ARO 2018) For $n \geq 3$. denote by s_n the sum of all primes less than n. Prove that there exists a number $m > 10^{2025}$ such that $(s_m, m) = 1$.

Solution. Assume that the statement is false, then there exists N such that for all $n \geq N$ $(s_n, n) = 1$. Denote by p_k the k-th prime number. Then $p_n \mid s_{p_n}$, let $s_{p_n} = p_n \cdot k$, then $p_{n+1} \mid s_{p_{n+1}} = s_{p_n} + p_n = (k+1)p_n$. Since $(p_n, p_{n+1}) = 1$, $p_{n+1} \mid k + 1$. Then

$$p_n p_{n+1} \leq (k+1)p_n = s_{p_{n+1}} = \sum_{k=1}^{n} p_i < np_n,$$

from where $p_{n+1} < n$, a contradiction ■

12. Let $n \geq 2$ and let $a_1, \ldots, a_n$ be distinct integers.

a) (Ukraine 2023) Call a pair (a_i, a_j) *elegant* if the sum $a_i + a_j$ is a power of 2. Find the largest possible number of elegant pairs.

b) (EMC 2024) Call a pair (a_i, a_j) *binary* if $a_i a_j + 1$ is a power of 2. Find the largest possible number of binary pairs.

Solution. (a) It's easy to construct n distinct integers forming $n-1$ elegant pairs. Let's prove more pairs is not possible. Consider a graph G on n vertices $a_1, \dots, a_n$ and draw an edge between a_i and a_j whenever (a_i, a_j) (or (a_j, a_i)) is an elegant pair.

It's well-known that a simple (i.e. having no double edges and loops) cycle-free graph on n vertices has at most $n-1$ edges. Assume that at least n elegant pairs are possible, then the corresponding graph G has at least n edges and hence contains a cycle. Let $(b_1, b_2), \dots, (b_{k-1}, b_k), (b_k, b_1)$ all be elegant pairs for $k \geq 3$, and let $b_i + b_{i+1} = 2^{c_i}$. WLOG assume b_1 has the greatest value among $b_1, \dots, b_k$ and $2^m \leq b_1 < 2^{m+1}$. Then

$$2^{c_1} = b_k + b_1 \leq 2b_1 < 2^{m+2}, \quad 2^{c_1} = b_k + b_1 > b_1 = 2^m,$$

hence we must have $c_k = m+1$. Analogously we obtain $2^m < b_1 + b_2 < 2^{m+2}$, hence $c_1 = m+1$. Therefore $b_k + b_1 = b_1 + b_2$ and $b_k = b_2$, contradicting that the numbers must be distinct.

Therefore $n-1$ is indeed the maximal possible number of elegant pairs.

Solution. (b) As in a), it's easy to construct n distinct integers forming $n-1$ binary pairs and we'll show that more pairs is not possible. Consider a graph G on n vertices $a_1, \dots, a_n$ and draw an edge between a_i and a_j whenever (a_i, a_j) (or (a_j, a_i)) is a binary pair. Assume that there are at least n binary pairs, then this graph has at least n edges and hence contains a cycle. Let $(b_1, b_2), \dots, (b_{k-1}, b_k), (b_k, b_1)$ all be binary pairs for $k \geq 3$ and let $b_i b_{i+1} + 1 = 2^{c_i}$.

WLOG assume b_1 has the greatest value among $b_1, \dots, b_k$ and WLOG $b_2 \geq b_k$. Then $2^{c_k} = b_k b_1 + 1 \leq b_1 b_2 + 1 = 2^{c_1}$, so $c_k \leq c_1$ and $b_k b_1 + 1 \mid b_1 b_2 + 1$. Then $b_k b_1 + 1 \mid (b_1 b_2 + 1) - (b_k b_1 + 1) = b_1(b_2 - b_k)$. Since $(b_1, b_k b_1 + 1) = 1$, it follows that $b_k b_1 + 1 \mid b_2 - b_k$. Since $b_2 \neq b_k$, we must have $b_2 > b_k$ and

$$0 < b_2 - b_k < b_2 < b_1 < b_k b_1 + 1,$$

which is a contradiction.

Therefore $n-1$ is indeed the maximal possible number of elegant pairs.