Shortlisted Problems with Solutions

53rd International Mathematical Olympiad

Mar del Plata, Argentina 2012

Note of Confidentiality

The shortlisted problems should be kept strictly confidential until IMO 2013

Contributing Countries

The Organizing Committee and the Problem Selection Committee of IMO 2012 thank the following 40 countries for contributing 136 problem proposals:

Australia, Austria, Belarus, Belgium, Bulgaria, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, India, Iran, Ireland, Israel, Japan, Kazakhstan, Luxembourg, Malaysia, Montenegro, Netherlands, Norway, Pakistan, Romania, Russia, Serbia, Slovakia, Slovenia, South Africa, South Korea, Sweden, Thailand, Ukraine, United Kingdom, United States of America, Uzbekistan

Problem Selection Committee

Martín Avendaño
Carlos di Fiore
Géza Kós
Svetoslav Savchev

Algebra

A1. Find all the functions $f : \mathbb{Z} \to \mathbb{Z}$ such that

$$f(a)^2 + f(b)^2 + f(c)^2 = 2f(a)f(b) + 2f(b)f(c) + 2f(c)f(a)$$

for all integers a, b, c satisfying $a + b + c = 0$.

A2. Let $\mathbb{Z}$ and $\mathbb{Q}$ be the sets of integers and rationals respectively.

a) Does there exist a partition of $\mathbb{Z}$ into three non-empty subsets A, B, C such that the sets $A + B$, $B + C$, $C + A$ are disjoint?

b) Does there exist a partition of $\mathbb{Q}$ into three non-empty subsets A, B, C such that the sets $A + B$, $B + C$, $C + A$ are disjoint?

Here $X + Y$ denotes the set $\{x + y \mid x \in X, y \in Y\}$, for $X, Y \subseteq \mathbb{Z}$ and $X, Y \subseteq \mathbb{Q}$.

A3. Let $a_2, \ldots, a_n$ be $n - 1$ positive real numbers, where $n \geq 3$, such that $a_2 a_3 \cdots a_n = 1$. Prove that

$$(1 + a_2)^2 (1 + a_3)^3 \cdots (1 + a_n)^n > n^n.$$

A4. Let f and g be two nonzero polynomials with integer coefficients and $\deg f > \deg g$. Suppose that for infinitely many primes p the polynomial $pf + g$ has a rational root. Prove that f has a rational root.

A5. Find all functions $f \colon \mathbb{R} \to \mathbb{R}$ that satisfy the conditions

$$f(1 + xy) - f(x + y) = f(x)f(y) \quad \text{for all } x, y \in \mathbb{R}$$

and $f(-1) \neq 0$.

A6. Let $f : \mathbb{N} \to \mathbb{N}$ be a function, and let f^m be f applied m times. Suppose that for every $n \in \mathbb{N}$ there exists a $k \in \mathbb{N}$ such that $f^{2k}(n) = n + k$, and let k_n be the smallest such k. Prove that the sequence $k_1, k_2, \ldots$ is unbounded.

A7. We say that a function $f : \mathbb{R}^k \to \mathbb{R}$ is a metapolynomial if, for some positive integers m and n, it can be represented in the form

$$f(x_1, \ldots, x_k) = \max_{i=1,\ldots,m} \min_{j=1,\ldots,n} P_{i,j}(x_1, \ldots, x_k)$$

where $P_{i,j}$ are multivariate polynomials. Prove that the product of two metapolynomials is also a metapolynomial.

Combinatorics

C1. Several positive integers are written in a row. Iteratively, Alice chooses two adjacent numbers x and y such that $x > y$ and x is to the left of y, and replaces the pair (x, y) by either $(y + 1, x)$ or $(x - 1, x)$. Prove that she can perform only finitely many such iterations.

C2. Let $n \geq 1$ be an integer. What is the maximum number of disjoint pairs of elements of the set $\{1, 2, \ldots, n\}$ such that the sums of the different pairs are different integers not exceeding n?

C3. In a 999×999 square table some cells are white and the remaining ones are red. Let T be the number of triples (C_1, C_2, C_3) of cells, the first two in the same row and the last two in the same column, with C_1 and C_3 white and C_2 red. Find the maximum value T can attain.

C4. Players A and B play a game with $N \geq 2012$ coins and 2012 boxes arranged around a circle. Initially A distributes the coins among the boxes so that there is at least 1 coin in each box. Then the two of them make moves in the order $B, A, B, A, \ldots$ by the following rules:

- On every move of his B passes 1 coin from every box to an adjacent box.
- On every move of hers A chooses several coins that were *not* involved in B's previous move and are in different boxes. She passes every chosen coin to an adjacent box.

Player A's goal is to ensure at least 1 coin in each box after every move of hers, regardless of how B plays and how many moves are made. Find the least N that enables her to succeed.

C5. The columns and the rows of a $3n \times 3n$ square board are numbered $1, 2, \ldots, 3n$. Every square (x, y) with $1 \leq x, y \leq 3n$ is colored asparagus, byzantium or citrine according as the modulo 3 remainder of $x + y$ is 0, 1 or 2 respectively. One token colored asparagus, byzantium or citrine is placed on each square, so that there are $3n^2$ tokens of each color.

Suppose that one can permute the tokens so that each token is moved to a distance of at most d from its original position, each asparagus token replaces a byzantium token, each byzantium token replaces a citrine token, and each citrine token replaces an asparagus token. Prove that it is possible to permute the tokens so that each token is moved to a distance of at most $d + 2$ from its original position, and each square contains a token with the same color as the square.

C6. Let k and n be fixed positive integers. In the liar's guessing game, Amy chooses integers x and N with $1 \leq x \leq N$. She tells Ben what N is, but not what x is. Ben may then repeatedly ask Amy whether $x \in S$ for arbitrary sets S of integers. Amy will always answer with *yes* or *no*, but she might lie. The only restriction is that she can lie at most k times in a row. After he has asked as many questions as he wants, Ben must specify a set of at most n positive integers. If x is in this set he wins; otherwise, he loses. Prove that:

a) If $n \geq 2^k$ then Ben can always win.

b) For sufficiently large k there exist $n \geq 1.99^k$ such that Ben cannot guarantee a win.

C7. There are given 2^{500} points on a circle labeled $1, 2, \ldots, 2^{500}$ in some order. Prove that one can choose 100 pairwise disjoint chords joining some of these points so that the 100 sums of the pairs of numbers at the endpoints of the chosen chords are equal.

Geometry

G1. In the triangle ABC the point J is the center of the excircle opposite to A. This excircle is tangent to the side BC at M, and to the lines AB and AC at K and L respectively. The lines LM and BJ meet at F, and the lines KM and CJ meet at G. Let S be the point of intersection of the lines AF and BC, and let T be the point of intersection of the lines AG and BC. Prove that M is the midpoint of ST.

G2. Let $ABCD$ be a cyclic quadrilateral whose diagonals AC and BD meet at E. The extensions of the sides AD and BC beyond A and B meet at F. Let G be the point such that $ECGD$ is a parallelogram, and let H be the image of E under reflection in AD. Prove that D, H, F, G are concyclic.

G3. In an acute triangle ABC the points D, E and F are the feet of the altitudes through A, B and C respectively. The incenters of the triangles AEF and BDF are I_1 and I_2 respectively; the circumcenters of the triangles ACI_1 and BCI_2 are O_1 and O_2 respectively. Prove that I_1I_2 and O_1O_2 are parallel.

G4. Let ABC be a triangle with $AB \neq AC$ and circumcenter O. The bisector of $\angle BAC$ intersects BC at D. Let E be the reflection of D with respect to the midpoint of BC. The lines through D and E perpendicular to BC intersect the lines AO and AD at X and Y respectively. Prove that the quadrilateral $BXCY$ is cyclic.

G5. Let ABC be a triangle with $\angle BCA = 90^\circ$, and let C_0 be the foot of the altitude from C. Choose a point X in the interior of the segment CC_0, and let K, L be the points on the segments AX, BX for which $BK = BC$ and $AL = AC$ respectively. Denote by M the intersection of AL and BK. Show that $MK = ML$.

G6. Let ABC be a triangle with circumcenter O and incenter I. The points D, E and F on the sides BC, CA and AB respectively are such that $BD + BF = CA$ and $CD + CE = AB$. The circumcircles of the triangles BFD and CDE intersect at $P \neq D$. Prove that $OP = OI$.

G7. Let $ABCD$ be a convex quadrilateral with non-parallel sides BC and AD. Assume that there is a point E on the side BC such that the quadrilaterals $ABED$ and $AECD$ are circumscribed. Prove that there is a point F on the side AD such that the quadrilaterals $ABCF$ and $BCDF$ are circumscribed if and only if AB is parallel to CD.

G8. Let ABC be a triangle with circumcircle ω and ℓ a line without common points with ω. Denote by P the foot of the perpendicular from the center of ω to ℓ. The side-lines BC, CA, AB intersect ℓ at the points X, Y, Z different from P. Prove that the circumcircles of the triangles AXP, BYP and CZP have a common point different from P or are mutually tangent at P.

Number Theory

N1. Call admissible a set A of integers that has the following property:

$$\text{If } x, y \in A \text{ (possibly } x = y) \text{ then } x^2 + kxy + y^2 \in A \text{ for every integer } k.$$

Determine all pairs m, n of nonzero integers such that the only admissible set containing both m and n is the set of all integers.

N2. Find all triples (x, y, z) of positive integers such that $x \leq y \leq z$ and

$$x^3(y^3 + z^3) = 2012(xyz + 2).$$

N3. Determine all integers $m \geq 2$ such that every n with $\frac{m}{3} \leq n \leq \frac{m}{2}$ divides the binomial coefficient $\binom{n}{m-2n}$.

N4. An integer a is called friendly if the equation $(m^2 + n)(n^2 + m) = a(m - n)^3$ has a solution over the positive integers.

a) Prove that there are at least 500 friendly integers in the set $\{1, 2, \ldots, 2012\}$.

b) Decide whether $a = 2$ is friendly.

N5. For a nonnegative integer n define $rad(n) = 1$ if $n = 0$ or $n = 1$, and $rad(n) = p_1 p_2 \cdots p_k$ where $p_1 < p_2 < \cdots < p_k$ are all prime factors of n. Find all polynomials $f(x)$ with nonnegative integer coefficients such that $rad(f(n))$ divides $rad(f(n^{rad(n)}))$ for every nonnegative integer n.

N6. Let x and y be positive integers. If $x^{2^n} - 1$ is divisible by $2^n y + 1$ for every positive integer n, prove that $x = 1$.

N7. Find all $n \in \mathbb{N}$ for which there exist nonnegative integers $a_1, a_2, \ldots, a_n$ such that

$$\frac{1}{2^{a_1}} + \frac{1}{2^{a_2}} + \cdots + \frac{1}{2^{a_n}} = \frac{1}{3^{a_1}} + \frac{2}{3^{a_2}} + \cdots + \frac{n}{3^{a_n}} = 1.$$

N8. Prove that for every prime $p > 100$ and every integer r there exist two integers a and b such that p divides $a^2 + b^5 - r$.

Algebra

A1. Find all the functions $f : \mathbb{Z} \to \mathbb{Z}$ such that

$$f(a)^2 + f(b)^2 + f(c)^2 = 2f(a)f(b) + 2f(b)f(c) + 2f(c)f(a)$$

for all integers a, b, c satisfying $a + b + c = 0$.

Solution. The substitution $a = b = c = 0$ gives $3f(0)^2 = 6f(0)^2$, hence

$$f(0) = 0. \tag{1}$$

The substitution $b = -a$ and $c = 0$ gives $((f(a) - f(-a))^2 = 0$. Hence f is an even function:

$$f(a) = f(-a) \quad \text{for all } a \in \mathbb{Z}. \tag{2}$$

Now set $b = a$ and $c = -2a$ to obtain $2f(a)^2 + f(2a)^2 = 2f(a)^2 + 4f(a)f(2a)$. Hence

$$f(2a) = 0 \ \text{ or } \ f(2a) = 4f(a) \quad \text{for all } a \in \mathbb{Z}. \tag{3}$$

If $f(r) = 0$ for some $r \geq 1$ then the substitution $b = r$ and $c = -a-r$ gives $(f(a+r)-f(a))^2 = 0$. So f is periodic with period r, i. e.

$$f(a + r) = f(a) \quad \text{for all } a \in \mathbb{Z}.$$

In particular, if $f(1) = 0$ then f is constant, thus $f(a) = 0$ for all $a \in \mathbb{Z}$. This function clearly satisfies the functional equation. For the rest of the analysis, we assume $f(1) = k \neq 0$.

By (3) we have $f(2) = 0$ or $f(2) = 4k$. If $f(2) = 0$ then f is periodic of period 2, thus $f(\text{even}) = 0$ and $f(\text{odd}) = k$. This function is a solution for every k. We postpone the verification; for the sequel assume $f(2) = 4k \neq 0$.

By (3) again, we have $f(4) = 0$ or $f(4) = 16k$. In the first case f is periodic of period 4, and $f(3) = f(-1) = f(1) = k$, so we have $f(4n) = 0$, $f(4n+1) = f(4n+3) = k$, and $f(4n+2) = 4k$ for all $n \in \mathbb{Z}$. This function is a solution too, which we justify later. For the rest of the analysis, we assume $f(4) = 16k \neq 0$.

We show now that $f(3) = 9k$. In order to do so, we need two substitutions:

$$a = 1, b = 2, c = -3 \Longrightarrow f(3)^2 - 10kf(3) + 9k^2 = 0 \Longrightarrow f(3) \in \{k, 9k\},$$
$$a = 1, b = 3, c = -4 \Longrightarrow f(3)^2 - 34kf(3) + 225k^2 = 0 \Longrightarrow f(3) \in \{9k, 25k\}.$$

Therefore $f(3) = 9k$, as claimed. Now we prove inductively that the only remaining function is $f(x) = kx^2$, $x \in \mathbb{Z}$. We proved this for $x = 0, 1, 2, 3, 4$. Assume that $n \geq 4$ and that $f(x) = kx^2$ holds for all integers $x \in [0, n]$. Then the substitutions $a = n$, $b = 1$, $c = -n-1$ and $a = n-1$, $b = 2$, $c = -n - 1$ lead respectively to

$$f(n + 1) \in \{k(n + 1)^2, k(n - 1)^2\} \qquad \text{and} \qquad f(n + 1) \in \{k(n + 1)^2, k(n - 3)^2\}.$$

Since $k(n - 1)^2 \neq k(n - 3)^2$ for $n \neq 2$, the only possibility is $f(n + 1) = k(n + 1)^2$. This completes the induction, so $f(x) = kx^2$ for all $x \geq 0$. The same expression is valid for negative values of x since f is even. To verify that $f(x) = kx^2$ is actually a solution, we need to check the identity $a^4 + b^4 + (a + b)^4 = 2a^2b^2 + 2a^2(a + b)^2 + 2b^2(a + b)^2$, which follows directly by expanding both sides.

Therefore the only possible solutions of the functional equation are the constant function $f_1(x) = 0$ and the following functions:

$$f_2(x) = kx^2 \qquad f_3(x) = \begin{cases} 0 & x \text{ even} \\ k & x \text{ odd} \end{cases} \qquad f_4(x) = \begin{cases} 0 & x \equiv 0 \pmod 4 \\ k & x \equiv 1 \pmod 2 \\ 4k & x \equiv 2 \pmod 4 \end{cases}$$

for any non-zero integer k. The verification that they are indeed solutions was done for the first two. For f_3 note that if $a + b + c = 0$ then either a, b, c are all even, in which case $f(a) = f(b) = f(c) = 0$, or one of them is even and the other two are odd, so both sides of the equation equal $2k^2$. For f_4 we use similar parity considerations and the symmetry of the equation, which reduces the verification to the triples $(0, k, k)$, $(4k, k, k)$, $(0, 0, 0)$, $(0, 4k, 4k)$. They all satisfy the equation.

Comment. We used several times the same fact: For any $a, b \in \mathbb{Z}$ the functional equation is a quadratic equation in $f(a + b)$ whose coefficients depend on $f(a)$ and $f(b)$:

$$f(a + b)^2 - 2(f(a) + f(b))f(a + b) + (f(a) - f(b))^2 = 0.$$

Its discriminant is $16f(a)f(b)$. Since this value has to be non-negative for any $a, b \in \mathbb{Z}$, we conclude that either f or $-f$ is always non-negative. Also, if f is a solution of the functional equation, then $-f$ is also a solution. Therefore we can assume $f(x) \geq 0$ for all $x \in \mathbb{Z}$. Now, the two solutions of the quadratic equation are

$$f(a + b) \in \left\{ \left(\sqrt{f(a)} + \sqrt{f(b)} \right)^2, \left(\sqrt{f(a)} - \sqrt{f(b)} \right)^2 \right\} \quad \text{for all } a, b \in \mathbb{Z}.$$

The computation of $f(3)$ from $f(1)$, $f(2)$ and $f(4)$ that we did above follows immediately by setting $(a, b) = (1, 2)$ and $(a, b) = (1, -4)$. The inductive step, where $f(n + 1)$ is derived from $f(n)$, $f(n - 1)$, $f(2)$ and $f(1)$, follows immediately using $(a, b) = (n, 1)$ and $(a, b) = (n - 1, 2)$.

A2. Let $\mathbb{Z}$ and $\mathbb{Q}$ be the sets of integers and rationals respectively.

a) Does there exist a partition of $\mathbb{Z}$ into three non-empty subsets A, B, C such that the sets $A+B$, $B+C$, $C+A$ are disjoint?

b) Does there exist a partition of $\mathbb{Q}$ into three non-empty subsets A, B, C such that the sets $A+B$, $B+C$, $C+A$ are disjoint?

Here $X+Y$ denotes the set $\{x+y \mid x \in X, y \in Y\}$, for $X, Y \subseteq \mathbb{Z}$ and $X, Y \subseteq \mathbb{Q}$.

Solution 1. a) The residue classes modulo 3 yield such a partition:

$$A = \{3k \mid k \in \mathbb{Z}\}, \quad B = \{3k+1 \mid k \in \mathbb{Z}\}, \quad C = \{3k+2 \mid k \in \mathbb{Z}\}.$$

b) The answer is *no*. Suppose that $\mathbb{Q}$ can be partitioned into non-empty subsets A, B, C as stated. Note that for all $a \in A$, $b \in B$, $c \in C$ one has

$$a+b-c \in C, \quad b+c-a \in A, \quad c+a-b \in B. \tag{1}$$

Indeed $a+b-c \notin A$ as $(A+B)\cap(A+C) = \emptyset$, and similarly $a+b-c \notin B$, hence $a+b-c \in C$. The other two relations follow by symmetry. Hence $A+B \subset C+C$, $B+C \subset A+A$, $C+A \subset B+B$.

The opposite inclusions also hold. Let $a, a' \in A$ and $b \in B$, $c \in C$ be arbitrary. By (1) $a'+c-b \in B$, and since $a \in A$, $c \in C$, we use (1) again to obtain

$$a+a'-b = a+(a'+c-b)-c \in C.$$

So $A+A \subset B+C$ and likewise $B+B \subset C+A$, $C+C \subset A+B$. In summary

$$B+C = A+A, \qquad C+A = B+B, \qquad A+B = C+C.$$

Furthermore suppose that $0 \in A$ without loss of generality. Then $B = \{0\}+B \subset A+B$ and $C = \{0\}+C \subset A+C$. So, since $B+C$ is disjoint with $A+B$ and $A+C$, it is also disjoint with B and C. Hence $B+C$ is contained in $\mathbb{Z} \setminus (B \cup C) = A$. Because $B+C = A+A$, we obtain $A+A \subset A$. On the other hand $A = \{0\}+A \subset A+A$, implying $A = A+A = B+C$.

Therefore $A+B+C = A+A+A = A$, and now $B+B = C+A$ and $C+C = A+B$ yield $B+B+B = A+B+C = A$, $C+C+C = A+B+C = A$. In particular if $r \in \mathbb{Q} = A \cup B \cup C$ is arbitrary then $3r \in A$.

However such a conclusion is impossible. Take any $b \in B$ ($B \neq \emptyset$) and let $r = b/3 \in \mathbb{Q}$. Then $b = 3r \in A$ which is a contradiction.

Solution 2. We prove that the example for $\mathbb{Z}$ from the first solution is unique, and then use this fact to solve part b).

Let $\mathbb{Z} = A \cup B \cup C$ be a partition of $\mathbb{Z}$ with $A, B, C \neq \emptyset$ and $A+B$, $B+C$, $C+A$ disjoint. We need the relations (1) which clearly hold for $\mathbb{Z}$. Fix two consecutive integers from different sets, say $b \in B$ and $c = b+1 \in C$. For every $a \in A$ we have, in view of (1), $a-1 = a+b-c \in C$ and $a+1 = a+c-b \in B$. So every $a \in A$ is preceded by a number from C and followed by a number from B.

In particular there are pairs of the form $c, c+1$ with $c \in C$, $c+1 \in A$. For such a pair and any $b \in B$ analogous reasoning shows that each $b \in B$ is preceded by a number from A and followed by a number from C. There are also pairs $b, b-1$ with $b \in B$, $b-1 \in A$. We use them in a similar way to prove that each $c \in C$ is preceded by a number from B and followed by a number from A.

By putting the observations together we infer that A, B, C are the three congruence classes modulo 3. Observe that all multiples of 3 are in the set of the partition that contains 0.

Now we turn to part b). Suppose that there is a partition of $\mathbb{Q}$ with the given properties. Choose three rationals $r_i = p_i/q_i$ from the three sets A, B, C, $i = 1, 2, 3$, and set $N = 3q_1q_2q_3$.

Let $S \subset \mathbb{Q}$ be the set of fractions with denominators N (irreducible or not). It is obtained through multiplication of every integer by the constant $1/N$, hence closed under sums and differences. Moreover, if we identify each $k \in \mathbb{Z}$ with $k/N \in S$ then S is essentially the set $\mathbb{Z}$ with respect to addition. The numbers r_i belong to S because

$$r_1 = \frac{3p_1q_2q_3}{N}, \qquad r_2 = \frac{3p_2q_3q_1}{N}, \qquad r_3 = \frac{3p_3q_1q_2}{N}.$$

The partition $\mathbb{Q} = A \cup B \cup C$ of $\mathbb{Q}$ induces a partition $S = A' \cup B' \cup C'$ of S, with $A' = A \cap S$, $B' = B \cap S$, $C' = C \cap S$. Clearly $A' + B'$, $B' + C'$, $C' + A'$ are disjoint, so this partition has the properties we consider.

By the uniqueness of the example for $\mathbb{Z}$ the sets A', B', C' are the congruence classes modulo 3, multiplied by $1/N$. Also all multiples of $3/N$ are in the same set, A', B' or C'. This holds for r_1, r_2, r_3 in particular as they are all multiples of $3/N$. However r_1, r_2, r_3 are in different sets A', B', C' since they were chosen from different sets A, B, C. The contradiction ends the proof.

Comment. The uniqueness of the example for $\mathbb{Z}$ can also be deduced from the argument in the first solution.

A3. Let $a_2, \ldots, a_n$ be $n-1$ positive real numbers, where $n \geq 3$, such that $a_2 a_3 \cdots a_n = 1$. Prove that

$$(1+a_2)^2(1+a_3)^3 \cdots (1+a_n)^n > n^n.$$

Solution. The substitution $a_2 = \dfrac{x_2}{x_1}$, $a_3 = \dfrac{x_3}{x_2}$, $\ldots$, $a_n = \dfrac{x_1}{x_{n-1}}$ transforms the original problem into the inequality

$$(x_1+x_2)^2(x_2+x_3)^3 \cdots (x_{n-1}+x_1)^n > n^n x_1^2 x_2^3 \cdots x_{n-1}^n \qquad (*)$$

for all $x_1, \ldots, x_{n-1} > 0$. To prove this, we use the AM-GM inequality for each factor of the left-hand side as follows:

$$\begin{array}{rcll}
(x_1+x_2)^2 & & & \geq 2^2 x_1 x_2 \\
(x_2+x_3)^3 & = & \left(2\left(\frac{x_2}{2}\right)+x_3\right)^3 & \geq 3^3\left(\frac{x_2}{2}\right)^2 x_3 \\
(x_3+x_4)^4 & = & \left(3\left(\frac{x_3}{3}\right)+x_4\right)^4 & \geq 4^4\left(\frac{x_3}{3}\right)^3 x_4 \\
 & \vdots & \vdots & \vdots \\
(x_{n-1}+x_1)^n & = & \left((n-1)\left(\frac{x_{n-1}}{n-1}\right)+x_1\right)^n & \geq n^n\left(\frac{x_{n-1}}{n-1}\right)^{n-1} x_1.
\end{array}$$

Multiplying these inequalities together gives (*), with inequality sign $\geq$ instead of $>$. However for the equality to occur it is necessary that $x_1 = x_2$, $x_2 = 2x_3$, $\ldots$, $x_{n-1} = (n-1)x_1$, implying $x_1 = (n-1)!x_1$. This is impossible since $x_1 > 0$ and $n \geq 3$. Therefore the inequality is strict.

Comment. One can avoid the substitution $a_i = x_i/x_{i-1}$. Apply the weighted AM-GM inequality to each factor $(1+a_k)^k$, with the same weights like above, to obtain

$$(1+a_k)^k = \left((k-1)\frac{1}{k-1} + a_k\right)^k \geq \frac{k^k}{(k-1)^{k-1}} a_k.$$

Multiplying all these inequalities together gives

$$(1+a_2)^2(1+a_3)^3 \cdots (1+a_n)^n \geq n^n a_2 a_3 \cdots a_n = n^n.$$

The same argument as in the proof above shows that the equality cannot be attained.

A4. Let f and g be two nonzero polynomials with integer coefficients and $\deg f > \deg g$. Suppose that for infinitely many primes p the polynomial $pf + g$ has a rational root. Prove that f has a rational root.

Solution 1. Since $\deg f > \deg g$, we have $|g(x)/f(x)| < 1$ for sufficiently large x; more precisely, there is a real number R such that $|g(x)/f(x)| < 1$ for all x with $|x| > R$. Then for all such x and all primes p we have

$$\big|pf(x) + g(x)\big| \geq \big|f(x)\big| \left(p - \frac{|g(x)|}{|f(x)|}\right) > 0.$$

Hence all real roots of the polynomials $pf + g$ lie in the interval $[-R, R]$.

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ where $n > m$, $a_n \neq 0$ and $b_m \neq 0$. Upon replacing $f(x)$ and $g(x)$ by $a_n^{n-1} f(x/a_n)$ and $a_n^{n-1} g(x/a_n)$ respectively, we reduce the problem to the case $a_n = 1$. In other words one can assume that f is monic. Then the leading coefficient of $pf + g$ is p, and if $r = u/v$ is a rational root of $pf + g$ with $(u, v) = 1$ and $v > 0$, then either $v = 1$ or $v = p$.

First consider the case when $v = 1$ infinitely many times. If $v = 1$ then $|u| \leq R$, so there are only finitely many possibilities for the integer u. Therefore there exist distinct primes p and q for which we have the same value of u. Then the polynomials $pf + g$ and $qf + g$ share this root, implying $f(u) = g(u) = 0$. So in this case f and g have an integer root in common.

Now suppose that $v = p$ infinitely many times. By comparing the exponent of p in the denominators of $pf(u/p)$ and $g(u/p)$ we get $m = n - 1$ and $pf(u/p) + g(u/p) = 0$ reduces to an equation of the form

$$\Big(u^n + a_{n-1}pu^{n-1} + \ldots + a_0 p^n\Big) + \Big(b_{n-1}u^{n-1} + b_{n-2}pu^{n-2} + \ldots + b_0 p^{n-1}\Big) = 0.$$

The equation above implies that $u^n + b_{n-1}u^{n-1}$ is divisible by p and hence, since $(u, p) = 1$, we have $u + b_{n-1} = pk$ with some integer k. On the other hand all roots of $pf + g$ lie in the interval $[-R, R]$, so that

$$\frac{|pk - b_{n-1}|}{p} = \frac{|u|}{p} < R,$$
$$|k| < R + \frac{|b_{n-1}|}{p} < R + |b_{n-1}|.$$

Therefore the integer k can attain only finitely many values. Hence there exists an integer k such that the number $\frac{pk - b_{n-1}}{p} = k - \frac{b_{n-1}}{p}$ is a root of $pf + g$ for infinitely many primes p. For these primes we have

$$f\left(k - b_{n-1}\frac{1}{p}\right) + \frac{1}{p} g\left(k - b_{n-1}\frac{1}{p}\right) = 0.$$

So the equation

$$f\left(k - b_{n-1}x\right) + x g\left(k - b_{n-1}x\right) = 0 \tag{1}$$

has infinitely many solutions of the form $x = 1/p$. Since the left-hand side is a polynomial, this implies that (1) is a polynomial identity, so it holds for all real x. In particular, by substituting $x = 0$ in (1) we get $f(k) = 0$. Thus the integer k is a root of f.

In summary the monic polynomial f obtained after the initial reduction always has an integer root. Therefore the original polynomial f has a rational root.

Solution 2. Analogously to the first solution, there exists a real number R such that the complex roots of all polynomials of the form $pf + g$ lie in the disk $|z| \le R$.

For each prime p such that $pf + g$ has a rational root, by GAUSS' lemma $pf + g$ is the product of two integer polynomials, one with degree 1 and the other with degree $\deg f - 1$. Since p is a prime, the leading coefficient of one of these factors divides the leading coefficient of f. Denote that factor by h_p.

By narrowing the set of the primes used we can assume that all polynomials h_p have the same degree and the same leading coefficient. Their complex roots lie in the disk $|z| \le R$, hence VIETA's formulae imply that all coefficients of all polynomials h_p form a bounded set. Since these coefficients are integers, there are only finitely many possible polynomials h_p. Hence there is a polynomial h such that $h_p = h$ for infinitely many primes p.

Finally, if p and q are distinct primes with $h_p = h_q = h$ then h divides $(p - q)f$. Since $\deg h = 1$ or $\deg h = \deg f - 1$, in both cases f has a rational root.

Comment. Clearly the polynomial h is a common factor of f and g. If $\deg h = 1$ then f and g share a rational root. Otherwise $\deg h = \deg f - 1$ forces $\deg g = \deg f - 1$ and g divides f over the rationals.

Solution 3. Like in the first solution, there is a real number R such that the real roots of all polynomials of the form $pf + g$ lie in the interval $[-R, R]$.

Let $p_1 < p_2 < \cdots$ be an infinite sequence of primes so that for every index k the polynomial $p_k f + g$ has a rational root r_k. The sequence $r_1, r_2, \dots$ is bounded, so it has a convergent subsequence $r_{k_1}, r_{k_2}, \dots$. Now replace the sequences $(p_1, p_2, \dots)$ and $(r_1, r_2, \dots)$ by $(p_{k_1}, p_{k_2}, \dots)$ and $(r_{k_1}, r_{k_2}, \dots)$; after this we can assume that the sequence $r_1, r_2, \dots$ is convergent. Let $\alpha = \lim\limits_{k\to\infty} r_k$. We show that α is a rational root of f.

Over the interval $[-R, R]$, the polynomial g is bounded, $|g(x)| \le M$ with some fixed M. Therefore

$$|f(r_k)| = \left| f(r_k) - \frac{p_k f(r_k) + g(r_k)}{p_k} \right| = \frac{|g(r_k)|}{p_k} \le \frac{M}{p_k} \to 0,$$

and

$$f(\alpha) = f\Big(\lim_{k\to\infty} r_k \Big) = \lim_{k\to\infty} f(r_k) = 0.$$

So α is a root of f indeed.

Now let u_k, v_k be relative prime integers for which $r_k = \frac{u_k}{v_k}$. Let a be the leading coefficient of f, let $b = f(0)$ and $c = g(0)$ be the constant terms of f and g, respectively. The leading coefficient of the polynomial $p_k f + g$ is $p_k a$, its constant term is $p_k b + c$. So v_k divides $p_k a$ and u_k divides $p_k b + c$. Let $p_k b + c = u_k e_k$ (if $p_k b + c = u_k = 0$ then let $e_k = 1$).

We prove that α is rational by using the following fact. *Let (p_n) and (q_n) be sequences of integers such that the sequence (p_n/q_n) converges. If (p_n) or (q_n) is bounded then* $\lim(p_n/q_n)$ *is rational.*

Case 1: There is an infinite subsequence (k_n) of indices such that v_{k_n} divides a. Then (v_{k_n}) is bounded, so $\alpha = \lim_{n\to\infty}(u_{k_n}/v_{k_n})$ is rational.

Case 2: There is an infinite subsequence (k_n) of indices such that v_{k_n} does not divide a. For such indices we have $v_{k_n} = p_{k_n} d_{k_n}$ where d_{k_n} is a divisor of a. Then

$$\alpha = \lim_{n\to\infty} \frac{u_{k_n}}{v_{k_n}} = \lim_{n\to\infty} \frac{p_{k_n} b + c}{p_{k_n} d_{k_n} e_{k_n}} = \lim_{n\to\infty} \frac{b}{d_{k_n} e_{k_n}} + \lim_{n\to\infty} \frac{c}{p_{k_n} d_{k_n} e_{k_n}} = \lim_{n\to\infty} \frac{b}{d_{k_n} e_{k_n}}.$$

Because the numerator b in the last limit is bounded, α is rational.

A5. Find all functions $f\colon \mathbb{R} \to \mathbb{R}$ that satisfy the conditions

$$f(1+xy) - f(x+y) = f(x)f(y) \quad \text{for all } x, y \in \mathbb{R}$$

and $f(-1) \neq 0$.

Solution. The only solution is the function $f(x) = x - 1$, $x \in \mathbb{R}$.

We set $g(x) = f(x) + 1$ and show that $g(x) = x$ for all real x. The conditions take the form

$$g(1+xy) - g(x+y) = \big(g(x) - 1\big)\big(g(y) - 1\big) \quad \text{for all } x, y \in \mathbb{R} \text{ and } g(-1) \neq 1. \tag{1}$$

Denote $C = g(-1) - 1 \neq 0$. Setting $y = -1$ in (1) gives

$$g(1-x) - g(x-1) = C(g(x) - 1). \tag{2}$$

Set $x = 1$ in (2) to obtain $C(g(1) - 1) = 0$. Hence $g(1) = 1$ as $C \neq 0$. Now plugging in $x = 0$ and $x = 2$ yields $g(0) = 0$ and $g(2) = 2$ respectively.

We pass on to the key observations

$$g(x) + g(2-x) = 2 \quad \text{for all } x \in \mathbb{R}, \tag{3}$$

$$g(x+2) - g(x) = 2 \quad \text{for all } x \in \mathbb{R}. \tag{4}$$

Replace x by $1 - x$ in (2), then change x to $-x$ in the resulting equation. We obtain the relations $g(x) - g(-x) = C(g(1-x) - 1)$, $g(-x) - g(x) = C(g(1+x) - 1)$. Then adding them up leads to $C(g(1-x) + g(1+x) - 2) = 0$. Thus $C \neq 0$ implies (3).

Let u, v be such that $u + v = 1$. Apply (1) to the pairs (u, v) and $(2-u, 2-v)$:

$$g(1+uv) - g(1) = \big(g(u) - 1\big)\big(g(v) - 1\big), \quad g(3+uv) - g(3) = \big(g(2-u) - 1\big)\big(g(2-v) - 1\big).$$

Observe that the last two equations have equal right-hand sides by (3). Hence $u+v = 1$ implies

$$g(uv+3) - g(uv+1) = g(3) - g(1).$$

Each $x \leq 5/4$ is expressible in the form $x = uv + 1$ with $u + v = 1$ (the quadratic function $t^2 - t + (x-1)$ has real roots for $x \leq 5/4$). Hence $g(x+2) - g(x) = g(3) - g(1)$ whenever $x \leq 5/4$. Because $g(x) = x$ holds for $x = 0, 1, 2$, setting $x = 0$ yields $g(3) = 3$. This proves (4) for $x \leq 5/4$. If $x > 5/4$ then $-x < 5/4$ and so $g(2-x) - g(-x) = 2$ by the above. On the other hand (3) gives $g(x) = 2 - g(2-x)$, $g(x+2) = 2 - g(-x)$, so that $g(x+2) - g(x) = g(2-x) - g(-x) = 2$. Thus (4) is true for all $x \in \mathbb{R}$.

Now replace x by $-x$ in (3) to obtain $g(-x) + g(2+x) = 2$. In view of (4) this leads to $g(x) + g(-x) = 0$, i. e. $g(-x) = -g(x)$ for all x. Taking this into account, we apply (1) to the pairs $(-x, y)$ and $(x, -y)$:

$$g(1-xy) - g(-x+y) = \big(g(x) + 1\big)\big(1 - g(y)\big), \quad g(1-xy) - g(x-y) = \big(1 - g(x)\big)\big(g(y) + 1\big).$$

Adding up yields $g(1-xy) = 1 - g(x)g(y)$. Then $g(1+xy) = 1 + g(x)g(y)$ by (3). Now the original equation (1) takes the form $g(x+y) = g(x) + g(y)$. Hence g is additive.

By additvity $g(1+xy) = g(1) + g(xy) = 1 + g(xy)$; since $g(1+xy) = 1 + g(x)g(y)$ was shown above, we also have $g(xy) = g(x)g(y)$ (g is multiplicative). In particular $y = x$ gives $g(x^2) = g(x)^2 \geq 0$ for all x, meaning that $g(x) \geq 0$ for $x \geq 0$. Since g is additive and bounded from below on $[0, +\infty)$, it is linear; more exactly $g(x) = g(1)x = x$ for all $x \in \mathbb{R}$.

In summary $f(x) = x - 1$, $x \in \mathbb{R}$. It is straightforward that this function satisfies the requirements.

Comment. There are functions that satisfy the given equation but vanish at -1, for instance the constant function 0 and $f(x) = x^2 - 1$, $x \in \mathbb{R}$.

A6. Let $f : \mathbb{N} \to \mathbb{N}$ be a function, and let f^m be f applied m times. Suppose that for every $n \in \mathbb{N}$ there exists a $k \in \mathbb{N}$ such that $f^{2k}(n) = n + k$, and let k_n be the smallest such k. Prove that the sequence $k_1, k_2, \ldots$ is unbounded.

Solution. We restrict attention to the set

$$S = \{1, f(1), f^2(1), \ldots\}.$$

Observe that S is unbounded because for every number n in S there exists a $k > 0$ such that $f^{2k}(n) = n + k$ is in S. Clearly f maps S into itself; moreover f is injective on S. Indeed if $f^i(1) = f^j(1)$ with $i \neq j$ then the values $f^m(1)$ start repeating periodically from some point on, and S would be finite.

Define $g : S \to S$ by $g(n) = f^{2k_n}(n) = n + k_n$. We prove that g is injective too. Suppose that $g(a) = g(b)$ with $a < b$. Then $a + k_a = f^{2k_a}(a) = f^{2k_b}(b) = b + k_b$ implies $k_a > k_b$. So, since f is injective on S, we obtain

$$f^{2(k_a - k_b)}(a) = b = a + (k_a - k_b).$$

However this contradicts the minimality of k_a as $0 < k_a - k_b < k_a$.

Let T be the set of elements of S that are not of the form $g(n)$ with $n \in S$. Note that $1 \in T$ by $g(n) > n$ for $n \in S$, so T is non-empty. For each $t \in T$ denote $C_t = \{t, g(t), g^2(t), \ldots\}$; call C_t the chain starting at t. Observe that distinct chains are disjoint because g is injective. Each $n \in S \backslash T$ has the form $n = g(n')$ with $n' < n$, $n' \in S$. Repeated applications of the same observation show that $n \in C_t$ for some $t \in T$, i. e. S is the disjoint union of the chains C_t.

If $f^n(1)$ is in the chain C_t starting at $t = f^{n_t}(1)$ then $n = n_t + 2a_1 + \cdots + 2a_j$ with

$$f^n(1) = g^j(f^{n_t}(1)) = f^{2a_j}(f^{2a_{j-1}}(\cdots f^{2a_1}(f^{n_t}(1)))) = f^{n_t}(1) + a_1 + \cdots + a_j.$$

Hence

$$f^n(1) = f^{n_t}(1) + \frac{n - n_t}{2} = t + \frac{n - n_t}{2}. \tag{1}$$

Now we show that T is infinite. We argue by contradiction. Suppose that there are only finitely many chains $C_{t_1}, \ldots, C_{t_r}$, starting at $t_1 < \cdots < t_r$. Fix N. If $f^n(1)$ with $1 \leq n \leq N$ is in C_t then $f^n(1) = t + \frac{n-n_t}{2} \leq t_r + \frac{N}{2}$ by (1). But then the $N + 1$ distinct natural numbers $1, f(1), \ldots, f^N(1)$ are all less than $t_r + \frac{N}{2}$ and hence $N + 1 \leq t_r + \frac{N}{2}$. This is a contradiction if N is sufficiently large, and hence T is infinite.

To complete the argument, choose any k in $\mathbb{N}$ and consider the $k + 1$ chains starting at the first $k + 1$ numbers in T. Let t be the greatest one among these numbers. Then each of the chains in question contains a number not exceeding t, and at least one of them does not contain any number among $t+1, \ldots, t+k$. So there is a number n in this chain such that $g(n) - n > k$, i. e. $k_n > k$. In conclusion $k_1, k_2, \ldots$ is unbounded.

A7. We say that a function $f : \mathbb{R}^k \to \mathbb{R}$ is a metapolynomial if, for some positive integers m and n, it can be represented in the form

$$f(x_1, \ldots, x_k) = \max_{i=1,\ldots,m} \min_{j=1,\ldots,n} P_{i,j}(x_1, \ldots, x_k)$$

where $P_{i,j}$ are multivariate polynomials. Prove that the product of two metapolynomials is also a metapolynomial.

Solution. We use the notation $f(x) = f(x_1, \ldots, x_k)$ for $x = (x_1, \ldots, x_k)$ and $[m] = \{1, 2, \ldots, m\}$. Observe that if a metapolynomial $f(x)$ admits a representation like the one in the statement for certain positive integers m and n, then they can be replaced by any $m' \geq m$ and $n' \geq n$. For instance, if we want to replace m by $m+1$ then it is enough to define $P_{m+1,j}(x) = P_{m,j}(x)$ and note that repeating elements of a set do not change its maximum nor its minimum. So one can assume that any two metapolynomials are defined with the same m and n. We reserve letters P and Q for polynomials, so every function called $P, P_{i,j}, Q, Q_{i,j}, \ldots$ is a polynomial function.

We start with a lemma that is useful to change expressions of the form $\min\max f_{i,j}$ to ones of the form $\max\min g_{i,j}$.

Lemma. Let $\{a_{i,j}\}$ be real numbers, for all $i \in [m]$ and $j \in [n]$. Then

$$\min_{i\in[m]} \max_{j\in[n]} a_{i,j} = \max_{j_1,\ldots,j_m\in[n]} \min_{i\in[m]} a_{i,j_i},$$

where the max in the right-hand side is over all vectors $(j_1, \ldots, j_m)$ with $j_1, \ldots, j_m \in [n]$.

Proof. We can assume for all i that $a_{i,n} = \max\{a_{i,1}, \ldots, a_{i,n}\}$ and $a_{m,n} = \min\{a_{1,n}, \ldots, a_{m,n}\}$. The left-hand side is $= a_{m,n}$ and hence we need to prove the same for the right-hand side. If $(j_1, j_2, \ldots, j_m) = (n, n, \ldots, n)$ then $\min\{a_{1,j_1}, \ldots, a_{m,j_m}\} = \min\{a_{1,n}, \ldots, a_{m,n}\} = a_{m,n}$ which implies that the right-hand side is $\geq a_{m,n}$. It remains to prove the opposite inequality and this is equivalent to $\min\{a_{1,j_1}, \ldots, a_{m,j_m}\} \leq a_{m,n}$ for all possible $(j_1, j_2, \ldots, j_m)$. This is true because $\min\{a_{1,j_1}, \ldots, a_{m,j_m}\} \leq a_{m,j_m} \leq a_{m,n}$. □

We need to show that the family $\mathcal{M}$ of metapolynomials is closed under multiplication, but it turns out easier to prove more: that it is also closed under addition, maxima and minima.

First we prove the assertions about the maxima and the minima. If $f_1, \ldots, f_r$ are metapolynomials, assume them defined with the same m and n. Then

$$f = \max\{f_1, \ldots, f_r\} = \max\{\max_{i\in[m]} \min_{j\in[n]} P^1_{i,j}, \ldots, \max_{i\in[m]} \min_{j\in[n]} P^r_{i,j}\} = \max_{s\in[r],i\in[m]} \min_{j\in[n]} P^s_{i,j}.$$

It follows that $f = \max\{f_1, \ldots, f_r\}$ is a metapolynomial. The same argument works for the minima, but first we have to replace *min max* by *max min*, and this is done via the lemma.

Another property we need is that if $f = \max\min P_{i,j}$ is a metapolynomial then so is $-f$. Indeed, $-f = \min(-\min P_{i,j}) = \min\max P_{i,j}$.

To prove $\mathcal{M}$ is closed under addition let $f = \max\min P_{i,j}$ and $g = \max\min Q_{i,j}$. Then

$$f(x) + g(x) = \max_{i\in[m]} \min_{j\in[n]} P_{i,j}(x) + \max_{i\in[m]} \min_{j\in[n]} Q_{i,j}(x)$$

$$= \max_{i_1,i_2\in[m]} (\min_{j\in[n]} P_{i_1,j}(x) + \min_{j\in[n]} Q_{i_2,j}(x)) = \max_{i_1,i_2\in[m]} \min_{j_1,j_2\in[n]} \big(P_{i_1,j_1}(x) + Q_{i_2,j_2}(x)\big),$$

and hence $f(x) + g(x)$ is a metapolynomial.

We proved that $\mathcal{M}$ is closed under sums, maxima and minima, in particular any function that can be expressed by sums, max, min, polynomials or even metapolynomials is in $\mathcal{M}$.

We would like to proceed with multiplication along the same lines like with addition, but there is an essential difference. In general the product of the maxima of two sets is not equal

to the maximum of the product of the sets. We need to deal with the fact that $a < b$ and $c < d$ do not imply $ac < bd$. However this is true for $a, b, c, d \geq 0$.

In view of this we decompose each function $f(x)$ into its positive part $f^+(x) = \max\{f(x), 0\}$ and its negative part $f^-(x) = \max\{0, -f(x)\}$. Note that $f = f^+ - f^-$ and $f^+, f^- \in \mathcal{M}$ if $f \in \mathcal{M}$. The whole problem reduces to the claim that if f and g are metapolynomials with $f, g \geq 0$ then fg it is also a metapolynomial.

Assuming this claim, consider arbitrary $f, g \in \mathcal{M}$. We have

$$fg = (f^+ - f^-)(g^+ - g^-) = f^+g^+ - f^+g^- - f^-g^+ + f^-g^-,$$

and hence $fg \in \mathcal{M}$. Indeed, $\mathcal{M}$ is closed under addition, also $f^+g^+, f^+g^-, f^-g^+, f^-g^- \in \mathcal{M}$ because $f^+, f^-, g^+, g^- \geq 0$.

It remains to prove the claim. In this case $f, g \geq 0$, and one can try to repeat the argument for the sum. More precisely, let $f = \max\min P_{ij} \geq 0$ and $g = \max\min Q_{ij} \geq 0$. Then

$$fg = \max\min P_{i,j} \cdot \max\min Q_{i,j} = \max\min P^+_{i,j} \cdot \max\min Q^+_{i,j} = \max\min P^+_{i_1,j_1} \cdot Q^+_{i_2,j_2}.$$

Hence it suffices to check that $P^+Q^+ \in \mathcal{M}$ for any pair of polynomials P and Q. This reduces to the identity

$$u^+v^+ = \max\{0, \min\{uv, u, v\}, \min\{uv, uv^2, u^2v\}, \min\{uv, u, u^2v\}, \min\{uv, uv^2, v\}\},$$

with u replaced by $P(x)$ and v replaced by $Q(x)$. The formula is proved by a case-by-case analysis. If $u \leq 0$ or $v \leq 0$ then both sides equal 0. In case $u, v \geq 0$, the right-hand side is clearly $\leq uv$. To prove the opposite inequality we use that uv equals

$$\begin{array}{ll} \min\{uv, u, v\} & \text{if } 0 \leq u, v \leq 1, \\ \min\{uv, uv^2, u^2v\} & \text{if } 1 \leq u, v, \\ \min\{uv, u, u^2v\} & \text{if } 0 \leq v \leq 1 \leq u, \\ \min\{uv, uv^2, v\} & \text{if } 0 \leq u \leq 1 \leq v. \end{array}$$

Comment. The case $k = 1$ is simpler and can be solved by proving that a function $f : \mathbb{R} \to \mathbb{R}$ is a metapolynomial if and only if it is a piecewise polinomial (and continuos) function.

It is enough to prove that all such functions are metapolynomials, and this easily reduces to the following case. Given a polynomial $P(x)$ with $P(0) = 0$, the function f defined by $f(x) = P(x)$ for $x \geq 0$ and 0 otherwise is a metapolynomial. For this last claim, it suffices to prove that $(x^+)^n$ is a metapolynomial, and this follows from the formula $(x^+)^n = \max\{0, \min\{x^{n-1}, x^n\}, \min\{x^n, x^{n+1}\}\}$.

Combinatorics

C1. Several positive integers are written in a row. Iteratively, Alice chooses two adjacent numbers x and y such that $x > y$ and x is to the left of y, and replaces the pair (x, y) by either $(y + 1, x)$ or $(x - 1, x)$. Prove that she can perform only finitely many such iterations.

Solution 1. Note first that the allowed operation does not change the maximum M of the initial sequence. Let $a_1, a_2, \ldots, a_n$ be the numbers obtained at some point of the process. Consider the sum

$$S = a_1 + 2a_2 + \cdots + na_n.$$

We claim that S increases by a positive integer amount with every operation. Let the operation replace the pair (a_i, a_{i+1}) by a pair (c, a_i), where $a_i > a_{i+1}$ and $c = a_{i+1}+1$ or $c = a_i-1$. Then the new and the old value of S differ by $d = (ic+(i+1)a_i)-(ia_i+(i+1)a_{i+1}) = a_i-a_{i+1}+i(c-a_{i+1})$. The integer d is positive since $a_i - a_{i+1} \geq 1$ and $c - a_{i+1} \geq 0$.

On the other hand $S \leq (1 + 2 + \cdots + n)M$ as $a_i \leq M$ for all $i = 1, \ldots, n$. Since S increases by at least 1 at each step and never exceeds the constant $(1 + 2 + \cdots + n)M$, the process stops after a finite number of iterations.

Solution 2. Like in the first solution note that the operations do not change the maximum M of the initial sequence. Now consider the reverse lexicographical order for n-tuples of integers. We say that $(x_1, \ldots, x_n) < (y_1, \ldots, y_n)$ if $x_n < y_n$, or if $x_n = y_n$ and $x_{n-1} < y_{n-1}$, or if $x_n = y_n$, $x_{n-1} = y_{n-1}$ and $x_{n-2} < y_{n-2}$, etc. Each iteration creates a sequence that is greater than the previous one with respect to this order, and no sequence occurs twice during the process. On the other hand there are finitely many possible sequences because their terms are always positive integers not exceeding M. Hence the process cannot continue forever.

Solution 3. Let the current numbers be $a_1, a_2, \ldots, a_n$. Define the *score* s_i of a_i as the number of a_j's that are less than a_i. Call the sequence $s_1, s_2, \ldots, s_n$ the score sequence of $a_1, a_2, \ldots, a_n$.

Let us say that a sequence $x_1, \ldots, x_n$ dominates a sequence $y_1, \ldots, y_n$ if the first index i with $x_i \neq y_i$ is such that $x_i < y_i$. We show that after each operation the new score sequence dominates the old one. Score sequences do not repeat, and there are finitely many possibilities for them, no more than $(n - 1)^n$. Hence the process will terminate.

Consider an operation that replaces (x, y) by (a, x), with $a = y + 1$ or $a = x - 1$. Suppose that x was originally at position i. For each $j < i$ the score s_j does not increase with the change because $y \leq a$ and $x \leq x$. If s_j decreases for some $j < i$ then the new score sequence dominates the old one. Assume that s_j stays the same for all $j < i$ and consider s_i. Since $x > y$ and $y \leq a \leq x$, we see that s_i decreases by at least 1. This concludes the proof.

Comment. All three proofs work if x and y are not necessarily adjacent, and if the pair (x, y) is replaced by any pair (a, x), with a an integer satisfying $y \leq a \leq x$. There is nothing special about the "weights" $1, 2, \ldots, n$ in the definition of $S = \sum_{i=1}^{n} ia_i$ from the first solution. For any sequence $w_1 < w_2 < \cdots < w_n$ of positive integers, the sum $\sum_{i=1}^{n} w_i a_i$ increases by at least 1 with each operation.

Consider the same problem, but letting Alice replace the pair (x, y) by (a, x), where a is any positive integer less than x. The same conclusion holds in this version, i. e. the process stops eventually. The solution using the reverse lexicographical order works without any change. The first solution would require a special set of weights like $w_i = M^i$ for $i = 1, \ldots, n$.

Comment. The first and the second solutions provide upper bounds for the number of possible operations, respectively of order Mn^2 and M^n where M is the maximum of the original sequence. The upper bound $(n - 1)^n$ in the third solution does not depend on M.

C2. Let $n \geq 1$ be an integer. What is the maximum number of disjoint pairs of elements of the set $\{1, 2, \ldots, n\}$ such that the sums of the different pairs are different integers not exceeding n?

Solution. Consider x such pairs in $\{1, 2, \ldots, n\}$. The sum S of the $2x$ numbers in them is at least $1+2+\cdots+2x$ since the pairs are disjoint. On the other hand $S \leq n+(n-1)+\cdots+(n-x+1)$ because the sums of the pairs are different and do not exceed n. This gives the inequality

$$\frac{2x(2x+1)}{2} \leq nx - \frac{x(x-1)}{2},$$

which leads to $x \leq \frac{2n-1}{5}$. Hence there are at most $\left\lfloor \frac{2n-1}{5} \right\rfloor$ pairs with the given properties.

We show a construction with exactly $\left\lfloor \frac{2n-1}{5} \right\rfloor$ pairs. First consider the case $n = 5k+3$ with $k \geq 0$, where $\left\lfloor \frac{2n-1}{5} \right\rfloor = 2k+1$. The pairs are displayed in the following table.

Pairs	$3k+1$ 2	$3k$ 4	$\cdots$ $\cdots$	$2k+2$ $2k$	$4k+2$ 1	$4k+1$ 3	$\cdots$ $\cdots$	$3k+3$ $2k-1$	$3k+2$ $2k+1$
Sums	$3k+3$	$3k+4$	$\cdots$	$4k+2$	$4k+3$	$4k+4$	$\cdots$	$5k+2$	$5k+3$

The $2k+1$ pairs involve all numbers from 1 to $4k+2$; their sums are all numbers from $3k+3$ to $5k+3$. The same construction works for $n = 5k+4$ and $n = 5k+5$ with $k \geq 0$. In these cases the required number $\left\lfloor \frac{2n-1}{5} \right\rfloor$ of pairs equals $2k+1$ again, and the numbers in the table do not exceed $5k+3$. In the case $n = 5k+2$ with $k \geq 0$ one needs only $2k$ pairs. They can be obtained by ignoring the last column of the table (thus removing $5k+3$). Finally, $2k$ pairs are also needed for the case $n = 5k+1$ with $k \geq 0$. Now it suffices to ignore the last column of the table and then subtract 1 from each number in the first row.

Comment. The construction above is not unique. For instance, the following table shows another set of $2k+1$ pairs for the cases $n = 5k+3$, $n = 5k+4$, and $n = 5k+5$.

Pairs	1 $4k+1$	2 $4k-1$	$\cdots$ $\cdots$	k $2k+3$	$k+1$ $4k+2$	$k+2$ $4k$	$\cdots$ $\cdots$	$2k+1$ $2k+2$
Sums	$4k+2$	$4k+1$	$\cdots$	$3k+3$	$5k+3$	$5k+2$	$\cdots$	$4k+3$

The table for the case $n = 5k+2$ would be the same, with the pair $(k+1, 4k+2)$ removed. For the case $n = 5k+1$ remove the last column and subtract 2 from each number in the second row.

C3. In a 999×999 square table some cells are white and the remaining ones are red. Let T be the number of triples (C_1, C_2, C_3) of cells, the first two in the same row and the last two in the same column, with C_1 and C_3 white and C_2 red. Find the maximum value T can attain.

Solution. We prove that in an $n \times n$ square table there are at most $\frac{4n^4}{27}$ such triples.

Let row i and column j contain a_i and b_j white cells respectively, and let R be the set of red cells. For every red cell (i, j) there are $a_i b_j$ admissible triples (C_1, C_2, C_3) with $C_2 = (i, j)$, therefore

$$T = \sum_{(i,j)\in R} a_i b_j.$$

We use the inequality $2ab \le a^2 + b^2$ to obtain

$$T \le \frac{1}{2} \sum_{(i,j)\in R} (a_i^2 + b_j^2) = \frac{1}{2} \sum_{i=1}^{n} (n - a_i) a_i^2 + \frac{1}{2} \sum_{j=1}^{n} (n - b_j) b_j^2.$$

This is because there are $n - a_i$ red cells in row i and $n - b_j$ red cells in column j. Now we maximize the right-hand side.

By the AM-GM inequality we have

$$(n - x)x^2 = \frac{1}{2}(2n - 2x) \cdot x \cdot x \le \frac{1}{2} \left(\frac{2n}{3} \right)^3 = \frac{4n^3}{27},$$

with equality if and only if $x = \frac{2n}{3}$. By putting everything together, we get

$$T \le \frac{n}{2} \frac{4n^3}{27} + \frac{n}{2} \frac{4n^3}{27} = \frac{4n^4}{27}.$$

If $n = 999$ then any coloring of the square table with $x = \frac{2n}{3} = 666$ white cells in each row and column attains the maximum as all inequalities in the previous argument become equalities. For example color a cell (i, j) white if $i - j \equiv 1, 2, \ldots, 666 \pmod{999}$, and red otherwise.

Therefore the maximum value T can attain is $T = \frac{4 \cdot 999^4}{27}$.

Comment. One can obtain a better preliminary estimate with the Cauchy-Schwarz inequality:

$$T = \sum_{(i,j)\in R} a_i b_j \le \left(\sum_{(i,j)\in R} a_i^2 \right)^{\frac{1}{2}} \cdot \left(\sum_{(i,j)\in R} b_j^2 \right)^{\frac{1}{2}} = \left(\sum_{i=1}^{n} (n - a_i) a_i^2 \right)^{\frac{1}{2}} \cdot \left(\sum_{j=1}^{n} (n - b_j) b_j^2 \right)^{\frac{1}{2}}.$$

It can be used to reach the same conclusion.

C4. Players A and B play a game with $N \geq 2012$ coins and 2012 boxes arranged around a circle. Initially A distributes the coins among the boxes so that there is at least 1 coin in each box. Then the two of them make moves in the order $B, A, B, A, \ldots$ by the following rules:

- On every move of his B passes 1 coin from every box to an adjacent box.
- On every move of hers A chooses several coins that were *not* involved in B's previous move and are in different boxes. She passes every chosen coin to an adjacent box.

Player A's goal is to ensure at least 1 coin in each box after every move of hers, regardless of how B plays and how many moves are made. Find the least N that enables her to succeed.

Solution. We argue for a general $n \geq 7$ instead of 2012 and prove that the required minimum N is $2n-2$. For $n = 2012$ this gives $N_{\min} = 4022$.

a) If $N = 2n-2$ player A can achieve her goal. Let her start the game with a *regular* distribution: $n-2$ boxes with 2 coins and 2 boxes with 1 coin. Call the boxes of the two kinds *red* and *white* respectively. We claim that on her first move A can achieve a regular distribution again, regardless of B's first move M. She acts according as the following situation S occurs after M or not: *The initial distribution contains a red box R with 2 white neighbors, and R receives no coins from them on move M.*

Suppose that S does not occur. Exactly one of the coins c_1 and c_2 in a given red box X is involved in M, say c_1. If M passes c_1 to the right neighbor of X, let A pass c_2 to its left neighbor, and vice versa. By doing so with all red boxes A performs a legal move M'. Thus M and M' combined move the 2 coins of every red box in opposite directions. Hence after M and M' are complete each neighbor of a red box X contains exactly 1 coin that was initially in X. So each box with a red neighbor is non-empty after M'. If initially there is a box X with 2 white neighbors (X is red and unique) then X receives a coin from at least one of them on move M since S does not occur. Such a coin is not involved in M', so X is also non-empty after M'. Furthermore each box Y has given away its initial content after M and M'. A red neighbor of Y adds 1 coin to it; a white neighbor adds at most 1 coin because it is not involved in M'. Hence each box contains 1 or 2 coins after M'. Because $N = 2n-2$, such a distribution is regular.

Now let S occur after move M. Then A leaves untouched the exceptional red box R. With all remaining red boxes she proceeds like in the previous case, thus making a legal move M''. Box R receives no coins from its neighbors on either move, so there is 1 coin in it after M''. Like above M and M'' combined pass exactly 1 coin from every red box different from R to each of its neighbors. Every box except R has a red neighbor different from R, hence all boxes are non-empty after M''. Next, each box Y except R loses its initial content after M and M''. A red neighbor of Y adds at most 1 coin to it; a white neighbor also adds at most 1 coin as it does not participate in M''. Thus each box has 1 or 2 coins after M'', and the obtained distribution is regular.

Player A can apply the described strategy indefinitely, so $N = 2n-2$ enables her to succeed.

b) For $N \leq 2n-3$ player B can achieve an empty box after some move of A. Let α be a set of ℓ consecutive boxes containing a total of $N(\alpha)$ coins. We call α an *arc* if $\ell \leq n-2$ and $N(\alpha) \leq 2\ell - 3$. Note that $\ell \geq 2$ by the last condition. Moreover if both extremes of α are non-empty boxes then $N(\alpha) \geq 2$, so that $N(\alpha) \leq 2\ell - 3$ implies $\ell \geq 3$. Observe also that if an extreme X of α has more than 1 coin then ignoring X yields a shorter arc. It follows that every arc contains an arc whose extremes have at most 1 coin each.

Given a clockwise labeling $1, 2, \ldots, n$ of the boxes, suppose that boxes $1, 2, \ldots, \ell$ form an arc α, with $\ell \leq n-2$ and $N(\alpha) \leq 2\ell - 3$. Suppose also that all $n \geq 7$ boxes are non-empty. Then B can move so that an arc α' with $N(\alpha') < N(\alpha)$ will appear after any response of A.

One may assume exactly 1 coin in boxes 1 and ℓ by a previous remark. Let B pass 1 coin in counterclockwise direction from box 1 and box n, and in clockwise direction from each remaining box. This leaves $N(\alpha)-2$ coins in the boxes of α. In addition, due to $3 \leq \ell \leq n-2$, box ℓ has exactly 1 coin c, the one received from box $\ell - 1$.

Let player A's next move M pass $k \leq 2$ coins to boxes $1, 2, \ldots, \ell$ from the remaining ones. Only boxes 1 and ℓ can receive such coins, at most 1 each. If $k < 2$ then after move M boxes $1, 2, \ldots, \ell$ form an arc α' with $N(\alpha') < N(\alpha)$. If $k = 2$ then M adds a coin to box ℓ. Also M does not move coin c from ℓ because c is involved in the previous move of B. In summary boxes $1, 2, \ldots, \ell$ contain $N(\alpha)$ coins like before, so they form an arc. However there are 2 coins now in the extreme ℓ of the arc. Ignore ℓ to obtain a shorter arc α' with $N(\alpha') < N(\alpha)$.

Consider any initial distribution without empty boxes. Since $N \leq 2n - 3$, there are at least 3 boxes in it with exactly 1 coin. It follows from $n \geq 7$ that some 2 of them are the extremes of an arc α. Hence B can make the move described above, which leads to an arc α' with $N(\alpha') < N(\alpha)$ after A's response. If all boxes in the new distribution are non-empty he can repeat the same, and so on. Because $N(\alpha)$ cannot decrease indefinitely, an empty box will occur after some move of A.

C5. The columns and the rows of a $3n \times 3n$ square board are numbered $1, 2, \ldots, 3n$. Every square (x, y) with $1 \leq x, y \leq 3n$ is colored asparagus, byzantium or citrine according as the modulo 3 remainder of $x + y$ is 0, 1 or 2 respectively. One token colored asparagus, byzantium or citrine is placed on each square, so that there are $3n^2$ tokens of each color.

Suppose that one can permute the tokens so that each token is moved to a distance of at most d from its original position, each asparagus token replaces a byzantium token, each byzantium token replaces a citrine token, and each citrine token replaces an asparagus token. Prove that it is possible to permute the tokens so that each token is moved to a distance of at most $d + 2$ from its original position, and each square contains a token with the same color as the square.

Solution. Without loss of generality it suffices to prove that the A-tokens can be moved to distinct A-squares in such a way that each A-token is moved to a distance at most $d + 2$ from its original place. This means we need a perfect matching between the $3n^2$ A-squares and the $3n^2$ A-tokens such that the distance in each pair of the matching is at most $d + 2$.

To find the matching, we construct a bipartite graph. The A-squares will be the vertices in one class of the graph; the vertices in the other class will be the A-tokens.

Split the board into 3×1 horizontal triminos; then each trimino contains exactly one A-square. Take a permutation π of the tokens which moves A-tokens to B-tokens, B-tokens to C-tokens, and C-tokens to A-tokens, in each case to a distance at most d. For each A-square S, and for each A-token T, connect S and T by an edge if T, $\pi(T)$ or $\pi^{-1}(T)$ is on the trimino containing S. We allow multiple edges; it is even possible that the same square and the same token are connected with three edges. Obviously the lengths of the edges in the graph do not exceed $d + 2$. By length of an edge we mean the distance between the A-square and the A-token it connects.

Each A-token T is connected with the three A-squares whose triminos contain T, $\pi(T)$ and $\pi^{-1}(T)$. Therefore in the graph all tokens are of degree 3. We show that the same is true for the A-squares. Let S be an arbitrary A-square, and let T_1, T_2, T_3 be the three tokens on the trimino containing S. For $i = 1, 2, 3$, if T_i is an A-token, then S is connected with T_i; if T_i is a B-token then S is connected with $\pi^{-1}(T_i)$; finally, if T_i is a C-token then S is connected with $\pi(T_i)$. Hence in the graph the A-squares also are of degree 3.

Since the A-squares are of degree 3, from every set $\mathcal{S}$ of A-squares exactly $3|\mathcal{S}|$ edges start. These edges end in at least $|\mathcal{S}|$ tokens because the A-tokens also are of degree 3. Hence every set $\mathcal{S}$ of A-squares has at least $|\mathcal{S}|$ neighbors among the A-tokens.

Therefore, by Hall's marriage theorem, the graph contains a perfect matching between the two vertex classes. So there is a perfect matching between the A-squares and A-tokens with edges no longer than $d + 2$. It follows that the tokens can be permuted as specified in the problem statement.

Comment 1. In the original problem proposal the board was infinite and there were only two colors. Having n colors for some positive integer n was an option; we chose $n = 3$. Moreover, we changed the board to a finite one to avoid dealing with infinite graphs (although Hall's theorem works in the infinite case as well).

With only two colors Hall's theorem is not needed. In this case we split the board into 2×1 dominos, and in the resulting graph all vertices are of degree 2. The graph consists of disjoint cycles with even length and infinite paths, so the existence of the matching is trivial.

Having more than three colors would make the problem statement more complicated, because we need a matching between every two color classes of tokens. However, this would not mean a significant increase in difficulty.

Comment 2. According to Wikipedia, the color *asparagus* (hexadecimal code `#87A96B`) is a tone of green that is named after the vegetable. Crayola created this color in 1993 as one of the 16 to be named in the Name The Color Contest. *Byzantium* (`#702963`) is a dark tone of purple. Its first recorded use as a color name in English was in 1926. *Citrine* (`#E4D00A`) is variously described as yellow, greenish-yellow, brownish-yellow or orange. The first known use of citrine as a color name in English was in the 14th century.

C6. Let k and n be fixed positive integers. In the liar's guessing game, Amy chooses integers x and N with $1 \leq x \leq N$. She tells Ben what N is, but not what x is. Ben may then repeatedly ask Amy whether $x \in S$ for arbitrary sets S of integers. Amy will always answer with *yes* or *no*, but she might lie. The only restriction is that she can lie at most k times in a row. After he has asked as many questions as he wants, Ben must specify a set of at most n positive integers. If x is in this set he wins; otherwise, he loses. Prove that:

a) If $n \geq 2^k$ then Ben can always win.

b) For sufficiently large k there exist $n \geq 1.99^k$ such that Ben cannot guarantee a win.

Solution. Consider an answer $A \in \{yes, no\}$ to a question of the kind "Is x in the set S?" We say that A is inconsistent with a number i if $A = yes$ and $i \notin S$, or if $A = no$ and $i \in S$. Observe that an answer inconsistent with the target number x is a lie.

a) Suppose that Ben has determined a set T of size m that contains x. This is true initially with $m = N$ and $T = \{1, 2, \ldots, N\}$. For $m > 2^k$ we show how Ben can find a number $y \in T$ that is different from x. By performing this step repeatedly he can reduce T to be of size $2^k \leq n$ and thus win.

Since only the size $m > 2^k$ of T is relevant, assume that $T = \{0, 1, \ldots, 2^k, \ldots, m-1\}$. Ben begins by asking repeatedly whether x is 2^k. If Amy answers *no* $k+1$ times in a row, one of these answers is truthful, and so $x \neq 2^k$. Otherwise Ben stops asking about 2^k at the first answer *yes*. He then asks, for each $i = 1, \ldots, k$, if the binary representation of x has a 0 in the ith digit. Regardless of what the k answers are, they are all inconsistent with a certain number $y \in \{0, 1, \ldots, 2^k - 1\}$. The preceding answer *yes* about 2^k is also inconsistent with y. Hence $y \neq x$. Otherwise the last $k+1$ answers are not truthful, which is impossible.

Either way, Ben finds a number in T that is different from x, and the claim is proven.

b) We prove that if $1 < \lambda < 2$ and $n = \left\lfloor (2-\lambda)\lambda^{k+1} \right\rfloor - 1$ then Ben cannot guarantee a win. To complete the proof, then it suffices to take λ such that $1.99 < \lambda < 2$ and k large enough so that

$$n = \left\lfloor (2-\lambda)\lambda^{k+1} \right\rfloor - 1 \geq 1.99^k.$$

Consider the following strategy for Amy. First she chooses $N = n+1$ and $x \in \{1, 2, \ldots, n+1\}$ arbitrarily. After every answer of hers Amy determines, for each $i = 1, 2, \ldots, n+1$, the number m_i of consecutive answers she has given by that point that are inconsistent with i. To decide on her next answer, she then uses the quantity

$$\phi = \sum_{i=1}^{n+1} \lambda^{m_i}.$$

No matter what Ben's next question is, Amy chooses the answer which minimizes ϕ.

We claim that with this strategy ϕ will always stay less than λ^{k+1}. Consequently no exponent m_i in ϕ will ever exceed k, hence Amy will never give more than k consecutive answers inconsistent with some i. In particular this applies to the target number x, so she will never lie more than k times in a row. Thus, given the claim, Amy's strategy is legal. Since the strategy does not depend on x in any way, Ben can make no deductions about x, and therefore he cannot guarantee a win.

It remains to show that $\phi < \lambda^{k+1}$ at all times. Initially each m_i is 0, so this condition holds in the beginning due to $1 < \lambda < 2$ and $n = \left\lfloor (2-\lambda)\lambda^{k+1} \right\rfloor - 1$. Suppose that $\phi < \lambda^{k+1}$ at some point, and Ben has just asked if $x \in S$ for some set S. According as Amy answers *yes* or *no*, the new value of ϕ becomes

$$\phi_1 = \sum_{i \in S} 1 + \sum_{i \notin S} \lambda^{m_i+1} \qquad \text{or} \qquad \phi_2 = \sum_{i \in S} \lambda^{m_i+1} + \sum_{i \notin S} 1.$$

Since Amy chooses the option minimizing ϕ, the new ϕ will equal $\min(\phi_1, \phi_2)$. Now we have

$$\min(\phi_1, \phi_2) \leq \frac{1}{2}(\phi_1 + \phi_2) = \frac{1}{2}\left(\sum_{i \in S}\left(1 + \lambda^{m_i+1}\right) + \sum_{i \notin S}\left(\lambda^{m_i+1} + 1\right)\right) = \frac{1}{2}(\lambda\phi + n + 1).$$

Because $\phi < \lambda^{k+1}$, the assumptions $\lambda < 2$ and $n = \left\lfloor (2-\lambda)\lambda^{k+1} \right\rfloor - 1$ lead to

$$\min(\phi_1, \phi_2) < \frac{1}{2}(\lambda^{k+2} + (2-\lambda)\lambda^{k+1}) = \lambda^{k+1}.$$

The claim follows, which completes the solution.

Comment. Given a fixed k, let $f(k)$ denote the minimum value of n for which Ben can guarantee a victory. The problem asks for a proof that for large k

$$1.99^k \leq f(k) \leq 2^k.$$

A computer search shows that $f(k) = 2, 3, 4, 7, 11, 17$ for $k = 1, 2, 3, 4, 5, 6$.

C7. There are given 2^{500} points on a circle labeled $1, 2, \ldots, 2^{500}$ in some order. Prove that one can choose 100 pairwise disjoint chords joining some of these points so that the 100 sums of the pairs of numbers at the endpoints of the chosen chords are equal.

Solution. The proof is based on the following general fact.

Lemma. In a graph G each vertex v has degree d_v. Then G contains an independent set S of vertices such that $|S| \geq f(G)$ where

$$f(G) = \sum_{v \in G} \frac{1}{d_v + 1}.$$

Proof. Induction on $n = |G|$. The base $n = 1$ is clear. For the inductive step choose a vertex v_0 in G of minimum degree d. Delete v_0 and all of its neighbors $v_1, \ldots, v_d$ and also all edges with endpoints $v_0, v_1, \ldots, v_d$. This gives a new graph G'. By the inductive assumption G' contains an independent set S' of vertices such that $|S'| \geq f(G')$. Since no vertex in S' is a neighbor of v_0 in G, the set $S = S' \cup \{v_0\}$ is independent in G.

Let d'_v be the degree of a vertex v in G'. Clearly $d'_v \leq d_v$ for every such vertex v, and also $d_{v_i} \geq d$ for all $i = 0, 1, \ldots, d$ by the minimal choice of v_0. Therefore

$$f(G') = \sum_{v \in G'} \frac{1}{d'_v + 1} \geq \sum_{v \in G'} \frac{1}{d_v + 1} = f(G) - \sum_{i=0}^{d} \frac{1}{d_{v_i} + 1} \geq f(G) - \frac{d+1}{d+1} = f(G) - 1.$$

Hence $|S| = |S'| + 1 \geq f(G') + 1 \geq f(G)$, and the induction is complete. □

We pass on to our problem. For clarity denote $n = 2^{499}$ and draw all chords determined by the given $2n$ points. Color each chord with one of the colors $3, 4, \ldots, 4n - 1$ according to the sum of the numbers at its endpoints. Chords with a common endpoint have different colors. For each color c consider the following graph G_c. Its vertices are the chords of color c, and two chords are neighbors in G_c if they intersect. Let $f(G_c)$ have the same meaning as in the lemma for all graphs G_c.

Every chord ℓ divides the circle into two arcs, and one of them contains $m(\ell) \leq n - 1$ given points. (In particular $m(\ell) = 0$ if ℓ joins two consecutive points.) For each $i = 0, 1, \ldots, n - 2$ there are $2n$ chords ℓ with $m(\ell) = i$. Such a chord has degree at most i in the respective graph. Indeed let $A_1, \ldots, A_i$ be all points on either arc determined by a chord ℓ with $m(\ell) = i$ and color c. Every A_j is an endpoint of at most 1 chord colored c, $j = 1, \ldots, i$. Hence at most i chords of color c intersect ℓ.

It follows that for each $i = 0, 1, \ldots, n - 2$ the $2n$ chords ℓ with $m(\ell) = i$ contribute at least $\frac{2n}{i+1}$ to the sum $\sum_c f(G_c)$. Summation over $i = 0, 1, \ldots, n - 2$ gives

$$\sum_c f(G_c) \geq 2n \sum_{i=1}^{n-1} \frac{1}{i}.$$

Because there are $4n - 3$ colors in all, averaging yields a color c such that

$$f(G_c) \geq \frac{2n}{4n-3} \sum_{i=1}^{n-1} \frac{1}{i} > \frac{1}{2} \sum_{i=1}^{n-1} \frac{1}{i}.$$

By the lemma there are at least $\frac{1}{2} \sum_{i=1}^{n-1} \frac{1}{i}$ pairwise disjoint chords of color c, i. e. with the same sum c of the pairs of numbers at their endpoints. It remains to show that $\frac{1}{2} \sum_{i=1}^{n-1} \frac{1}{i} \geq 100$ for $n = 2^{499}$. Indeed we have

$$\sum_{i=1}^{n-1} \frac{1}{i} > \sum_{i=1}^{2^{400}} \frac{1}{i} = 1 + \sum_{k=1}^{400} \sum_{i=2^{k-1}+1}^{2^k} \frac{1}{i} > 1 + \sum_{k=1}^{400} \frac{2^{k-1}}{2^k} = 201 > 200.$$

This completes the solution.

Geometry

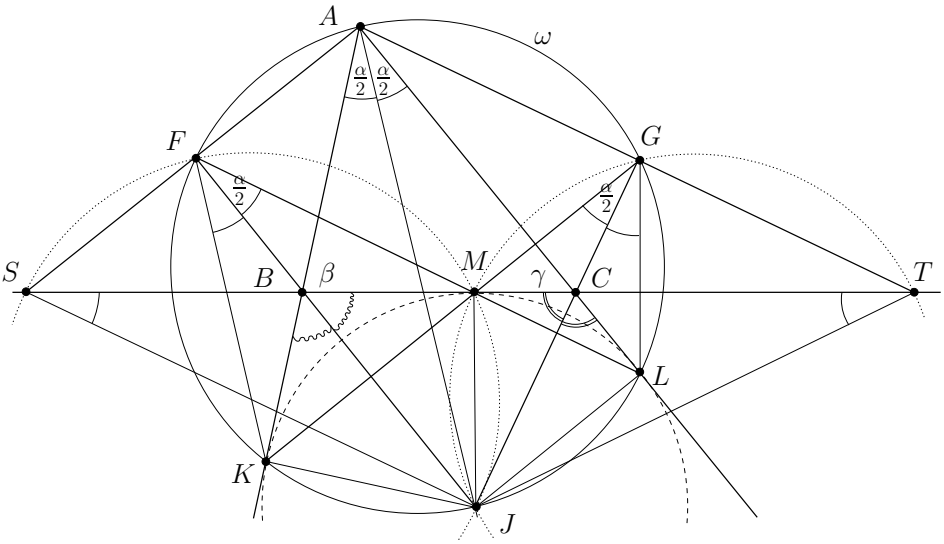
G1. In the triangle ABC the point J is the center of the excircle opposite to A. This excircle is tangent to the side BC at M, and to the lines AB and AC at K and L respectively. The lines LM and BJ meet at F, and the lines KM and CJ meet at G. Let S be the point of intersection of the lines AF and BC, and let T be the point of intersection of the lines AG and BC. Prove that M is the midpoint of ST.

Solution. Let $\alpha = \angle CAB$, $\beta = \angle ABC$ and $\gamma = \angle BCA$. The line AJ is the bisector of $\angle CAB$, so $\angle JAK = \angle JAL = \frac{\alpha}{2}$. By $\angle AKJ = \angle ALJ = 90^\circ$ the points K and L lie on the circle ω with diameter AJ.

The triangle KBM is isosceles as BK and BM are tangents to the excircle. Since BJ is the bisector of $\angle KBM$, we have $\angle MBJ = 90^\circ - \frac{\beta}{2}$ and $\angle BMK = \frac{\beta}{2}$. Likewise $\angle MCJ = 90^\circ - \frac{\gamma}{2}$ and $\angle CML = \frac{\gamma}{2}$. Also $\angle BMF = \angle CML$, therefore

$$\angle LFJ = \angle MBJ - \angle BMF = \left(90^\circ - \frac{\beta}{2}\right) - \frac{\gamma}{2} = \frac{\alpha}{2} = \angle LAJ.$$

Hence F lies on the circle ω. (By the angle computation, F and A are on the same side of BC.) Analogously, G also lies on ω. Since AJ is a diameter of ω, we obtain $\angle AFJ = \angle AGJ = 90^\circ$.



The lines AB and BC are symmetric with respect to the external bisector BF. Because $AF \perp BF$ and $KM \perp BF$, the segments SM and AK are symmetric with respect to BF, hence $SM = AK$. By symmetry $TM = AL$. Since AK and AL are equal as tangents to the excircle, it follows that $SM = TM$, and the proof is complete.

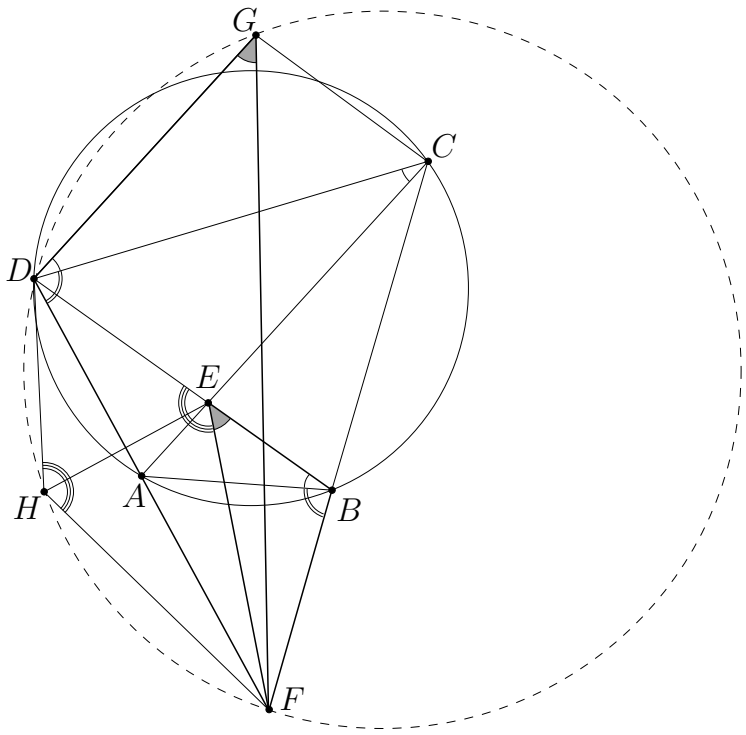
Comment. After discovering the circle $AFKJLG$, there are many other ways to complete the solution. For instance, from the cyclic quadrilaterals $JMFS$ and $JMGT$ one can find $\angle TSJ = \angle STJ = \frac{\alpha}{2}$. Another possibility is to use the fact that the lines AS and GM are parallel (both are perpendicular to the external angle bisector BJ), so $\frac{MS}{MT} = \frac{AG}{GT} = 1$.

G2. Let $ABCD$ be a cyclic quadrilateral whose diagonals AC and BD meet at E. The extensions of the sides AD and BC beyond A and B meet at F. Let G be the point such that $ECGD$ is a parallelogram, and let H be the image of E under reflection in AD. Prove that D, H, F, G are concyclic.

Solution. We show first that the triangles FDG and FBE are similar. Since $ABCD$ is cyclic, the triangles EAB and EDC are similar, as well as FAB and FCD. The parallelogram $ECGD$ yields $GD = EC$ and $\angle CDG = \angle DCE$; also $\angle DCE = \angle DCA = \angle DBA$ by inscribed angles. Therefore

$$\angle FDG = \angle FDC + \angle CDG = \angle FBA + \angle ABD = \angle FBE,$$
$$\frac{GD}{EB} = \frac{CE}{EB} = \frac{CD}{AB} = \frac{FD}{FB}.$$

It follows that FDG and FBE are similar, and so $\angle FGD = \angle FEB$.



Since H is the reflection of E with respect to FD, we conclude that

$$\angle FHD = \angle FED = 180^\circ - \angle FEB = 180^\circ - \angle FGD.$$

This proves that D, H, F, G are concyclic.

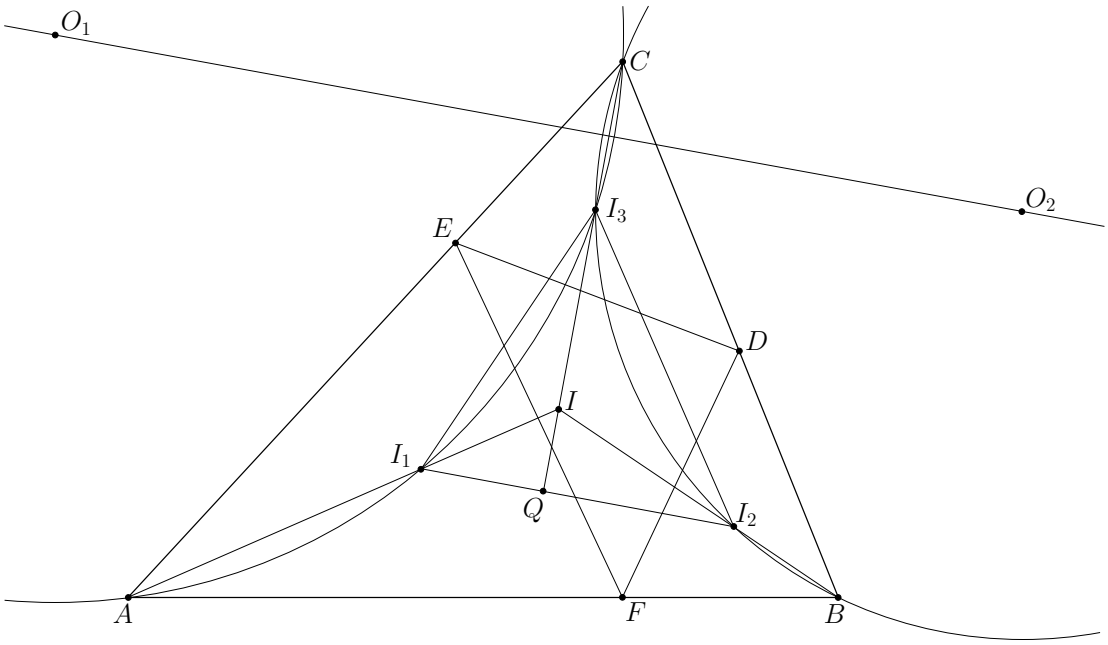
Comment. Points E and G are always in the half-plane determined by the line FD that contains B and C, but H is always in the other half-plane. In particular, $DHFG$ is cyclic if and only if $\angle FHD + \angle FGD = 180^\circ$.

G3. In an acute triangle ABC the points D, E and F are the feet of the altitudes through A, B and C respectively. The incenters of the triangles AEF and BDF are I_1 and I_2 respectively; the circumcenters of the triangles ACI_1 and BCI_2 are O_1 and O_2 respectively. Prove that I_1I_2 and O_1O_2 are parallel.

Solution. Let $\angle CAB = \alpha$, $\angle ABC = \beta$, $\angle BCA = \gamma$. We start by showing that A, B, I_1 and I_2 are concyclic. Since AI_1 and BI_2 bisect $\angle CAB$ and $\angle ABC$, their extensions beyond I_1 and I_2 meet at the incenter I of the triangle. The points E and F are on the circle with diameter BC, so $\angle AEF = \angle ABC$ and $\angle AFE = \angle ACB$. Hence the triangles AEF and ABC are similar with ratio of similitude $\frac{AE}{AB} = \cos\alpha$. Because I_1 and I are their incenters, we obtain $I_1A = IA\cos\alpha$ and $II_1 = IA - I_1A = 2IA\sin^2\frac{\alpha}{2}$. By symmetry $II_2 = 2IB\sin^2\frac{\beta}{2}$. The law of sines in the triangle ABI gives $IA\sin\frac{\alpha}{2} = IB\sin\frac{\beta}{2}$. Hence

$$II_1 \cdot IA = 2\left(IA\sin\tfrac{\alpha}{2}\right)^2 = 2\left(IB\sin\tfrac{\beta}{2}\right)^2 = II_2 \cdot IB.$$

Therefore A, B, I_1 and I_2 are concyclic, as claimed.



In addition $II_1 \cdot IA = II_2 \cdot IB$ implies that I has the same power with respect to the circles (ACI_1), (BCI_2) and (ABI_1I_2). Then CI is the radical axis of (ACI_1) and (BCI_2); in particular CI is perpendicular to the line of centers O_1O_2.

Now it suffices to prove that $CI \perp I_1I_2$. Let CI meet I_1I_2 at Q, then it is enough to check that $\angle II_1Q + \angle I_1IQ = 90^\circ$. Since $\angle I_1IQ$ is external for the triangle ACI, we have

$$\angle II_1Q + \angle I_1IQ = \angle II_1Q + (\angle ACI + \angle CAI) = \angle II_1I_2 + \angle ACI + \angle CAI.$$

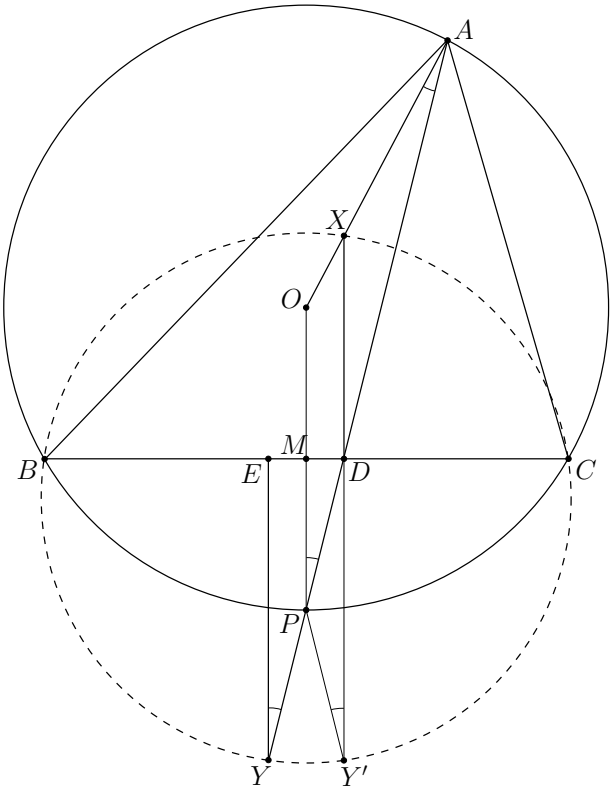
It remains to note that $\angle II_1I_2 = \frac{\beta}{2}$ from the cyclic quadrilateral ABI_1I_2, and $\angle ACI = \frac{\gamma}{2}$, $\angle CAI = \frac{\alpha}{2}$. Therefore $\angle II_1Q + \angle I_1IQ = \frac{\alpha}{2} + \frac{\beta}{2} + \frac{\gamma}{2} = 90^\circ$, completing the proof.

Comment. It follows from the first part of the solution that the common point $I_3 \neq C$ of the circles (ACI_1) and (BCI_2) is the incenter of the triangle CDE.

G4. Let ABC be a triangle with $AB \neq AC$ and circumcenter O. The bisector of $\angle BAC$ intersects BC at D. Let E be the reflection of D with respect to the midpoint of BC. The lines through D and E perpendicular to BC intersect the lines AO and AD at X and Y respectively. Prove that the quadrilateral $BXCY$ is cyclic.

Solution. The bisector of $\angle BAC$ and the perpendicular bisector of BC meet at P, the midpoint of the minor arc $\widehat{BC}$ (they are different lines as $AB \neq AC$). In particular OP is perpendicular to BC and intersects it at M, the midpoint of BC.

Denote by Y' the reflexion of Y with respect to OP. Since $\angle BYC = \angle BY'C$, it suffices to prove that $BXCY'$ is cyclic.



We have

$$\angle XAP = \angle OPA = \angle EYP.$$

The first equality holds because $OA = OP$, and the second one because EY and OP are both perpendicular to BC and hence parallel. But $\{Y, Y'\}$ and $\{E, D\}$ are pairs of symmetric points with respect to OP, it follows that $\angle EYP = \angle DY'P$ and hence

$$\angle XAP = \angle DY'P = \angle XY'P.$$

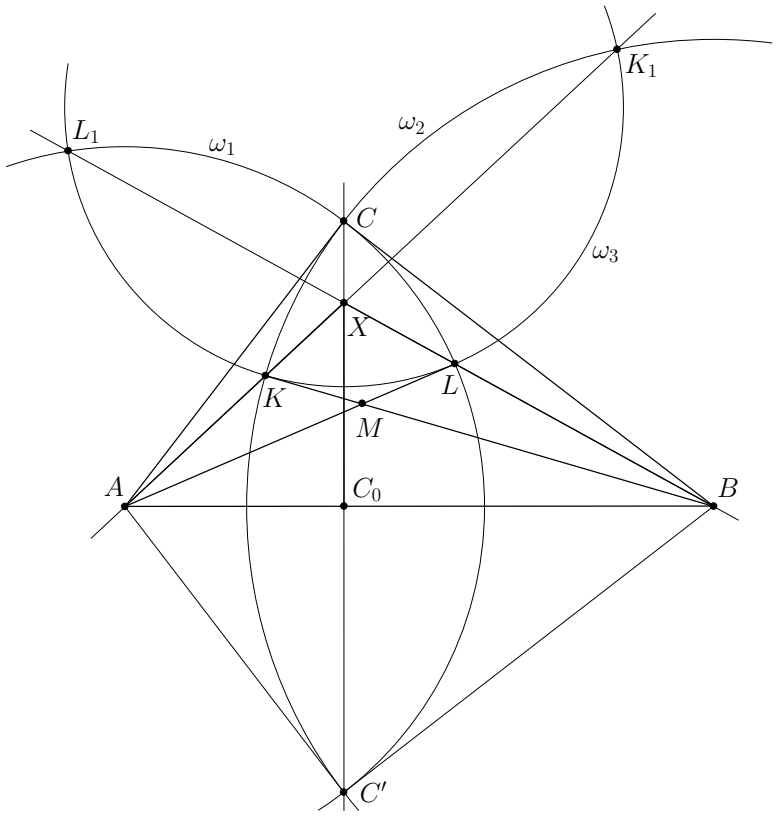
The last equation implies that $XAY'P$ is cyclic. By the powers of D with respect to the circles $(XAY'P)$ and $(ABPC)$ we obtain

$$XD \cdot DY' = AD \cdot DP = BD \cdot DC.$$

It follows that $BXCY'$ is cyclic, as desired.

G5. Let ABC be a triangle with $\angle BCA = 90°$, and let C_0 be the foot of the altitude from C. Choose a point X in the interior of the segment CC_0, and let K, L be the points on the segments AX, BX for which $BK = BC$ and $AL = AC$ respectively. Denote by M the intersection of AL and BK. Show that $MK = ML$.

Solution. Let C' be the reflection of C in the line AB, and let ω_1 and ω_2 be the circles with centers A and B, passing through L and K respectively. Since $AC' = AC = AL$ and $BC' = BC = BK$, both ω_1 and ω_2 pass through C and C'. By $\angle BCA = 90°$, AC is tangent to ω_2 at C, and BC is tangent to ω_1 at C. Let $K_1 \neq K$ be the second intersection of AX and ω_2, and let $L_1 \neq L$ be the second intersection of BX and ω_1.



By the powers of X with respect to ω_2 and ω_1,

$$XK \cdot XK_1 = XC \cdot XC' = XL \cdot XL_1,$$

so the points K_1, L, K, L_1 lie on a circle ω_3.

The power of A with respect to ω_2 gives

$$AL^2 = AC^2 = AK \cdot AK_1,$$

indicating that AL is tangent to ω_3 at L. Analogously, BK is tangent to ω_3 at K. Hence MK and ML are the two tangents from M to ω_3 and therefore $MK = ML$.

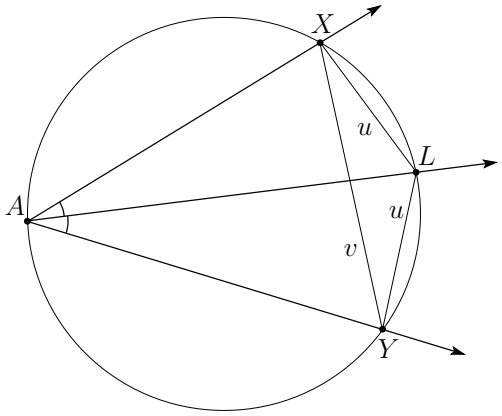
G6. Let ABC be a triangle with circumcenter O and incenter I. The points D, E and F on the sides BC, CA and AB respectively are such that $BD + BF = CA$ and $CD + CE = AB$. The circumcircles of the triangles BFD and CDE intersect at $P \neq D$. Prove that $OP = OI$.

Solution. By MIQUEL's theorem the circles $(AEF) = \omega_A$, $(BFD) = \omega_B$ and $(CDE) = \omega_C$ have a common point, for arbitrary points D, E and F on BC, CA and AB. So ω_A passes through the common point $P \neq D$ of ω_B and ω_C.

Let ω_A, ω_B and ω_C meet the bisectors AI, BI and CI at $A \neq A'$, $B \neq B'$ and $C \neq C'$ respectively. The key observation is that A', B' and C' do not depend on the particular choice of D, E and F, provided that $BD + BF = CA$, $CD + CE = AB$ and $AE + AF = BC$ hold true (the last equality follows from the other two). For a proof we need the following fact.

Lemma. Given is an angle with vertex A and measure α. A circle ω through A intersects the angle bisector at L and sides of the angle at X and Y. Then $AX + AY = 2AL\cos\frac{\alpha}{2}$.

Proof. Note that L is the midpoint of arc $\widehat{XLY}$ in ω and set $XL = YL = u$, $XY = v$. By PTOLEMY's theorem $AX \cdot YL + AY \cdot XL = AL \cdot XY$, which rewrites as $(AX + AY)u = AL \cdot v$. Since $\angle LXY = \frac{\alpha}{2}$ and $\angle XLY = 180^\circ - \alpha$, we have $v = 2\cos\frac{\alpha}{2}u$ by the law of sines, and the claim follows. □



Apply the lemma to $\angle BAC = \alpha$ and the circle $\omega = \omega_A$, which intersects AI at A'. This gives $2AA'\cos\frac{\alpha}{2} = AE + AF = BC$; by symmetry analogous relations hold for BB' and CC'. It follows that A', B' and C' are independent of the choice of D, E and F, as stated.

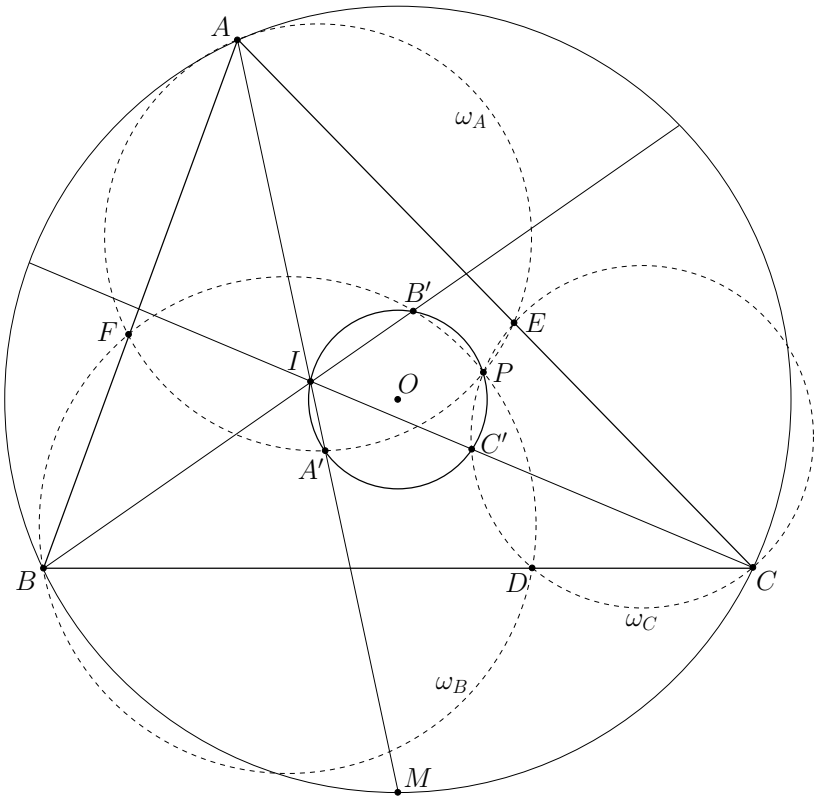
We use the lemma two more times with $\angle BAC = \alpha$. Let ω be the circle with diameter AI. Then X and Y are the tangency points of the incircle of ABC with AB and AC, and hence $AX = AY = \frac{1}{2}(AB + AC - BC)$. So the lemma yields $2AI\cos\frac{\alpha}{2} = AB + AC - BC$. Next, if ω is the circumcircle of ABC and AI intersects ω at $M \neq A$ then $\{X, Y\} = \{B, C\}$, and so $2AM\cos\frac{\alpha}{2} = AB + AC$ by the lemma. To summarize,

$$2AA'\cos\tfrac{\alpha}{2} = BC, \qquad 2AI\cos\tfrac{\alpha}{2} = AB + AC - BC, \qquad 2AM\cos\tfrac{\alpha}{2} = AB + AC. \qquad (*)$$

These equalities imply $AA' + AI = AM$, hence the segments AM and IA' have a common midpoint. It follows that I and A' are equidistant from the circumcenter O. By symmetry $OI = OA' = OB' = OC'$, so I, A', B', C' are on a circle centered at O.

To prove $OP = OI$, now it suffices to show that I, A', B', C' and P are concyclic. Clearly one can assume $P \neq I, A', B', C'$.

We use oriented angles to avoid heavy case distinction. The oriented angle between the lines l and m is denoted by $\angle(l, m)$. We have $\angle(l, m) = -\angle(m, l)$ and $\angle(l, m) + \angle(m, n) = \angle(l, n)$ for arbitrary lines l, m and n. Four distinct non-collinear points U, V, X, Y are concyclic if and only if $\angle(UX, VX) = \angle(UY, VY)$.



Suppose for the moment that A', B', P, I are distinct and noncollinear; then it is enough to check the equality $\angle(A'P, B'P) = \angle(A'I, B'I)$. Because A, F, P, A' are on the circle ω_A, we have $\angle(A'P, FP) = \angle(A'A, FA) = \angle(A'I, AB)$. Likewise $\angle(B'P, FP) = \angle(B'I, AB)$. Therefore

$$\angle(A'P, B'P) = \angle(A'P, FP) + \angle(FP, B'P) = \angle(A'I, AB) - \angle(B'I, AB) = \angle(A'I, B'I).$$

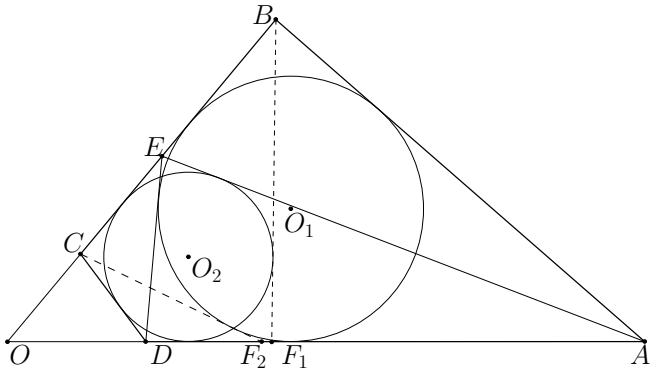
Here we assumed that $P \neq F$. If $P = F$ then $P \neq D, E$ and the conclusion follows similarly (use $\angle(A'F, B'F) = \angle(A'F, EF) + \angle(EF, DF) + \angle(DF, B'F)$ and inscribed angles in $\omega_A, \omega_B, \omega_C$).

There is no loss of generality in assuming A', B', P, I distinct and noncollinear. If ABC is an equilateral triangle then the equalities (*) imply that A', B', C', I, O and P coincide, so $OP = OI$. Otherwise at most one of A', B', C' coincides with I. If say $C' = I$ then $OI \perp CI$ by the previous reasoning. It follows that $A', B' \neq I$ and hence $A' \neq B'$. Finally A', B' and I are noncollinear because I, A', B', C' are concyclic.

Comment. The proposer remarks that the locus γ of the points P is an arc of the circle $(A'B'C'I)$. The reflection I' of I in O belongs to γ; it is obtained by choosing D, E and F to be the tangency points of the three excircles with their respective sides. The rest of the circle $(A'B'C'I)$, except I, can be included in γ by letting D, E and F vary on the extensions of the sides and assuming signed lengths. For instance if B is between C and D then the length BD must be taken with a negative sign. The incenter I corresponds to the limit case where D tends to infinity.

G7. Let $ABCD$ be a convex quadrilateral with non-parallel sides BC and AD. Assume that there is a point E on the side BC such that the quadrilaterals $ABED$ and $AECD$ are circumscribed. Prove that there is a point F on the side AD such that the quadrilaterals $ABCF$ and $BCDF$ are circumscribed if and only if AB is parallel to CD.

Solution. Let ω_1 and ω_2 be the incircles and O_1 and O_2 the incenters of the quadrilaterals $ABED$ and $AECD$ respectively. A point F with the stated property exists only if ω_1 and ω_2 are also the incircles of the quadrilaterals $ABCF$ and $BCDF$.



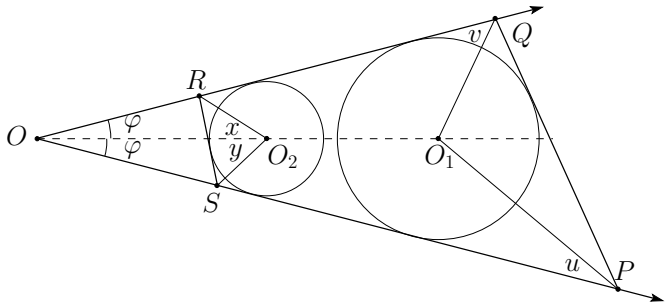
Let the tangents from B to ω_2 and from C to ω_1 (other than BC) meet AD at F_1 and F_2 respectively. We need to prove that $F_1 = F_2$ if and only if $AB \parallel CD$.

Lemma. The circles ω_1 and ω_2 with centers O_1 and O_2 are inscribed in an angle with vertex O. The points P, S on one side of the angle and Q, R on the other side are such that ω_1 is the incircle of the triangle PQO, and ω_2 is the excircle of the triangle RSO opposite to O. Denote $p = OO_1 \cdot OO_2$. Then exactly one of the following relations holds:

$$OP \cdot OR < p < OQ \cdot OS, \qquad OP \cdot OR > p > OQ \cdot OS, \qquad OP \cdot OR = p = OQ \cdot OS.$$

Proof. Denote $\angle OPO_1 = u$, $\angle OQO_1 = v$, $\angle OO_2R = x$, $\angle OO_2S = y$, $\angle POQ = 2\varphi$. Because PO_1, QO_1, RO_2, SO_2 are internal or external bisectors in the triangles PQO and RSO, we have

$$u + v = x + y \ (= 90^\circ - \varphi). \tag{1}$$



By the law of sines

$$\frac{OP}{OO_1} = \frac{\sin(u+\varphi)}{\sin u} \quad \text{and} \quad \frac{OO_2}{OR} = \frac{\sin(x+\varphi)}{\sin x}.$$

Therefore, since x, u and φ are acute,

$$OP \cdot OR \geq p \Leftrightarrow \frac{OP}{OO_1} \geq \frac{OO_2}{OR} \Leftrightarrow \sin x \sin(u+\varphi) \geq \sin u \sin(x+\varphi) \Leftrightarrow \sin(x-u) \geq 0 \Leftrightarrow x \geq u.$$

Thus $OP \cdot OR \geq p$ is equivalent to $x \geq u$, with $OP \cdot OR = p$ if and only if $x = u$.

Analogously, $p \geq OQ \cdot OS$ is equivalent to $v \geq y$, with $p = OQ \cdot OS$ if and only if $v = y$. On the other hand $x \geq u$ and $v \geq y$ are equivalent by (1), with $x = u$ if and only if $v = y$. The conclusion of the lemma follows from here. $\square$

Going back to the problem, apply the lemma to the quadruples $\{B, E, D, F_1\}$, $\{A, B, C, D\}$ and $\{A, E, C, F_2\}$. Assuming $OE \cdot OF_1 > p$, we obtain

$$OE \cdot OF_1 > p \;\Rightarrow\; OB \cdot OD < p \;\Rightarrow\; OA \cdot OC > p \;\Rightarrow\; OE \cdot OF_2 < p.$$

In other words, $OE \cdot OF_1 > p$ implies

$$OB \cdot OD < p < OA \cdot OC \quad \text{and} \quad OE \cdot OF_1 > p > OE \cdot OF_2.$$

Similarly, $OE \cdot OF_1 < p$ implies

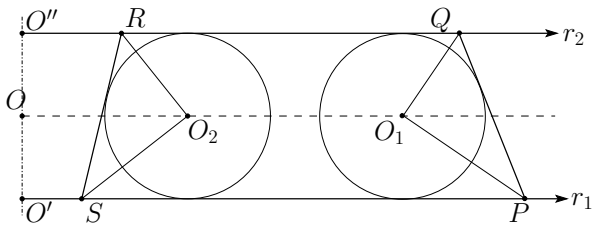
$$OB \cdot OD > p > OA \cdot OC \quad \text{and} \quad OE \cdot OF_1 < p < OE \cdot OF_2.$$

In these cases $F_1 \neq F_2$ and $OB \cdot OD \neq OA \cdot OC$, so the lines AB and CD are not parallel.

There remains the case $OE \cdot OF_1 = p$. Here the lemma leads to $OB \cdot OD = p = OA \cdot OC$ and $OE \cdot OF_1 = p = OE \cdot OF_2$. Therefore $F_1 = F_2$ and $AB \parallel CD$.

Comment. The conclusion is also true if BC and AD are parallel. One can prove a limit case of the lemma for the configuration shown in the figure below, where r_1 and r_2 are parallel rays starting at O' and O'', with $O'O'' \perp r_1, r_2$ and O the midpoint of $O'O''$. Two circles with centers O_1 and O_2 are inscribed in the strip between r_1 and r_2. The lines PQ and RS are tangent to the circles, with P, S on r_1, and Q, R on r_2, so that O, O_1 are on the same side of PQ and O, O_2 are on different sides of RS. Denote $s = OO_1 + OO_2$. Then exactly one of the following relations holds:

$$O'P + O''R < s < O''Q + O'S, \quad O'P + O''R > s > O''Q + O'S, \quad O'P + O''R = s = O''Q + O'S.$$

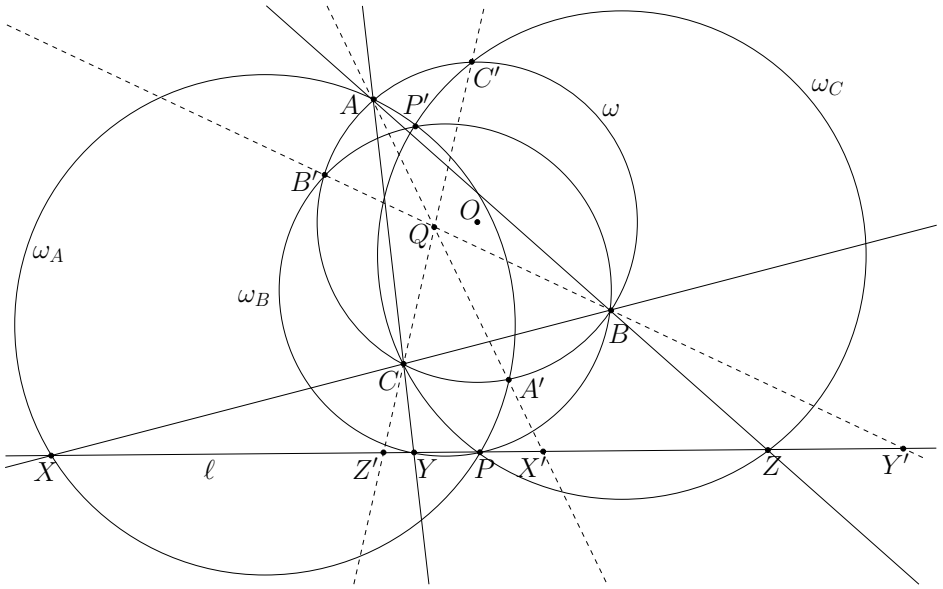


Once this is established, the proof of the original statement for $BC \parallel AD$ is analogous to the one in the intersecting case. One replaces products by sums of relevant segments.

G8. Let ABC be a triangle with circumcircle ω and ℓ a line without common points with ω. Denote by P the foot of the perpendicular from the center of ω to ℓ. The side-lines BC, CA, AB intersect ℓ at the points X, Y, Z different from P. Prove that the circumcircles of the triangles AXP, BYP and CZP have a common point different from P or are mutually tangent at P.

Solution 1. Let $\omega_A, \omega_B, \omega_C$ and ω be the circumcircles of triangles AXP, BYP, CZP and ABC respectively. The strategy of the proof is to construct a point Q with the same power with respect to the four circles. Then each of P and Q has the same power with respect to $\omega_A, \omega_B, \omega_C$ and hence the three circles are coaxial. In other words they have another common point P' or the three of them are tangent at P.

We first give a description of the point Q. Let $A' \neq A$ be the second intersection of ω and ω_A; define B' and C' analogously. We claim that AA', BB' and CC' have a common point. Once this claim is established, the point just constructed will be on the radical axes of the three pairs of circles $\{\omega, \omega_A\}, \{\omega, \omega_B\}, \{\omega, \omega_C\}$. Hence it will have the same power with respect to $\omega, \omega_A, \omega_B, \omega_C$.



We proceed to prove that AA', BB' and CC' intersect at one point. Let r be the circumradius of triangle ABC. Define the points X', Y', Z' as the intersections of AA', BB', CC' with ℓ. Observe that X', Y', Z' do exist. If AA' is parallel to ℓ then ω_A is tangent to ℓ; hence $X = P$ which is a contradiction. Similarly, BB' and CC' are not parallel to ℓ.

From the powers of the point X' with respect to the circles ω_A and ω we get

$$X'P \cdot (X'P + PX) = X'P \cdot X'X = X'A' \cdot X'A = X'O^2 - r^2,$$

hence

$$X'P \cdot PX = X'O^2 - r^2 - X'P^2 = OP^2 - r^2.$$

We argue analogously for the points Y' and Z', obtaining

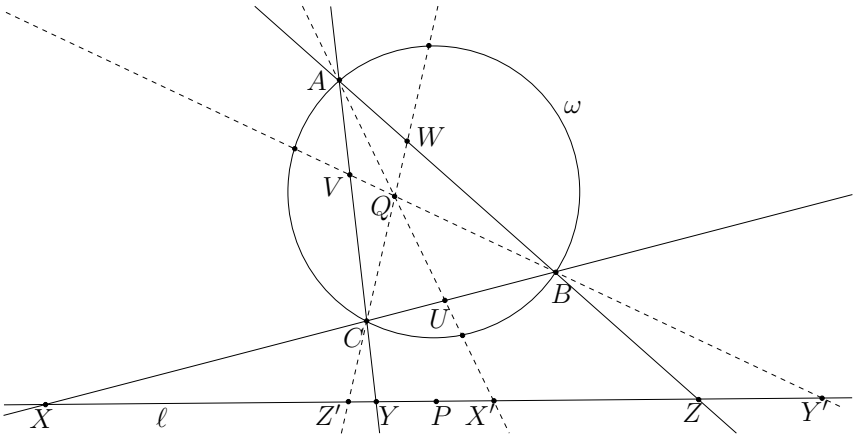
$$X'P \cdot PX = Y'P \cdot PY = Z'P \cdot PZ = OP^2 - r^2 = k^2. \tag{1}$$

In these computations all segments are regarded as directed segments. We keep the same convention for the sequel.

We prove that the lines AA', BB', CC' intersect at one point by Ceva's theorem. To avoid distracting remarks we interpret everything projectively, i. e. whenever two lines are parallel they meet at a point on the line at infinity.

Let U, V, W be the intersections of AA', BB', CC' with BC, CA, AB respectively. The idea is that although it is difficult to calculate the ratio $\frac{BU}{CU}$, it is easier to deal with the cross-ratio $\frac{BU}{CU}/\frac{BX}{CX}$ because we can send it to the line ℓ. With this in mind we apply Menelaus' theorem to the triangle ABC and obtain $\frac{BX}{CX} \cdot \frac{CY}{AY} \cdot \frac{AZ}{BZ} = 1$. Hence Ceva's ratio can be expressed as

$$\frac{BU}{CU} \cdot \frac{CV}{AV} \cdot \frac{AW}{BW} = \frac{BU}{CU}/\frac{BX}{CX} \cdot \frac{CV}{AV}/\frac{CY}{AY} \cdot \frac{AW}{BW}/\frac{AZ}{BZ}.$$



Project the line BC to ℓ from A. The cross-ratio between BC and UX equals the cross-ratio between ZY and $X'X$. Repeating the same argument with the lines CA and AB gives

$$\frac{BU}{CU} \cdot \frac{CV}{AV} \cdot \frac{AW}{BW} = \frac{ZX'}{YX'}/\frac{ZX}{YX} \cdot \frac{XY'}{ZY'}/\frac{XY}{ZY} \cdot \frac{YZ'}{XZ'}/\frac{YZ}{XZ}$$

and hence

$$\frac{BU}{CU} \cdot \frac{CV}{AV} \cdot \frac{AW}{BW} = (-1) \cdot \frac{ZX'}{YX'} \cdot \frac{XY'}{ZY'} \cdot \frac{YZ'}{XZ'}.$$

The equations (1) reduce the problem to a straightforward computation on the line ℓ. For instance, the transformation $t \mapsto -k^2/t$ preserves cross-ratio and interchanges the points X, Y, Z with the points X', Y', Z'. Then

$$\frac{BU}{CU} \cdot \frac{CV}{AV} \cdot \frac{AW}{BW} = (-1) \cdot \frac{ZX'}{YX'}/\frac{ZZ'}{YZ'} \cdot \frac{XY'}{ZY'}/\frac{XZ'}{ZZ'} = -1.$$

We proved that Ceva's ratio equals -1, so AA', BB', CC' intersect at one point Q.

Comment 1. There is a nice projective argument to prove that AX', BY', CZ' intersect at one point. Suppose that ℓ and ω intersect at a pair of complex conjugate points D and E. Consider a projective transformation that takes D and E to $[i; 1, 0]$ and $[-i, 1, 0]$. Then ℓ is the line at infinity, and ω is a conic through the special points $[i; 1, 0]$ and $[-i, 1, 0]$, hence it is a circle. So one can assume that AX, BY, CZ are parallel to BC, CA, AB. The involution on ℓ taking X, Y, Z to X', Y', Z' and leaving D, E fixed is the involution changing each direction to its perpendicular one. Hence AX, BY, CZ are also perpendicular to AX', BY', CZ'.

It follows from the above that AX', BY', CZ' intersect at the orthocenter of triangle ABC.

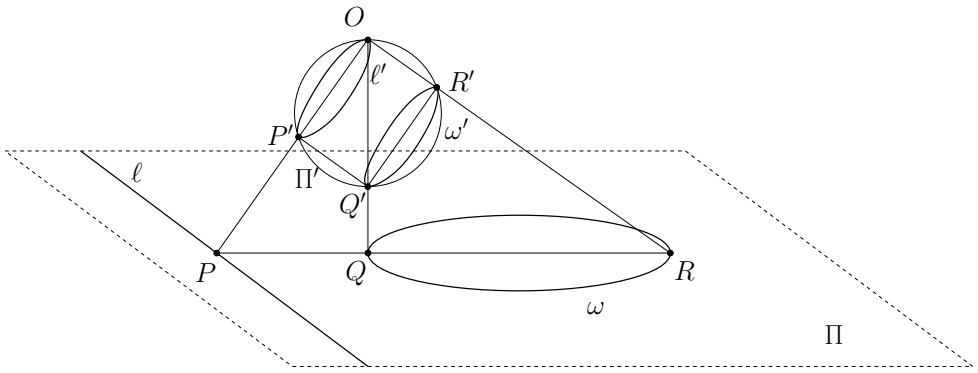
Comment 2. The restriction that the line ℓ does not intersect the circumcricle ω is unnecessary. The proof above works in general. In case ℓ intersects ω at D and E point P is the midpoint of DE, and some equations can be interpreted differently. For instance

$$X'P \cdot X'X = X'A' \cdot X'A = X'D \cdot X'E,$$

and hence the pairs $X'X$ and DE are harmonic conjugates. This means that X', Y', Z' are the harmonic conjugates of X, Y, Z with respect to the segment DE.

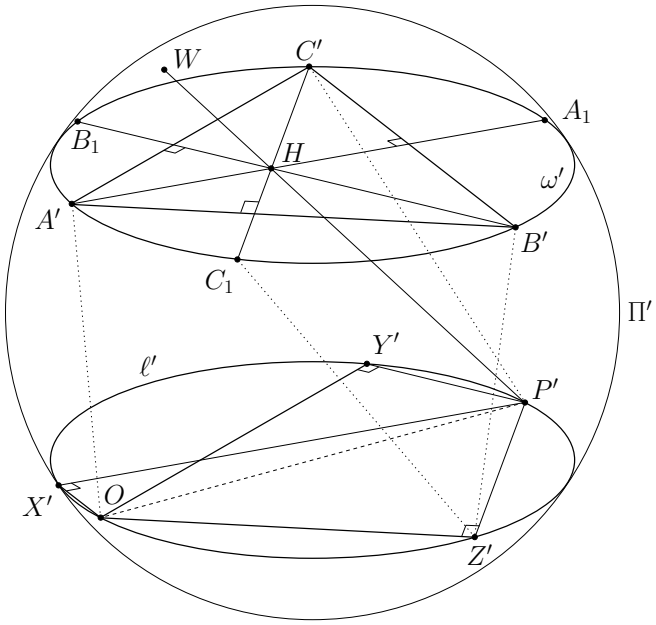
Solution 2. First we prove that there is an inversion in space that takes ℓ and ω to parallel circles on a sphere. Let QR be the diameter of ω whose extension beyond Q passes through P. Let Π be the plane carrying our objects. In space, choose a point O such that the line QO is perpendicular to Π and $\angle POR = 90°$, and apply an inversion with pole O (the radius of the inversion does not matter). For any object $\mathcal{T}$ denote by $\mathcal{T}'$ the image of $\mathcal{T}$ under this inversion.

The inversion takes the plane Π to a sphere Π'. The lines in Π are taken to circles through O, and the circles in Π also are taken to circles on Π'.



Since the line ℓ and the circle ω are perpendicular to the plane OPQ, the circles ℓ' and ω' also are perpendicular to this plane. Hence, the planes of the circles ℓ' and ω' are parallel.

Now consider the circles $A'X'P'$, $B'Y'P'$ and $C'Z'P'$. We want to prove that either they have a common point (on Π'), different from P', or they are tangent to each other.



The point X' is the second intersection of the circles $B'C'O$ and ℓ', other than O. Hence, the lines OX' and $B'C'$ are coplanar. Moreover, they lie in the parallel planes of ℓ' and ω'. Therefore, OX' and $B'C'$ are parallel. Analogously, OY' and OZ' are parallel to $A'C'$ and $A'B'$.

Let A_1 be the second intersection of the circles $A'X'P'$ and ω', other than A'. The segments $A'A_1$ and $P'X'$ are coplanar, and therefore parallel. Now we know that $B'C'$ and $A'A_1$ are parallel to OX' and $X'P'$ respectively, but these two segments are perpendicular because OP' is a diameter in ℓ'. We found that $A'A_1$ and $B'C'$ are perpendicular, hence $A'A_1$ is the altitude in the triangle $A'B'C'$, starting from A.

Analogously, let B_1 and C_1 be the second intersections of ω' with the circles $B'P'Y'$ and $C'P'Z'$, other than B' and C' respectively. Then $B'B_1$ and $C'C_1$ are the other two altitudes in the triangle $A'B'C'$.

Let H be the orthocenter of the triangle $A'B'C'$. Let W be the second intersection of the line $P'H$ with the sphere Π', other than P'. The point W lies on the sphere Π', in the plane of the circle $A'P'X'$, so W lies on the circle $A'P'X'$. Similarly, W lies on the circles $B'P'Y'$ and $C'P'Z'$ as well; indeed W is the second common point of the three circles.

If the line $P'H$ is tangent to the sphere then W coincides with P', and $P'H$ is the common tangent of the three circles.

Number Theory

N1. Call admissible a set A of integers that has the following property:

$$\text{If } x, y \in A \text{ (possibly } x = y) \text{ then } x^2 + kxy + y^2 \in A \text{ for every integer } k.$$

Determine all pairs m, n of nonzero integers such that the only admissible set containing both m and n is the set of all integers.

Solution. A pair of integers m, n fulfills the condition if and only if $gcd(m, n) = 1$. Suppose that $gcd(m, n) = d > 1$. The set

$$A = \{\ldots, -2d, -d, 0, d, 2d, \ldots\}$$

is admissible, because if d divides x and y then it divides $x^2 + kxy + y^2$ for every integer k. Also $m, n \in A$ and $A \neq \mathbb{Z}$.

Now let $gcd(m, n) = 1$, and let A be an admissible set containing m and n. We use the following observations to prove that $A = \mathbb{Z}$:

(i) $kx^2 \in A$ for every $x \in A$ and every integer k.

(ii) $(x + y)^2 \in A$ for all $x, y \in A$.

To justify (i) let $y = x$ in the definition of an admissible set; to justify (ii) let $k = 2$.

Since $gcd(m, n) = 1$, we also have $gcd(m^2, n^2) = 1$. Hence one can find integers a, b such that $am^2 + bn^2 = 1$. It follows from (i) that $am^2 \in A$ and $bn^2 \in A$. Now we deduce from (ii) that $1 = (am^2 + bn^2)^2 \in A$. But if $1 \in A$ then (i) implies $k \in A$ for every integer k.

N2. Find all triples (x, y, z) of positive integers such that $x \le y \le z$ and

$$x^3(y^3 + z^3) = 2012(xyz + 2).$$

Solution. First note that x divides $2012 \cdot 2 = 2^3 \cdot 503$. If $503 \mid x$ then the right-hand side of the equation is divisible by 503^3, and it follows that $503^2 \mid xyz + 2$. This is false as $503 \mid x$. Hence $x = 2^m$ with $m \in \{0, 1, 2, 3\}$. If $m \ge 2$ then $2^6 \mid 2012(xyz + 2)$. However the highest powers of 2 dividing 2012 and $xyz + 2 = 2^m yz + 2$ are 2^2 and 2^1 respectively. So $x = 1$ or $x = 2$, yielding the two equations

$$y^3 + z^3 = 2012(yz + 2), \qquad \text{and} \qquad y^3 + z^3 = 503(yz + 1).$$

In both cases the prime $503 = 3 \cdot 167 + 2$ divides $y^3 + z^3$. We claim that $503 \mid y + z$. This is clear if $503 \mid y$, so let $503 \nmid y$ and $503 \nmid z$. Then $y^{502} \equiv z^{502} \pmod{503}$ by FERMAT's little theorem. On the other hand $y^3 \equiv -z^3 \pmod{503}$ implies $y^{3 \cdot 167} \equiv -z^{3 \cdot 167} \pmod{503}$, i. e. $y^{501} \equiv -z^{501} \pmod{503}$. It follows that $y \equiv -z \pmod{503}$ as claimed.

Therefore $y + z = 503k$ with $k \ge 1$. In view of $y^3 + z^3 = (y + z)\big((y - z)^2 + yz\big)$ the two equations take the form

$$k(y - z)^2 + (k - 4)yz = 8, \tag{1}$$

$$k(y - z)^2 + (k - 1)yz = 1. \tag{2}$$

In (1) we have $(k - 4)yz \le 8$, which implies $k \le 4$. Indeed if $k > 4$ then $1 \le (k - 4)yz \le 8$, so that $y \le 8$ and $z \le 8$. This is impossible as $y + z = 503k \ge 503$. Note next that $y^3 + z^3$ is even in the first equation. Hence $y + z = 503k$ is even too, meaning that k is even. Thus $k = 2$ or $k = 4$. Clearly (1) has no integer solutions for $k = 4$. If $k = 2$ then (1) takes the form $(y + z)^2 - 5yz = 4$. Since $y + z = 503k = 503 \cdot 2$, this leads to $5yz = 503^2 \cdot 2^2 - 4$. However $503^2 \cdot 2^2 - 4$ is not a multiple of 5. Therefore (1) has no integer solutions.

Equation (2) implies $0 \le (k - 1)yz \le 1$, so that $k = 1$ or $k = 2$. Also $0 \le k(y - z)^2 \le 1$, hence $k = 2$ only if $y = z$. However then $y = z = 1$, which is false in view of $y + z \ge 503$. Therefore $k = 1$ and (2) takes the form $(y - z)^2 = 1$, yielding $z - y = |y - z| = 1$. Combined with $k = 1$ and $y + z = 503k$, this leads to $y = 251$, $z = 252$.

In summary the triple $(2, 251, 252)$ is the only solution.

N3. Determine all integers $m \geq 2$ such that every n with $\frac{m}{3} \leq n \leq \frac{m}{2}$ divides the binomial coefficient $\binom{n}{m-2n}$.

Solution. The integers in question are all prime numbers.

First we check that all primes satisfy the condition, and even a stronger one. Namely, if p is a prime then every n with $1 \leq n \leq \frac{p}{2}$ divides $\binom{n}{p-2n}$. This is true for $p = 2$ where $n = 1$ is the only possibility. For an odd prime p take $n \in [1, \frac{p}{2}]$ and consider the following identity of binomial coefficients:

$$(p-2n) \cdot \binom{n}{p-2n} = n \cdot \binom{n-1}{p-2n-1}.$$

Since $p \geq 2n$ and p is odd, all factors are non-zero. If $d = gcd(p-2n, n)$ then d divides p, but $d \leq n < p$ and hence $d = 1$. It follows that $p - 2n$ and n are relatively prime, and so the factor n in the right-hand side divides the binomial coefficient $\binom{n}{p-2n}$.

Next we show that no composite number m has the stated property. Consider two cases.

- If $m = 2k$ with $k > 1$, pick $n = k$. Then $\frac{m}{3} \leq n \leq \frac{m}{2}$ but $\binom{n}{m-2n} = \binom{k}{0} = 1$ is not divisible by $k > 1$.

- If m is odd then there exist an odd prime p and an integer $k \geq 1$ with $m = p(2k+1)$. Pick $n = pk$, then $\frac{m}{3} \leq n \leq \frac{m}{2}$ by $k \geq 1$. However

$$\frac{1}{n}\binom{n}{m-2n} = \frac{1}{pk}\binom{pk}{p} = \frac{(pk-1)(pk-2)\cdots(pk-(p-1))}{p!}$$

  is not an integer, because p divides the denominator but not the numerator.

N4. An integer a is called friendly if the equation $(m^2+n)(n^2+m) = a(m-n)^3$ has a solution over the positive integers.

a) Prove that there are at least 500 friendly integers in the set $\{1, 2, \ldots, 2012\}$.

b) Decide whether $a = 2$ is friendly.

Solution. a) Every a of the form $a = 4k-3$ with $k \geq 2$ is friendly. Indeed the numbers $m = 2k-1 > 0$ and $n = k-1 > 0$ satisfy the given equation with $a = 4k-3$:

$$(m^2+n)(n^2+m) = \big((2k-1)^2+(k-1)\big)\big((k-1)^2+(2k-1)\big) = (4k-3)k^3 = a(m-n)^3.$$

Hence $5, 9, \ldots, 2009$ are friendly and so $\{1, 2, \ldots, 2012\}$ contains at least 502 friendly numbers.

b) We show that $a = 2$ is not friendly. Consider the equation with $a = 2$ and rewrite its left-hand side as a difference of squares:

$$\frac{1}{4}\left((m^2+n+n^2+m)^2 - (m^2+n-n^2-m)^2\right) = 2(m-n)^3.$$

Since $m^2+n-n^2-m = (m-n)(m+n-1)$, we can further reformulate the equation as

$$(m^2+n+n^2+m)^2 = (m-n)^2\left(8(m-n)+(m+n-1)^2\right).$$

It follows that $8(m-n)+(m+n-1)^2$ is a perfect square. Clearly $m > n$, hence there is an integer $s \geq 1$ such that

$$(m+n-1+2s)^2 = 8(m-n)+(m+n-1)^2.$$

Subtracting the squares gives $s(m+n-1+s) = 2(m-n)$. Since $m+n-1+s > m-n$, we conclude that $s < 2$. Therefore the only possibility is $s = 1$ and $m = 3n$. However then the left-hand side of the given equation (with $a = 2$) is greater than $m^3 = 27n^3$, whereas its right-hand side equals $16n^3$. The contradiction proves that $a = 2$ is not friendly.

Comment. A computer search shows that there are 561 friendly numbers in $\{1, 2, \ldots, 2012\}$.

N5. For a nonnegative integer n define $rad(n) = 1$ if $n = 0$ or $n = 1$, and $rad(n) = p_1 p_2 \cdots p_k$ where $p_1 < p_2 < \cdots < p_k$ are all prime factors of n. Find all polynomials $f(x)$ with nonnegative integer coefficients such that $rad(f(n))$ divides $rad(f(n^{rad(n)}))$ for every nonnegative integer n.

Solution 1. We are going to prove that $f(x) = ax^m$ for some nonnegative integers a and m. If $f(x)$ is the zero polynomial we are done, so assume that $f(x)$ has at least one positive coefficient. In particular $f(1) > 0$.

Let p be a prime number. The condition is that $f(n) \equiv 0 \pmod{p}$ implies

$$f(n^{rad(n)}) \equiv 0 \pmod{p}. \tag{1}$$

Since $rad(n^{rad(n)^k}) = rad(n)$ for all k, repeated applications of the preceding implication show that if p divides $f(n)$ then

$$f(n^{rad(n)^k}) \equiv 0 \pmod{p} \quad \text{for all } k.$$

The idea is to construct a prime p and a positive integer n such that $p-1$ divides n and p divides $f(n)$. In this case, for k large enough $p-1$ divides $rad(n)^k$. Hence if $(p, n) = 1$ then $n^{rad(n)^k} \equiv 1 \pmod{p}$ by FERMAT's little theorem, so that

$$f(1) \equiv f(n^{rad(n)^k}) \equiv 0 \pmod{p}. \tag{2}$$

Suppose that $f(x) = g(x)x^m$ with $g(0) \neq 0$. Let t be a positive integer, p any prime factor of $g(-t)$ and $n = (p-1)t$. So $p-1$ divides n and $f(n) = f((p-1)t) \equiv f(-t) \equiv 0 \pmod{p}$, hence either $(p, n) > 1$ or (2) holds. If $(p, (p-1)t) > 1$ then p divides t and $g(0) \equiv g(-t) \equiv 0 \pmod{p}$, meaning that p divides $g(0)$.

In conclusion we proved that each prime factor of $g(-t)$ divides $g(0)f(1) \neq 0$, and thus the set of prime factors of $g(-t)$ when t ranges through the positive integers is finite. This is known to imply that $g(x)$ is a constant polynomial, and so $f(x) = ax^m$.

Solution 2. Let $f(x)$ be a polynomial with integer coefficients (not necessarily nonnegative) such that $rad(f(n))$ divides $rad(f(n^{rad(n)}))$ for any nonnegative integer n. We give a complete description of all polynomials with this property. More precisely, we claim that if $f(x)$ is such a polynomial and ξ is a root of $f(x)$ then so is ξ^d for every positive integer d.

Therefore each root of $f(x)$ is zero or a root of unity. In particular, if a root of unity ξ is a root of $f(x)$ then $1 = \xi^d$ is a root too (for some positive integer d). In the original problem $f(x)$ has nonnegative coefficients. Then either $f(x)$ is the zero polynomial or $f(1) > 0$ and $\xi = 0$ is the only possible root. In either case $f(x) = ax^m$ with a and m nonnegative integers.

To prove the claim let ξ be a root of $f(x)$, and let $g(x)$ be an irreducible factor of $f(x)$ such that $g(\xi) = 0$. If 0 or 1 are roots of $g(x)$ then either $\xi = 0$ or $\xi = 1$ (because $g(x)$ is irreducible) and we are done. So assume that $g(0), g(1) \neq 0$. By decomposing d as a product of prime numbers, it is enough to consider the case $d = p$ prime. We argue for $p = 2$. Since $rad(2^k) = 2$ for every k, we have

$$rad(f(2^k)) \mid rad(f(2^{2k})).$$

Now we prove that $g(x)$ divides $f(x^2)$. Suppose that this is not the case. Then, since $g(x)$ is irreducible, there are integer-coefficient polynomials $a(x)$, $b(x)$ and an integer N such that

$$a(x)g(x) + b(x)f(x^2) = N. \tag{3}$$

Each prime factor p of $g(2^k)$ divides $f(2^k)$, so by $rad(f(2^k))|rad(f(2^{2k}))$ it also divides $f(2^{2k})$. From the equation above with $x = 2^k$ it follows that p divides N.

In summary, each prime divisor of $g(2^k)$ divides N, for all $k \geq 0$. Let $p_1, \ldots, p_n$ be the odd primes dividing N, and suppose that

$$g(1) = 2^{\alpha} p_1^{\alpha_1} \cdots p_n^{\alpha_n}.$$

If k is divisible by $\varphi(p_1^{\alpha_1+1} \cdots p_n^{\alpha_n+1})$ then

$$2^k \equiv 1 \pmod{p_1^{\alpha_1+1} \cdots p_n^{\alpha_n+1}},$$

yielding

$$g(2^k) \equiv g(1) \pmod{p_1^{\alpha_1+1} \cdots p_n^{\alpha_n+1}}.$$

It follows that for each i the maximal power of p_i dividing $g(2^k)$ and $g(1)$ is the same, namely $p_i^{\alpha_i}$. On the other hand, for large enough k, the maximal power of 2 dividing $g(2^k)$ and $g(0) \neq 0$ is the same. From the above, for k divisible by $\varphi(p_1^{\alpha_1+1} \cdots p_n^{\alpha_n+1})$ and large enough, we obtain that $g(2^k)$ divides $g(0) \cdot g(1)$. This is impossible because $g(0), g(1) \neq 0$ are fixed and $g(2^k)$ is arbitrarily large.

In conclusion, $g(x)$ divides $f(x^2)$. Recall that ξ is a root of $f(x)$ such that $g(\xi) = 0$; then $f(\xi^2) = 0$, i. e. ξ^2 is a root of $f(x)$.

Likewise if ξ is a root of $f(x)$ and p an arbitrary prime then ξ^p is a root too. The argument is completely analogous, in the proof above just replace 2 by p and "odd prime" by "prime different from p."

Comment. The claim in the second solution can be proved by varying $n \pmod{p}$ in (1). For instance, we obtain

$$f(n^{rad(n+pk)}) \equiv 0 \pmod{p}$$

for every positive integer k. One can prove that if $(n, p) = 1$ then $rad(n+pk)$ runs through all residue classes $r \pmod{p-1}$ with $(r, p-1)$ squarefree. Hence if $f(n) \equiv 0 \pmod{p}$ then $f(n^r) \equiv 0 \pmod{p}$ for all integers r. This implies the claim by an argument leading to the identity (3).

N6. Let x and y be positive integers. If $x^{2^n}-1$ is divisible by $2^n y+1$ for every positive integer n, prove that $x=1$.

Solution. First we prove the following fact: For every positive integer y there exist infinitely many primes $p \equiv 3 \pmod 4$ such that p divides some number of the form $2^n y+1$.

Clearly it is enough to consider the case y odd. Let

$$2y+1 = p_1^{e_1} \cdots p_r^{e_r}$$

be the prime factorization of $2y+1$. Suppose on the contrary that there are finitely many primes $p_{r+1}, \ldots, p_{r+s} \equiv 3 \pmod 4$ that divide some number of the form $2^n y+1$ but do not divide $2y+1$.

We want to find an n such that $p_i^{e_i} || 2^n y+1$ for $1 \le i \le r$ and $p_i \nmid 2^n y+1$ for $r+1 \le i \le r+s$. For this it suffices to take

$$n = 1 + \varphi(p_1^{e_1+1} \cdots p_r^{e_r+1} p_{r+1}^1 \cdots p_{r+s}^1),$$

because then

$$2^n y+1 \equiv 2y+1 \pmod{p_1^{e_1+1} \cdots p_r^{e_r+1} p_{r+1}^1 \cdots p_{r+s}^1}.$$

The last congruence means that $p_1^{e_1}, \ldots, p_r^{e_r}$ divide exactly $2^n y+1$ and no prime $p_{r+1}, \ldots, p_{r+s}$ divides $2^n y+1$. It follows that the prime factorization of $2^n y+1$ consists of the prime powers $p_1^{e_1}, \ldots, p_r^{e_r}$ and powers of primes $\equiv 1 \pmod 4$. Because y is odd, we obtain

$$2^n y+1 \equiv p_1^{e_1} \cdots p_r^{e_r} \equiv 2y+1 \equiv 3 \pmod 4.$$

This is a contradiction since $n>1$, and so $2^n y+1 \equiv 1 \pmod 4$.

Now we proceed to the problem. If p is a prime divisor of $2^n y+1$ the problem statement implies that $x^d \equiv 1 \pmod p$ for $d=2^n$. By FERMAT's little theorem the same congruence holds for $d=p-1$, so it must also hold for $d=(2^n, p-1)$. For $p \equiv 3 \pmod 4$ we have $(2^n, p-1)=2$, therefore in this case $x^2 \equiv 1 \pmod p$.

In summary, we proved that every prime $p \equiv 3 \pmod 4$ that divides some number of the form $2^n y+1$ also divides x^2-1. This is possible only if $x=1$, otherwise by the above x^2-1 would be a positive integer with infinitely many prime factors.

Comment. For each x and each odd prime p the maximal power of p dividing $x^{2^n}-1$ for some n is bounded and hence the same must be true for the numbers $2^n y+1$. We infer that p^2 divides $2^{p-1}-1$ for each prime divisor p of $2^n y+1$. However trying to reach a contradiction with this conclusion alone seems hopeless, since it is not even known if there are infinitely many primes p *without* this property.

N7. Find all $n \in \mathbb{N}$ for which there exist nonnegative integers $a_1, a_2, \ldots, a_n$ such that

$$\frac{1}{2^{a_1}} + \frac{1}{2^{a_2}} + \cdots + \frac{1}{2^{a_n}} = \frac{1}{3^{a_1}} + \frac{2}{3^{a_2}} + \cdots + \frac{n}{3^{a_n}} = 1.$$

Solution. Such numbers $a_1, a_2, \ldots, a_n$ exist if and only if $n \equiv 1 \pmod 4$ or $n \equiv 2 \pmod 4$.

Let $\sum_{k=1}^{n} \frac{k}{3^{a_k}} = 1$ with $a_1, a_2, \ldots, a_n$ nonnegative integers. Then $1 \cdot x_1 + 2 \cdot x_2 + \cdots + n \cdot x_n = 3^a$ with $x_1, \ldots, x_n$ powers of 3 and $a \geq 0$. The right-hand side is odd, and the left-hand side has the same parity as $1 + 2 + \cdots + n$. Hence the latter sum is odd, which implies $n \equiv 1, 2 \pmod 4$. Now we prove the converse.

Call *feasible* a sequence $b_1, b_2, \ldots, b_n$ if there are nonnegative integers $a_1, a_2, \ldots, a_n$ such that

$$\frac{1}{2^{a_1}} + \frac{1}{2^{a_2}} + \cdots + \frac{1}{2^{a_n}} = \frac{b_1}{3^{a_1}} + \frac{b_2}{3^{a_2}} + \cdots + \frac{b_n}{3^{a_n}} = 1.$$

Let b_k be a term of a feasible sequence $b_1, b_2, \ldots, b_n$ with exponents $a_1, a_2, \ldots, a_n$ like above, and let u, v be nonnegative integers with sum $3b_k$. Observe that

$$\frac{1}{2^{a_k+1}} + \frac{1}{2^{a_k+1}} = \frac{1}{2^{a_k}} \qquad \text{and} \qquad \frac{u}{3^{a_k+1}} + \frac{v}{3^{a_k+1}} = \frac{b_k}{3^{a_k}}.$$

It follows that the sequence $b_1, \ldots, b_{k-1}, u, v, b_{k+1}, \ldots, b_n$ is feasible. The exponents a_i are the same for the unchanged terms b_i, $i \neq k$; the new terms u, v have exponents $a_k + 1$.

We state the conclusion in reverse. If two terms u, v of a sequence are replaced by one term $\frac{u+v}{3}$ and the obtained sequence is feasible, then the original sequence is feasible too. Denote by α_n the sequence $1, 2, \ldots, n$. To show that α_n is feasible for $n \equiv 1, 2 \pmod 4$, we transform it by $n - 1$ replacements $\{u, v\} \mapsto \frac{u+v}{3}$ to the one-term sequence α_1. The latter is feasible, with $a_1 = 0$. Note that if m and $2m$ are terms of a sequence then $\{m, 2m\} \mapsto m$, so $2m$ can be ignored if necessary.

Let $n \geq 16$. We prove that α_n can be reduced to α_{n-12} by 12 operations. Write $n = 12k + r$ where $k \geq 1$ and $0 \leq r \leq 11$. If $0 \leq r \leq 5$ then the last 12 terms of α_n can be partitioned into 2 singletons $\{12k - 6\}$, $\{12k\}$ and the following 5 pairs:

$$\{12k - 6 - i, 12k - 6 + i\}, i = 1, \ldots, 5 - r; \qquad \{12k - j, 12k + j\}, j = 1, \ldots, r.$$

(There is only one kind of pairs if $r \in \{0, 5\}$.) One can ignore $12k - 6$ and $12k$ since α_n contains $6k - 3$ and $6k$. Furthermore the 5 operations $\{12k - 6 - i, 12k - 6 + i\} \mapsto 8k - 4$ and $\{12k - j, 12k + j\} \mapsto 8k$ remove the 10 terms in the pairs and bring in 5 new terms equal to $8k - 4$ or $8k$. All of these can be ignored too as $4k - 2$ and $4k$ are still present in the sequence. Indeed $4k \leq n - 12$ is equivalent to $8k \geq 12 - r$, which is true for $r \in \{4, 5\}$. And if $r \in \{0, 1, 2, 3\}$ then $n \geq 16$ implies $k \geq 2$, so $8k \geq 12 - r$ also holds. Thus α_n reduces to α_{n-12}.

The case $6 \leq r \leq 11$ is analogous. Consider the singletons $\{12k\}$, $\{12k + 6\}$ and the 5 pairs

$$\{12k - i, 12k + i\}, i = 1, \ldots, 11 - r; \qquad \{12k + 6 - j, 12k + 6 + j\}, j = 1, \ldots, r - 6.$$

Ignore the singletons like before, then remove the pairs via operations $\{12k - i, 12k + i\} \mapsto 8k$ and $\{12k + 6 - j, 12k + 6 + j\} \mapsto 8k + 4$. The 5 newly-appeared terms $8k$ and $8k + 4$ can be ignored too since $4k + 2 \leq n - 12$ (this follows from $k \geq 1$ and $r \geq 6$). We obtain α_{n-12} again.

The problem reduces to $2 \leq n \leq 15$. In fact $n \in \{2, 5, 6, 9, 10, 13, 14\}$ by $n \equiv 1, 2 \pmod 4$. The cases $n = 2, 6, 10, 14$ reduce to $n = 1, 5, 9, 13$ respectively because the last even term of α_n can be ignored. For $n = 5$ apply $\{4, 5\} \mapsto 3$, then $\{3, 3\} \mapsto 2$, then ignore the 2 occurrences of 2. For $n = 9$ ignore 6 first, then apply $\{5, 7\} \mapsto 4$, $\{4, 8\} \mapsto 4$, $\{3, 9\} \mapsto 4$. Now ignore the 3 occurrences of 4, then ignore 2. Finally $n = 13$ reduces to $n = 10$ by $\{11, 13\} \mapsto 8$ and ignoring 8 and 12. The proof is complete.

N8. Prove that for every prime $p > 100$ and every integer r there exist two integers a and b such that p divides $a^2 + b^5 - r$.

Solution 1. Throughout the solution, all congruence relations are meant modulo p.

Fix p, and let $\mathcal{P} = \{0, 1, \ldots, p-1\}$ be the set of residue classes modulo p. For every $r \in \mathcal{P}$, let $S_r = \big\{(a, b) \in \mathcal{P} \times \mathcal{P} \colon a^2 + b^5 \equiv r\big\}$, and let $s_r = |S_r|$. Our aim is to prove $s_r > 0$ for all $r \in \mathcal{P}$.

We will use the well-known fact that for every residue class $r \in \mathcal{P}$ and every positive integer k, there are at most k values $x \in \mathcal{P}$ such that $x^k \equiv r$.

Lemma. Let N be the number of quadruples $(a, b, c, d) \in \mathcal{P}^4$ for which $a^2 + b^5 \equiv c^2 + d^5$. Then

$$N = \sum_{r \in \mathcal{P}} s_r^2 \tag{a}$$

and

$$N \le p(p^2 + 4p - 4). \tag{b}$$

Proof. (a) For each residue class r there exist exactly s_r pairs (a, b) with $a^2 + b^5 \equiv r$ and s_r pairs (c, d) with $c^2 + d^5 \equiv r$. So there are s_r^2 quadruples with $a^2 + b^5 \equiv c^2 + d^5 \equiv r$. Taking the sum over all $r \in \mathcal{P}$, the statement follows.

(b) Choose an arbitrary pair $(b, d) \in \mathcal{P}$ and look for the possible values of a, c.

1. Suppose that $b^5 \equiv d^5$, and let k be the number of such pairs (b, d). The value b can be chosen in p different ways. For $b \equiv 0$ only $d = 0$ has this property; for the nonzero values of b there are at most 5 possible values for d. So we have $k \le 1 + 5(p-1) = 5p - 4$.

The values a and c must satisfy $a^2 \equiv c^2$, so $a \equiv \pm c$, and there are exactly $2p - 1$ such pairs (a, c).

2. Now suppose $b^5 \not\equiv d^5$. In this case a and c must be distinct. By $(a - c)(a + c) = d^5 - b^5$, the value of $a - c$ uniquely determines $a + c$ and thus a and c as well. Hence, there are $p - 1$ suitable pairs (a, c).

Thus, for each of the k pairs (b, d) with $b^5 \equiv d^5$ there are $2p - 1$ pairs (a, c), and for each of the other $p^2 - k$ pairs (b, d) there are $p - 1$ pairs (a, c). Hence,

$$N = k(2p-1) + (p^2 - k)(p-1) = p^2(p-1) + kp \le p^2(p-1) + (5p-4)p = p(p^2 + 4p - 4). \quad \square$$

To prove the statement of the problem, suppose that $S_r = \emptyset$ for some $r \in \mathcal{P}$; obviously $r \not\equiv 0$. Let $T = \big\{x^{10} \colon x \in \mathcal{P} \setminus \{0\}\big\}$ be the set of nonzero 10th powers modulo p. Since each residue class is the 10th power of at most 10 elements in $\mathcal{P}$, we have $|T| \ge \frac{p-1}{10} \ge 4$ by $p > 100$.

For every $t \in T$, we have $S_{tr} = \emptyset$. Indeed, if $(x, y) \in S_{tr}$ and $t \equiv z^{10}$ then

$$(z^{-5}x)^2 + (z^{-2}y)^5 \equiv t^{-1}(x^2 + y^5) \equiv r,$$

so $(z^{-5}x, z^{-2}y) \in S_r$. So, there are at least $\frac{p-1}{10} \ge 4$ empty sets among $S_1, \ldots, S_{p-1}$, and there are at most $p - 4$ nonzero values among $s_0, s_2, \ldots, s_{p-1}$. Then by the AM-QM inequality we obtain

$$N = \sum_{r \in \mathcal{P} \setminus rT} s_r^2 \ge \frac{1}{p-4} \left(\sum_{r \in \mathcal{P} \setminus rT} s_r \right)^2 = \frac{|\mathcal{P} \times \mathcal{P}|^2}{p-4} = \frac{p^4}{p-4} > p(p^2 + 4p - 4),$$

which is impossible by the lemma.

Solution 2. If $5 \nmid p-1$, then all modulo p residue classes are complete fifth powers and the statement is trivial. So assume that $p = 10k+1$ where $k \geq 10$. Let g be a primitive root modulo p.

We will use the following facts:

(F1) If some residue class x is not quadratic then $x^{(p-1)/2} \equiv -1 \pmod{p}$.

(F2) For every integer d, as a simple corollary of the summation formula for geometric progressions,

$$\sum_{i=0}^{2k-1} g^{5di} \equiv \begin{cases} 2k & \text{if } 2k \mid d \\ 0 & \text{if } 2k \nmid d \end{cases} \pmod{p}.$$

Suppose that, contrary to the statement, some modulo p residue class r cannot be expressed as a^2+b^5. Of course $r \not\equiv 0 \pmod{p}$. By (F1) we have $(r-b^5)^{(p-1)/2} = (r-b^5)^{5k} \equiv -1 \pmod{p}$ for all residue classes b.

For $t = 1, 2 \ldots, k-1$ consider the sums

$$S(t) = \sum_{i=0}^{2k-1} \left(r - g^{5i}\right)^{5k} g^{5ti}.$$

By the indirect assumption and (F2),

$$S(t) = \sum_{i=0}^{2k-1} \left(r - (g^i)^5\right)^{5k} g^{5ti} \equiv \sum_{i=0}^{2k-1} (-1) g^{5ti} \equiv -\sum_{i=0}^{2k-1} g^{5ti} \equiv 0 \pmod{p}$$

because $2k$ cannot divide t.

On the other hand, by the binomial theorem,

$$S(t) = \sum_{i=0}^{2k-1} \left(\sum_{j=0}^{5k} \binom{5k}{j} r^{5k-j} \left(-g^{5i}\right)^j \right) g^{5ti} = \sum_{j=0}^{5k} (-1)^j \binom{5k}{j} r^{5k-j} \left(\sum_{i=0}^{2k-1} g^{5(j+t)i} \right) \equiv$$

$$\equiv \sum_{j=0}^{5k} (-1)^j \binom{5k}{j} r^{5k-j} \begin{cases} 2k & \text{if } 2k \mid j+t \\ 0 & \text{if } 2k \nmid j+t \end{cases} \pmod{p}.$$

Since $1 \leq j+t < 6k$, the number $2k$ divides $j+t$ only for $j = 2k-t$ and $j = 4k-t$. Hence,

$$0 \equiv S(t) \equiv (-1)^t \left(\binom{5k}{2k-t} r^{3k+t} + \binom{5k}{4k-t} r^{k+t} \right) \cdot 2k \pmod{p},$$

$$\binom{5k}{2k-t} r^{2k} + \binom{5k}{4k-t} \equiv 0 \pmod{p}.$$

Taking this for $t = 1, 2$ and eliminating r, we get

$$\begin{aligned} 0 &\equiv \binom{5k}{2k-2} \left(\binom{5k}{2k-1} r^{2k} + \binom{5k}{4k-1} \right) - \binom{5k}{2k-1} \left(\binom{5k}{2k-2} r^{2k} + \binom{5k}{4k-2} \right) \\ &= \binom{5k}{2k-2} \binom{5k}{4k-1} - \binom{5k}{2k-1} \binom{5k}{4k-2} \\ &= \frac{(5k)!^2}{(2k-1)!(3k+2)!(4k-1)!(k+2)!} \Big((2k-1)(k+2) - (3k+2)(4k-1) \Big) \\ &= \frac{-(5k)!^2 \cdot 2k(5k+1)}{(2k-1)!(3k+2)!(4k-1)!(k+2)!} \pmod{p}. \end{aligned}$$

But in the last expression none of the numbers is divisible by $p = 10k+1$, a contradiction.

Comment 1. The argument in the second solution is valid whenever $k \geq 3$, that is for all primes $p = 10k + 1$ except $p = 11$. This is an exceptional case when the statement is not true; $r = 7$ cannot be expressed as desired.

Comment 2. The statement is true in a more general setting: for every positive integer n, for all sufficiently large p, each residue class modulo p can be expressed as $a^2 + b^n$. Choosing $t = 3$ would allow using the Cauchy-Davenport theorem (together with some analysis on the case of equality).

In the literature more general results are known. For instance, the statement easily follows from the *Hasse-Weil bound*.