IMO 2017
RIO DE JANEIRO - BRAZIL

58th International Mathematical Olympiad

Shortlisted Problems
(with solutions)

Shortlisted Problems
(with solutions)

58th International Mathematical Olympiad

Rio de Janeiro, 12–23 July 2017

Note of Confidentiality

Contributing Countries

The Organizing Committee and the Problem Selection Committee of IMO 2017 thank the following 51 countries for contributing 150 problem proposals:

Albania, Algeria, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Bulgaria, Cuba, Cyprus, Czech Republic, Denmark, Estonia, France, Georgia, Germany, Greece, Hong Kong, India, Iran, Ireland, Israel, Italy, Japan, Kazakhstan, Latvia, Lithuania, Luxembourg, Mexico, Montenegro, Morocco, Netherlands, Romania, Russia, Serbia, Singapore, Slovakia, Slovenia, South Africa, Sweden, Switzerland, Taiwan, Tajikistan, Tanzania, Thailand, Trinidad and Tobago, Turkey, Ukraine, United Kingdom, U.S.A.

Problem Selection Committee

Carlos Gustavo Tamm de Araújo Moreira (Gugu) (chairman),
Luciano Monteiro de Castro, Ilya I. Bogdanov, Géza Kós, Carlos Yuzo Shine,
Zhuo Qun (Alex) Song, Ralph Costa Teixeira, Eduardo Tengan

Problems

Algebra

A1. Let $a_1, a_2, \ldots, a_n, k$, and M be positive integers such that

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} = k \quad \text{and} \quad a_1 a_2 \ldots a_n = M.$$

If $M > 1$, prove that the polynomial

$$P(x) = M(x+1)^k - (x+a_1)(x+a_2)\cdots(x+a_n)$$

has no positive roots.

(Trinidad and Tobago)

A2. Let q be a real number. Gugu has a napkin with ten distinct real numbers written on it, and he writes the following three lines of real numbers on the blackboard:

- In the first line, Gugu writes down every number of the form $a - b$, where a and b are two (not necessarily distinct) numbers on his napkin.

- In the second line, Gugu writes down every number of the form qab, where a and b are two (not necessarily distinct) numbers from the *first line*.

- In the third line, Gugu writes down every number of the form $a^2 + b^2 - c^2 - d^2$, where a, b, c, d are four (not necessarily distinct) numbers from the *first line*.

Determine all values of q such that, regardless of the numbers on Gugu's napkin, every number in the second line is also a number in the third line.

(Austria)

A3. Let S be a finite set, and let $\mathcal{A}$ be the set of all functions from S to S. Let f be an element of $\mathcal{A}$, and let $T = f(S)$ be the image of S under f. Suppose that $f \circ g \circ f \neq g \circ f \circ g$ for every g in $\mathcal{A}$ with $g \neq f$. Show that $f(T) = T$.

(India)

A4. A sequence of real numbers $a_1, a_2, \ldots$ satisfies the relation

$$a_n = -\max_{i+j=n}(a_i + a_j) \qquad \text{for all } n > 2017.$$

Prove that this sequence is bounded, i.e., there is a constant M such that $|a_n| \leq M$ for all positive integers n.

(Russia)

A5. An integer $n \geqslant 3$ is given. We call an n-tuple of real numbers $(x_1, x_2, \ldots, x_n)$ *Shiny* if for each permutation $y_1, y_2, \ldots, y_n$ of these numbers we have

$$\sum_{i=1}^{n-1} y_i y_{i+1} = y_1 y_2 + y_2 y_3 + y_3 y_4 + \cdots + y_{n-1} y_n \geqslant -1.$$

Find the largest constant $K = K(n)$ such that

$$\sum_{1 \leqslant i < j \leqslant n} x_i x_j \geqslant K$$

holds for every Shiny n-tuple $(x_1, x_2, \ldots, x_n)$.

(Serbia)

A6. Find all functions $f \colon \mathbb{R} \to \mathbb{R}$ such that

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

for all $x, y \in \mathbb{R}$.

(Albania)

A7. Let $a_0, a_1, a_2, \ldots$ be a sequence of integers and $b_0, b_1, b_2, \ldots$ be a sequence of *positive* integers such that $a_0 = 0, a_1 = 1$, and

$$a_{n+1} = \begin{cases} a_n b_n + a_{n-1}, & \text{if } b_{n-1} = 1 \\ a_n b_n - a_{n-1}, & \text{if } b_{n-1} > 1 \end{cases} \qquad \text{for } n = 1, 2, \ldots.$$

Prove that at least one of the two numbers a_{2017} and a_{2018} must be greater than or equal to 2017.

(Australia)

A8. Assume that a function $f \colon \mathbb{R} \to \mathbb{R}$ satisfies the following condition:

For every $x, y \in \mathbb{R}$ such that $\big(f(x) + y\big)\big(f(y) + x\big) > 0$, we have $f(x) + y = f(y) + x$.

Prove that $f(x) + y \leqslant f(y) + x$ whenever $x > y$.

(Netherlands)

Combinatorics

C1. A rectangle $\mathcal{R}$ with odd integer side lengths is divided into small rectangles with integer side lengths. Prove that there is at least one among the small rectangles whose distances from the four sides of $\mathcal{R}$ are either all odd or all even.

(Singapore)

C2. Let n be a positive integer. Define a *chameleon* to be any sequence of $3n$ letters, with exactly n occurrences of each of the letters a, b, and c. Define a *swap* to be the transposition of two adjacent letters in a chameleon. Prove that for any chameleon X, there exists a chameleon Y such that X cannot be changed to Y using fewer than $3n^2/2$ swaps.

(Australia)

C3. Sir Alex plays the following game on a row of 9 cells. Initially, all cells are empty. In each move, Sir Alex is allowed to perform exactly one of the following two operations:

(1) Choose any number of the form 2^j, where j is a non-negative integer, and put it into an empty cell.

(2) Choose two (not necessarily adjacent) cells with the same number in them; denote that number by 2^j. Replace the number in one of the cells with 2^{j+1} and erase the number in the other cell.

At the end of the game, one cell contains the number 2^n, where n is a given positive integer, while the other cells are empty. Determine the maximum number of moves that Sir Alex could have made, in terms of n.

(Thailand)

C4. Let $N \geqslant 2$ be an integer. $N(N+1)$ soccer players, no two of the same height, stand in a row in some order. Coach Ralph wants to remove $N(N-1)$ people from this row so that in the remaining row of $2N$ players, no one stands between the two tallest ones, no one stands between the third and the fourth tallest ones, ..., and finally no one stands between the two shortest ones. Show that this is always possible.

(Russia)

C5. A hunter and an invisible rabbit play a game in the Euclidean plane. The hunter's starting point H_0 coincides with the rabbit's starting point R_0. In the nth round of the game ($n \geqslant 1$), the following happens.

(1) First the invisible rabbit moves secretly and unobserved from its current point R_{n-1} to some new point R_n with $R_{n-1}R_n = 1$.

(2) The hunter has a tracking device (e.g. dog) that returns an approximate position R'_n of the rabbit, so that $R_nR'_n \leqslant 1$.

(3) The hunter then visibly moves from point H_{n-1} to a new point H_n with $H_{n-1}H_n = 1$.

Is there a strategy for the hunter that guarantees that after 10^9 such rounds the distance between the hunter and the rabbit is below 100?

(Austria)

C6. Let $n > 1$ be an integer. An $n \times n \times n$ cube is composed of n^3 unit cubes. Each unit cube is painted with one color. For each $n \times n \times 1$ box consisting of n^2 unit cubes (of any of the three possible orientations), we consider the set of the colors present in that box (each color is listed only once). This way, we get $3n$ sets of colors, split into three groups according to the orientation. It happens that for every set in any group, the same set appears in both of the other groups. Determine, in terms of n, the maximal possible number of colors that are present.

(Russia)

C7. For any finite sets X and Y of positive integers, denote by $f_X(k)$ the kth smallest positive integer not in X, and let

$$X * Y = X \cup \{f_X(y) \colon y \in Y\}.$$

Let A be a set of $a > 0$ positive integers, and let B be a set of $b > 0$ positive integers. Prove that if $A * B = B * A$, then

$$\underbrace{A * (A * \cdots * (A * (A * A)) \ldots)}_{A \text{ appears } b \text{ times}} = \underbrace{B * (B * \cdots * (B * (B * B)) \ldots)}_{B \text{ appears } a \text{ times}}.$$

(U.S.A.)

C8. Let n be a given positive integer. In the Cartesian plane, each lattice point with nonnegative coordinates initially contains a butterfly, and there are no other butterflies. The *neighborhood* of a lattice point c consists of all lattice points within the axis-aligned $(2n+1) \times (2n+1)$ square centered at c, apart from c itself. We call a butterfly *lonely, crowded,* or *comfortable*, depending on whether the number of butterflies in its neighborhood N is respectively less than, greater than, or equal to half of the number of lattice points in N.

Every minute, all lonely butterflies fly away simultaneously. This process goes on for as long as there are any lonely butterflies. Assuming that the process eventually stops, determine the number of comfortable butterflies at the final state.

(Bulgaria)

Geometry

G1. Let $ABCDE$ be a convex pentagon such that $AB = BC = CD$, $\angle EAB = \angle BCD$, and $\angle EDC = \angle CBA$. Prove that the perpendicular line from E to BC and the line segments AC and BD are concurrent.

(Italy)

G2. Let R and S be distinct points on circle Ω, and let t denote the tangent line to Ω at R. Point R' is the reflection of R with respect to S. A point I is chosen on the smaller arc RS of Ω so that the circumcircle Γ of triangle ISR' intersects t at two different points. Denote by A the common point of Γ and t that is closest to R. Line AI meets Ω again at J. Show that JR' is tangent to Γ.

(Luxembourg)

G3. Let O be the circumcenter of an acute scalene triangle ABC. Line OA intersects the altitudes of ABC through B and C at P and Q, respectively. The altitudes meet at H. Prove that the circumcenter of triangle PQH lies on a median of triangle ABC.

(Ukraine)

G4. In triangle ABC, let ω be the excircle opposite A. Let D, E, and F be the points where ω is tangent to lines BC, CA, and AB, respectively. The circle AEF intersects line BC at P and Q. Let M be the midpoint of AD. Prove that the circle MPQ is tangent to ω.

(Denmark)

G5. Let $ABCC_1B_1A_1$ be a convex hexagon such that $AB = BC$, and suppose that the line segments AA_1, BB_1, and CC_1 have the same perpendicular bisector. Let the diagonals AC_1 and A_1C meet at D, and denote by ω the circle ABC. Let ω intersect the circle A_1BC_1 again at $E \neq B$. Prove that the lines BB_1 and DE intersect on ω.

(Ukraine)

G6. Let $n \geqslant 3$ be an integer. Two regular n-gons $\mathcal{A}$ and $\mathcal{B}$ are given in the plane. Prove that the vertices of $\mathcal{A}$ that lie inside $\mathcal{B}$ or on its boundary are consecutive.

(That is, prove that there exists a line separating those vertices of $\mathcal{A}$ that lie inside $\mathcal{B}$ or on its boundary from the other vertices of $\mathcal{A}$.)

(Czech Republic)

G7. A convex quadrilateral $ABCD$ has an inscribed circle with center I. Let I_a, I_b, I_c, and I_d be the incenters of the triangles DAB, ABC, BCD, and CDA, respectively. Suppose that the common external tangents of the circles AI_bI_d and CI_bI_d meet at X, and the common external tangents of the circles BI_aI_c and DI_aI_c meet at Y. Prove that $\angle XIY = 90°$.

(Kazakhstan)

G8. There are 2017 mutually external circles drawn on a blackboard, such that no two are tangent and no three share a common tangent. A *tangent segment* is a line segment that is a common tangent to two circles, starting at one tangent point and ending at the other one. Luciano is drawing tangent segments on the blackboard, one at a time, so that no tangent segment intersects any other circles or previously drawn tangent segments. Luciano keeps drawing tangent segments until no more can be drawn. Find all possible numbers of tangent segments when he stops drawing.

(Australia)

This page is intentionally left blank

Number Theory

N1. The sequence $a_0, a_1, a_2, \ldots$ of positive integers satisfies

$$a_{n+1} = \begin{cases} \sqrt{a_n}, & \text{if } \sqrt{a_n} \text{ is an integer} \\ a_n + 3, & \text{otherwise} \end{cases} \qquad \text{for every } n \geqslant 0.$$

Determine all values of $a_0 > 1$ for which there is at least one number a such that $a_n = a$ for infinitely many values of n.

(South Africa)

N2. Let $p \geqslant 2$ be a prime number. Eduardo and Fernando play the following game making moves alternately: in each move, the current player chooses an index i in the set $\{0, 1, \ldots, p-1\}$ that was not chosen before by either of the two players and then chooses an element a_i of the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Eduardo has the first move. The game ends after all the indices $i \in \{0, 1, \ldots, p-1\}$ have been chosen. Then the following number is computed:

$$M = a_0 + 10 \cdot a_1 + \cdots + 10^{p-1} \cdot a_{p-1} = \sum_{j=0}^{p-1} a_j \cdot 10^j.$$

The goal of Eduardo is to make the number M divisible by p, and the goal of Fernando is to prevent this.

Prove that Eduardo has a winning strategy.

(Morocco)

N3. Determine all integers $n \geqslant 2$ with the following property: for any integers $a_1, a_2, \ldots, a_n$ whose sum is not divisible by n, there exists an index $1 \leqslant i \leqslant n$ such that none of the numbers

$$a_i, a_i + a_{i+1}, \ldots, a_i + a_{i+1} + \cdots + a_{i+n-1}$$

is divisible by n. (We let $a_i = a_{i-n}$ when $i > n$.)

(Thailand)

N4. Call a rational number *short* if it has finitely many digits in its decimal expansion. For a positive integer m, we say that a positive integer t is *m-tastic* if there exists a number $c \in \{1, 2, 3, \ldots, 2017\}$ such that $\dfrac{10^t - 1}{c \cdot m}$ is short, and such that $\dfrac{10^k - 1}{c \cdot m}$ is not short for any $1 \leqslant k < t$. Let $S(m)$ be the set of m-tastic numbers. Consider $S(m)$ for $m = 1, 2, \ldots$. What is the maximum number of elements in $S(m)$?

(Turkey)

N5. Find all pairs (p, q) of prime numbers with $p > q$ for which the number

$$\frac{(p+q)^{p+q}(p-q)^{p-q} - 1}{(p+q)^{p-q}(p-q)^{p+q} - 1}$$

is an integer.

(Japan)

N6. Find the smallest positive integer n, or show that no such n exists, with the following property: there are infinitely many distinct n-tuples of positive rational numbers $(a_1, a_2, \ldots, a_n)$ such that both

$$a_1 + a_2 + \cdots + a_n \qquad \text{and} \qquad \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}$$

are integers.

(Singapore)

N7. Say that an ordered pair (x, y) of integers is an *irreducible lattice point* if x and y are relatively prime. For any finite set S of irreducible lattice points, show that there is a homogenous polynomial in two variables, $f(x, y)$, with integer coefficients, of degree at least 1, such that $f(x, y) = 1$ for each (x, y) in the set S.

Note: A homogenous polynomial of degree n is any nonzero polynomial of the form

$$f(x, y) = a_0 x^n + a_1 x^{n-1} y + a_2 x^{n-2} y^2 + \cdots + a_{n-1} x y^{n-1} + a_n y^n.$$

(U.S.A.)

N8. Let p be an odd prime number and $\mathbb{Z}_{>0}$ be the set of positive integers. Suppose that a function $f \colon \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \to \{0, 1\}$ satisfies the following properties:

- $f(1, 1) = 0$;

- $f(a, b) + f(b, a) = 1$ for any pair of relatively prime positive integers (a, b) not both equal to 1;

- $f(a + b, b) = f(a, b)$ for any pair of relatively prime positive integers (a, b).

Prove that

$$\sum_{n=1}^{p-1} f(n^2, p) \geqslant \sqrt{2p} - 2.$$

(Italy)

Solutions

Algebra

A1. Let $a_1, a_2, \ldots, a_n, k$, and M be positive integers such that

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} = k \quad \text{and} \quad a_1 a_2 \ldots a_n = M.$$

If $M > 1$, prove that the polynomial

$$P(x) = M(x+1)^k - (x+a_1)(x+a_2)\cdots(x+a_n)$$

has no positive roots.

(Trinidad and Tobago)

Solution 1. We first prove that, for $x > 0$,

$$a_i(x+1)^{1/a_i} \leqslant x + a_i, \tag{1}$$

with equality if and only if $a_i = 1$. It is clear that equality occurs if $a_i = 1$.

If $a_i > 1$, the AM–GM inequality applied to a single copy of $x + 1$ and $a_i - 1$ copies of 1 yields

$$\frac{(x+1) + \overbrace{1 + 1 + \cdots + 1}^{a_i - 1 \text{ ones}}}{a_i} \geqslant \sqrt[a_i]{(x+1) \cdot 1^{a_i - 1}} \implies a_i(x+1)^{1/a_i} \leqslant x + a_i.$$

Since $x + 1 > 1$, the inequality is strict for $a_i > 1$.

Multiplying the inequalities (1) for $i = 1, 2, \ldots, n$ yields

$$\prod_{i=1}^{n} a_i(x+1)^{1/a_i} \leqslant \prod_{i=1}^{n}(x+a_i) \iff M(x+1)^{\sum_{i=1}^{n} 1/a_i} - \prod_{i=1}^{n}(x+a_i) \leqslant 0 \iff P(x) \leqslant 0$$

with equality iff $a_i = 1$ for all $i \in \{1, 2, \ldots, n\}$. But this implies $M = 1$, which is not possible. Hence $P(x) < 0$ for all $x \in \mathbb{R}^+$, and P has no positive roots.

Comment 1. Inequality (1) can be obtained in several ways. For instance, we may also use the binomial theorem: since $a_i \geqslant 1$,

$$\left(1 + \frac{x}{a_i}\right)^{a_i} = \sum_{j=0}^{a_i} \binom{a_i}{j} \left(\frac{x}{a_i}\right)^j \geqslant \binom{a_i}{0} + \binom{a_i}{1} \cdot \frac{x}{a_i} = 1 + x.$$

Both proofs of (1) mimic proofs to Bernoulli's inequality for a positive integer exponent a_i; we can use this inequality directly:

$$\left(1 + \frac{x}{a_i}\right)^{a_i} \geqslant 1 + a_i \cdot \frac{x}{a_i} = 1 + x,$$

and so

$$x + a_i = a_i \left(1 + \frac{x}{a_i}\right) \geqslant a_i(1+x)^{1/a_i},$$

or its (reversed) formulation, with exponent $1/a_i \leqslant 1$:

$$(1+x)^{1/a_i} \leqslant 1 + \frac{1}{a_i} \cdot x = \frac{x + a_i}{a_i} \implies a_i(1+x)^{1/a_i} \leqslant x + a_i.$$

Solution 2. We will prove that, in fact, all coefficients of the polynomial $P(x)$ are non-positive, and at least one of them is negative, which implies that $P(x) < 0$ for $x > 0$.

Indeed, since $a_j \geqslant 1$ for all j and $a_j > 1$ for some j (since $a_1 a_2 \ldots a_n = M > 1$), we have $k = \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} < n$, so the coefficient of x^n in $P(x)$ is $-1 < 0$. Moreover, the coefficient of x^r in $P(x)$ is negative for $k < r \leqslant n = \deg(P)$.

For $0 \leqslant r \leqslant k$, the coefficient of x^r in $P(x)$ is

$$M \cdot \binom{k}{r} - \sum_{1 \leqslant i_1 < i_2 < \cdots < i_{n-r} \leqslant n} a_{i_1} a_{i_2} \cdots a_{i_{n-r}} = a_1 a_2 \cdots a_n \cdot \binom{k}{r} - \sum_{1 \leqslant i_1 < i_2 < \cdots < i_{n-r} \leqslant n} a_{i_1} a_{i_2} \cdots a_{i_{n-r}},$$

which is non-positive iff

$$\binom{k}{r} \leqslant \sum_{1 \leqslant j_1 < j_2 < \cdots < j_r \leqslant n} \frac{1}{a_{j_1} a_{j_2} \cdots a_{j_r}}. \tag{2}$$

We will prove (2) by induction on r. For $r = 0$ it is an equality because the constant term of $P(x)$ is $P(0) = 0$, and if $r = 1$, (2) becomes $k = \sum_{i=1}^{n} \frac{1}{a_i}$. For $r > 1$, if (2) is true for a given $r < k$, we have

$$\binom{k}{r+1} = \frac{k-r}{r+1} \cdot \binom{k}{r} \leqslant \frac{k-r}{r+1} \cdot \sum_{1 \leqslant j_1 < j_2 < \cdots < j_r \leqslant n} \frac{1}{a_{j_1} a_{j_2} \cdots a_{j_r}},$$

and it suffices to prove that

$$\frac{k-r}{r+1} \cdot \sum_{1 \leqslant j_1 < j_2 < \cdots < j_r \leqslant n} \frac{1}{a_{j_1} a_{j_2} \cdots a_{j_r}} \leqslant \sum_{1 \leqslant j_1 < \cdots < j_r < j_{r+1} \leqslant n} \frac{1}{a_{j_1} a_{j_2} \cdots a_{j_r} a_{j_{r+1}}},$$

which is equivalent to

$$\left(\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} - r \right) \sum_{1 \leqslant j_1 < j_2 < \cdots < j_r \leqslant n} \frac{1}{a_{j_1} a_{j_2} \cdots a_{j_r}} \leqslant (r+1) \sum_{1 \leqslant j_1 < \cdots < j_r < j_{r+1} \leqslant n} \frac{1}{a_{j_1} a_{j_2} \cdots a_{j_r} a_{j_{r+1}}}.$$

Since there are $r + 1$ ways to choose a fraction $\frac{1}{a_{j_i}}$ from $\frac{1}{a_{j_1} a_{j_2} \cdots a_{j_r} a_{j_{r+1}}}$ to factor out, every term $\frac{1}{a_{j_1} a_{j_2} \cdots a_{j_r} a_{j_{r+1}}}$ in the right hand side appears exactly $r + 1$ times in the product

$$\left(\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} \right) \sum_{1 \leqslant j_1 < j_2 < \cdots < j_r \leqslant n} \frac{1}{a_{j_1} a_{j_2} \cdots a_{j_r}}.$$

Hence all terms in the right hand side cancel out.

The remaining terms in the left hand side can be grouped in sums of the type

$$\frac{1}{a_{j_1}^2 a_{j_2} \cdots a_{j_r}} + \frac{1}{a_{j_1} a_{j_2}^2 \cdots a_{j_r}} + \cdots + \frac{1}{a_{j_1} a_{j_2} \cdots a_{j_r}^2} - \frac{r}{a_{j_1} a_{j_2} \cdots a_{j_r}}$$

$$= \frac{1}{a_{j_1} a_{j_2} \cdots a_{j_r}} \left(\frac{1}{a_{j_1}} + \frac{1}{a_{j_2}} + \cdots + \frac{1}{a_{j_r}} - r \right),$$

which are all non-positive because $a_i \geqslant 1 \implies \frac{1}{a_i} \leqslant 1$, $i = 1, 2, \ldots, n$.

Comment 2. The result is valid for any real numbers a_i, $i = 1, 2, \ldots, n$ with $a_i \geqslant 1$ and product M greater than 1. A variation of Solution 1, namely using *weighted* AM–GM (or the Bernoulli inequality for real exponents), actually proves that $P(x) < 0$ for $x > -1$ and $x \neq 0$.

A 2.   Let q be a real number. Gugu has a napkin with ten distinct real numbers written on it, and he writes the following three lines of real numbers on the blackboard:

- In the first line, Gugu writes down every number of the form $a - b$, where a and b are two (not necessarily distinct) numbers on his napkin.

- In the second line, Gugu writes down every number of the form qab, where a and b are two (not necessarily distinct) numbers from the *first line*.

- In the third line, Gugu writes down every number of the form $a^2 + b^2 - c^2 - d^2$, where a, b, c, d are four (not necessarily distinct) numbers from the *first line*.

Determine all values of q such that, regardless of the numbers on Gugu's napkin, every number in the second line is also a number in the third line.

(Austria)

Answer: $-2, 0, 2$.

Solution 1.   Call a number q *good* if every number in the second line appears in the third line unconditionally. We first show that the numbers 0 and ± 2 are good. The third line necessarily contains 0, so 0 is good. For any two numbers a, b in the first line, write $a = x - y$ and $b = u - v$, where x, y, u, v are (not necessarily distinct) numbers on the napkin. We may now write

$$2ab = 2(x - y)(u - v) = (x - v)^2 + (y - u)^2 - (x - u)^2 - (y - v)^2,$$

which shows that 2 is good. By negating both sides of the above equation, we also see that -2 is good.

We now show that $-2, 0,$ and 2 are the only good numbers. Assume for sake of contradiction that q is a good number, where $q \notin \{-2, 0, 2\}$. We now consider some particular choices of numbers on Gugu's napkin to arrive at a contradiction.

Assume that the napkin contains the integers $1, 2, \ldots, 10$. Then, the first line contains the integers $-9, -8, \ldots, 9$. The second line then contains q and $81q$, so the third line must also contain both of them. But the third line only contains integers, so q must be an integer. Furthermore, the third line contains no number greater than $162 = 9^2 + 9^2 - 0^2 - 0^2$ or less than -162, so we must have $-162 \leqslant 81q \leqslant 162$. This shows that the only possibilities for q are ± 1.

Now assume that $q = \pm 1$. Let the napkin contain $0, 1, 4, 8, 12, 16, 20, 24, 28, 32$. The first line contains ± 1 and ± 4, so the second line contains ± 4. However, for every number a in the first line, $a \not\equiv 2 \pmod 4$, so we may conclude that $a^2 \equiv 0, 1 \pmod 8$. Consequently, every number in the third line must be congruent to $-2, -1, 0, 1, 2 \pmod 8$; in particular, ± 4 cannot be in the third line, which is a contradiction.

Solution 2.   Let q be a good number, as defined in the first solution, and define the polynomial $P(x_1, \ldots, x_{10})$ as

$$\prod_{i < j}(x_i - x_j) \prod_{a_i \in S}\big(q(x_1 - x_2)(x_3 - x_4) - (a_1 - a_2)^2 - (a_3 - a_4)^2 + (a_5 - a_6)^2 + (a_7 - a_8)^2\big),$$

where $S = \{x_1, \ldots, x_{10}\}$.

We claim that $P(x_1, \ldots, x_{10}) = 0$ for every choice of real numbers $(x_1, \ldots, x_{10})$. If any two of the x_i are equal, then $P(x_1, \ldots, x_{10}) = 0$ trivially. If no two are equal, assume that Gugu has those ten numbers $x_1, \ldots, x_{10}$ on his napkin. Then, the number $q(x_1 - x_2)(x_3 - x_4)$ is in the second line, so we must have some $a_1, \ldots, a_8$ so that

$$q(x_1 - x_2)(x_3 - x_4) - (a_1 - a_2)^2 - (a_3 - a_4)^2 + (a_5 - a_6)^2 + (a_7 - a_8)^2 = 0,$$

and hence $P(x_1, \ldots, x_{10}) = 0$.

Since every polynomial that evaluates to zero everywhere is the zero polynomial, and the product of two nonzero polynomials is necessarily nonzero, we may define F such that

$$F(x_1, \ldots, x_{10}) \equiv q(x_1 - x_2)(x_3 - x_4) - (a_1 - a_2)^2 - (a_3 - a_4)^2 + (a_5 - a_6)^2 + (a_7 - a_8)^2 \equiv 0 \ (1)$$

for some particular choice $a_i \in S$.

Each of the sets $\{a_1, a_2\}$, $\{a_3, a_4\}$, $\{a_5, a_6\}$, and $\{a_7, a_8\}$ is equal to at most one of the four sets $\{x_1, x_3\}, \{x_2, x_3\}, \{x_1, x_4\}$, and $\{x_2, x_4\}$. Thus, without loss of generality, we may assume that at most one of the sets $\{a_1, a_2\}$, $\{a_3, a_4\}$, $\{a_5, a_6\}$, and $\{a_7, a_8\}$ is equal to $\{x_1, x_3\}$. Let u_1, u_3, u_5, u_7 be the indicator functions for this equality of sets: that is, $u_i = 1$ if and only if $\{a_i, a_{i+1}\} = \{x_1, x_3\}$. By assumption, at least three of the u_i are equal to 0.

We now compute the coefficient of $x_1 x_3$ in F. It is equal to $q + 2(u_1 + u_3 - u_5 - u_7) = 0$, and since at least three of the u_i are zero, we must have that $q \in \{-2, 0, 2\}$, as desired.

A3.   Let S be a finite set, and let $\mathcal{A}$ be the set of all functions from S to S. Let f be an element of $\mathcal{A}$, and let $T = f(S)$ be the image of S under f. Suppose that $f \circ g \circ f \neq g \circ f \circ g$ for every g in $\mathcal{A}$ with $g \neq f$. Show that $f(T) = T$.

(India)

Solution. For $n \geqslant 1$, denote the n-th composition of f with itself by

$$f^n \stackrel{\text{def}}{=} \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}.$$

By hypothesis, if $g \in \mathcal{A}$ satisfies $f \circ g \circ f = g \circ f \circ g$, then $g = f$. A natural idea is to try to plug in $g = f^n$ for some n in the expression $f \circ g \circ f = g \circ f \circ g$ in order to get $f^n = f$, which solves the problem:

Claim. If there exists $n \geqslant 3$ such that $f^{n+2} = f^{2n+1}$, then the restriction $f \colon T \to T$ of f to T is a bijection.

Proof. Indeed, by hypothesis, $f^{n+2} = f^{2n+1} \iff f \circ f^n \circ f = f^n \circ f \circ f^n \implies f^n = f$. Since $n - 2 \geqslant 1$, the image of f^{n-2} is contained in $T = f(S)$, hence f^{n-2} restricts to a function $f^{n-2} \colon T \to T$. This is the inverse of $f \colon T \to T$. In fact, given $t \in T$, say $t = f(s)$ with $s \in S$, we have

$$t = f(s) = f^n(s) = f^{n-2}(f(t)) = f(f^{n-2}(t)), \qquad \text{i.e.,} \qquad f^{n-2} \circ f = f \circ f^{n-2} = \text{id} \ \text{ on } T$$

(here id stands for the identity function). Hence, the restriction $f \colon T \to T$ of f to T is bijective with inverse given by $f^{n-2} \colon T \to T$. $\square$

It remains to show that n as in the claim exists. For that, define

$$S_m \stackrel{\text{def}}{=} f^m(S) \qquad\qquad (S_m \text{ is image of } f^m)$$

Clearly the image of f^{m+1} is contained in the image of f^m, i.e., there is a descending chain of subsets of S

$$S \supseteq S_1 \supseteq S_2 \supseteq S_3 \supseteq S_4 \supseteq \cdots,$$

which must eventually stabilise since S is finite, i.e., there is a $k \geqslant 1$ such that

$$S_k = S_{k+1} = S_{k+2} = S_{k+3} = \cdots \stackrel{\text{def}}{=} S_\infty.$$

Hence f restricts to a *surjective* function $f \colon S_\infty \to S_\infty$, which is also *bijective* since $S_\infty \subseteq S$ is finite. To sum up, $f \colon S_\infty \to S_\infty$ is a permutation of the elements of the finite set S_∞, hence there exists an integer $r \geqslant 1$ such that $f^r = \text{id}$ on S_∞ (for example, we may choose $r = |S_\infty|!$). In other words,

$$f^{m+r} = f^m \text{ on } S \text{ for all } m \geqslant k. \tag{$*$}$$

Clearly, $(*)$ also implies that $f^{m+tr} = f^m$ for all integers $t \geqslant 1$ and $m \geqslant k$. So, to find n as in the claim and finish the problem, it is enough to choose m and t in order to ensure that there exists $n \geqslant 3$ satisfying

$$\begin{cases} 2n + 1 = m + tr \\ n + 2 = m \end{cases} \iff \begin{cases} m = 3 + tr \\ n = m - 2. \end{cases}$$

This can be clearly done by choosing m large enough with $m \equiv 3 \pmod{r}$. For instance, we may take $n = 2kr + 1$, so that

$$f^{n+2} = f^{2kr+3} = f^{4kr+3} = f^{2n+1}$$

where the middle equality follows by $(*)$ since $2kr + 3 \geqslant k$.

A4. A sequence of real numbers $a_1, a_2, \ldots$ satisfies the relation

$$a_n = -\max_{i+j=n}(a_i + a_j) \qquad \text{for all } n > 2017.$$

Prove that this sequence is bounded, i.e., there is a constant M such that $|a_n| \leqslant M$ for all positive integers n.

(Russia)

Solution 1. Set $D = 2017$. Denote

$$M_n = \max_{k<n} a_k \qquad \text{and} \qquad m_n = -\min_{k<n} a_k = \max_{k<n}(-a_k).$$

Clearly, the sequences (m_n) and (M_n) are nondecreasing. We need to prove that both are bounded.

Consider an arbitrary $n > D$; our first aim is to bound a_n in terms of m_n and M_n.

(i) There exist indices p and q such that $a_n = -(a_p + a_q)$ and $p + q = n$. Since $a_p, a_q \leqslant M_n$, we have $a_n \geqslant -2M_n$.

(ii) On the other hand, choose an index $k < n$ such that $a_k = M_n$. Then, we have

$$a_n = -\max_{\ell<n}(a_{n-\ell} + a_\ell) \leqslant -(a_{n-k} + a_k) = -a_{n-k} - M_n \leqslant m_n - M_n.$$

Summarizing (i) and (ii), we get

$$-2M_n \leqslant a_n \leqslant m_n - M_n,$$

whence

$$m_n \leqslant m_{n+1} \leqslant \max\{m_n, 2M_n\} \quad \text{and} \quad M_n \leqslant M_{n+1} \leqslant \max\{M_n, m_n - M_n\}. \tag{1}$$

Now, say that an index $n > D$ is *lucky* if $m_n \leqslant 2M_n$. Two cases are possible.

Case 1. Assume that there exists a lucky index n. In this case, (1) yields $m_{n+1} \leqslant 2M_n$ and $M_n \leqslant M_{n+1} \leqslant M_n$. Therefore, $M_{n+1} = M_n$ and $m_{n+1} \leqslant 2M_n = 2M_{n+1}$. So, the index $n + 1$ is also lucky, and $M_{n+1} = M_n$. Applying the same arguments repeatedly, we obtain that all indices $k > n$ are lucky (i.e., $m_k \leqslant 2M_k$ for all these indices), and $M_k = M_n$ for all such indices. Thus, all of the m_k and M_k are bounded by $2M_n$.

Case 2. Assume now that there is no lucky index, i.e., $2M_n < m_n$ for all $n > D$. Then (1) shows that for all $n > D$ we have $m_n \leqslant m_{n+1} \leqslant m_n$, so $m_n = m_{D+1}$ for all $n > D$. Since $M_n < m_n/2$ for all such indices, all of the m_n and M_n are bounded by m_{D+1}.

Thus, in both cases the sequences (m_n) and (M_n) are bounded, as desired.

Solution 2. As in the previous solution, let $D = 2017$. If the sequence is bounded above, say, by Q, then we have that $a_n \geqslant \min\{a_1, \ldots, a_D, -2Q\}$ for all n, so the sequence is bounded. Assume for sake of contradiction that the sequence is not bounded above. Let $\ell = \min\{a_1, \ldots, a_D\}$, and $L = \max\{a_1, \ldots, a_D\}$. Call an index n *good* if the following criteria hold:

$$a_n > a_i \text{ for each } i < n, \quad a_n > -2\ell, \quad \text{and} \quad n > D \tag{2}$$

We first show that there must be some good index n. By assumption, we may take an index N such that $a_N > \max\{L, -2\ell\}$. Choose n minimally such that $a_n = \max\{a_1, a_2, \ldots, a_N\}$. Now, the first condition in (2) is satisfied because of the minimality of n, and the second and third conditions are satisfied because $a_n \geqslant a_N > L, -2\ell$, and $L \geqslant a_i$ for every i such that $1 \leqslant i \leqslant D$.

Let n be a good index. We derive a contradiction. We have that

$$a_n + a_u + a_v \leqslant 0, \tag{3}$$

whenever $u + v = n$.

We define the index u to maximize a_u over $1 \leqslant u \leqslant n - 1$, and let $v = n - u$. Then, we note that $a_u \geqslant a_v$ by the maximality of a_u.

Assume first that $v \leqslant D$. Then, we have that

$$a_N + 2\ell \leqslant 0,$$

because $a_u \geqslant a_v \geqslant \ell$. But this contradicts our assumption that $a_n > -2\ell$ in the second criteria of (2).

Now assume that $v > D$. Then, there exist some indices w_1, w_2 summing up to v such that

$$a_v + a_{w_1} + a_{w_2} = 0.$$

But combining this with (3), we have

$$a_n + a_u \leqslant a_{w_1} + a_{w_2}.$$

Because $a_n > a_u$, we have that $\max\{a_{w_1}, a_{w_2}\} > a_u$. But since each of the w_i is less than v, this contradicts the maximality of a_u.

Comment 1. We present two harder versions of this problem below.

Version 1. Let $a_1, a_2, \ldots$ be a sequence of numbers that satisfies the relation

$$a_n = - \max_{i+j+k=n} (a_i + a_j + a_k) \qquad \text{for all } n > 2017.$$

Then, this sequence is bounded.

Proof. Set $D = 2017$. Denote

$$M_n = \max_{k<n} a_k \qquad \text{and} \qquad m_n = -\min_{k<n} a_k = \max_{k<n}(-a_k).$$

Clearly, the sequences (m_n) and (M_n) are nondecreasing. We need to prove that both are bounded.

Consider an arbitrary $n > 2D$; our first aim is to bound a_n in terms of m_i and M_i. Set $k = \lfloor n/2 \rfloor$.
(i) Choose indices p, q, and r such that $a_n = -(a_p + a_q + a_r)$ and $p + q + r = n$. Without loss of generality, $p \geqslant q \geqslant r$.

Assume that $p \geqslant k + 1(> D)$; then $p > q + r$. Hence

$$-a_p = \max_{i_1+i_2+i_3=p} (a_{i_1} + a_{i_2} + a_{i_3}) \geqslant a_q + a_r + a_{p-q-r},$$

and therefore $a_n = -(a_p + a_q + a_r) \geqslant (a_q + a_r + a_{p-q-r}) - a_q - a_r = a_{p-q-r} \geqslant -m_n$.

Otherwise, we have $k \geqslant p \geqslant q \geqslant r$. Since $n < 3k$, we have $r < k$. Then $a_p, a_q \leqslant M_{k+1}$ and $a_r \leqslant M_k$, whence $a_n \geqslant -2M_{k+1} - M_k$.

Thus, in any case $a_n \geqslant -\max\{m_n, 2M_{k+1} + M_k\}$.
(ii) On the other hand, choose $p \leqslant k$ and $q \leqslant k-1$ such that $a_p = M_{k+1}$ and $a_q = M_k$. Then $p+q < n$, so $a_n \leqslant -(a_p + a_q + a_{n-p-q}) = -a_{n-p-q} - M_{k+1} - M_k \leqslant m_n - M_{k+1} - M_k$.

To summarize,

$$-\max\{m_n, 2M_{k+1} + M_k\} \leqslant a_n \leqslant m_n - M_{k+1} - M_k,$$

whence

$$m_n \leqslant m_{n+1} \leqslant \max\{m_n, 2M_{k+1} + M_k\} \quad \text{and} \quad M_n \leqslant M_{n+1} \leqslant \max\{M_n, m_n - M_{k+1} - M_k\}. \tag{4}$$

Now, say that an index $n > 2D$ is *lucky* if $m_n \leqslant 2M_{\lfloor n/2 \rfloor + 1} + M_{\lfloor n/2 \rfloor}$. Two cases are possible.

Case 1. Assume that there exists a lucky index n; set $k = \lfloor n/2 \rfloor$. In this case, (4) yields $m_{n+1} \leqslant 2M_{k+1} + M_k$ and $M_n \leqslant M_{n+1} \leqslant M_n$ (the last relation holds, since $m_n - M_{k+1} - M_k \leqslant (2M_{k+1} + M_k) - M_{k+1} - M_k = M_{k+1} \leqslant M_n$). Therefore, $M_{n+1} = M_n$ and $m_{n+1} \leqslant 2M_{k+1} + M_k$; the last relation shows that the index $n + 1$ is also lucky.

Thus, all indices $N > n$ are lucky, and $M_N = M_n \geqslant m_N/3$, whence all the m_N and M_N are bounded by $3M_n$.

Case 2. Conversely, assume that there is no lucky index, i.e., $2M_{\lfloor n/2 \rfloor + 1} + M_{\lfloor n/2 \rfloor} < m_n$ for all $n > 2D$. Then (4) shows that for all $n > 2D$ we have $m_n \leqslant m_{n+1} \leqslant m_n$, i.e., $m_N = m_{2D+1}$ for all $N > 2D$. Since $M_N < m_{2N+1}/3$ for all such indices, all the m_N and M_N are bounded by m_{2D+1}.

Thus, in both cases the sequences (m_n) and (M_n) are bounded, as desired. $\qquad\square$

Version 2. Let $a_1, a_2, \ldots$ be a sequence of numbers that satisfies the relation

$$a_n = - \max_{i_1 + \cdots + i_k = n} (a_{i_1} + \cdots + a_{i_k}) \qquad \text{for all } n > 2017.$$

Then, this sequence is bounded.

Proof. As in the solutions above, let $D = 2017$. If the sequence is bounded above, say, by Q, then we have that $a_n \geqslant \min\{a_1, \ldots, a_D, -kQ\}$ for all n, so the sequence is bounded. Assume for sake of contradiction that the sequence is not bounded above. Let $\ell = \min\{a_1, \ldots, a_D\}$, and $L = \max\{a_1, \ldots, a_D\}$. Call an index n *good* if the following criteria hold:

$$a_n > a_i \text{ for each } i < n, \quad a_n > -k\ell, \quad \text{and} \quad n > D \tag{5}$$

We first show that there must be some good index n. By assumption, we may take an index N such that $a_N > \max\{L, -k\ell\}$. Choose n minimally such that $a_n = \max\{a_1, a_2, \ldots, a_N\}$. Now, the first condition is satisfied because of the minimality of n, and the second and third conditions are satisfied because $a_n \geqslant a_N > L, -k\ell$, and $L \geqslant a_i$ for every i such that $1 \leqslant i \leqslant D$.

Let n be a good index. We derive a contradiction. We have that

$$a_n + a_{v_1} + \cdots + a_{v_k} \leqslant 0, \tag{6}$$

whenever $v_1 + \cdots + v_k = n$.

We define the sequence of indices $v_1, \ldots, v_{k-1}$ to greedily maximize a_{v_1}, then a_{v_2}, and so forth, selecting only from indices such that the equation $v_1 + \cdots + v_k = n$ can be satisfied by positive integers $v_1, \ldots, v_k$. More formally, we define them inductively so that the following criteria are satisfied by the v_i:

1. $1 \leqslant v_i \leqslant n - (k - i) - (v_1 + \cdots + v_{i-1})$.

2. a_{v_i} is maximal among all choices of v_i from the first criteria.

First of all, we note that for each i, the first criteria is always satisfiable by some v_i, because we are guaranteed that

$$v_{i-1} \leqslant n - (k - (i - 1)) - (v_1 + \cdots + v_{i-2}),$$

which implies

$$1 \leqslant n - (k - i) - (v_1 + \cdots + v_{i-1}).$$

Secondly, the sum $v_1 + \cdots + v_{k-1}$ is at most $n - 1$. Define $v_k = n - (v_1 + \cdots + v_{k-1})$. Then, (6) is satisfied by the v_i. We also note that $a_{v_i} \geqslant a_{v_j}$ for all $i < j$; otherwise, in the definition of v_i, we could have selected v_j instead.

Assume first that $v_k \leqslant D$. Then, from (6), we have that

$$a_n + k\ell \leqslant 0,$$

by using that $a_{v_1} \geqslant \cdots \geqslant a_{v_k} \geqslant \ell$. But this contradicts our assumption that $a_n > -k\ell$ in the second criteria of (5).

Now assume that $v_k > D$, and then we must have some indices $w_1, \ldots, w_k$ summing up to v_k such that

$$a_{v_k} + a_{w_1} + \cdots + a_{w_k} = 0.$$

But combining this with (6), we have

$$a_n + a_{v_1} + \cdots + a_{v_{k-1}} \leqslant a_{w_1} + \cdots + a_{w_k}.$$

Because $a_n > a_{v_1} \geqslant \cdots \geqslant a_{v_{k-1}}$, we have that $\max\{a_{w_1}, \ldots, a_{w_k}\} > a_{v_{k-1}}$. But since each of the w_i is less than v_k, in the definition of the v_{k-1} we could have chosen one of the w_i instead, which is a contradiction. $\square$

Comment 2. It seems that each sequence satisfying the condition in Version 2 is eventually periodic, at least when its terms are integers.

However, up to this moment, the Problem Selection Committee is not aware of a proof for this fact (even in the case $k = 2$).

A5. An integer $n \geqslant 3$ is given. We call an n-tuple of real numbers $(x_1, x_2, \ldots, x_n)$ *Shiny* if for each permutation $y_1, y_2, \ldots, y_n$ of these numbers we have

$$\sum_{i=1}^{n-1} y_i y_{i+1} = y_1 y_2 + y_2 y_3 + y_3 y_4 + \cdots + y_{n-1} y_n \geqslant -1.$$

Find the largest constant $K = K(n)$ such that

$$\sum_{1 \leqslant i < j \leqslant n} x_i x_j \geqslant K$$

holds for every Shiny n-tuple $(x_1, x_2, \ldots, x_n)$.

(Serbia)

Answer: $K = -(n-1)/2$.

Solution 1. First of all, we show that we may not take a larger constant K. Let t be a positive number, and take $x_2 = x_3 = \cdots = t$ and $x_1 = -1/(2t)$. Then, every product $x_i x_j$ $(i \neq j)$ is equal to either t^2 or $-1/2$. Hence, for every permutation y_i of the x_i, we have

$$y_1 y_2 + \cdots + y_{n-1} y_n \geqslant (n-3)t^2 - 1 \geqslant -1.$$

This justifies that the n-tuple $(x_1, \ldots, x_n)$ is Shiny. Now, we have

$$\sum_{i<j} x_i x_j = -\frac{n-1}{2} + \frac{(n-1)(n-2)}{2} t^2.$$

Thus, as t approaches 0 from above, $\sum_{i<j} x_i x_j$ gets arbitrarily close to $-(n-1)/2$. This shows that we may not take K any larger than $-(n-1)/2$. It remains to show that $\sum_{i<j} x_i x_j \geqslant -(n-1)/2$ for any Shiny choice of the x_i.

From now onward, assume that $(x_1, \ldots, x_n)$ is a Shiny n-tuple. Let the z_i $(1 \leqslant i \leqslant n)$ be some permutation of the x_i to be chosen later. The indices for z_i will always be taken modulo n. We will first split up the sum $\sum_{i<j} x_i x_j = \sum_{i<j} z_i z_j$ into $\lfloor (n-1)/2 \rfloor$ expressions, each of the form $y_1 y_2 + \cdots + y_{n-1} y_n$ for some permutation y_i of the z_i, and some leftover terms. More specifically, write

$$\sum_{i<j} z_i z_j = \sum_{q=0}^{n-1} \sum_{\substack{i+j \equiv q \pmod{n} \\ i \not\equiv j \pmod{n}}} z_i z_j = \sum_{p=1}^{\lfloor \frac{n-1}{2} \rfloor} \sum_{\substack{i+j \equiv 2p-1, 2p \pmod{n} \\ i \not\equiv j \pmod{n}}} z_i z_j + L, \tag{1}$$

where $L = z_1 z_{-1} + z_2 z_{-2} + \cdots + z_{(n-1)/2} z_{-(n-1)/2}$ if n is odd, and $L = z_1 z_{-1} + z_1 z_{-2} + z_2 z_{-2} + \cdots + z_{(n-2)/2} z_{-n/2}$ if n is even. We note that for each $p = 1, 2, \ldots, \lfloor (n-1)/2 \rfloor$, there is some permutation y_i of the z_i such that

$$\sum_{\substack{i+j \equiv 2p-1, 2p \pmod{n} \\ i \not\equiv j \pmod{n}}} z_i z_j = \sum_{k=1}^{n-1} y_k y_{k+1},$$

because we may choose $y_{2i-1} = z_{i+p-1}$ for $1 \leqslant i \leqslant (n+1)/2$ and $y_{2i} = z_{p-i}$ for $1 \leqslant i \leqslant n/2$.

We show (1) graphically for $n = 6, 7$ in the diagrams below. The edges of the graphs each represent a product $z_i z_j$, and the dashed and dotted series of lines represents the sum of the edges, which is of the form $y_1 y_2 + \cdots + y_{n-1} y_n$ for some permutation y_i of the z_i precisely when the series of lines is a Hamiltonian path. The filled edges represent the summands of L.
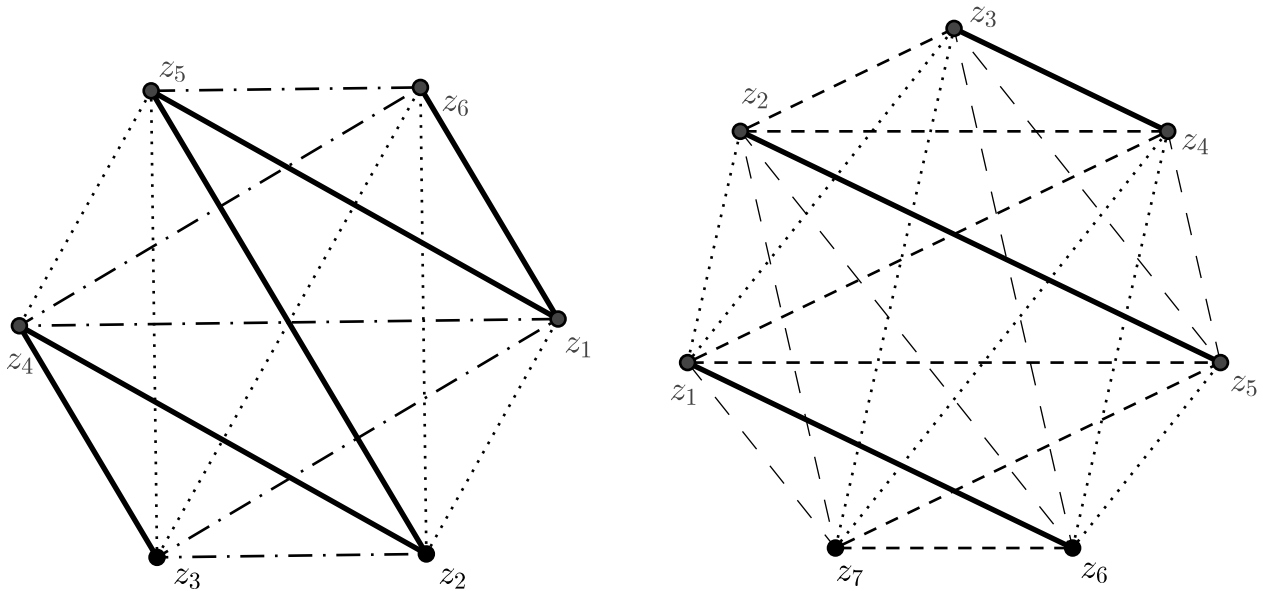
Now, because the z_i are Shiny, we have that (1) yields the following bound:

$$\sum_{i<j} z_i z_j \geq -\left\lfloor \frac{n-1}{2} \right\rfloor + L.$$

It remains to show that, for each n, there exists some permutation z_i of the x_i such that $L \geq 0$ when n is odd, and $L \geq -1/2$ when n is even. We now split into cases based on the parity of n and provide constructions of the permutations z_i.

Since we have not made any assumptions yet about the x_i, we may now assume without loss of generality that

$$x_1 \leq x_2 \leq \cdots \leq x_k \leq 0 \leq x_{k+1} \leq \cdots \leq x_n. \tag{2}$$

Case 1: n is odd.

Without loss of generality, assume that k (from (2)) is even, because we may negate all the x_i if k is odd. We then have $x_1 x_2, x_3 x_4, \ldots, x_{n-2} x_{n-1} \geq 0$ because the factors are of the same sign. Let $L = x_1 x_2 + x_3 x_4 + \cdots + x_{n-2} x_{n-1} \geq 0$. We choose our z_i so that this definition of L agrees with the sum of the leftover terms in (1). Relabel the x_i as z_i such that

$$\{z_1, z_{n-1}\}, \{z_2, z_{n-2}\}, \ldots, \{z_{(n-1)/2}, z_{(n+1)/2}\}$$

are some permutation of

$$\{x_1, x_2\}, \{x_3, x_4\}, \ldots, \{x_{n-2}, x_{n-1}\},$$

and $z_n = x_n$. Then, we have $L = z_1 z_{n-1} + \cdots + z_{(n-1)/2} z_{(n+1)/2}$, as desired.

Case 2: n is even.

Let $L = x_1 x_2 + x_2 x_3 + \cdots + x_{n-1} x_n$. Assume without loss of generality $k \neq 1$. Now, we have

$$2L = (x_1 x_2 + \cdots + x_{n-1} x_n) + (x_1 x_2 + \cdots + x_{n-1} x_n) \geq (x_2 x_3 + \cdots + x_{n-1} x_n) + x_k x_{k+1}$$

$$\geq x_2 x_3 + \cdots + x_{n-1} x_n + x_n x_1 \geq -1,$$

where the first inequality holds because the only negative term in L is $x_k x_{k+1}$, the second inequality holds because $x_1 \leq x_k \leq 0 \leq x_{k+1} \leq x_n$, and the third inequality holds because the x_i are assumed to be Shiny. We thus have that $L \geq -1/2$. We now choose a suitable z_i such that the definition of L matches the leftover terms in (1).

Relabel the x_i with z_i in the following manner: $x_{2i-1} = z_{-i}, x_{2i} = z_i$ (again taking indices modulo n). We have that

$$L = \sum_{\substack{i+j \equiv 0,-1 \pmod{n} \\ i \not\equiv j \pmod{n}}} z_i z_j,$$

as desired.

Solution 2. We present another proof that $\sum_{i<j} x_i x_j \geqslant -(n-1)/2$ for any Shiny n-tuple $(x_1, \ldots, x_n)$. Assume an ordering of the x_i as in (2), and let $\ell = n - k$. Assume without loss of generality that $k \geqslant \ell$. Also assume $k \neq n$, (as otherwise, all of the x_i are nonpositive, and so the inequality is trivial). Define the sets of indices $S = \{1, 2, \ldots, k\}$ and $T = \{k+1, \ldots, n\}$. Define the following sums:

$$K = \sum_{\substack{i<j \\ i,j \in S}} x_i x_j, \quad M = \sum_{\substack{i \in S \\ j \in T}} x_i x_j, \quad \text{and} \quad L = \sum_{\substack{i<j \\ i,j \in T}} x_i x_j$$

By definition, $K, L \geqslant 0$ and $M \leqslant 0$. We aim to show that $K + L + M \geqslant -(n-1)/2$.

We split into cases based on whether $k = \ell$ or $k > \ell$.

Case 1: $k > \ell$.

Consider all permutations $\phi \colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ such that $\phi^{-1}(T) = \{2, 4, \ldots, 2\ell\}$. Note that there are $k!\ell!$ such permutations ϕ. Define

$$f(\phi) = \sum_{i=1}^{n-1} x_{\phi(i)} x_{\phi(i+1)}.$$

We know that $f(\phi) \geqslant -1$ for every permutation ϕ with the above property. Averaging $f(\phi)$ over all ϕ gives

$$-1 \leqslant \frac{1}{k!\ell!} \sum_\phi f(\phi) = \frac{2\ell}{k\ell} M + \frac{2(k - \ell - 1)}{k(k-1)} K,$$

where the equality holds because there are $k\ell$ products in M, of which 2ℓ are selected for each ϕ, and there are $k(k-1)/2$ products in K, of which $k - \ell - 1$ are selected for each ϕ. We now have

$$K + L + M \geqslant K + L + \left(-\frac{k}{2} - \frac{k-\ell-1}{k-1} K \right) = -\frac{k}{2} + \frac{\ell}{k-1} K + L.$$

Since $k \leqslant n - 1$ and $K, L \geqslant 0$, we get the desired inequality.

Case 2: $k = \ell = n/2$.

We do a similar approach, considering all $\phi \colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ such that $\phi^{-1}(T) = \{2, 4, \ldots, 2\ell\}$, and defining f the same way. Analogously to Case 1, we have

$$-1 \leqslant \frac{1}{k!\ell!} \sum_\phi f(\phi) = \frac{2\ell - 1}{k\ell} M,$$

because there are $k\ell$ products in M, of which $2\ell - 1$ are selected for each ϕ. Now, we have that

$$K + L + M \geqslant M \geqslant -\frac{n^2}{4(n-1)} \geqslant -\frac{n-1}{2},$$

where the last inequality holds because $n \geqslant 4$.

A6. Find all functions $f\colon \mathbb{R} \to \mathbb{R}$ such that

$$f(f(x)f(y)) + f(x + y) = f(xy) \qquad (*)$$

for all $x, y \in \mathbb{R}$.

(Albania)

Answer: There are 3 solutions:

$$x \mapsto 0 \qquad \text{or} \qquad x \mapsto x - 1 \qquad \text{or} \qquad x \mapsto 1 - x \qquad (x \in \mathbb{R}).$$

Solution. An easy check shows that all the 3 above mentioned functions indeed satisfy the original equation $(*)$.

In order to show that these are the only solutions, first observe that if $f(x)$ is a solution then $-f(x)$ is also a solution. Hence, without loss of generality we may (and will) assume that $f(0) \leqslant 0$ from now on. We have to show that either f is identically zero or $f(x) = x - 1$ ($\forall x \in \mathbb{R}$).

Observe that, for a fixed $x \neq 1$, we may choose $y \in \mathbb{R}$ so that $x + y = xy \iff y = \frac{x}{x-1}$, and therefore from the original equation $(*)$ we have

$$f\left(f(x) \cdot f\left(\frac{x}{x-1}\right)\right) = 0 \qquad (x \neq 1). \tag{1}$$

In particular, plugging in $x = 0$ in (1), we conclude that f has at least one zero, namely $(f(0))^2$:

$$f\big((f(0))^2\big) = 0. \tag{2}$$

We analyze two cases (recall that $f(0) \leqslant 0$):

Case 1: $f(0) = 0$.

Setting $y = 0$ in the original equation we get the identically zero solution:

$$f(f(x)f(0)) + f(x) = f(0) \implies f(x) = 0 \text{ for all } x \in \mathbb{R}.$$

From now on, we work on the main

Case 2: $f(0) < 0$.

We begin with the following

Claim 1.

$$f(1) = 0, \qquad f(a) = 0 \implies a = 1, \qquad \text{and} \qquad f(0) = -1. \tag{3}$$

Proof. We need to show that 1 is the *unique* zero of f. First, observe that f has at least one zero a by (2); if $a \neq 1$ then setting $x = a$ in (1) we get $f(0) = 0$, a contradiction. Hence from (2) we get $(f(0))^2 = 1$. Since we are assuming $f(0) < 0$, we conclude that $f(0) = -1$. $\square$

Setting $y = 1$ in the original equation $(*)$ we get

$$f(f(x)f(1)) + f(x+1) = f(x) \iff f(0) + f(x+1) = f(x) \iff f(x+1) = f(x) + 1 \qquad (x \in \mathbb{R}).$$

An easy induction shows that

$$f(x + n) = f(x) + n \qquad (x \in \mathbb{R}, \ n \in \mathbb{Z}). \tag{4}$$

Now we make the following

Claim 2. f is injective.

Proof. Suppose that $f(a) = f(b)$ with $a \neq b$. Then by (4), for all $N \in \mathbb{Z}$,

$$f(a + N + 1) = f(b + N) + 1.$$

Choose any integer $N < -b$; then there exist $x_0, y_0 \in \mathbb{R}$ with $x_0 + y_0 = a + N + 1$, $x_0 y_0 = b + N$. Since $a \neq b$, we have $x_0 \neq 1$ and $y_0 \neq 1$. Plugging in x_0 and y_0 in the original equation $(*)$ we get

$$f(f(x_0)f(y_0)) + f(a + N + 1) = f(b + N) \iff f(f(x_0)f(y_0)) + 1 = 0$$
$$\iff f(f(x_0)f(y_0) + 1) = 0 \qquad \text{by (4)}$$
$$\iff f(x_0)f(y_0) = 0 \qquad \text{by (3)}.$$

However, by Claim 1 we have $f(x_0) \neq 0$ and $f(y_0) \neq 0$ since $x_0 \neq 1$ and $y_0 \neq 1$, a contradiction. $\square$

Now the end is near. For any $t \in \mathbb{R}$, plug in $(x, y) = (t, -t)$ in the original equation $(*)$ to get

$$f(f(t)f(-t)) + f(0) = f(-t^2) \iff f(f(t)f(-t)) = f(-t^2) + 1 \qquad \text{by (3)}$$
$$\iff f(f(t)f(-t)) = f(-t^2 + 1) \qquad \text{by (4)}$$
$$\iff f(t)f(-t) = -t^2 + 1 \qquad \text{by injectivity of } f.$$

Similarly, plugging in $(x, y) = (t, 1 - t)$ in $(*)$ we get

$$f(f(t)f(1 - t)) + f(1) = f(t(1 - t)) \iff f(f(t)f(1 - t)) = f(t(1 - t)) \quad \text{by (3)}$$
$$\iff f(t)f(1 - t) = t(1 - t) \qquad \text{by injectivity of } f.$$

But since $f(1 - t) = 1 + f(-t)$ by (4), we get

$$f(t)f(1 - t) = t(1 - t) \iff f(t)(1 + f(-t)) = t(1 - t) \iff f(t) + (-t^2 + 1) = t(1 - t)$$
$$\iff f(t) = t - 1,$$

as desired.

Comment. Other approaches are possible. For instance, after Claim 1, we may define

$$g(x) \overset{\text{def}}{=} f(x) + 1.$$

Replacing $x + 1$ and $y + 1$ in place of x and y in the original equation $(*)$, we get

$$f(f(x + 1)f(y + 1)) + f(x + y + 2) = f(xy + x + y + 1) \qquad (x, y \in \mathbb{R}),$$

and therefore, using (4) (so that in particular $g(x) = f(x + 1)$), we may rewrite $(*)$ as

$$g(g(x)g(y)) + g(x + y) = g(xy + x + y) \qquad (x, y \in \mathbb{R}). \qquad (**)$$

We are now to show that $g(x) = x$ for all $x \in \mathbb{R}$ under the assumption (Claim 1) that 0 is the unique zero of g.

Claim 3. Let $n \in \mathbb{Z}$ and $x \in \mathbb{R}$. Then

   (a) $g(x + n) = x + n$, and the conditions $g(x) = n$ and $x = n$ are equivalent.

   (b) $g(nx) = ng(x)$.

Proof. For part (a), just note that $g(x + n) = x + n$ is just a reformulation of (4). Then $g(x) = n \iff$ $g(x - n) = 0 \iff x - n = 0$ since 0 is the unique zero of g. For part (b), we may assume that $x \neq 0$ since the result is obvious when $x = 0$. Plug in $y = n/x$ in $(**)$ and use part (a) to get

$$g\left(g(x)g\left(\frac{n}{x}\right)\right) + g\left(x + \frac{n}{x}\right) = g\left(n + x + \frac{n}{x}\right) \iff g\left(g(x)g\left(\frac{n}{x}\right)\right) = n \iff g(x)g\left(\frac{n}{x}\right) = n.$$

In other words, for $x \neq 0$ we have

$$g(x) = \frac{n}{g(n/x)}.$$

In particular, for $n = 1$, we get $g(1/x) = 1/g(x)$, and therefore replacing $x \leftarrow nx$ in the last equation we finally get

$$g(nx) = \frac{n}{g(1/x)} = ng(x),$$

as required.

Claim 4. The function g is *additive*, i.e., $g(a + b) = g(a) + g(b)$ for all $a, b \in \mathbb{R}$.

Proof. Set $x \leftarrow -x$ and $y \leftarrow -y$ in $(**)$; since g is an odd function (by Claim 3(b) with $n = -1$), we get

$$g(g(x)g(y)) - g(x + y) = -g(-xy + x + y).$$

Subtracting the last relation from $(**)$ we have

$$2g(x + y) = g(xy + x + y) + g(-xy + x + y)$$

and since by Claim 3(b) we have $2g(x + y) = g(2(x + y))$, we may rewrite the last equation as

$$g(\alpha + \beta) = g(\alpha) + g(\beta) \qquad \text{where} \qquad \begin{cases} \alpha = xy + x + y \\ \beta = -xy + x + y. \end{cases}$$

In other words, we have additivity for all $\alpha, \beta \in \mathbb{R}$ for which there are real numbers x and y satisfying

$$x + y = \frac{\alpha + \beta}{2} \qquad \text{and} \qquad xy = \frac{\alpha - \beta}{2},$$

i.e., for all $\alpha, \beta \in \mathbb{R}$ such that $(\frac{\alpha + \beta}{2})^2 - 4 \cdot \frac{\alpha - \beta}{2} \geqslant 0$. Therefore, given any $a, b \in \mathbb{R}$, we may choose $n \in \mathbb{Z}$ large enough so that we have additivity for $\alpha = na$ and $\beta = nb$, i.e.,

$$g(na) + g(nb) = g(na + nb) \iff ng(a) + ng(b) = ng(a + b)$$

by Claim 3(b). Cancelling n, we get the desired result. (Alternatively, setting either $(\alpha, \beta) = (a, b)$ or $(\alpha, \beta) = (-a, -b)$ will ensure that $(\frac{\alpha + \beta}{2})^2 - 4 \cdot \frac{\alpha - \beta}{2} \geqslant 0$). $\qquad \square$

Now we may finish the solution. Set $y = 1$ in $(**)$, and use Claim 3 to get

$$g(g(x)g(1)) + g(x + 1) = g(2x + 1) \iff g(g(x)) + g(x) + 1 = 2g(x) + 1 \iff g(g(x)) = g(x).$$

By additivity, this is equivalent to $g(g(x) - x) = 0$. Since 0 is the unique zero of g by assumption, we finally get $g(x) - x = 0 \iff g(x) = x$ for all $x \in \mathbb{R}$.

A7.   Let $a_0, a_1, a_2, \ldots$ be a sequence of integers and $b_0, b_1, b_2, \ldots$ be a sequence of *positive* integers such that $a_0 = 0, a_1 = 1$, and

$$a_{n+1} = \begin{cases} a_n b_n + a_{n-1}, & \text{if } b_{n-1} = 1 \\ a_n b_n - a_{n-1}, & \text{if } b_{n-1} > 1 \end{cases} \qquad \text{for } n = 1, 2, \ldots.$$

Prove that at least one of the two numbers a_{2017} and a_{2018} must be greater than or equal to 2017.

(Australia)

Solution 1.   The value of b_0 is irrelevant since $a_0 = 0$, so we may assume that $b_0 = 1$.

Lemma. We have $a_n \geqslant 1$ for all $n \geqslant 1$.

Proof. Let us suppose otherwise in order to obtain a contradiction. Let

$$n \geqslant 1 \text{ be the smallest integer with } a_n \leqslant 0. \tag{1}$$

Note that $n \geqslant 2$. It follows that $a_{n-1} \geqslant 1$ and $a_{n-2} \geqslant 0$. Thus we cannot have $a_n = a_{n-1}b_{n-1} + a_{n-2}$, so we must have $a_n = a_{n-1}b_{n-1} - a_{n-2}$. Since $a_n \leqslant 0$, we have $a_{n-1} \leqslant a_{n-2}$. Thus we have $a_{n-2} \geqslant a_{n-1} \geqslant a_n$.

Let

$$r \text{ be the smallest index with } a_r \geqslant a_{r+1} \geqslant a_{r+2}. \tag{2}$$

Then $r \leqslant n-2$ by the above, but also $r \geqslant 2$: if $b_1 = 1$, then $a_2 = a_1 = 1$ and $a_3 = a_2 b_2 + a_1 > a_2$; if $b_1 > 1$, then $a_2 = b_1 > 1 = a_1$.

By the minimal choice (2) of r, it follows that $a_{r-1} < a_r$. And since $2 \leqslant r \leqslant n-2$, by the minimal choice (1) of n we have $a_{r-1}, a_r, a_{r+1} > 0$. In order to have $a_{r+1} \geqslant a_{r+2}$, we must have $a_{r+2} = a_{r+1}b_{r+1} - a_r$ so that $b_r \geqslant 2$. Putting everything together, we conclude that

$$a_{r+1} = a_r b_r \pm a_{r-1} \geqslant 2a_r - a_{r-1} = a_r + (a_r - a_{r-1}) > a_r,$$

which contradicts (2).   □

To complete the problem, we prove that $\max\{a_n, a_{n+1}\} \geqslant n$ by induction. The cases $n = 0, 1$ are given. Assume it is true for all non-negative integers strictly less than n, where $n \geqslant 2$. There are two cases:

Case 1: $b_{n-1} = 1$.

Then $a_{n+1} = a_n b_n + a_{n-1}$. By the inductive assumption one of a_{n-1}, a_n is at least $n-1$ and the other, by the lemma, is at least 1. Hence

$$a_{n+1} = a_n b_n + a_{n-1} \geqslant a_n + a_{n-1} \geqslant (n-1) + 1 = n.$$

Thus $\max\{a_n, a_{n+1}\} \geqslant n$, as desired.

Case 2: $b_{n-1} > 1$.

Since we defined $b_0 = 1$ there is an index r with $1 \leqslant r \leqslant n-1$ such that

$$b_{n-1}, b_{n-2}, \ldots, b_r \geqslant 2 \qquad \text{and} \qquad b_{r-1} = 1.$$

We have $a_{r+1} = a_r b_r + a_{r-1} \geqslant 2a_r + a_{r-1}$. Thus $a_{r+1} - a_r \geqslant a_r + a_{r-1}$.

Now we claim that $a_r + a_{r-1} \geqslant r$. Indeed, this holds by inspection for $r = 1$; for $r \geqslant 2$, one of a_r, a_{r-1} is at least $r-1$ by the inductive assumption, while the other, by the lemma, is at least 1. Hence $a_r + a_{r-1} \geqslant r$, as claimed, and therefore $a_{r+1} - a_r \geqslant r$ by the last inequality in the previous paragraph.

Since $r \geqslant 1$ and, by the lemma, $a_r \geqslant 1$, from $a_{r+1} - a_r \geqslant r$ we get the following two inequalities:

$$a_{r+1} \geqslant r + 1 \qquad \text{and} \qquad a_{r+1} > a_r.$$

Now observe that

$$a_m > a_{m-1} \implies a_{m+1} > a_m \text{ for } m = r+1, r+2, \ldots, n-1,$$

since $a_{m+1} = a_m b_m - a_{m-1} \geqslant 2a_m - a_{m-1} = a_m + (a_m - a_{m-1}) > a_m$. Thus

$$a_n > a_{n-1} > \cdots > a_{r+1} \geqslant r+1 \implies a_n \geqslant n.$$

So $\max\{a_n, a_{n+1}\} \geqslant n$, as desired.

Solution 2. We say that an index $n > 1$ is *bad* if $b_{n-1} = 1$ and $b_{n-2} > 1$; otherwise n is *good*. The value of b_0 is irrelevant to the definition of (a_n) since $a_0 = 0$; so we assume that $b_0 > 1$.

Lemma 1. (a) $a_n \geqslant 1$ for all $n > 0$.

(b) If $n > 1$ is good, then $a_n > a_{n-1}$.

Proof. Induction on n. In the base cases $n = 1, 2$ we have $a_1 = 1 \geqslant 1$, $a_2 = b_1 a_1 \geqslant 1$, and finally $a_2 > a_1$ if 2 is good, since in this case $b_1 > 1$.

Now we assume that the lemma statement is proved for $n = 1, 2, \ldots, k$ with $k \geqslant 2$, and prove it for $n = k + 1$. Recall that a_k and a_{k-1} are positive by the induction hypothesis.

Case 1: k is bad.

We have $b_{k-1} = 1$, so $a_{k+1} = b_k a_k + a_{k-1} \geqslant a_k + a_{k-1} > a_k \geqslant 1$, as required.

Case 2: k is good.

We already have $a_k > a_{k-1} \geqslant 1$ by the induction hypothesis. We consider three easy subcases.

Subcase 2.1: $b_k > 1$.

Then $a_{k+1} \geqslant b_k a_k - a_{k-1} \geqslant a_k + (a_k - a_{k-1}) > a_k \geqslant 1$.

Subcase 2.2: $b_k = b_{k-1} = 1$.

Then $a_{k+1} = a_k + a_{k-1} > a_k \geqslant 1$.

Subcase 2.3: $b_k = 1$ but $b_{k-1} > 1$.

Then $k + 1$ is bad, and we need to prove only (a), which is trivial: $a_{k+1} = a_k - a_{k-1} \geqslant 1$.

So, in all three subcases we have verified the required relations. $\qquad\square$

Lemma 2. Assume that $n > 1$ is bad. Then there exists a $j \in \{1, 2, 3\}$ such that $a_{n+j} \geqslant a_{n-1} + j + 1$, and $a_{n+i} \geqslant a_{n-1} + i$ for all $1 \leqslant i < j$.

Proof. Recall that $b_{n-1} = 1$. Set

$$m = \inf\{i > 0 \colon b_{n+i-1} > 1\}$$

(possibly $m = +\infty$). We claim that $j = \min\{m, 3\}$ works. Again, we distinguish several cases, according to the value of m; in each of them we use Lemma 1 without reference.

Case 1: $m = 1$, so $b_n > 1$.

Then $a_{n+1} \geqslant 2a_n + a_{n-1} \geqslant a_{n-1} + 2$, as required.

Case 2: $m = 2$, so $b_n = 1$ and $b_{n+1} > 1$.

Then we successively get

$$a_{n+1} = a_n + a_{n-1} \geqslant a_{n-1} + 1,$$
$$a_{n+2} \geqslant 2a_{n+1} + a_n \geqslant 2(a_{n-1} + 1) + a_n = a_{n-1} + (a_{n-1} + a_n + 2) \geqslant a_{n-1} + 4,$$

which is even better than we need.

Case 3: $m > 2$, so $b_n = b_{n+1} = 1$.

Then we successively get

$$a_{n+1} = a_n + a_{n-1} \geqslant a_{n-1} + 1, \quad a_{n+2} = a_{n+1} + a_n \geqslant a_{n-1} + 1 + a_n \geqslant a_{n-1} + 2,$$
$$a_{n+3} \geqslant a_{n+2} + a_{n+1} \geqslant (a_{n-1} + 1) + (a_{n-1} + 2) \geqslant a_{n-1} + 4,$$

as required. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

Lemmas 1(b) and 2 provide enough information to prove that $\max\{a_n, a_{n+1}\} \geqslant n$ for all n and, moreover, that $a_n \geqslant n$ often enough. Indeed, assume that we have found some n with $a_{n-1} \geqslant n-1$. If n is good, then by Lemma 1(b) we have $a_n \geqslant n$ as well. If n is bad, then Lemma 2 yields $\max\{a_{n+i}, a_{n+i+1}\} \geqslant a_{n-1}+i+1 \geqslant n+i$ for all $0 \leqslant i < j$ and $a_{n+j} \geqslant a_{n-1}+j+1 \geqslant n+j$; so $n + j$ is the next index to start with.

A8.   Assume that a function $f\colon \mathbb{R} \to \mathbb{R}$ satisfies the following condition:

   For every $x, y \in \mathbb{R}$ such that $\big(f(x) + y\big)\big(f(y) + x\big) > 0$, we have $f(x) + y = f(y) + x$.

Prove that $f(x) + y \leqslant f(y) + x$ whenever $x > y$.

<div align="right">(Netherlands)</div>

Solution 1. Define $g(x) = x - f(x)$. The condition on f then rewrites as follows:

   For every $x, y \in \mathbb{R}$ such that $\big((x + y) - g(x)\big)\big((x + y) - g(y)\big) > 0$, we have $g(x) = g(y)$.

This condition may in turn be rewritten in the following form:

   If $g(x) \neq g(y)$, then the number $x + y$ lies (non-strictly) between $g(x)$ and $g(y)$. $(*)$

Notice here that the function $g_1(x) = -g(-x)$ also satisfies $(*)$, since

$$g_1(x) \neq g_1(y) \quad \Longrightarrow \quad g(-x) \neq g(-y) \quad \Longrightarrow \quad -(x + y) \text{ lies between } g(-x) \text{ and } g(-y)$$
$$\Longrightarrow \quad x + y \text{ lies between } g_1(x) \text{ and } g_1(y).$$

On the other hand, the relation we need to prove reads now as

$$g(x) \leqslant g(y) \qquad \text{whenever } x < y. \tag{1}$$

Again, this condition is equivalent to the same one with g replaced by g_1.

   If $g(x) = 2x$ for all $x \in \mathbb{R}$, then $(*)$ is obvious; so in what follows we consider the other case. We split the solution into a sequence of lemmas, strengthening one another. We always consider some value of x with $g(x) \neq 2x$ and denote $X = g(x)$.

Lemma 1. Assume that $X < 2x$. Then on the interval $(X - x; x]$ the function g attains at most two values — namely, X and, possibly, some $Y > X$. Similarly, if $X > 2x$, then g attains at most two values on $[x; X - x)$ — namely, X and, possibly, some $Y < X$.

Proof. We start with the first claim of the lemma. Notice that $X - x < x$, so the considered interval is nonempty.

   Take any $a \in (X - x; x)$ with $g(a) \neq X$ (if it exists). If $g(a) < X$, then $(*)$ yields $g(a) \leqslant a + x \leqslant g(x) = X$, so $a \leqslant X - x$ which is impossible. Thus, $g(a) > X$ and hence by $(*)$ we get $X \leqslant a + x \leqslant g(a)$.

   Now, for any $b \in (X - x; x)$ with $g(b) \neq X$ we similarly get $b + x \leqslant g(b)$. Therefore, the number $a + b$ (which is smaller than each of $a + x$ and $b + x$) cannot lie between $g(a)$ and $g(b)$, which by $(*)$ implies that $g(a) = g(b)$. Hence g may attain only two values on $(X - x; x]$, namely X and $g(a) > X$.

   To prove the second claim, notice that $g_1(-x) = -X < 2 \cdot (-x)$, so g_1 attains at most two values on $(-X + x, -x]$, i.e., $-X$ and, possibly, some $-Y > -X$. Passing back to g, we get what we need. $\qquad\square$

Lemma 2. If $X < 2x$, then g is constant on $(X - x; x)$. Similarly, if $X > 2x$, then g is constant on $(x; X - x)$.

Proof. Again, it suffices to prove the first claim only. Assume, for the sake of contradiction, that there exist $a, b \in (X - x; x)$ with $g(a) \neq g(b)$; by Lemma 1, we may assume that $g(a) = X$ and $Y = g(b) > X$.

   Notice that $\min\{X - a, X - b\} > X - x$, so there exists a $u \in (X - x; x)$ such that $u < \min\{X - a, X - b\}$. By Lemma 1, we have either $g(u) = X$ or $g(u) = Y$. In the former case, by $(*)$ we have $X \leqslant u + b \leqslant Y$ which contradicts $u < X - b$. In the second case, by $(*)$ we have $X \leqslant u + a \leqslant Y$ which contradicts $u < X - a$. Thus the lemma is proved. $\qquad\square$

Lemma 3. If $X < 2x$, then $g(a) = X$ for all $a \in (X - x; x)$. Similarly, if $X > 2x$, then $g(a) = X$ for all $a \in (x; X - x)$.

Proof. Again, we only prove the first claim.

By Lemmas 1 and 2, this claim may be violated only if g takes on a constant value $Y > X$ on $(X - x, x)$. Choose any $a, b \in (X - x; x)$ with $a < b$. By $(*)$, we have

$$Y \geqslant b + x \geqslant X. \tag{2}$$

In particular, we have $Y \geqslant b + x > 2a$. Applying Lemma 2 to a in place of x, we obtain that g is constant on $(a, Y - a)$. By (2) again, we have $x \leqslant Y - b < Y - a$; so $x, b \in (a; Y - a)$. But $X = g(x) \neq g(b) = Y$, which is a contradiction. $\qquad\square$

Now we are able to finish the solution. Assume that $g(x) > g(y)$ for some $x < y$. Denote $X = g(x)$ and $Y = g(y)$; by $(*)$, we have $X \geqslant x + y \geqslant Y$, so $Y - y \leqslant x < y \leqslant X - x$, and hence $(Y - y; y) \cap (x; X - x) = (x, y) \neq \varnothing$. On the other hand, since $Y - y < y$ and $x < X - x$, Lemma 3 shows that g should attain a constant value X on $(x; X - x)$ and a constant value $Y \neq X$ on $(Y - y; y)$. Since these intervals overlap, we get the final contradiction.

Solution 2. As in the previous solution, we pass to the function g satisfying $(*)$ and notice that we need to prove the condition (1). We will also make use of the function g_1.

If g is constant, then (1) is clearly satisfied. So, in the sequel we assume that g takes on at least two different values. Now we collect some information about the function g.

Claim 1. For any $c \in \mathbb{R}$, all the solutions of $g(x) = c$ are bounded.

Proof. Fix any $y \in \mathbb{R}$ with $g(y) \neq c$. Assume first that $g(y) > c$. Now, for any x with $g(x) = c$, by $(*)$ we have $c \leqslant x + y \leqslant g(y)$, or $c - y \leqslant x \leqslant g(y) - y$. Since c and y are constant, we get what we need.

If $g(y) < c$, we may switch to the function g_1 for which we have $g_1(-y) > -c$. By the above arguments, we obtain that all the solutions of $g_1(-x) = -c$ are bounded, which is equivalent to what we need. $\qquad\square$

As an immediate consequence, the function g takes on infinitely many values, which shows that the next claim is indeed widely applicable.

Claim 2. If $g(x) < g(y) < g(z)$, then $x < z$.

Proof. By $(*)$, we have $g(x) \leqslant x + y \leqslant g(y) \leqslant z + y \leqslant g(z)$, so $x + y \leqslant z + y$, as required. $\qquad\square$

Claim 3. Assume that $g(x) > g(y)$ for some $x < y$. Then $g(a) \in \{g(x), g(y)\}$ for all $a \in [x; y]$.

Proof. If $g(y) < g(a) < g(x)$, then the triple (y, a, x) violates Claim 2. If $g(a) < g(y) < g(x)$, then the triple (a, y, x) violates Claim 2. If $g(y) < g(x) < g(a)$, then the triple (y, x, a) violates Claim 2. The only possible cases left are $g(a) \in \{g(x), g(y)\}$. $\qquad\square$

In view of Claim 3, we say that an interval I (which may be open, closed, or semi-open) is a *Dirichlet interval*[*] if the function g takes on just two values on I.

Assume now, for the sake of contradiction, that (1) is violated by some $x < y$. By Claim 3, $[x; y]$ is a Dirichlet interval. Set

$$r = \inf\{a\colon (a; y] \text{ is a Dirichlet interval}\} \quad \text{and} \quad s = \sup\{b\colon [x; b) \text{ is a Dirichlet interval}\}.$$

Clearly, $r \leqslant x < y \leqslant s$. By Claim 1, r and s are finite. Denote $X = g(x)$, $Y = g(y)$, and $\Delta = (y - x)/2$.

Suppose first that there exists a $t \in (r; r + \Delta)$ with $f(t) = Y$. By the definition of r, the interval $(r - \Delta; y]$ is not Dirichlet, so there exists an $r' \in (r - \Delta; r]$ such that $g(r') \notin \{X, Y\}$.

---

[*]The name *Dirichlet interval* is chosen for the reason that g theoretically might act similarly to the Dirichlet function on this interval.

The function g attains at least three distinct values on $[r'; y]$, namely $g(r')$, $g(x)$, and $g(y)$. Claim 3 now yields $g(r') \leqslant g(y)$; the equality is impossible by the choice of r', so in fact $g(r') < Y$. Applying $(*)$ to the pairs (r', y) and (t, x) we obtain $r' + y \leqslant Y \leqslant t + x$, whence $r - \Delta + y < r' + y \leqslant t + x < r + \Delta + x$, or $y - x < 2\Delta$. This is a contradiction.

Thus, $g(t) = X$ for all $t \in (r; r + \Delta)$. Applying the same argument to g_1, we get $g(t) = Y$ for all $t \in (s - \Delta; s)$.

Finally, choose some $s_1, s_2 \in (s - \Delta; s)$ with $s_1 < s_2$ and denote $\delta = (s_2 - s_1)/2$. As before, we choose $r' \in (r - \delta; r)$ with $g(r') \notin \{X, Y\}$ and obtain $g(r') < Y$. Choose any $t \in (r; r + \delta)$; by the above arguments, we have $g(t) = X$ and $g(s_1) = g(s_2) = Y$. As before, we apply $(*)$ to the pairs (r', s_2) and (t, s_1) obtaining $r - \delta + s_2 < r' + s_2 \leqslant Y \leqslant t + s_1 < r + \delta + s_1$, or $s_2 - s_1 < 2\delta$. This is a final contradiction.

Comment 1. The original submission discussed the same functions f, but the question was different — namely, the following one:

Prove that the equation $f(x) = 2017x$ has at most one solution, and the equation $f(x) = -2017x$ has at least one solution.

The Problem Selection Committee decided that the question we are proposing is more natural, since it provides more natural information about the function g (which is indeed the main character in this story). On the other hand, the new problem statement is strong enough in order to imply the original one easily.

Namely, we will deduce from the new problem statement (along with the facts used in the solutions) that (i) for every $N > 0$ the equation $g(x) = -Nx$ has at most one solution, and (ii) for every $N > 1$ the equation $g(x) = Nx$ has at least one solution.

Claim (i) is now trivial. Indeed, g is proven to be non-decreasing, so $g(x) + Nx$ is strictly increasing and thus has at most one zero.

We proceed on claim (ii). If $g(0) = 0$, then the required root has been already found. Otherwise, we may assume that $g(0) > 0$ and denote $c = g(0)$. We intend to prove that $x = c/N$ is the required root. Indeed, by monotonicity we have $g(c/N) \geqslant g(0) = c$; if we had $g(c/N) > c$, then $(*)$ would yield $c \leqslant 0 + c/N \leqslant g(c/N)$ which is false. Thus, $g(x) = c = Nx$.

Comment 2. There are plenty of functions g satisfying $(*)$ (and hence of functions f satisfying the problem conditions). One simple example is $g_0(x) = 2x$. Next, for any increasing sequence $A = (\ldots, a_{-1}, a_0, a_1, \ldots)$ which is unbounded in both directions (i.e., for every N this sequence contains terms greater than N, as well as terms smaller than $-N$), the function g_A defined by

$$g_A(x) = a_i + a_{i+1} \qquad \text{whenever } x \in [a_i; a_{i+1})$$

satisfies $(*)$. Indeed, pick any $x < y$ with $g(x) \neq g(y)$; this means that $x \in [a_i; a_{i+1})$ and $y \in [a_j; a_{j+1})$ for some $i < j$. Then we have $g(x) = a_i + a_{i+1} \leqslant x + y < a_j + a_{j+1} = g(y)$, as required.

There also exist examples of the mixed behavior; e.g., for an arbitrary sequence A as above and an arbitrary subset $I \subseteq \mathbb{Z}$ the function

$$g_{A,I}(x) = \begin{cases} g_0(x), & x \in [a_i; a_{i+1}) \quad \text{with } i \in I; \\ g_A(x), & x \in [a_i; a_{i+1}) \quad \text{with } i \notin I \end{cases}$$

also satisfies $(*)$.

Finally, it is even possible to provide a complete description of all functions g satisfying $(*)$ (and hence of all functions f satisfying the problem conditions); however, it seems to be far out of scope for the IMO. This description looks as follows.

Let A be any closed subset of $\mathbb{R}$ which is unbounded in both directions. Define the functions i_A, s_A, and g_A as follows:

$$i_A(x) = \inf\{a \in A : a \geqslant x\}, \quad s_A(x) = \sup\{a \in A : a \leqslant x\}, \quad g_A(x) = i_A(x) + s_A(x).$$

It is easy to see that for different sets A and B the functions g_A and g_B are also different (since, e.g., for any $a \in A \setminus B$ the function g_B is constant in a small neighborhood of a, but the function g_A is not). One may check, similarly to the arguments above, that each such function satisfies $(*)$.

Finally, one more modification is possible. Namely, for any $x \in A$ one may redefine $g_A(x)$ (which is $2x$) to be any of the numbers

$$g_{A+}(x) = i_{A+}(x) + x \quad \text{or} \quad g_{A-}(x) = x + s_{A-}(x),$$
$$\text{where} \qquad i_{A+}(x) = \inf\{a \in A : a > x\} \quad \text{and} \quad s_{A-}(x) = \sup\{a \in A : a < x\}.$$

This really changes the value if x has some right (respectively, left) semi-neighborhood disjoint from A, so there are at most countably many possible changes; all of them can be performed independently.

With some effort, one may show that the construction above provides all functions g satisfying $(*)$.

Combinatorics

C1. A rectangle $\mathcal{R}$ with odd integer side lengths is divided into small rectangles with integer side lengths. Prove that there is at least one among the small rectangles whose distances from the four sides of $\mathcal{R}$ are either all odd or all even.

(Singapore)

Solution. Let the width and height of $\mathcal{R}$ be odd numbers a and b. Divide $\mathcal{R}$ into ab unit squares and color them green and yellow in a checkered pattern. Since the side lengths of a and b are odd, the corner squares of $\mathcal{R}$ will all have the same color, say green.

Call a rectangle (either $\mathcal{R}$ or a small rectangle) *green* if its corners are all green; call it *yellow* if the corners are all yellow, and call it *mixed* if it has both green and yellow corners. In particular, $\mathcal{R}$ is a green rectangle.

We will use the following trivial observations.
- Every mixed rectangle contains the same number of green and yellow squares;
- Every green rectangle contains one more green square than yellow square;
- Every yellow rectangle contains one more yellow square than green square.

The rectangle $\mathcal{R}$ is green, so it contains more green unit squares than yellow unit squares. Therefore, among the small rectangles, at least one is green. Let $\mathcal{S}$ be such a small green rectangle, and let its distances from the sides of $\mathcal{R}$ be x, y, u and v, as shown in the picture. The top-left corner of $\mathcal{R}$ and the top-left corner of $\mathcal{S}$ have the same color, which happen if and only if x and u have the same parity. Similarly, the other three green corners of $\mathcal{S}$ indicate that x and v have the same parity, y and u have the same parity, i.e. x, y, u and v are all odd or all even.
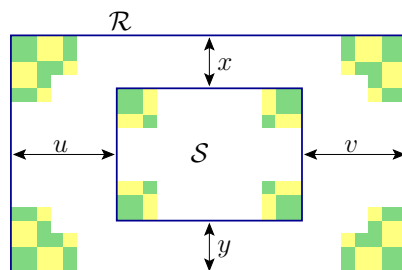
C2. Let n be a positive integer. Define a *chameleon* to be any sequence of $3n$ letters, with exactly n occurrences of each of the letters a, b, and c. Define a *swap* to be the transposition of two adjacent letters in a chameleon. Prove that for any chameleon X, there exists a chameleon Y such that X cannot be changed to Y using fewer than $3n^2/2$ swaps.

(Australia)

Solution 1. To start, notice that the swap of two identical letters does not change a chameleon, so we may assume there are no such swaps.

For any two chameleons X and Y, define their *distance* $d(X,Y)$ to be the minimal number of swaps needed to transform X into Y (or vice versa). Clearly, $d(X,Y) + d(Y,Z) \geqslant d(X,Z)$ for any three chameleons X, Y, and Z.

Lemma. Consider two chameleons

$$P = \underbrace{aa\ldots a}_{n}\underbrace{bb\ldots b}_{n}\underbrace{cc\ldots c}_{n} \quad \text{and} \quad Q = \underbrace{cc\ldots c}_{n}\underbrace{bb\ldots b}_{n}\underbrace{aa\ldots a}_{n}.$$

Then $d(P,Q) \geqslant 3n^2$.

Proof. For any chameleon X and any pair of distinct letters $u,v \in \{a,b,c\}$, we define $f_{u,v}(X)$ to be the number of pairs of positions in X such that the left one is occupied by u, and the right one is occupied by v. Define $f(X) = f_{a,b}(X) + f_{a,c}(X) + f_{b,c}(X)$. Notice that $f_{a,b}(P) = f_{a,c}(P) = f_{b,c}(P) = n^2$ and $f_{a,b}(Q) = f_{a,c}(Q) = f_{b,c}(Q) = 0$, so $f(P) = 3n^2$ and $f(Q) = 0$.

Now consider some swap changing a chameleon X to X'; say, the letters a and b are swapped. Then $f_{a,b}(X)$ and $f_{a,b}(X')$ differ by exactly 1, while $f_{a,c}(X) = f_{a,c}(X')$ and $f_{b,c}(X) = f_{b,c}(X')$. This yields $|f(X) - f(X')| = 1$, i.e., on any swap the value of f changes by 1. Hence $d(X,Y) \geqslant |f(X) - f(Y)|$ for any two chameleons X and Y. In particular, $d(P,Q) \geqslant |f(P) - f(Q)| = 3n^2$, as desired. □

Back to the problem, take any chameleon X and notice that $d(X,P) + d(X,Q) \geqslant d(P,Q) \geqslant 3n^2$ by the lemma. Consequently, $\max\{d(X,P), d(X,Q)\} \geqslant \frac{3n^2}{2}$, which establishes the problem statement.

Comment 1. The problem may be reformulated in a graph language. Construct a graph G with the chameleons as vertices, two vertices being connected with an edge if and only if these chameleons differ by a single swap. Then $d(X,Y)$ is the usual distance between the vertices X and Y in this graph. Recall that the *radius* of a connected graph G is defined as

$$r(G) = \min_{v \in V} \max_{u \in V} d(u,v).$$

So we need to prove that the radius of the constructed graph is at least $3n^2/2$.

It is well-known that the radius of any connected graph is at least the half of its diameter (which is simply $\max_{u,v \in V} d(u,v)$). Exactly this fact has been used above in order to finish the solution.

Solution 2. We use the notion of distance from Solution 1, but provide a different lower bound for it.

In any chameleon X, we enumerate the positions in it from left to right by $1, 2, \ldots, 3n$. Define $s_c(X)$ as the sum of positions occupied by c. The value of s_c changes by at most 1 on each swap, but this fact alone does not suffice to solve the problem; so we need an improvement.

For every chameleon X, denote by $X_{\overline{c}}$ the sequence obtained from X by removing all n letters c. Enumerate the positions in $X_{\overline{c}}$ from left to right by $1, 2, \ldots, 2n$, and define $s_{\overline{c},b}(X)$ as the sum of positions in $X_{\overline{c}}$ occupied by b. (In other words, here we consider the positions of the b's relatively to the a's only.) Finally, denote

$$d'(X,Y) := |s_c(X) - s_c(Y)| + |s_{\overline{c},b}(X) - s_{\overline{c},b}(Y)|.$$

Now consider any swap changing a chameleon X to X'. If no letter c is involved into this swap, then $s_c(X) = s_c(X')$; on the other hand, exactly one letter b changes its position in $X_{\overline{c}}$, so $|s_{\overline{c},b}(X) - s_{\overline{c},b}(X')| = 1$. If a letter c is involved into a swap, then $X_{\overline{c}} = X'_{\overline{c}}$, so $s_{\overline{c},b}(X) = s_{\overline{c},b}(X')$ and $|s_c(X) - s_c(X')| = 1$. Thus, in all cases we have $d'(X, X') = 1$.

As in the previous solution, this means that $d(X, Y) \geqslant d'(X, Y)$ for any two chameleons X and Y. Now, for any chameleon X we will indicate a chameleon Y with $d'(X, Y) \geqslant 3n^2/2$, thus finishing the solution.

The function s_c attains all integer values from $1 + \cdots + n = \frac{n(n+1)}{2}$ to $(2n+1) + \cdots + 3n = 2n^2 + \frac{n(n+1)}{2}$. If $s_c(X) \leqslant n^2 + \frac{n(n+1)}{2}$, then we put the letter c into the last n positions in Y; otherwise we put the letter c into the first n positions in Y. In either case we already have $|s_c(X) - s_c(Y)| \geqslant n^2$.

Similarly, $s_{\overline{c},b}$ ranges from $\frac{n(n+1)}{2}$ to $n^2 + \frac{n(n+1)}{2}$. So, if $s_{\overline{c},b}(X) \leqslant \frac{n^2}{2} + \frac{n(n+1)}{2}$, then we put the letter b into the last n positions in Y which are still free; otherwise, we put the letter b into the first n such positions. The remaining positions are occupied by a. In any case, we have $|s_{\overline{c},b}(X) - s_{\overline{c},b}(Y)| \geqslant \frac{n^2}{2}$, thus $d'(X, Y) \geqslant n^2 + \frac{n^2}{2} = \frac{3n^2}{2}$, as desired.

Comment 2. The two solutions above used two lower bounds $|f(X) - f(Y)|$ and $d'(X, Y)$ for the number $d(X, Y)$. One may see that these bounds are closely related to each other, as

$$f_{a,c}(X) + f_{b,c}(X) = s_c(X) - \frac{n(n+1)}{2} \quad \text{and} \quad f_{a,b}(X) = s_{\overline{c},b}(X) - \frac{n(n+1)}{2}.$$

One can see that, e.g., the bound $d'(X, Y)$ could as well be used in the proof of the lemma in Solution 1.

Let us describe here an even sharper bound which also can be used in different versions of the solutions above.

In each chameleon X, enumerate the occurrences of a from the left to the right as $a_1, a_2, \ldots, a_n$. Since we got rid of swaps of identical letters, the relative order of these letters remains the same during the swaps. Perform the same operation with the other letters, obtaining new letters $b_1, \ldots, b_n$ and $c_1, \ldots, c_n$. Denote by A the set of the $3n$ obtained letters.

Since all $3n$ letters became different, for any chameleon X and any $s \in A$ we may define the position $N_s(X)$ of s in X (thus $1 \leqslant N_s(X) \leqslant 3n$). Now, for any two chameleons X and Y we say that a pair of letters $(s, t) \in A \times A$ is an (X, Y)-*inversion* if $N_s(X) < N_t(X)$ but $N_s(Y) > N_t(Y)$, and define $d^*(X, Y)$ to be the number of (X, Y)-inversions. Then for any two chameleons Y and Y' differing by a single swap, we have $|d^*(X, Y) - d^*(X, Y')| = 1$. Since $d^*(X, X) = 0$, this yields $d(X, Y) \geqslant d^*(X, Y)$ for any pair of chameleons X and Y. The bound d^* may also be used in both Solution 1 and Solution 2.

Comment 3. In fact, one may prove that the distance d^* defined in the previous comment *coincides* with d. Indeed, if $X \neq Y$, then there exist an (X, Y)-inversion (s, t). One can show that such s and t may be chosen to occupy consecutive positions in Y. Clearly, s and t correspond to different letters among $\{a, b, c\}$. So, swapping them in Y we get another chameleon Y' with $d^*(X, Y') = d^*(X, Y) - 1$. Proceeding in this manner, we may change Y to X in $d^*(X, Y)$ steps.

Using this fact, one can show that the estimate in the problem statement is sharp for all $n \geqslant 2$. (For $n = 1$ it is not sharp, since any permutation of three letters can be changed to an opposite one in no less than three swaps.) We outline the proof below.

For any $k \geqslant 0$, define

$$X_{2k} = \underbrace{abc\,abc\ldots abc}_{3k \text{ letters}}\underbrace{cba\,cba\ldots cba}_{3k \text{ letters}} \quad \text{and} \quad X_{2k+3} = \underbrace{abc\,abc\ldots abc}_{3k \text{ letters}}abc\,bca\,cab\underbrace{cba\,cba\ldots cba}_{3k \text{ letters}}.$$

We claim that for every $n \geqslant 2$ and every chameleon Y, we have $d^*(X_n, Y) \leqslant \lceil 3n^2/2 \rceil$. This will mean that for every $n \geqslant 2$ the number $3n^2/2$ in the problem statement cannot be changed by any number larger than $\lceil 3n^2/2 \rceil$.

For any distinct letters $u, v \in \{a, b, c\}$ and any two chameleons X and Y, we define $d^*_{u,v}(X, Y)$ as the number of (X, Y)-inversions (s, t) such that s and t are instances of u and v (in any of the two possible orders). Then $d^*(X, Y) = d^*_{a,b}(X, Y) + d^*_{b,c}(X, Y) + d^*_{c,a}(X, Y)$.

We start with the case when $n = 2k$ is even; denote $X = X_{2k}$. We show that $d_{a,b}^*(X, Y) \leqslant 2k^2$ for any chameleon Y; this yields the required estimate. Proceed by the induction on k with the trivial base case $k = 0$. To perform the induction step, notice that $d_{a,b}^*(X, Y)$ is indeed the minimal number of swaps needed to change $Y_{\overline{c}}$ into $X_{\overline{c}}$. One may show that moving a_1 and a_{2k} in Y onto the first and the last positions in Y, respectively, takes at most $2k$ swaps, and that subsequent moving b_1 and b_{2k} onto the second and the second last positions takes at most $2k - 2$ swaps. After performing that, one may delete these letters from both $X_{\overline{c}}$ and $Y_{\overline{c}}$ and apply the induction hypothesis; so $X_{\overline{c}}$ can be obtained from $Y_{\overline{c}}$ using at most $2(k-1)^2 + 2k + (2k - 2) = 2k^2$ swaps, as required.

If $n = 2k + 3$ is odd, the proof is similar but more technically involved. Namely, we claim that $d_{a,b}^*(X_{2k+3}, Y) \leqslant 2k^2 + 6k + 5$ for any chameleon Y, and that the equality is achieved only if $Y_{\overline{c}} = bb\ldots baa\ldots a$. The proof proceeds by a similar induction, with some care taken of the base case, as well as of extracting the equality case. Similar estimates hold for $d_{b,c}^*$ and $d_{c,a}^*$. Summing three such estimates, we obtain

$$d^*(X_{2k+3}, Y) \leqslant 3(2k^2 + 6k + 5) = \left\lceil \frac{3n^2}{2} \right\rceil + 1,$$

which is by 1 more than we need. But the equality could be achieved only if $Y_{\overline{c}} = bb\ldots baa\ldots a$ and, similarly, $Y_{\overline{b}} = aa\ldots acc\ldots c$ and $Y_{\overline{a}} = cc\ldots cbb\ldots b$. Since these three equalities cannot hold simultaneously, the proof is finished.

C3.   Sir Alex plays the following game on a row of 9 cells. Initially, all cells are empty. In each move, Sir Alex is allowed to perform exactly one of the following two operations:

(1) Choose any number of the form 2^j, where j is a non-negative integer, and put it into an empty cell.

(2) Choose two (not necessarily adjacent) cells with the same number in them; denote that number by 2^j. Replace the number in one of the cells with 2^{j+1} and erase the number in the other cell.

At the end of the game, one cell contains the number 2^n, where n is a given positive integer, while the other cells are empty. Determine the maximum number of moves that Sir Alex could have made, in terms of n.

(Thailand)

Answer: $2\sum_{j=0}^{8}\binom{n}{j} - 1$.

Solution 1.   We will solve a more general problem, replacing the row of 9 cells with a row of k cells, where k is a positive integer. Denote by $m(n,k)$ the maximum possible number of moves Sir Alex can make starting with a row of k empty cells, and ending with one cell containing the number 2^n and all the other $k-1$ cells empty. Call an operation of type (1) an *insertion*, and an operation of type (2) a *merge*.

Only one move is possible when $k=1$, so we have $m(n,1)=1$. From now on we consider $k \geqslant 2$, and we may assume Sir Alex's last move was a merge. Then, just before the last move, there were exactly two cells with the number 2^{n-1}, and the other $k-2$ cells were empty.

Paint one of those numbers 2^{n-1} blue, and the other one red. Now trace back Sir Alex's moves, always painting the numbers blue or red following this rule: *if a and b merge into c, paint a and b with the same color as c.* Notice that in this backward process new numbers are produced only by reversing merges, since reversing an insertion simply means deleting one of the numbers. Therefore, all numbers appearing in the whole process will receive one of the two colors.

Sir Alex's first move is an insertion. Without loss of generality, assume this first number inserted is blue. Then, from this point on, until the last move, there is always at least one cell with a blue number.

Besides the last move, there is no move involving a blue and a red number, since all merges involves numbers with the same color, and insertions involve only one number. Call an insertion of a blue number or merge of two blue numbers a *blue move*, and define a *red move* analogously.

The whole sequence of blue moves could be repeated on another row of k cells to produce one cell with the number 2^{n-1} and all the others empty, so there are at most $m(n-1,k)$ blue moves.

Now we look at the red moves. Since every time we perform a red move there is at least one cell occupied with a blue number, the whole sequence of red moves could be repeated on a row of $k-1$ cells to produce one cell with the number 2^{n-1} and all the others empty, so there are at most $m(n-1,k-1)$ red moves. This proves that

$$m(n,k) \leqslant m(n-1,k) + m(n-1,k-1) + 1.$$

On the other hand, we can start with an empty row of k cells and perform $m(n-1,k)$ moves to produce one cell with the number 2^{n-1} and all the others empty, and after that perform $m(n-1,k-1)$ moves on those $k-1$ empty cells to produce the number 2^{n-1} in one of them, leaving $k-2$ empty. With one more merge we get one cell with 2^n and the others empty, proving that

$$m(n,k) \geqslant m(n-1,k) + m(n-1,k-1) + 1.$$

It follows that

$$m(n, k) = m(n - 1, k) + m(n - 1, k - 1) + 1, \tag{1}$$

for $n \geqslant 1$ and $k \geqslant 2$.

If $k = 1$ or $n = 0$, we must insert 2^n on our first move and immediately get the final configuration, so $m(0, k) = 1$ and $m(n, 1) = 1$, for $n \geqslant 0$ and $k \geqslant 1$. These initial values, together with the recurrence relation (1), determine $m(n, k)$ uniquely.

Finally, we show that

$$m(n, k) = 2 \sum_{j=0}^{k-1} \binom{n}{j} - 1, \tag{2}$$

for all integers $n \geqslant 0$ and $k \geqslant 1$.

We use induction on n. Since $m(0, k) = 1$ for $k \geqslant 1$, (2) is true for the base case. We make the induction hypothesis that (2) is true for some fixed positive integer n and all $k \geqslant 1$. We have $m(n + 1, 1) = 1 = 2\binom{n+1}{0} - 1$, and for $k \geqslant 2$ the recurrence relation (1) and the induction hypothesis give us

$$m(n + 1, k) = m(n, k) + m(n, k - 1) + 1 = 2 \sum_{j=0}^{k-1} \binom{n}{j} - 1 + 2 \sum_{j=0}^{k-2} \binom{n}{j} - 1 + 1$$

$$= 2 \sum_{j=0}^{k-1} \binom{n}{j} + 2 \sum_{j=0}^{k-1} \binom{n}{j-1} - 1 = 2 \sum_{j=0}^{k-1} \left(\binom{n}{j} + \binom{n}{j-1} \right) - 1 = 2 \sum_{j=0}^{k-1} \binom{n+1}{j} - 1,$$

which completes the proof.

Comment 1. After deducing the recurrence relation (1), it may be convenient to homogenize the recurrence relation by defining $h(n, k) = m(n, k) + 1$. We get the new relation

$$h(n, k) = h(n - 1, k) + h(n - 1, k), \tag{3}$$

for $n \geqslant 1$ and $k \geqslant 2$, with initial values $h(0, k) = h(n, 1) = 2$, for $n \geqslant 0$ and $k \geqslant 1$.

This may help one to guess the answer, and also with other approaches like the one we develop next.

Comment 2. We can use a generating function to find the answer without guessing. We work with the homogenized recurrence relation (3). Define $h(n, 0) = 0$ so that (3) is valid for $k = 1$ as well. Now we set up the generating function $f(x, y) = \sum_{n,k \geqslant 0} h(n, k) x^n y^k$. Multiplying the recurrence relation (3) by $x^n y^k$ and summing over $n, k \geqslant 1$, we get

$$\sum_{n,k \geqslant 1} h(n, k) x^n y^k = x \sum_{n,k \geqslant 1} h(n - 1, k) x^{n-1} y^k + xy \sum_{n,k \geqslant 1} h(n - 1, k - 1) x^{n-1} y^{k-1}.$$

Completing the missing terms leads to the following equation on $f(x, y)$:

$$f(x, y) - \sum_{n \geqslant 0} h(n, 0) x^n - \sum_{k \geqslant 1} h(0, k) y^k = xf(x, y) - x \sum_{n \geqslant 0} h(n, 0) x^n + xyf(x, y).$$

Substituting the initial values, we obtain

$$f(x, y) = \frac{2y}{1 - y} \cdot \frac{1}{1 - x(1 + y)}.$$

Developing as a power series, we get

$$f(x, y) = 2 \sum_{j \geqslant 1} y^j \cdot \sum_{n \geqslant 0} (1 + y)^n x^n.$$

The coefficient of x^n in this power series is

$$2\sum_{j\geqslant 1} y^j \cdot (1+y)^n = 2\sum_{j\geqslant 1} y^j \cdot \sum_{i\geqslant 0}\binom{n}{i}y^i,$$

and extracting the coefficient of y^k in this last expression we finally obtain the value for $h(n,k)$,

$$h(n,k) = 2\sum_{j=0}^{k-1}\binom{n}{j}.$$

This proves that

$$m(n,k) = 2\sum_{j=0}^{k-1}\binom{n}{j} - 1.$$

The generating function approach also works if applied to the non-homogeneous recurrence relation (1), but the computations are less straightforward.

Solution 2. Define merges and insertions as in Solution 1. After each move made by Sir Alex we compute the number N of empty cells, and the sum S of all the numbers written in the cells. Insertions always increase S by some power of 2, and increase N exactly by 1. Merges do not change S and decrease N exactly by 1. Since the initial value of N is 0 and its final value is 1, the total number of insertions exceeds that of merges by exactly one. So, to maximize the number of moves, we need to maximize the number of insertions.

We will need the following lemma.

Lemma. If the binary representation of a positive integer A has d nonzero digits, then A cannot be represented as a sum of fewer than d powers of 2. Moreover, any representation of A as a sum of d powers of 2 must coincide with its binary representation.

Proof. Let s be the minimum number of summands in all possible representations of A as sum of powers of 2. Suppose there is such a representation with s summands, where two of the summands are equal to each other. Then, replacing those two summands with the result of their sum, we obtain a representation with fewer than s summands, which is a contradiction. We deduce that in any representation with s summands, the summands are all distinct, so any such representation must coincide with the unique binary representation of A, and $s = d$. $\qquad\square$

Now we split the solution into a sequence of claims.

Claim 1. After every move, the number S is the sum of at most $k-1$ distinct powers of 2.

Proof. If S is the sum of k (or more) distinct powers of 2, the Lemma implies that the k cells are filled with these numbers. This is a contradiction since no more merges or insertions can be made. $\qquad\square$

Let $A(n,k-1)$ denote the set of all positive integers not exceeding 2^n with at most $k-1$ nonzero digits in its base 2 representation. Since every insertion increases the value of S, by Claim 1, the total number of insertions is at most $|A(n,k-1)|$. We proceed to prove that it is possible to achieve this number of insertions.

Claim 2. Let $A(n,k-1) = \{a_1, a_2, \ldots, a_m\}$, with $a_1 < a_2 < \cdots < a_m$. If after some of Sir Alex's moves the value of S is a_j, with $j \in \{1, 2, \ldots, m-1\}$, then there is a sequence of moves after which the value of S is exactly a_{j+1}.

Proof. Suppose $S = a_j$. Performing all possible merges, we eventually get different powers of 2 in all nonempty cells. After that, by Claim 1 there will be at least one empty cell, in which we want to insert $a_{j+1} - a_j$. It remains to show that $a_{j+1} - a_j$ is a power of 2.

For this purpose, we notice that if a_j has less than $k-1$ nonzero digits in base 2 then $a_{j+1} = a_j + 1$. Otherwise, we have $a_j = 2^{b_{k-1}} + \cdots + 2^{b_2} + 2^{b_1}$ with $b_1 < b_2 < \cdots < b_{k-1}$. Then, adding any number less than 2^{b_1} to a_j will result in a number with more than $k-1$ nonzero

binary digits. On the other hand, $a_j + 2^{b_1}$ is a sum of k powers of 2, not all distinct, so by the Lemma it will be a sum of less then k distinct powers of 2. This means that $a_{j+1} - a_j = 2^{b_1}$, completing the proof. $\qquad\square$

Claims 1 and 2 prove that the maximum number of insertions is $|A(n, k-1)|$. We now compute this number.

Claim 3. $|A(n, k-1)| = \sum_{j=0}^{k-1} \binom{n}{j}$.

Proof. The number 2^n is the only element of $A(n, k-1)$ with $n+1$ binary digits. Any other element has at most n binary digits, at least one and at most $k-1$ of them are nonzero (so they are ones). For each $j \in \{1, 2, \ldots, k-1\}$, there are $\binom{n}{j}$ such elements with exactly j binary digits equal to one. We conclude that $|A(n, k-1)| = 1 + \sum_{j=1}^{k-1} \binom{n}{j} = \sum_{j=0}^{k-1} \binom{n}{j}$. $\qquad\square$

Recalling that the number of insertions exceeds that of merges by exactly 1, we deduce that the maximum number of moves is $2\sum_{j=0}^{k-1} \binom{n}{j} - 1$.

C4.   Let $N \geqslant 2$ be an integer. $N(N + 1)$ soccer players, no two of the same height, stand in a row in some order. Coach Ralph wants to remove $N(N - 1)$ people from this row so that in the remaining row of $2N$ players, no one stands between the two tallest ones, no one stands between the third and the fourth tallest ones, ..., and finally no one stands between the two shortest ones. Show that this is always possible.

(Russia)

Solution 1.   Split the row into N blocks with $N + 1$ consecutive people each. We will show how to remove $N - 1$ people from each block in order to satisfy the coach's wish.

First, construct a $(N + 1) \times N$ matrix where $x_{i,j}$ is the height of the ith tallest person of the jth block—in other words, each column lists the heights within a single block, sorted in decreasing order from top to bottom.

We will reorder this matrix by repeatedly swapping whole columns. First, by column permutation, make sure that $x_{2,1} = \max\{x_{2,i} : i = 1, 2, \ldots, N\}$ (the first column contains the largest height of the *second* row). With the first column fixed, permute the other ones so that $x_{3,2} = \max\{x_{3,i} : i = 2, \ldots, N\}$ (the second column contains the tallest person of the *third* row, first column excluded). In short, at step k ($k = 1, 2, \ldots, N - 1$), we permute the columns from k to N so that $x_{k+1,k} = \max\{x_{i,k} : i = k, k + 1, \ldots, N\}$, and end up with an array like this:

$$
\begin{array}{ccccc}
\boldsymbol{x_{1,1}} & x_{1,2} & x_{1,3} \cdots & x_{1,N-1} & x_{1,N} \\
\vee & \vee & \vee & \vee & \vee \\
\boldsymbol{x_{2,1}} > \boldsymbol{x_{2,2}} & x_{2,3} \cdots & x_{2,N-1} & x_{2,N} \\
\vee & \vee & \vee & \vee & \vee \\
x_{3,1} & \boldsymbol{x_{3,2}} > \boldsymbol{x_{3,3}} \cdots & x_{3,N-1} & x_{3,N} \\
\vee & \vee & \vee & \vee & \vee \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\vee & \vee & \vee & \vee & \vee \\
x_{N,1} & x_{N,2} & x_{N,3} \cdots \boldsymbol{x_{N,N-1}} > \boldsymbol{x_{N,N}} \\
\vee & \vee & \vee & \vee & \vee \\
x_{N+1,1} & x_{N+1,2} & x_{N+1,3} \cdots x_{N+1,N-1} & \boldsymbol{x_{N+1,N}}
\end{array}
$$

Now we make the bold choice: from the original row of people, remove everyone but those with heights

$$x_{1,1} > x_{2,1} > x_{2,2} > x_{3,2} > \cdots > x_{N,N-1} > x_{N,N} > x_{N+1,N} \tag{$*$}$$

Of course this *height* order $(*)$ is not necessarily their *spatial* order in the new row. We now need to convince ourselves that each pair $(x_{k,k}; x_{k+1,k})$ remains spatially together in this new row. But $x_{k,k}$ and $x_{k+1,k}$ belong to the same column/block of consecutive $N + 1$ people; the only people that could possibly stand between them were also in this block, and they are all gone.

Solution 2.   Split the people into N groups *by height*: group G_1 has the $N + 1$ tallest ones, group G_2 has the next $N + 1$ tallest, and so on, up to group G_N with the $N + 1$ shortest people.

Now scan the original row from left to right, stopping as soon as you have scanned two people (consecutively or not) from the same group, say, G_i. Since we have N groups, this must happen before or at the $(N + 1)^{\text{th}}$ person of the row. Choose this pair of people, removing all the other people from the same group G_i and also all people that have been scanned so far. The only people that could separate this pair's heights were in group G_i (and they are gone); the only people that could separate this pair's positions were already scanned (and they are gone too).

We are now left with $N - 1$ groups (all except G_i). Since each of them lost at most one person, each one has at least N unscanned people left in the row. Repeat the scanning process from left to right, choosing the next two people from the same group, removing this group and

everyone scanned up to that point. Once again we end up with two people who are next to each other in the remaining row and whose heights cannot be separated by anyone else who remains (since the rest of their group is gone). After picking these 2 pairs, we still have $N - 2$ groups with at least $N - 1$ people each.

If we repeat the scanning process a total of N times, it is easy to check that we will end up with 2 people from each group, for a total of $2N$ people remaining. The height order is guaranteed by the grouping, and the scanning construction from left to right guarantees that each pair from a group stand next to each other in the final row. We are done.

Solution 3. This is essentially the same as solution 1, but presented inductively. The essence of the argument is the following lemma.

Lemma. Assume that we have N disjoint groups of at least $N + 1$ people in each, all people have distinct heights. Then one can choose two people from each group so that among the chosen people, the two tallest ones are in one group, the third and the fourth tallest ones are in one group, ..., and the two shortest ones are in one group.

Proof. Induction on $N \geqslant 1$; for $N = 1$, the statement is trivial.

Consider now N groups $G_1, \ldots, G_N$ with at least $N+1$ people in each for $N \geqslant 2$. Enumerate the people by $1, 2, \ldots, N(N + 1)$ according to their height, say, from tallest to shortest. Find the least s such that two people among $1, 2, \ldots, s$ are in one group (without loss of generality, say this group is G_N). By the minimality of s, the two mentioned people in G_N are s and some $i < s$.

Now we choose people i and s in G_N, forget about this group, and remove the people $1, 2, \ldots, s$ from $G_1, \ldots, G_{N-1}$. Due to minimality of s again, each of the obtained groups $G'_1, \ldots, G'_{N-1}$ contains at least N people. By the induction hypothesis, one can choose a pair of people from each of $G'_1, \ldots, G'_{N-1}$ so as to satisfy the required conditions. Since all these people have numbers greater than s, addition of the pair (s, i) from G_N does not violate these requirements. $\square$

To solve the problem, it suffices now to split the row into N contiguous groups with $N + 1$ people in each and apply the Lemma to those groups.

Comment 1. One can identify each person with a pair of indices (p, h) $(p, h \in \{1, 2, \ldots, N(N + 1)\})$ so that the pth person in the row (say, from left to right) is the hth tallest person in the group. Say that (a, b) *separates* (x_1, y_1) and (x_2, y_2) whenever a is strictly between x_1 and y_1, *or* b is strictly between x_2 and y_2. So the coach wants to pick $2N$ people $(p_i, h_i)(i = 1, 2, \ldots, 2N)$ such that no chosen person separates (p_1, h_1) from (p_2, h_2), no chosen person separates (p_3, h_3) and (p_4, h_4), and so on. This formulation reveals a duality between positions and heights. In that sense, solutions 1 and 2 are dual of each other.

Comment 2. The number $N(N + 1)$ is sharp for $N = 2$ and $N = 3$, due to arrangements $1, 5, 3, 4, 2$ and $1, 10, 6, 4, 3, 9, 5, 8, 7, 2, 11$.

C5.   A hunter and an invisible rabbit play a game in the Euclidean plane. The hunter's starting point H_0 coincides with the rabbit's starting point R_0. In the nth round of the game ($n \geqslant 1$), the following happens.

(1) First the invisible rabbit moves secretly and unobserved from its current point R_{n-1} to some new point R_n with $R_{n-1}R_n = 1$.

(2) The hunter has a tracking device (e.g. dog) that returns an approximate position R'_n of the rabbit, so that $R_nR'_n \leqslant 1$.

(3) The hunter then visibly moves from point H_{n-1} to a new point H_n with $H_{n-1}H_n = 1$.

Is there a strategy for the hunter that guarantees that after 10^9 such rounds the distance between the hunter and the rabbit is below 100?

(Austria)

Answer: There is no such strategy for the hunter. The rabbit "wins".

Solution. If the answer were "yes", the hunter would have a strategy that would "work", no matter how the rabbit moved or where the radar pings R'_n appeared. We will show the opposite: with bad luck from the radar pings, there is no strategy for the hunter that guarantees that the distance stays below 100 in 10^9 rounds.

So, let d_n be the distance between the hunter and the rabbit after n rounds. Of course, if $d_n \geqslant 100$ for any $n < 10^9$, the rabbit has won — it just needs to move straight away from the hunter, and the distance will be kept at or above 100 thereon.

We will now show that, while $d_n < 100$, whatever given strategy the hunter follows, the rabbit has a way of increasing d_n^2 by at least $\frac{1}{2}$ every 200 rounds (as long as the radar pings are lucky enough for the rabbit). This way, d_n^2 will reach 10^4 in less than $2 \cdot 10^4 \cdot 200 = 4 \cdot 10^6 < 10^9$ rounds, and the rabbit wins.

Suppose the hunter is at H_n and the rabbit is at R_n. Suppose even that the rabbit *reveals* its position at this moment to the hunter (this allows us to ignore all information from previous radar pings). Let r be the line H_nR_n, and Y_1 and Y_2 be points which are 1 unit away from r and 200 units away from R_n, as in the figure below.
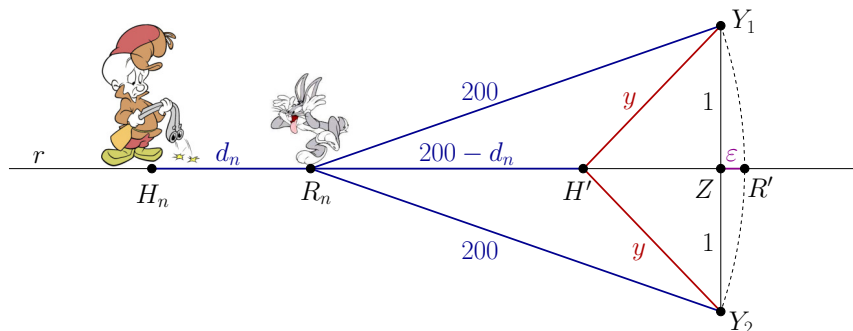
The rabbit's plan is simply to choose one of the points Y_1 or Y_2 and hop 200 rounds straight towards it. Since all hops stay within 1 distance unit from r, it is possible that all radar pings stay on r. In particular, in this case, the hunter has no way of knowing whether the rabbit chose Y_1 or Y_2.

Looking at such pings, what is the hunter going to do? If the hunter's strategy tells him to go 200 rounds straight to the right, he ends up at point H' in the figure. Note that the hunter does not have a better alternative! Indeed, after these 200 rounds he will always end up at a point to the left of H'. If his strategy took him to a point above r, he would end up even further from Y_2; and if his strategy took him below r, he would end up even further from Y_1. In other words, no matter what strategy the hunter follows, he can never be sure his distance to the rabbit will be less than $y \stackrel{\text{def}}{=} H'Y_1 = H'Y_2$ after these 200 rounds.

To estimate y^2, we take Z as the midpoint of segment Y_1Y_2, we take R' as a point 200 units to the right of R_n and we define $\varepsilon = ZR'$ (note that $H'R' = d_n$). Then

$$y^2 = 1 + (H'Z)^2 = 1 + (d_n - \varepsilon)^2$$

where

$$\varepsilon = 200 - R_n Z = 200 - \sqrt{200^2 - 1} = \frac{1}{200 + \sqrt{200^2 - 1}} > \frac{1}{400}.$$

In particular, $\varepsilon^2 + 1 = 400\varepsilon$, so

$$y^2 = d_n^2 - 2\varepsilon d_n + \varepsilon^2 + 1 = d_n^2 + \varepsilon(400 - 2d_n).$$

Since $\varepsilon > \frac{1}{400}$ and we assumed $d_n < 100$, this shows that $y^2 > d_n^2 + \frac{1}{2}$. So, as we claimed, with this list of radar pings, no matter what the hunter does, the rabbit might achieve $d_{n+200}^2 > d_n^2 + \frac{1}{2}$. The wabbit wins.

Comment 1. Many different versions of the solution above can be found by replacing 200 with some other number N for the number of hops the rabbit takes between reveals. If this is done, we have:

$$\varepsilon = N - \sqrt{N^2 - 1} > \frac{1}{N + \sqrt{N^2 - 1}} > \frac{1}{2N}$$

and

$$\varepsilon^2 + 1 = 2N\varepsilon,$$

so, as long as $N > d_n$, we would find

$$y^2 = d_n^2 + \varepsilon(2N - 2d_n) > d_n^2 + \frac{N - d_n}{N}.$$

For example, taking $N = 101$ is already enough—the squared distance increases by at least $\frac{1}{101}$ every 101 rounds, and $101^2 \cdot 10^4 = 1.0201 \cdot 10^8 < 10^9$ rounds are enough for the rabbit. If the statement is made sharper, some such versions might not work any longer.

Comment 2. The original statement asked whether the distance could be kept under 10^{10} in 10^{100} rounds.

C6.   Let $n > 1$ be an integer. An $n \times n \times n$ cube is composed of n^3 unit cubes. Each unit cube is painted with one color. For each $n \times n \times 1$ box consisting of n^2 unit cubes (of any of the three possible orientations), we consider the set of the colors present in that box (each color is listed only once). This way, we get $3n$ sets of colors, split into three groups according to the orientation. It happens that for every set in any group, the same set appears in both of the other groups. Determine, in terms of n, the maximal possible number of colors that are present.

(Russia)

Answer: The maximal number is $\frac{n(n+1)(2n+1)}{6}$.

Solution 1.   Call a $n \times n \times 1$ box an *x-box*, a *y-box*, or a *z-box*, according to the direction of its short side. Let C be the number of colors in a valid configuration. We start with the upper bound for C.

Let $\mathcal{C}_1$, $\mathcal{C}_2$, and $\mathcal{C}_3$ be the sets of colors which appear in the big cube exactly once, exactly twice, and at least thrice, respectively. Let M_i be the set of unit cubes whose colors are in $\mathcal{C}_i$, and denote $n_i = |M_i|$.

Consider any x-box X, and let Y and Z be a y- and a z-box containing the same set of colors as X does.

Claim. $4|X \cap M_1| + |X \cap M_2| \leqslant 3n + 1$.

Proof. We distinguish two cases.

Case 1: $X \cap M_1 \neq \varnothing$.

A cube from $X \cap M_1$ should appear in all three boxes X, Y, and Z, so it should lie in $X \cap Y \cap Z$. Thus $X \cap M_1 = X \cap Y \cap Z$ and $|X \cap M_1| = 1$.

Consider now the cubes in $X \cap M_2$. There are at most $2(n-1)$ of them lying in $X \cap Y$ or $X \cap Z$ (because the cube from $X \cap Y \cap Z$ is in M_1). Let a be some *other* cube from $X \cap M_2$. Recall that there is just one other cube a' sharing a color with a. But both Y and Z should contain such cube, so $a' \in Y \cap Z$ (but $a' \notin X \cap Y \cap Z$). The map $a \mapsto a'$ is clearly injective, so the number of cubes a we are interested in does not exceed $|(Y \cap Z) \setminus X| = n - 1$. Thus $|X \cap M_2| \leqslant 2(n-1) + (n-1) = 3(n-1)$, and hence $4|X \cap M_1| + |X \cap M_2| \leqslant 4 + 3(n-1) = 3n+1$.

Case 2: $X \cap M_1 = \varnothing$.

In this case, the same argument applies with several changes. Indeed, $X \cap M_2$ contains at most $2n - 1$ cubes from $X \cap Y$ or $X \cap Z$. Any other cube a in $X \cap M_2$ corresponds to some $a' \in Y \cap Z$ (possibly with $a' \in X$), so there are at most n of them. All this results in $|X \cap M_2| \leqslant (2n-1) + n = 3n - 1$, which is even better than we need (by the assumptions of our case). $\square$

Summing up the inequalities from the Claim over all x-boxes X, we obtain

$$4n_1 + n_2 \leqslant n(3n + 1).$$

Obviously, we also have $n_1 + n_2 + n_3 = n^3$.

Now we are prepared to estimate C. Due to the definition of the M_i, we have $n_i \geqslant i|\mathcal{C}_i|$, so

$$C \leqslant n_1 + \frac{n_2}{2} + \frac{n_3}{3} = \frac{n_1 + n_2 + n_3}{3} + \frac{4n_1 + n_2}{6} \leqslant \frac{n^3}{3} + \frac{3n^2 + n}{6} = \frac{n(n+1)(2n+1)}{6}.$$

It remains to present an example of an appropriate coloring in the above-mentioned number of colors. For each color, we present the set of all cubes of this color. These sets are:

1. n singletons of the form $S_i = \{(i, i, i)\}$ (with $1 \leqslant i \leqslant n$);

2. $3\binom{n}{2}$ doubletons of the forms $D_{i,j}^1 = \{(i, j, j), (j, i, i)\}$, $D_{i,j}^2 = \{(j, i, j), (i, j, i)\}$, and $D_{i,j}^3 = \{(j, j, i), (i, i, j)\}$ (with $1 \leqslant i < j \leqslant n$);

3. $2\binom{n}{3}$ triplets of the form $T_{i,j,k} = \{(i,j,k),(j,k,i),(k,i,j)\}$ (with $1 \leqslant i < j < k \leqslant n$ or $1 \leqslant i < k < j \leqslant n$).

One may easily see that the ith boxes of each orientation contain the same set of colors, and that
$$n + \frac{3n(n-1)}{2} + \frac{n(n-1)(n-2)}{3} = \frac{n(n+1)(2n+1)}{6}$$
colors are used, as required.

Solution 2. We will approach a new version of the original problem. In this new version, each cube may have a color, or be *invisible* (not both). Now we make sets of colors for each $n \times n \times 1$ box as before (where "invisible" is not considered a color) and group them by orientation, also as before. Finally, we require that, for every *non-empty* set in any group, the same set must appear in the other 2 groups. What is the maximum number of colors present with these new requirements?

Let us call *strange* a big $n \times n \times n$ cube whose painting scheme satisfies the new requirements, and let D be the number of colors in a strange cube. Note that any cube that satisfies the original requirements is also strange, so $\max(D)$ is an upper bound for the original answer.

Claim. $D \leqslant \frac{n(n+1)(2n+1)}{6}$.

Proof. The proof is by induction on n. If $n = 1$, we must paint the cube with at most 1 color.

Now, pick a $n \times n \times n$ strange cube A, where $n \geqslant 2$. If A is completely invisible, $D = 0$ and we are done. Otherwise, pick a non-empty set of colors $\mathcal{S}$ which corresponds to, say, the boxes X, Y and Z of different orientations.

Now find all cubes in A whose colors are in $\mathcal{S}$ and make them invisible. Since X, Y and Z are now completely invisible, we can throw them away and focus on the remaining $(n-1) \times (n-1) \times (n-1)$ cube B. The sets of colors in all the groups for B are the same as the sets for A, removing exactly the colors in $\mathcal{S}$, and no others! Therefore, every nonempty set that appears in one group for B still shows up in all possible orientations (it is possible that an empty set of colors in B only matched X, Y or Z before these were thrown away, but remember we do not require empty sets to match anyway). In summary, B is also strange.

By the induction hypothesis, we may assume that B has at most $\frac{(n-1)n(2n-1)}{6}$ colors. Since there were at most n^2 different colors in $\mathcal{S}$, we have that A has at most $\frac{(n-1)n(2n-1)}{6} + n^2 = \frac{n(n+1)(2n+1)}{6}$ colors. $\qquad\square$

Finally, the construction in the previous solution shows a painting scheme (with no invisible cubes) that reaches this maximum, so we are done.

C7.   For any finite sets X and Y of positive integers, denote by $f_X(k)$ the kth smallest positive integer not in X, and let

$$X * Y = X \cup \{f_X(y) \colon y \in Y\}.$$

Let A be a set of $a > 0$ positive integers, and let B be a set of $b > 0$ positive integers. Prove that if $A * B = B * A$, then

$$\underbrace{A * (A * \cdots * (A * (A * A)) \ldots)}_{A \text{ appears } b \text{ times}} = \underbrace{B * (B * \cdots * (B * (B * B)) \ldots)}_{B \text{ appears } a \text{ times}}.$$

(U.S.A.)

Solution 1.   For any function $g \colon \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ and any subset $X \subset \mathbb{Z}_{>0}$, we define $g(X) = \{g(x) \colon x \in X\}$. We have that the image of f_X is $f_X(\mathbb{Z}_{>0}) = \mathbb{Z}_{>0} \setminus X$. We now show a general lemma about the operation $*$, with the goal of showing that $*$ is associative.

Lemma 1. Let X and Y be finite sets of positive integers. The functions f_{X*Y} and $f_X \circ f_Y$ are equal.

Proof. We have

$$f_{X*Y}(\mathbb{Z}_{>0}) = \mathbb{Z}_{>0} \setminus (X*Y) = (\mathbb{Z}_{>0} \setminus X) \setminus f_X(Y) = f_X(\mathbb{Z}_{>0}) \setminus f_X(Y) = f_X(\mathbb{Z}_{>0} \setminus Y) = f_X(f_Y(\mathbb{Z}_{>0})).$$

Thus, the functions f_{X*Y} and $f_X \circ f_Y$ are strictly increasing functions with the same range. Because a strictly function is uniquely defined by its range, we have $f_{X*Y} = f_X \circ f_Y$. $\square$

Lemma 1 implies that $*$ is associative, in the sense that $(A * B) * C = A * (B * C)$ for any finite sets A, B, and C of positive integers. We prove the associativity by noting

$$\mathbb{Z}_{>0} \setminus ((A * B) * C) = f_{(A*B)*C}(\mathbb{Z}_{>0}) = f_{A*B}(f_C(\mathbb{Z}_{>0})) = f_A(f_B(f_C(\mathbb{Z}_{>0})))$$

$$= f_A(f_{B*C}(\mathbb{Z}_{>0}) = f_{A*(B*C)}(\mathbb{Z}_{>0}) = \mathbb{Z}_{>0} \setminus (A * (B * C)).$$

In light of the associativity of $*$, we may drop the parentheses when we write expressions like $A * (B * C)$. We also introduce the notation

$$X^{*k} = \underbrace{X * (X * \cdots * (X * (X * X)) \ldots)}_{X \text{ appears } k \text{ times}}.$$

Our goal is then to show that $A * B = B * A$ implies $A^{*b} = B^{*a}$. We will do so via the following general lemma.

Lemma 2. Suppose that X and Y are finite sets of positive integers satisfying $X * Y = Y * X$ and $|X| = |Y|$. Then, we must have $X = Y$.

Proof. Assume that X and Y are not equal. Let s be the largest number in exactly one of X and Y. Without loss of generality, say that $s \in X \setminus Y$. The number $f_X(s)$ counts the sth number not in X, which implies that

$$f_X(s) = s + \big| X \cap \{1, 2, \ldots, f_X(s)\} \big|. \tag{1}$$

Since $f_X(s) \geqslant s$, we have that

$$\big\{f_X(s) + 1, f_X(s) + 2, \ldots \big\} \cap X = \big\{f_X(s) + 1, f_X(s) + 2, \ldots \big\} \cap Y,$$

which, together with the assumption that $|X| = |Y|$, gives

$$\big| X \cap \{1, 2, \ldots, f_X(s)\} \big| = \big| Y \cap \{1, 2, \ldots, f_X(s)\} \big|. \tag{2}$$

Now consider the equation

$$t - \big| Y \cap \{1, 2, \ldots, t\} \big| = s.$$

This equation is satisfied only when $t \in \big[f_Y(s), f_Y(s+1) \big)$, because the left hand side counts the number of elements up to t that are not in Y. We have that the value $t = f_X(s)$ satisfies the above equation because of (1) and (2). Furthermore, since $f_X(s) \notin X$ and $f_X(s) \geqslant s$, we have that $f_X(s) \notin Y$ due to the maximality of s. Thus, by the above discussion, we must have $f_X(s) = f_Y(s)$.

Finally, we arrive at a contradiction. The value $f_X(s)$ is neither in X nor in $f_X(Y)$, because s is not in Y by assumption. Thus, $f_X(s) \notin X * Y$. However, since $s \in X$, we have $f_Y(s) \in Y * X$, a contradiction. $\qquad\square$

We are now ready to finish the proof. Note first of all that $|A^{*b}| = ab = |B^{*a}|$. Moreover, since $A * B = B * A$, and $*$ is associative, it follows that $A^{*b} * B^{*a} = B^{*a} * A^{*b}$. Thus, by Lemma 2, we have $A^{*b} = B^{*a}$, as desired.

Comment 1. Taking $A = X^{*k}$ and $B = X^{*l}$ generates many non-trivial examples where $A * B = B * A$. There are also other examples not of this form. For example, if $A = \{1, 2, 4\}$ and $B = \{1, 3\}$, then $A * B = \{1, 2, 3, 4, 6\} = B * A$.

Solution 2. We will use Lemma 1 from Solution 1. Additionally, let X^{*k} be defined as in Solution 1. If X and Y are finite sets, then

$$f_X = f_Y \iff f_X(\mathbb{Z}_{>0}) = f_Y(\mathbb{Z}_{>0}) \iff (\mathbb{Z}_{>0} \setminus X) = (\mathbb{Z}_{>0} \setminus Y) \iff X = Y, \qquad (3)$$

where the first equivalence is because f_X and f_Y are strictly increasing functions, and the second equivalence is because $f_X(\mathbb{Z}_{>0}) = \mathbb{Z}_{>0} \setminus X$ and $f_Y(\mathbb{Z}_{>0}) = \mathbb{Z}_{>0} \setminus Y$.

Denote $g = f_A$ and $h = f_B$. The given relation $A * B = B * A$ is equivalent to $f_{A*B} = f_{B*A}$ because of (3), and by Lemma 1 of the first solution, this is equivalent to $g \circ h = h \circ g$. Similarly, the required relation $A^{*b} = B^{*a}$ is equivalent to $g^b = h^a$. We will show that

$$g^b(n) = h^a(n) \qquad (4)$$

for all $n \in \mathbb{Z}_{>0}$, which suffices to solve the problem.

To start, we claim that (4) holds for all sufficiently large n. Indeed, let p and q be the maximal elements of A and B, respectively; we may assume that $p \geqslant q$. Then, for every $n \geqslant p$ we have $g(n) = n + a$ and $h(n) = n + b$, whence $g^b(n) = n + ab = h^a(n)$, as was claimed.

In view of this claim, if (4) is not identically true, then there exists a maximal s with $g^b(s) \neq h^a(s)$. Without loss of generality, we may assume that $g(s) \neq s$, for if we had $g(s) = h(s) = s$, then s would satisfy (4). As g is increasing, we then have $g(s) > s$, so (4) holds for $n = g(s)$. But then we have

$$g(g^b(s)) = g^{b+1}(s) = g^b(n) = h^a(n) = h^a(g(s)) = g(h^a(s)),$$

where the last equality holds in view of $g \circ h = h \circ g$. By the injectivity of g, the above equality yields $g^b(s) = h^a(s)$, which contradicts the choice of s. Thus, we have proved that (4) is identically true on $\mathbb{Z}_{>0}$, as desired.

Comment 2. We present another proof of Lemma 2 of the first solution.

Let $x = |X| = |Y|$. Say that u is the smallest number in X and v is the smallest number in Y; assume without loss of generality that $u \leqslant v$.

Let T be any finite set of positive integers, and define $t = |T|$. Enumerate the elements of X as $x_1 < x_2 < \cdots < x_n$. Define $S_m = f_{(T * X^{*(m-1)})}(X)$, and enumerate its elements $s_{m,1} < s_{m,2} < \cdots < s_{m,n}$. Note that the S_m are pairwise disjoint; indeed, if we have $m < m'$, then

$$S_m \subset T * X^{*m} \subset T * X^{*(m'-1)} \quad \text{and} \quad S_{m'} = (T * X^{*m'}) \setminus (T * X^{*(m'-1)})$$

We claim the following statement, which essentially says that the S_m are eventually linear translates of each other:

Claim. For every i, there exists some m_i and c_i such that for all $m > m_i$, we have that $s_{m,i} = t + mn - c_i$. Furthermore, the c_i do not depend on the choice of T.

First, we show that this claim implies Lemma 2. We may choose $T = X$ and $T = Y$. Then, there is some m' such that for all $m \geqslant m'$, we have

$$f_{X*m}(X) = f_{(Y*X*(m-1))}(X). \tag{5}$$

Because u is the minimum element of X, v is the minimum element of Y, and $u \leqslant v$, we have that

$$\left(\bigcup_{m=m'}^{\infty} f_{X*m}(X) \right) \cup X^{*m'} = \left(\bigcup_{m=m'}^{\infty} f_{(Y*X*(m-1))}(X) \right) \cup \left(Y * X^{*(m'-1)} \right) = \{u, u+1, \dots \},$$

and in both the first and second expressions, the unions are of pairwise distinct sets. By (5), we obtain $X^{*m'} = Y * X^{*(m'-1)}$. Now, because X and Y commute, we get $X^{*m'} = X^{*(m'-1)} * Y$, and so $X = Y$.

We now prove the claim.

Proof of the claim. We induct downwards on i, first proving the statement for $i = n$, and so on.

Assume that m is chosen so that all elements of S_m are greater than all elements of T (which is possible because T is finite). For $i = n$, we have that $s_{m,n} > s_{k,n}$ for every $k < m$. Thus, all $(m-1)n$ numbers of the form $s_{k,u}$ for $k < m$ and $1 \leqslant u \leqslant n$ are less than $s_{m,n}$. We then have that $s_{m,n}$ is the $((m-1)n + x_n)^{th}$ number not in T, which is equal to $t + (m-1)n + x_n$. So we may choose $c_n = x_n - n$, which does not depend on T, which proves the base case for the induction.

For $i < n$, we have again that all elements $s_{m,j}$ for $j < i$ and $s_{p,i}$ for $p < m$ are less than $s_{m,i}$, so $s_{m,i}$ is the $((m-1)i + x_i)^{th}$ element not in T or of the form $s_{p,j}$ for $j > i$ and $p < m$. But by the inductive hypothesis, each of the sequences $s_{p,j}$ is eventually periodic with period n, and thus the sequence $s_{m,i}$ such must be as well. Since each of the sequences $s_{p,j} - t$ with $j > i$ eventually do not depend on T, the sequence $s_{m,i} - t$ eventually does not depend on T either, so the inductive step is complete. This proves the claim and thus Lemma 2. $\qquad\square$

C8. Let n be a given positive integer. In the Cartesian plane, each lattice point with nonnegative coordinates initially contains a butterfly, and there are no other butterflies. The *neighborhood* of a lattice point c consists of all lattice points within the axis-aligned $(2n + 1) \times (2n + 1)$ square centered at c, apart from c itself. We call a butterfly *lonely, crowded*, or *comfortable*, depending on whether the number of butterflies in its neighborhood N is respectively less than, greater than, or equal to half of the number of lattice points in N.

Every minute, all lonely butterflies fly away simultaneously. This process goes on for as long as there are any lonely butterflies. Assuming that the process eventually stops, determine the number of comfortable butterflies at the final state.

(Bulgaria)

Answer: $n^2 + 1$.

Solution. We always identify a butterfly with the lattice point it is situated at. For two points p and q, we write $p \geqslant q$ if each coordinate of p is at least the corresponding coordinate of q. Let O be the origin, and let $\mathcal{Q}$ be the set of initially occupied points, i.e., of all lattice points with nonnegative coordinates. Let $\mathcal{R}_\mathrm{H} = \{(x, 0) \colon x \geqslant 0\}$ and $\mathcal{R}_\mathrm{V} = \{(0, y) \colon y \geqslant 0\}$ be the sets of the lattice points lying on the horizontal and vertical boundary rays of $\mathcal{Q}$. Denote by $N(a)$ the neighborhood of a lattice point a.

1. Initial observations. We call a set of lattice points *up-right closed* if its points stay in the set after being shifted by any lattice vector (i, j) with $i, j \geqslant 0$. Whenever the butterflies form a up-right closed set $\mathcal{S}$, we have $|N(p) \cap \mathcal{S}| \geqslant |N(q) \cap \mathcal{S}|$ for any two points $p, q \in \mathcal{S}$ with $p \geqslant q$. So, since $\mathcal{Q}$ is up-right closed, the set of butterflies at any moment also preserves this property. We assume all forthcoming sets of lattice points to be up-right closed.

When speaking of some set $\mathcal{S}$ of lattice points, we call its points *lonely, comfortable*, or *crowded* with respect to this set (i.e., as if the butterflies were exactly at all points of $\mathcal{S}$). We call a set $\mathcal{S} \subset \mathcal{Q}$ *stable* if it contains no lonely points. In what follows, we are interested only in those stable sets whose complements in $\mathcal{Q}$ are finite, because one can easily see that only a finite number of butterflies can fly away on each minute.

If the initial set $\mathcal{Q}$ of butterflies contains some stable set $\mathcal{S}$, then, clearly no butterfly of this set will fly away. On the other hand, the set $\mathcal{F}$ of all butterflies in the end of the process is stable. This means that $\mathcal{F}$ is the largest (with respect to inclusion) stable set within $\mathcal{Q}$, and we are about to describe this set.

2. A description of a final set. The following notion will be useful. Let $\mathcal{U} = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_d\}$ be a set of d pairwise non-parallel lattice vectors, each having a positive x- and a negative y-coordinate. Assume that they are numbered in increasing order according to slope. We now define a $\mathcal{U}$-*curve* to be the broken line $p_0 p_1 \ldots p_d$ such that $p_0 \in \mathcal{R}_\mathrm{V}$, $p_d \in \mathcal{R}_\mathrm{H}$, and $\overrightarrow{p_{i-1} p_i} = \vec{u}_i$ for all $i = 1, 2, \ldots, m$ (see the Figure below to the left).
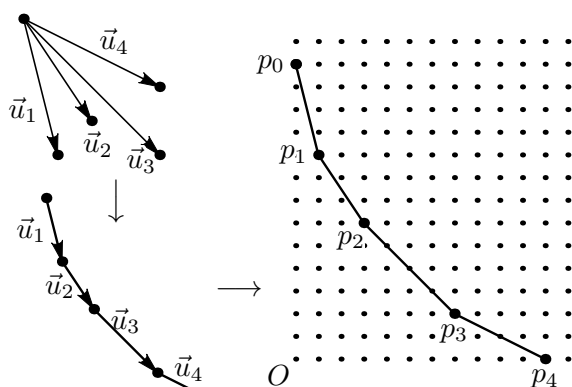
Construction of $\mathcal{U}$-curve
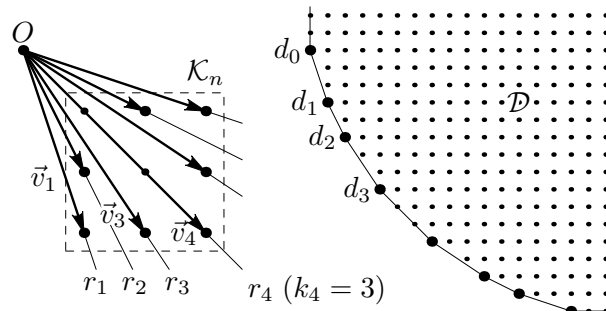
Construction of $\mathcal{D}$

Now, let $\mathcal{K}_n = \{(i, j) \colon 1 \leqslant i \leqslant n, \ -n \leqslant j \leqslant -1\}$. Consider all the rays emerging at O and passing through a point from $\mathcal{K}_n$; number them as $r_1, \ldots, r_m$ in increasing order according to slope. Let A_i be the farthest from O lattice point in $r_i \cap \mathcal{K}_n$, set $k_i = |r_i \cap \mathcal{K}_n|$, let $\vec{v}_i = \overrightarrow{OA_i}$, and finally denote $\mathcal{V} = \{\vec{v}_i \colon 1 \leqslant i \leqslant m\}$; see the Figure above to the right. We will concentrate on the $\mathcal{V}$-curve $d_0 d_1 \ldots d_m$; let $\mathcal{D}$ be the set of all lattice points p such that $p \geqslant p'$ for some (not necessarily lattice) point p' on the $\mathcal{V}$-curve. In fact, we will show that $\mathcal{D} = \mathcal{F}$.

Clearly, the $\mathcal{V}$-curve is symmetric in the line $y = x$. Denote by D the convex hull of $\mathcal{D}$.

3. We prove that the set $\mathcal{D}$ contains all stable sets. Let $\mathcal{S} \subset \mathcal{Q}$ be a stable set (recall that it is assumed to be up-right closed and to have a finite complement in $\mathcal{Q}$). Denote by S its convex hull; clearly, the vertices of S are lattice points. The boundary of S consists of two rays (horizontal and vertical ones) along with some $\mathcal{V}_*$-curve for some set of lattice vectors $\mathcal{V}_*$.

Claim 1. For every $\vec{v}_i \in \mathcal{V}$, there is a $\vec{v}_i^* \in \mathcal{V}_*$ co-directed with $\vec{v}$ with $|\vec{v}_i^*| \geqslant |\vec{v}|$.

Proof. Let ℓ be the supporting line of S parallel to $\vec{v}_i$ (i.e., ℓ contains some point of S, and the set S lies on one side of ℓ). Take any point $b \in \ell \cap \mathcal{S}$ and consider $N(b)$. The line ℓ splits the set $N(b) \setminus \ell$ into two congruent parts, one having an empty intersection with $\mathcal{S}$. Hence, in order for b not to be lonely, at least half of the set $\ell \cap N(b)$ (which contains $2k_i$ points) should lie in S. Thus, the boundary of S contains a segment $\ell \cap S$ with at least $k_i + 1$ lattice points (including b) on it; this segment corresponds to the required vector $\vec{v}_i^* \in \mathcal{V}_*$. $\qquad\square$
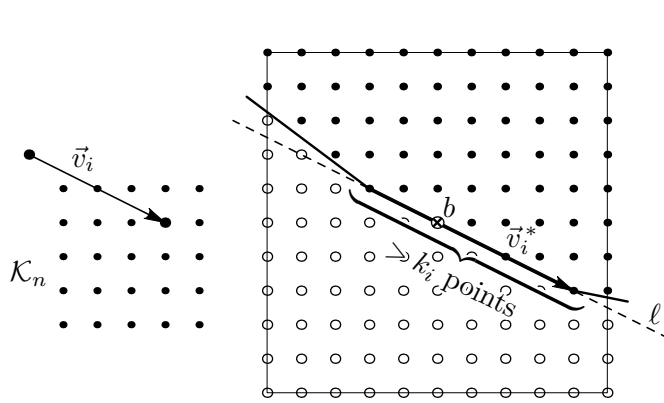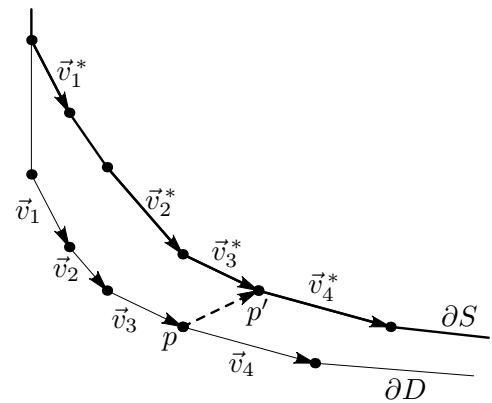
Proof of Claim 1   Proof of Claim 2

Claim 2. Each stable set $\mathcal{S} \subseteq \mathcal{Q}$ lies in $\mathcal{D}$.

Proof. To show this, it suffices to prove that the $\mathcal{V}_*$-curve lies in D, i.e., that all its vertices do so. Let p' be an arbitrary vertex of the $\mathcal{V}_*$-curve; p' partitions this curve into two parts, $\mathcal{X}$ (being down-right of p) and $\mathcal{Y}$ (being up-left of p). The set $\mathcal{V}$ is split now into two parts: $\mathcal{V}_{\mathcal{X}}$ consisting of those $\vec{v}_i \in \mathcal{V}$ for which $\vec{v}_i^*$ corresponds to a segment in $\mathcal{X}$, and a similar part $\mathcal{V}_{\mathcal{Y}}$. Notice that the $\mathcal{V}$-curve consists of several segments corresponding to $\mathcal{V}_{\mathcal{X}}$, followed by those corresponding to $\mathcal{V}_{\mathcal{Y}}$. Hence there is a vertex p of the $\mathcal{V}$-curve separating $\mathcal{V}_{\mathcal{X}}$ from $\mathcal{V}_{\mathcal{Y}}$. Claim 1 now yields that $p' \geqslant p$, so $p' \in \mathcal{D}$, as required. $\qquad\square$

Claim 2 implies that the final set $\mathcal{F}$ is contained in $\mathcal{D}$.

4. $\mathcal{D}$ is stable, and its comfortable points are known. Recall the definitions of r_i; let r_i' be the ray complementary to r_i. By our definitions, the set $N(O)$ contains no points between the rays r_i and r_{i+1}, as well as between r_i' and r_{i+1}'.

Claim 3. In the set $\mathcal{D}$, all lattice points of the $\mathcal{V}$-curve are comfortable.

Proof. Let p be any lattice point of the $\mathcal{V}$-curve, belonging to some segment $d_i d_{i+1}$. Draw the line ℓ containing this segment. Then $\ell \cap \mathcal{D}$ contains exactly $k_i + 1$ lattice points, all of which lie in $N(p)$ except for p. Thus, exactly half of the points in $N(p) \cap \ell$ lie in $\mathcal{D}$. It remains to show that all points of $N(p)$ above ℓ lie in $\mathcal{D}$ (recall that all the points below ℓ lack this property).

Notice that each vector in $\mathcal{V}$ has one coordinate greater than $n/2$; thus the neighborhood of p contains parts of at most two segments of the $\mathcal{V}$-curve succeeding $d_i d_{i+1}$, as well as at most two of those preceding it.

The angles formed by these consecutive segments are obtained from those formed by r_j and r'_{j-1} (with $i-1 \leqslant j \leqslant i+2$) by shifts; see the Figure below. All the points in $N(p)$ above ℓ which could lie outside $\mathcal{D}$ lie in shifted angles between r_j, r_{j+1} or r'_j, r'_{j-1}. But those angles, restricted to $N(p)$, have no lattice points due to the above remark. The claim is proved. $\qquad\square$
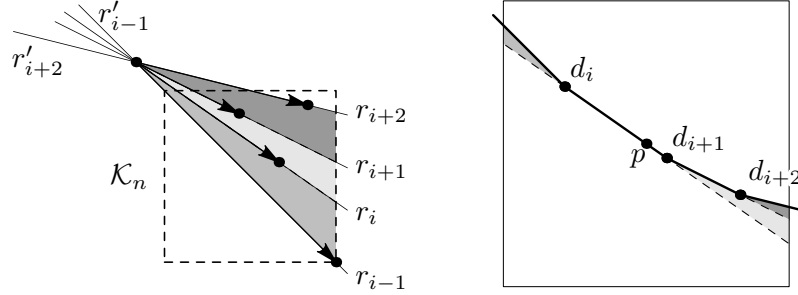
Proof of Claim 3

Claim 4. All the points of $\mathcal{D}$ which are not on the boundary of D are crowded.

Proof. Let $p \in \mathcal{D}$ be such a point. If it is to the up-right of some point p' on the curve, then the claim is easy: the shift of $N(p') \cap \mathcal{D}$ by $\overrightarrow{p'p}$ is still in $\mathcal{D}$, and $N(p)$ contains at least one more point of $\mathcal{D}$ — either below or to the left of p. So, we may assume that p lies in a right triangle constructed on some hypothenuse $d_i d_{i+1}$. Notice here that $d_i, d_{i+1} \in N(p)$.

Draw a line $\ell \parallel d_i d_{i+1}$ through p, and draw a vertical line h through d_i; see Figure below. Let $\mathcal{D}_L$ and $\mathcal{D}_R$ be the parts of $\mathcal{D}$ lying to the left and to the right of h, respectively (points of $\mathcal{D} \cap h$ lie in both parts).
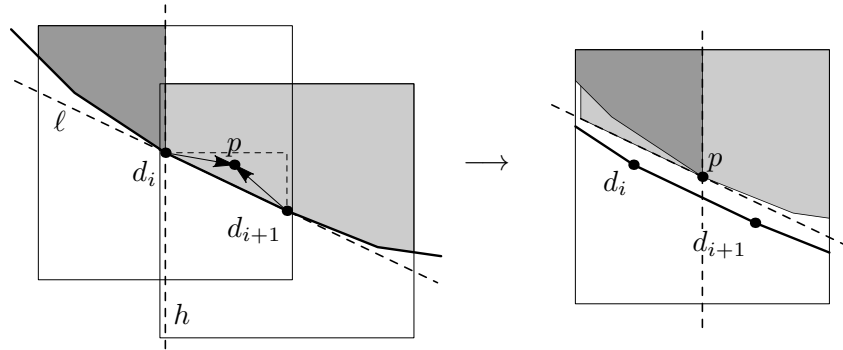
Proof of Claim 4

Notice that the vectors $\overrightarrow{d_i p}$, $\overrightarrow{d_{i+1} d_{i+2}}$, $\overrightarrow{d_i d_{i+1}}$, $\overrightarrow{d_{i-1} d_i}$, and $\overrightarrow{p d_{i+1}}$ are arranged in non-increasing order by slope. This means that $\mathcal{D}_L$ shifted by $\overrightarrow{d_i p}$ still lies in $\mathcal{D}$, as well as $\mathcal{D}_R$ shifted by $\overrightarrow{d_{i+1} p}$. As we have seen in the proof of Claim 3, these two shifts cover all points of $N(p)$ above ℓ, along with those on ℓ to the left of p. Since $N(p)$ contains also d_i and d_{i+1}, the point p is crowded. $\qquad\square$

Thus, we have proved that $\mathcal{D} = \mathcal{F}$, and have shown that the lattice points on the $\mathcal{V}$-curve are exactly the comfortable points of $\mathcal{D}$. It remains to find their number.

Recall the definition of $\mathcal{K}_n$ (see Figure on the first page of the solution). Each segment $d_i d_{i+1}$ contains k_i lattice points different from d_i. Taken over all i, these points exhaust all the lattice points in the $\mathcal{V}$-curve, except for d_1, and thus the number of lattice points on the $\mathcal{V}$-curve is $1 + \sum_{i=1}^m k_i$. On the other hand, $\sum_{i=1}^m k_i$ is just the number of points in $\mathcal{K}_n$, so it equals n^2. Hence the answer to the problem is $n^2 + 1$.

Comment 1. The assumption that the process eventually stops is unnecessary for the problem, as one can see that, in fact, the process stops for every $n \geqslant 1$. Indeed, the proof of Claims 3 and 4 do not rely essentially on this assumption, and they together yield that the set $\mathcal{D}$ is stable. So, only butterflies that are not in $\mathcal{D}$ may fly away, and this takes only a finite time.

This assumption has been inserted into the problem statement in order to avoid several technical details regarding finiteness issues. It may also simplify several other arguments.

Comment 2. The description of the final set $\mathcal{F}(=\mathcal{D})$ seems to be crucial for the solution; the Problem Selection Committee is not aware of any solution that completely avoids such a description.

On the other hand, after the set $\mathcal{D}$ has been defined, the further steps may be performed in several ways. For example, in order to prove that all butterflies outside $\mathcal{D}$ will fly away, one may argue as follows. (Here we will also make use of the assumption that the process eventually stops.)

First of all, notice that the process can be modified in the following manner: *Each minute, exactly one of the lonely butterflies flies away, until there are no more lonely butterflies.* The modified process necessarily stops at the same state as the initial one. Indeed, one may observe, as in solution above, that the (unique) largest stable set is still the final set for the modified process.

Thus, in order to prove our claim, it suffices to indicate an order in which the butterflies should fly away in the new process; if we are able to exhaust the whole set $\mathcal{Q} \setminus \mathcal{D}$, we are done.

Let $\mathcal{C}_0 = d_0 d_1 \ldots d_m$ be the $\mathcal{V}$-curve. Take its copy $\mathcal{C}$ and shift it downwards so that d_0 comes to some point below the origin O. Now we start moving $\mathcal{C}$ upwards continuously, until it comes back to its initial position $\mathcal{C}_0$. At each moment when $\mathcal{C}$ meets some lattice points, we convince all the butterflies at those points to fly away in a certain order. We will now show that we always have enough arguments for butterflies to do so, which will finish our argument for the claim..

Let $\mathcal{C}' = d_0' d_1' \ldots d_m'$ be a position of $\mathcal{C}$ when it meets some butterflies. We assume that all butterflies under this current position of $\mathcal{C}$ were already convinced enough and flied away. Consider the lowest butterfly b on $\mathcal{C}'$. Let $d_i' d_{i+1}'$ be the segment it lies on; we choose i so that $b \neq d_{i+1}'$ (this is possible because $\mathcal{C}$ as not yet reached $\mathcal{C}_0$).

Draw a line ℓ containing the segment $d_i' d_{i+1}'$. Then all the butterflies in $N(b)$ are situated on or above ℓ; moreover, those on ℓ all lie on the segment $d_i d_{i+1}$. But this segment now contains at most k_i butterflies (including b), since otherwise some butterfly had to occupy d_{i+1}' which is impossible by the choice of b. Thus, b is lonely and hence may be convinced to fly away.

After b has flied away, we switch to the lowest of the remaining butterflies on $\mathcal{C}'$, and so on.

Claims 3 and 4 also allow some different proofs which are not presented here.

This page is intentionally left blank

Geometry

G1. Let $ABCDE$ be a convex pentagon such that $AB = BC = CD$, $\angle EAB = \angle BCD$, and $\angle EDC = \angle CBA$. Prove that the perpendicular line from E to BC and the line segments AC and BD are concurrent.

(Italy)

Solution 1. Throughout the solution, we refer to $\angle A$, $\angle B$, $\angle C$, $\angle D$, and $\angle E$ as internal angles of the pentagon $ABCDE$. Let the perpendicular bisectors of AC and BD, which pass respectively through B and C, meet at point I. Then $BD \perp CI$ and, similarly, $AC \perp BI$. Hence AC and BD meet at the orthocenter H of the triangle BIC, and $IH \perp BC$. It remains to prove that E lies on the line IH or, equivalently, $EI \perp BC$.

Lines IB and IC bisect $\angle B$ and $\angle C$, respectively. Since $IA = IC$, $IB = ID$, and $AB = BC = CD$, the triangles IAB, ICB and ICD are congruent. Hence $\angle IAB = \angle ICB = \angle C/2 = \angle A/2$, so the line IA bisects $\angle A$. Similarly, the line ID bisects $\angle D$. Finally, the line IE bisects $\angle E$ because I lies on all the other four internal bisectors of the angles of the pentagon.

The sum of the internal angles in a pentagon is $540°$, so

$$\angle E = 540° - 2\angle A + 2\angle B.$$

In quadrilateral $ABIE$,

$$\angle BIE = 360° - \angle EAB - \angle ABI - \angle AEI = 360° - \angle A - \frac{1}{2}\angle B - \frac{1}{2}\angle E$$

$$= 360° - \angle A - \frac{1}{2}\angle B - (270° - \angle A - \angle B)$$

$$= 90° + \frac{1}{2}\angle B = 90° + \angle IBC,$$

which means that $EI \perp BC$, completing the proof.
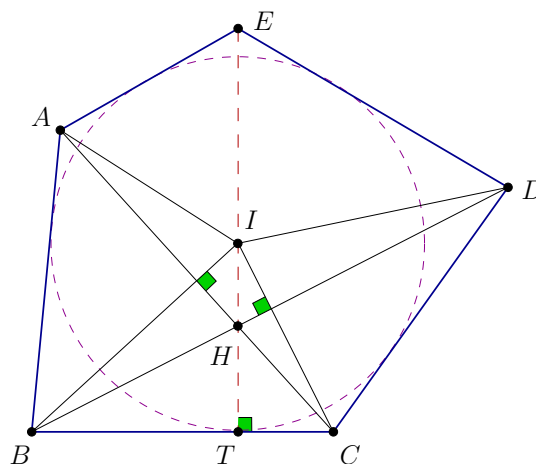
Solution 2. We present another proof of the fact that E lies on line IH. Since all five internal bisectors of $ABCDE$ meet at I, this pentagon has an inscribed circle with center I. Let this circle touch side BC at T.

Applying Brianchon's theorem to the (degenerate) hexagon $ABTCDE$ we conclude that AC, BD and ET are concurrent, so point E also lies on line IHT, completing the proof.

Solution 3. We present yet another proof that $EI \perp BC$. In pentagon $ABCDE$, $\angle E < 180° \iff \angle A + \angle B + \angle C + \angle D > 360°$. Then $\angle A + \angle B = \angle C + \angle D > 180°$, so rays EA and CB meet at a point P, and rays BC and ED meet at a point Q. Now,

$$\angle PBA = 180° - \angle B = 180° - \angle D = \angle QDC$$

and, similarly, $\angle PAB = \angle QCD$. Since $AB = CD$, the triangles PAB and QCD are congruent with the same orientation. Moreover, PQE is isosceles with $EP = EQ$.
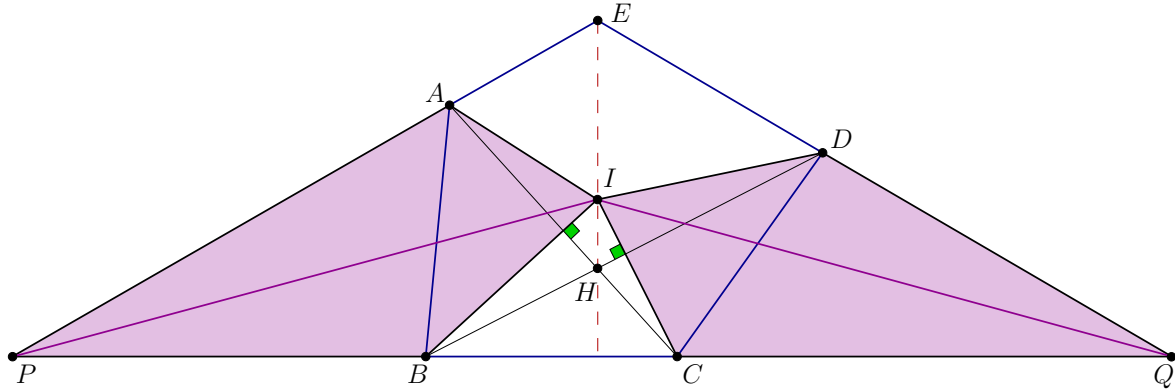
In Solution 1 we have proved that triangles IAB and ICD are also congruent with the same orientation. Then we conclude that quadrilaterals $PBIA$ and $QDIC$ are congruent, which implies $IP = IQ$. Then EI is the perpendicular bisector of PQ and, therefore, $EI \perp PQ \iff EI \perp BC$.

Comment. Even though all three solutions used the point I, there are solutions that do not need it. We present an outline of such a solution: if J is the incenter of $\triangle QCD$ (with P and Q as defined in Solution 3), then a simple angle chasing shows that triangles CJD and BHC are congruent. Then if S is the projection of J onto side CD and T is the orthogonal projection of H onto side BC, one can verify that

$$QT = QC + CT = QC + DS = QC + \frac{CD + DQ - QC}{2} = \frac{PB + BC + QC}{2} = \frac{PQ}{2},$$

so T is the midpoint of PQ, and E, H and T all lie on the perpendicular bisector of PQ.

G2. Let R and S be distinct points on circle Ω, and let t denote the tangent line to Ω at R. Point R' is the reflection of R with respect to S. A point I is chosen on the smaller arc RS of Ω so that the circumcircle Γ of triangle ISR' intersects t at two different points. Denote by A the common point of Γ and t that is closest to R. Line AI meets Ω again at J. Show that JR' is tangent to Γ.

(Luxembourg)

Solution 1. In the circles Ω and Γ we have $\angle JRS = \angle JIS = \angle AR'S$. On the other hand, since RA is tangent to Ω, we get $\angle SJR = \angle SRA$. So the triangles ARR' and SJR are similar, and

$$\frac{R'R}{RJ} = \frac{AR'}{SR} = \frac{AR'}{SR'}.$$

The last relation, together with $\angle AR'S = \angle JRR'$, yields $\triangle ASR' \sim \triangle R'JR$, hence $\angle SAR' = \angle RR'J$. It follows that JR' is tangent to Γ at R'.
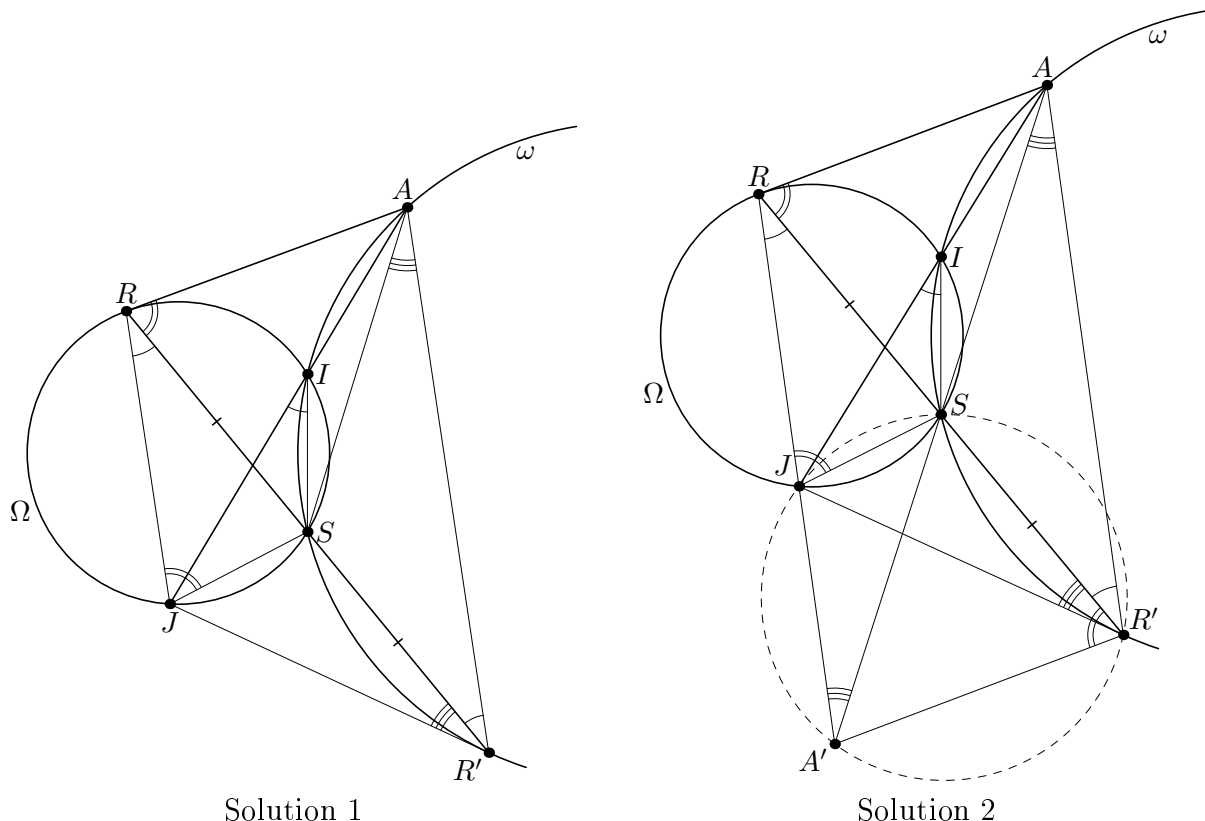
Solution 1   Solution 2

Solution 2. As in Solution 1, we notice that $\angle JRS = \angle JIS = \angle AR'S$, so we have $RJ \parallel AR'$.

Let A' be the reflection of A about S; then $ARA'R'$ is a parallelogram with center S, and hence the point J lies on the line RA'.

From $\angle SR'A' = \angle SRA = \angle SJR$ we get that the points S, J, A', R' are concyclic. This proves that $\angle SR'J = \angle SA'J = \angle SA'R = \angle SAR'$, so JR' is tangent to Γ at R'.

G3. Let O be the circumcenter of an acute scalene triangle ABC. Line OA intersects the altitudes of ABC through B and C at P and Q, respectively. The altitudes meet at H. Prove that the circumcenter of triangle PQH lies on a median of triangle ABC.

(Ukraine)

Solution. Suppose, without loss of generality, that $AB < AC$. We have $\angle PQH = 90° - \angle QAB = 90° - \angle OAB = \frac{1}{2}\angle AOB = \angle ACB$, and similarly $\angle QPH = \angle ABC$. Thus triangles ABC and HPQ are similar. Let Ω and ω be the circumcircles of ABC and HPQ, respectively. Since $\angle AHP = 90° - \angle HAC = \angle ACB = \angle HQP$, line AH is tangent to ω.
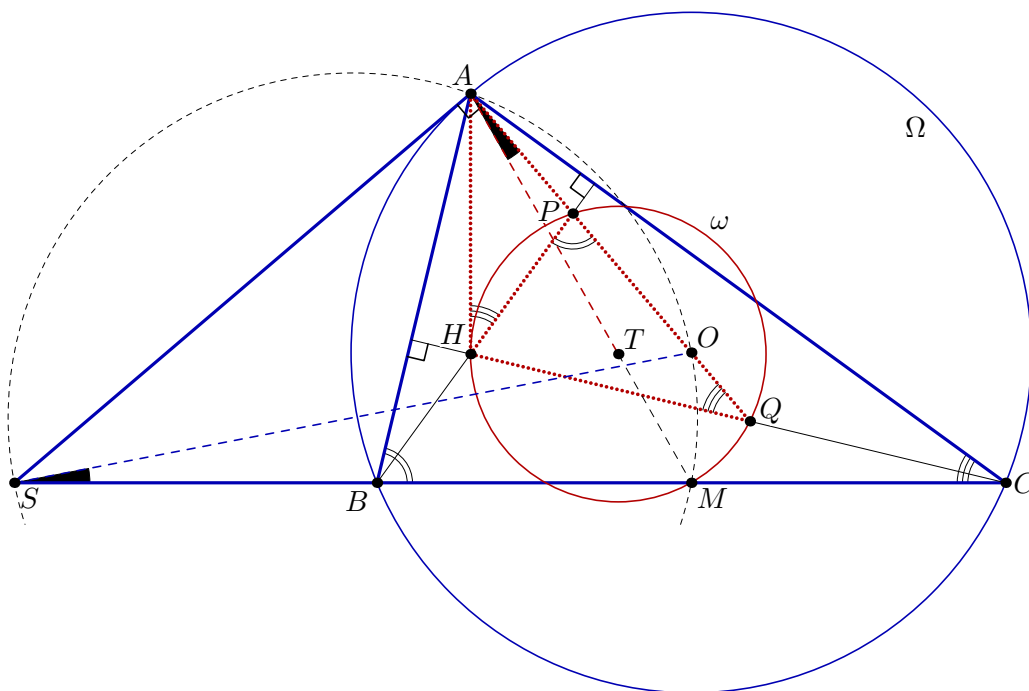
Let T be the center of ω and let lines AT and BC meet at M. We will take advantage of the similarity between ABC and HPQ and the fact that AH is tangent to ω at H, with A on line PQ. Consider the corresponding tangent AS to Ω, with $S \in BC$. Then S and A correspond to each other in $\triangle ABC \sim \triangle HPQ$, and therefore $\angle OSM = \angle OAT = \angle OAM$. Hence quadrilateral $SAOM$ is cyclic, and since the tangent line AS is perpendicular to AO, $\angle OMS = 180° - \angle OAS = 90°$. This means that M is the orthogonal projection of O onto BC, which is its midpoint. So T lies on median AM of triangle ABC.

G4.   In triangle ABC, let ω be the excircle opposite A. Let D, E, and F be the points where ω is tangent to lines BC, CA, and AB, respectively. The circle AEF intersects line BC at P and Q. Let M be the midpoint of AD. Prove that the circle MPQ is tangent to ω.

(Denmark)

Solution 1. Denote by Ω the circle $AEFPQ$, and denote by γ the circle PQM. Let the line AD meet ω again at $T \neq D$. We will show that γ is tangent to ω at T.

We first prove that points P, Q, M, T are concyclic. Let A' be the center of ω. Since $A'E \perp AE$ and $A'F \perp AF$, AA' is a diameter in Ω. Let N be the midpoint of DT; from $A'D = A'T$ we can see that $\angle A'NA = 90°$ and therefore N also lies on the circle Ω. Now, from the power of D with respect to the circles γ and Ω we get

$$DP \cdot DQ = DA \cdot DN = 2DM \cdot \frac{DT}{2} = DM \cdot DT,$$

so P, Q, M, T are concyclic.

If $EF \parallel BC$, then ABC is isosceles and the problem is now immediate by symmetry. Otherwise, let the tangent line to ω at T meet line BC at point R. The tangent line segments RD and RT have the same length, so $A'R$ is the perpendicular bisector of DT; since $ND = NT$, N lies on this perpendicular bisector.

In right triangle $A'RD$, $RD^2 = RN \cdot RA' = RP \cdot RQ$, in which the last equality was obtained from the power of R with respect to Ω. Hence $RT^2 = RP \cdot RQ$, which implies that RT is also tangent to γ. Because RT is a common tangent to ω and γ, these two circles are tangent at T.
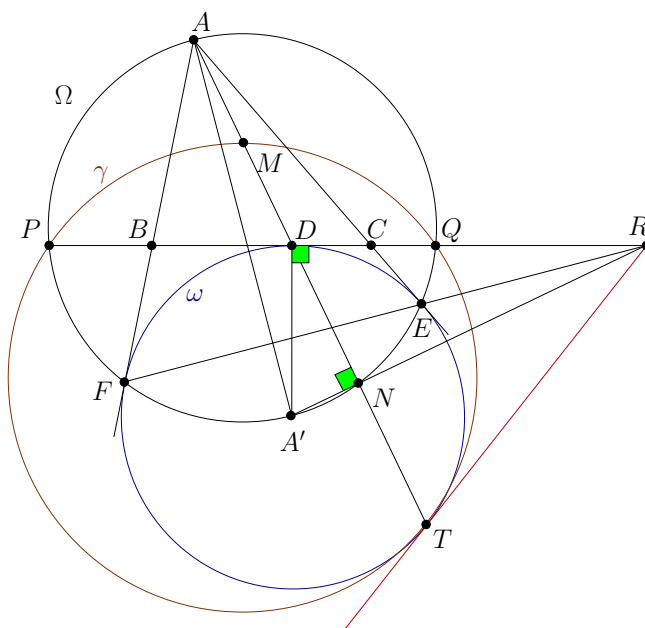

Solution 2. After proving that P, Q, M, T are concyclic, we finish the problem in a different fashion. We only consider the case in which EF and BC are not parallel. Let lines PQ and EF meet at point R. Since PQ and EF are radical axes of Ω, γ and ω, γ, respectively, R is the radical center of these three circles.

With respect to the circle ω, the line DR is the polar of D, and the line EF is the polar of A. So the pole of line ADT is $DR \cap EF = R$, and therefore RT is tangent to ω.

Finally, since T belongs to γ and ω and R is the radical center of γ, ω and Ω, line RT is the radical axis of γ and ω, and since it is tangent to ω, it is also tangent to γ. Because RT is a common tangent to ω and γ, these two circles are tangent at T.

Comment. In Solution 2 we defined the point R from Solution 1 in a different way.

Solution 3. We give an alternative proof that the circles are tangent at the common point T. Again, we start from the fact that P, Q, M, T are concyclic. Let point O be the midpoint of diameter AA'. Then MO is the midline of triangle ADA', so $MO \parallel A'D$. Since $A'D \perp PQ$, MO is perpendicular to PQ as well.

Looking at circle Ω, which has center O, $MO \perp PQ$ implies that MO is the perpendicular bisector of the chord PQ. Thus M is the midpoint of arc $\overarc{PQ}$ from γ, and the tangent line m to γ at M is parallel to PQ.
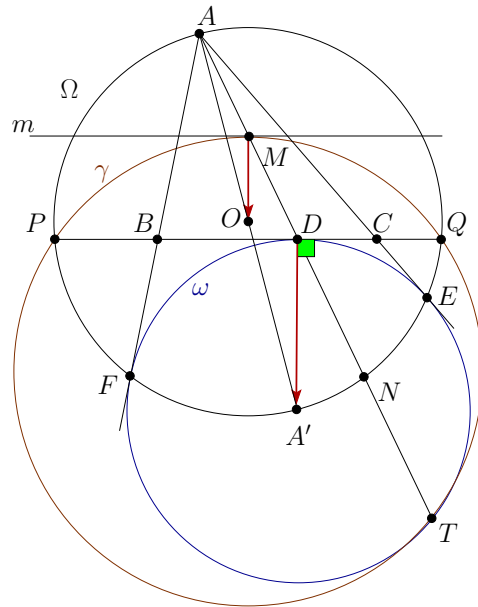
Consider the homothety with center T and ratio $\frac{TD}{TM}$. It takes D to M, and the line PQ to the line m. Since the circle that is tangent to a line at a given point and that goes through another given point is unique, this homothety also takes ω (tangent to PQ and going through T) to γ (tangent to m and going through T). We conclude that ω and γ are tangent at T.

G5. Let $ABCC_1B_1A_1$ be a convex hexagon such that $AB = BC$, and suppose that the line segments AA_1, BB_1, and CC_1 have the same perpendicular bisector. Let the diagonals AC_1 and A_1C meet at D, and denote by ω the circle ABC. Let ω intersect the circle A_1BC_1 again at $E \neq B$. Prove that the lines BB_1 and DE intersect on ω.

(Ukraine)

Solution 1. If $AA_1 = CC_1$, then the hexagon is symmetric about the line BB_1; in particular the circles ABC and A_1BC_1 are tangent to each other. So AA_1 and CC_1 must be different. Since the points A and A_1 can be interchanged with C and C_1, respectively, we may assume $AA_1 < CC_1$.

Let R be the radical center of the circles $AEBC$ and A_1EBC_1, and the circumcircle of the symmetric trapezoid ACC_1A_1; that is the common point of the pairwise radical axes AC, A_1C_1, and BE. By the symmetry of AC and A_1C_1, the point R lies on the common perpendicular bisector of AA_1 and CC_1, which is the external bisector of $\angle ADC$.

Let F be the second intersection of the line DR and the circle ACD. From the power of R with respect to the circles ω and $ACFD$ we have $RB \cdot RE = RA \cdot RC = RD \cdot DF$, so the points B, E, D and F are concyclic.

The line RDF is the external bisector of $\angle ADC$, so the point F bisects the arc $\overarc{CDA}$. By $AB = BC$, on circle ω, the point B is the midpoint of arc $\overarc{AEC}$; let M be the point diametrically opposite to B, that is the midpoint of the opposite arc $\overarc{CA}$ of ω. Notice that the points B, F and M lie on the perpendicular bisector of AC, so they are collinear.
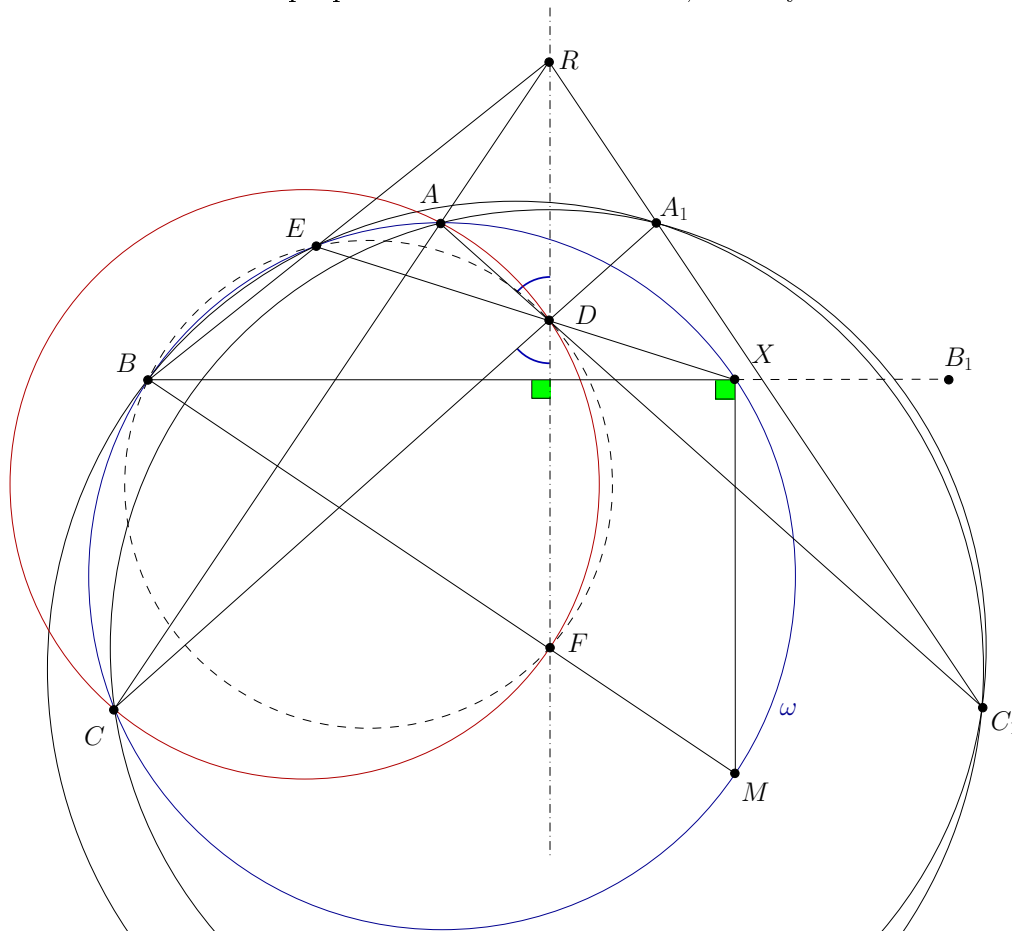
Finally, let X be the second intersection point of ω and the line DE. Since BM is a diameter in ω, we have $\angle BXM = 90°$. Moreover,

$$\angle EXM = 180° - \angle MBE = 180° - \angle FBE = \angle EDF,$$

so MX and FD are parallel. Since BX is perpendicular to MX and BB_1 is perpendicular to FD, this shows that X lies on line BB_1.

Solution 2. Define point M as the point opposite to B on circle ω, and point R as the intersection of lines AC, A_1C_1 and BE, and show that R lies on the external bisector of $\angle ADC$, like in the first solution.

Since B is the midpoint of the arc $\widehat{AEC}$, the line BER is the external bisector of $\angle CEA$. Now we show that the internal angle bisectors of $\angle ADC$ and $\angle CEA$ meet on the segment AC. Let the angle bisector of $\angle ADC$ meet AC at S, and let the angle bisector of $\angle CEA$, which is line EM, meet AC at S'. By applying the angle bisector theorem to both internal and external bisectors of $\angle ADC$ and $\angle CEA$,

$$AS : CS = AD : CD = AR : CR = AE : CE = AS' : CS',$$

so indeed $S = S'$.

By $\angle RDS = \angle SER = 90°$ the points R, S, D and E are concyclic.

Now let the lines BB_1 and DE meet at point X. Notice that $\angle EXB = \angle EDS$ because both BB_1 and DS are perpendicular to the line DR, we have that $\angle EDS = \angle ERS$ in circle $SRDE$, and $\angle ERS = \angle EMB$ because $SR \perp BM$ and $ER \perp ME$. Therefore, $\angle EXB = \angle EMB$, so indeed, the point X lies on ω.

G6.   Let $n \geqslant 3$ be an integer. Two regular n-gons $\mathcal{A}$ and $\mathcal{B}$ are given in the plane. Prove that the vertices of $\mathcal{A}$ that lie inside $\mathcal{B}$ or on its boundary are consecutive.

(That is, prove that there exists a line separating those vertices of $\mathcal{A}$ that lie inside $\mathcal{B}$ or on its boundary from the other vertices of $\mathcal{A}$.)

(Czech Republic)

Solution 1.   In both solutions, by a *polygon* we always mean its interior together with its boundary.

We start with finding a regular n-gon $\mathcal{C}$ which (i) is inscribed into $\mathcal{B}$ (that is, all vertices of $\mathcal{C}$ lie on the perimeter of $\mathcal{B}$); and (ii) is either a translation of $\mathcal{A}$, or a homothetic image of $\mathcal{A}$ with a positive factor.

Such a polygon may be constructed as follows. Let O_A and O_B be the centers of $\mathcal{A}$ and $\mathcal{B}$, respectively, and let A be an arbitrary vertex of $\mathcal{A}$. Let $\overrightarrow{O_B C}$ be the vector co-directional to $\overrightarrow{O_A A}$, with C lying on the perimeter of $\mathcal{B}$. The rotations of C around O_B by multiples of $2\pi/n$ form the required polygon. Indeed, it is regular, inscribed into $\mathcal{B}$ (due to the rotational symmetry of $\mathcal{B}$), and finally the translation/homothety mapping $\overrightarrow{O_A A}$ to $\overrightarrow{O_B C}$ maps $\mathcal{A}$ to $\mathcal{C}$.

Now we separate two cases.
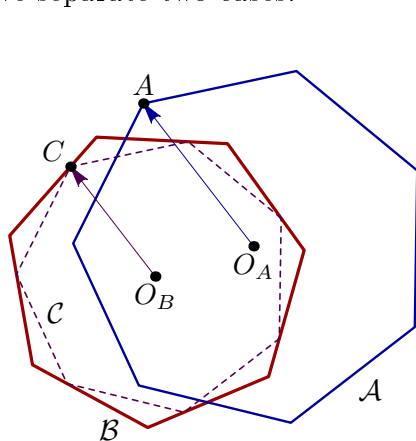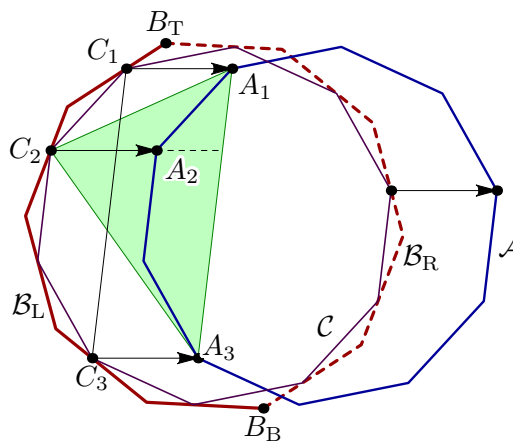
Construction of $\mathcal{C}$ Case 1: Translation

Case 1: $\mathcal{C}$ is a translation of $\mathcal{A}$ by a vector $\vec{v}$.

Denote by t the translation transform by vector $\vec{v}$. We need to prove that the vertices of $\mathcal{C}$ which stay in $\mathcal{B}$ under t are consecutive. To visualize the argument, we refer the plane to Cartesian coordinates so that the x-axis is co-directional with $\vec{v}$. This way, the notions of right/left and top/bottom are also introduced, according to the x- and y-coordinates, respectively.

Let B_T and B_B be the top and the bottom vertices of $\mathcal{B}$ (if several vertices are extremal, we take the rightmost of them). They split the perimeter of $\mathcal{B}$ into the *right part* $\mathcal{B}_\mathrm{R}$ and the *left part* $\mathcal{B}_\mathrm{L}$ (the vertices B_T and B_B are assumed to lie in both parts); each part forms a connected subset of the perimeter of $\mathcal{B}$. So the vertices of $\mathcal{C}$ are also split into two parts $\mathcal{C}_\mathrm{L} \subset \mathcal{B}_\mathrm{L}$ and $\mathcal{C}_\mathrm{R} \subset \mathcal{B}_\mathrm{R}$, each of which consists of consecutive vertices.

Now, all the points in $\mathcal{B}_\mathrm{R}$ (and hence in $\mathcal{C}_\mathrm{R}$) move out from $\mathcal{B}$ under t, since they are the rightmost points of $\mathcal{B}$ on the corresponding horizontal lines. It remains to prove that the vertices of $\mathcal{C}_\mathrm{L}$ which stay in $\mathcal{B}$ under t are consecutive.

For this purpose, let C_1, C_2, and C_3 be three vertices in $\mathcal{C}_\mathrm{L}$ such that C_2 is between C_1 and C_3, and $t(C_1)$ and $t(C_3)$ lie in $\mathcal{B}$; we need to prove that $t(C_2) \in \mathcal{B}$ as well. Let $A_i = t(C_i)$. The line through C_2 parallel to $\vec{v}$ crosses the segment $C_1 C_3$ to the right of C_2; this means that this line crosses $A_1 A_3$ to the right of A_2, so A_2 lies inside the triangle $A_1 C_2 A_3$ which is contained in $\mathcal{B}$. This yields the desired result.

Case 2: $\mathcal{C}$ is a homothetic image of $\mathcal{A}$ centered at X with factor $k > 0$.

Denote by h the homothety mapping $\mathcal{C}$ to $\mathcal{A}$. We need now to prove that the vertices of $\mathcal{C}$ which stay in $\mathcal{B}$ after applying h are consecutive. If $X \in \mathcal{B}$, the claim is easy. Indeed, if $k < 1$, then the vertices of $\mathcal{A}$ lie on the segments of the form XC (C being a vertex of $\mathcal{C}$) which lie in $\mathcal{B}$. If $k > 1$, then the vertices of $\mathcal{A}$ lie on the extensions of such segments XC beyond C, and almost all these extensions lie outside $\mathcal{B}$. The exceptions may occur only in case when X lies on the boundary of $\mathcal{B}$, and they may cause one or two vertices of $\mathcal{A}$ stay on the boundary of $\mathcal{B}$. But even in this case those vertices are still consecutive.

So, from now on we assume that $X \notin \mathcal{B}$.

Now, there are two vertices B_T and $\mathcal{B}_B$ of $\mathcal{B}$ such that $\mathcal{B}$ is contained in the angle $\angle B_T X B_B$; if there are several options, say, for B_T, then we choose the farthest one from X if $k > 1$, and the nearest one if $k < 1$. For the visualization purposes, we refer the plane to Cartesian coordinates so that the y-axis is co-directional with $\overrightarrow{B_B B_T}$, and X lies to the left of the line $B_T B_B$. Again, the perimeter of $\mathcal{B}$ is split by B_T and B_B into the *right part* $\mathcal{B}_R$ and the *left part* $\mathcal{B}_L$, and the set of vertices of $\mathcal{C}$ is split into two subsets $\mathcal{C}_R \subset \mathcal{B}_R$ and $\mathcal{C}_L \subset \mathcal{B}_L$.

Case 2, X inside $\mathcal{B}$ Subcase 2.1: $k > 1$
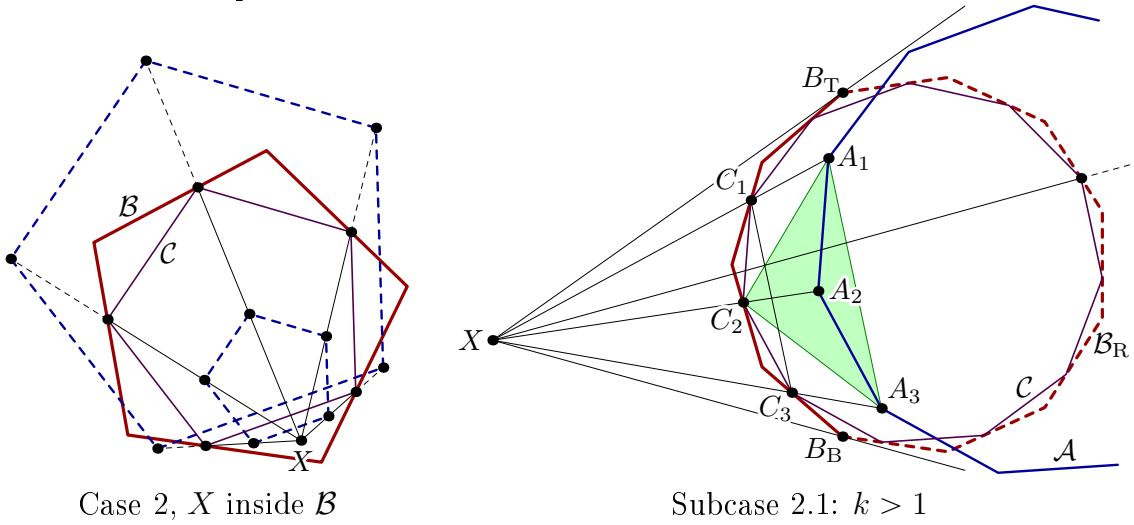
Subcase 2.1: $k > 1$.

In this subcase, all points from $\mathcal{B}_R$ (and hence from $\mathcal{C}_R$) move out from $\mathcal{B}$ under h, because they are the farthest points of $\mathcal{B}$ on the corresponding rays emanated from X. It remains to prove that the vertices of $\mathcal{C}_L$ which stay in $\mathcal{B}$ under h are consecutive.

Again, let C_1, C_2, C_3 be three vertices in $\mathcal{C}_L$ such that C_2 is between C_1 and C_3, and $h(C_1)$ and $h(C_3)$ lie in $\mathcal{B}$. Let $A_i = h(C_i)$. Then the ray XC_2 crosses the segment C_1C_3 beyond C_2, so this ray crosses A_1A_3 beyond A_2; this implies that A_2 lies in the triangle $A_1C_2A_3$, which is contained in $\mathcal{B}$.
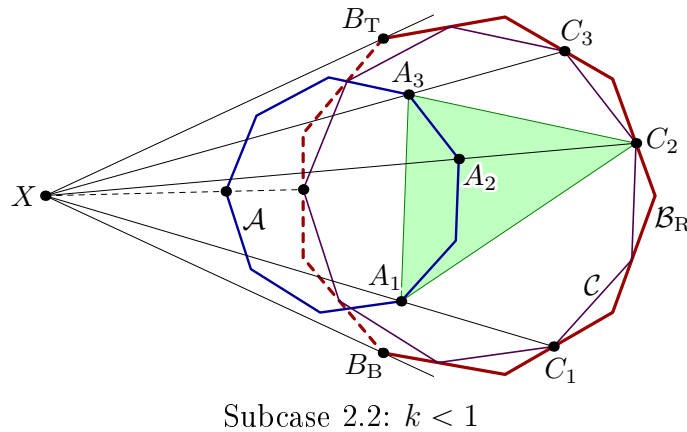
Subcase 2.2: $k < 1$

Subcase 2.2: $k < 1$.

This case is completely similar to the previous one. All points from $\mathcal{B}_L$ (and hence from $\mathcal{C}_L$ move out from $\mathcal{B}$ under h, because they are the nearest points of $\mathcal{B}$ on the corresponding

rays emanated from X. Assume that C_1, C_2, and C_3 are three vertices in $\mathcal{C}_R$ such that C_2 lies between C_1 and C_3, and $h(C_1)$ and $h(C_3)$ lie in $\mathcal{B}$; let $A_i = h(C_i)$. Then A_2 lies on the segment XC_2, and the segments XA_2 and A_1A_3 cross each other. Thus A_2 lies in the triangle $A_1C_2A_3$, which is contained in $\mathcal{B}$.

Comment 1. In fact, Case 1 can be reduced to Case 2 via the following argument.

Assume that $\mathcal{A}$ and $\mathcal{C}$ are congruent. Apply to $\mathcal{A}$ a homothety centered at O_B with a factor slightly smaller than 1 to obtain a polygon $\mathcal{A}'$. With appropriately chosen factor, the vertices of $\mathcal{A}$ which were outside/inside $\mathcal{B}$ stay outside/inside it, so it suffices to prove our claim for $\mathcal{A}'$ instead of $\mathcal{A}$. And now, the polygon $\mathcal{A}'$ is a homothetic image of $\mathcal{C}$, so the arguments from Case 2 apply.

Comment 2. After the polygon $\mathcal{C}$ has been found, the rest of the solution uses only the convexity of the polygons, instead of regularity. Thus, it proves a more general statement:

Assume that $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ are three convex polygons in the plane such that $\mathcal{C}$ is inscribed into $\mathcal{B}$, and $\mathcal{A}$ can be obtained from it via either translation or positive homothety. Then the vertices of $\mathcal{A}$ that lie inside $\mathcal{B}$ or on its boundary are consecutive.

Solution 2. Let O_A and O_B be the centers of $\mathcal{A}$ and $\mathcal{B}$, respectively. Denote $[n] = \{1, 2, \ldots, n\}$.

We start with introducing appropriate enumerations and notations. Enumerate the *sidelines* of $\mathcal{B}$ clockwise as $\ell_1, \ell_2, \ldots, \ell_n$. Denote by $\mathcal{H}_i$ the half-plane of ℓ_i that contains $\mathcal{B}$ ($\mathcal{H}_i$ is assumed to contain ℓ_i); by B_i the *midpoint* of the side belonging to ℓ_i; and finally denote $\overrightarrow{b_i} = \overrightarrow{B_iO_B}$. (As usual, the numbering is cyclic modulo n, so $\ell_{n+i} = \ell_i$ etc.)

Now, choose a vertex A_1 of $\mathcal{A}$ such that the vector $\overrightarrow{O_AA_1}$ points "mostly outside $\mathcal{H}_1$"; strictly speaking, this means that the scalar product $\langle \overrightarrow{O_AA_1}, \overrightarrow{b_1} \rangle$ is minimal. Starting from A_1, enumerate the vertices of $\mathcal{A}$ clockwise as $A_1, A_2, \ldots, A_n$; by the rotational symmetry, the choice of A_1 yields that the vector $\overrightarrow{O_AA_i}$ points "mostly outside $\mathcal{H}_i$", i.e.,

$$\langle \overrightarrow{O_AA_i}, \overrightarrow{b_i} \rangle = \min_{j \in [n]} \langle \overrightarrow{O_AA_j}, \overrightarrow{b_i} \rangle. \tag{1}$$
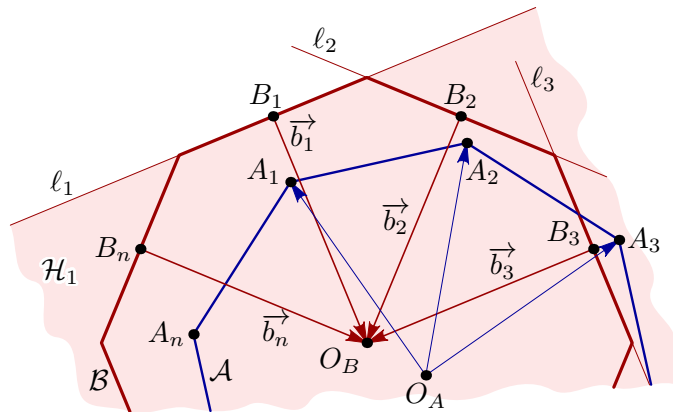

Enumerations and notations

We intend to reformulate the problem in more combinatorial terms, for which purpose we introduce the following notion. Say that a subset $I \subseteq [n]$ is *connected* if the elements of this set are consecutive in the cyclic order (in other words, if we join each i with $i+1 \mod n$ by an edge, this subset is connected in the usual graph sense). Clearly, the union of two connected subsets sharing at least one element is connected too. Next, for any half-plane $\mathcal{H}$ the indices of vertices of, say, $\mathcal{A}$ that lie in $\mathcal{H}$ form a connected set.

To access the problem, we denote

$$M = \{j \in [n] : A_j \notin \mathcal{B}\}, \qquad M_i = \{j \in [n] : A_j \notin \mathcal{H}_i\} \quad \text{for } i \in [n].$$

We need to prove that $[n] \setminus M$ is connected, which is equivalent to M being connected. On the other hand, since $\mathcal{B} = \bigcap_{i \in [n]} \mathcal{H}_i$, we have $M = \bigcup_{i \in [n]} M_i$, where the sets M_i are easier to investigate. We will utilize the following properties of these sets; the first one holds by the definition of M_i, along with the above remark.

The sets M_i
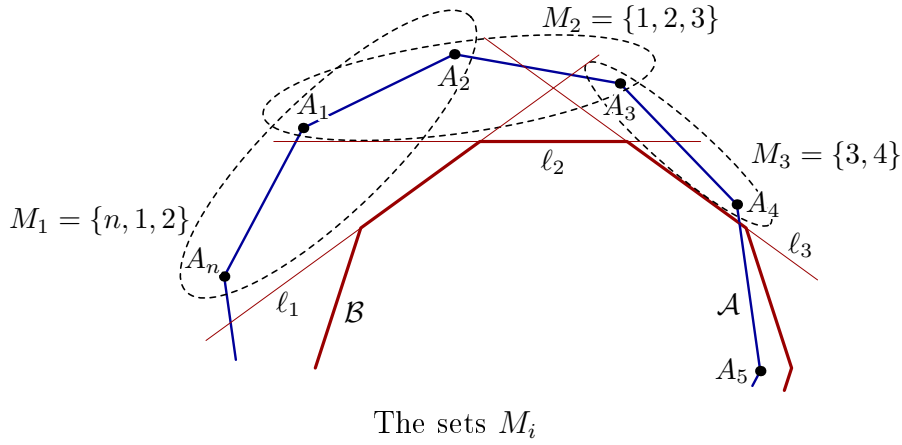
Property 1: Each set M_i is connected. □

Property 2: If M_i is nonempty, then $i \in M_i$.

Proof. Indeed, we have

$$j \in M_i \iff A_j \notin \mathcal{H}_i \iff \langle \overrightarrow{B_i A_j}, \overrightarrow{b_i} \rangle < 0 \iff \langle \overrightarrow{O_A A_j}, \overrightarrow{b_i} \rangle < \langle \overrightarrow{O_A B_i}, \overrightarrow{b_i} \rangle. \qquad (2)$$

The right-hand part of the last inequality does not depend on j. Therefore, if some j lies in M_i, then by (1) so does i. □

In view of Property 2, it is useful to define the set

$$M' = \{i \in [n] \colon i \in M_i\} = \{i \in [n] \colon M_i \neq \varnothing\}.$$

Property 3: The set M' is connected.

Proof. To prove this property, we proceed on with the investigation started in (2) to write

$$i \in M' \iff A_i \in M_i \iff \langle \overrightarrow{B_i A_i}, \overrightarrow{b_i} \rangle < 0 \iff \langle \overrightarrow{O_B O_A}, \overrightarrow{b_i} \rangle < \langle \overrightarrow{O_B B_i}, \overrightarrow{b_i} \rangle + \langle \overrightarrow{A_i O_A}, \overrightarrow{b_i} \rangle.$$

The right-hand part of the obtained inequality does not depend on i, due to the rotational symmetry; denote its constant value by μ. Thus, $i \in M'$ if and only if $\langle \overrightarrow{O_B O_A}, \overrightarrow{b_i} \rangle < \mu$. This condition is in turn equivalent to the fact that B_i lies in a certain (open) half-plane whose boundary line is orthogonal to $O_B O_A$; thus, it defines a connected set. □

Now we can finish the solution. Since $M' \subseteq M$, we have

$$M = \bigcup_{i \in [n]} M_i = M' \cup \bigcup_{i \in [n]} M_i,$$

so M can be obtained from M' by adding all the sets M_i one by one. All these sets are connected, and each nonempty M_i contains an element of M' (namely, i). Thus their union is also connected.

Comment 3. Here we present a way in which one can come up with a solution like the one above.

Assume, for sake of simplicity, that O_A lies inside $\mathcal{B}$. Let us first put onto the plane a very small regular n-gon $\mathcal{A}'$ centered at O_A and aligned with $\mathcal{A}$; all its vertices lie inside $\mathcal{B}$. Now we start blowing it up, looking at the order in which the vertices leave $\mathcal{B}$. To go out of $\mathcal{B}$, a vertex should cross a certain side of $\mathcal{B}$ (which is hard to describe), or, equivalently, to cross at least one *sideline* of $\mathcal{B}$ — and this event is easier to describe. Indeed, the first vertex of $\mathcal{A}'$ to cross ℓ_i is the vertex A_i' (corresponding to A_i in $\mathcal{A}$); more generally, the vertices A_j' cross ℓ_i in such an order that the scalar product $\langle \overrightarrow{O_A A_j}, \overrightarrow{b_i} \rangle$ does not increase. For different indices i, these orders are just cyclic shifts of each other; and this provides some intuition for the notions and claims from Solution 2.

G7. A convex quadrilateral $ABCD$ has an inscribed circle with center I. Let I_a, I_b, I_c, and I_d be the incenters of the triangles DAB, ABC, BCD, and CDA, respectively. Suppose that the common external tangents of the circles AI_bI_d and CI_bI_d meet at X, and the common external tangents of the circles BI_aI_c and DI_aI_c meet at Y. Prove that $\angle XIY = 90°$.

(Kazakhstan)

Solution. Denote by ω_a, ω_b, ω_c and ω_d the circles AI_bI_d, BI_aI_c, CI_bI_d, and DI_aI_c, let their centers be O_a, O_b, O_c and O_d, and let their radii be r_a, r_b, r_c and r_d, respectively.

Claim 1. $I_bI_d \perp AC$ and $I_aI_c \perp BD$.

Proof. Let the incircles of triangles ABC and ACD be tangent to the line AC at T and T', respectively. (See the figure to the left.) We have $AT = \frac{AB+AC-BC}{2}$ in triangle ABC, $AT' = \frac{AD+AC-CD}{2}$ in triangle ACD, and $AB - BC = AD - CD$ in quadrilateral $ABCD$, so

$$AT = \frac{AC + AB - BC}{2} = \frac{AC + AD - CD}{2} = AT'.$$

This shows $T = T'$. As an immediate consequence, $I_bI_d \perp AC$.

The second statement can be shown analogously. $\qquad \square$
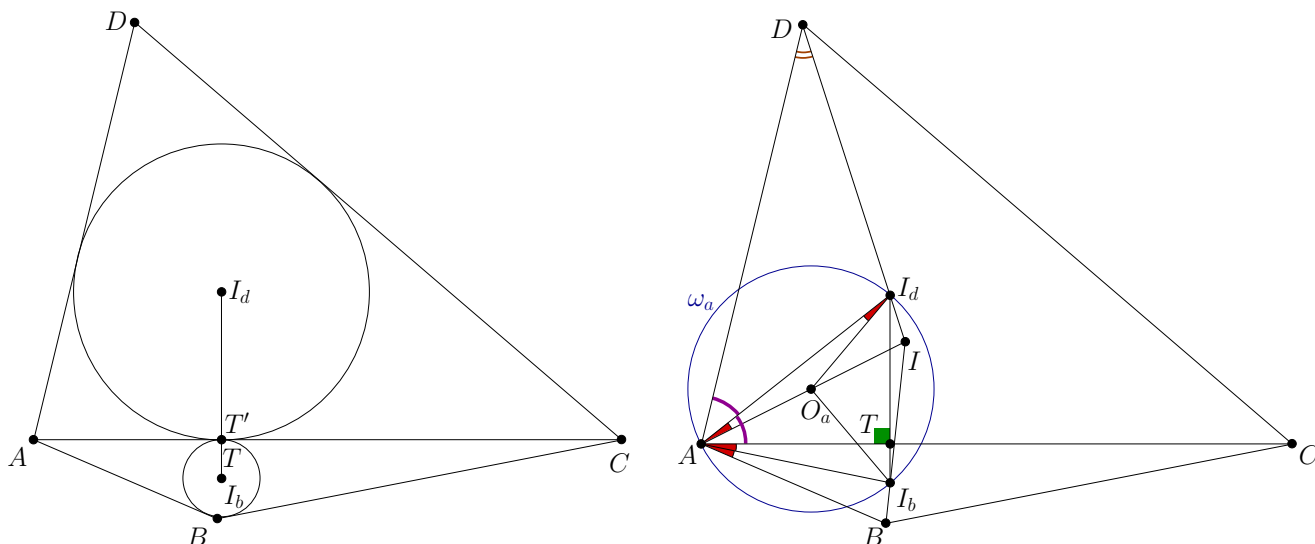
Claim 2. The points O_a, O_b, O_c and O_d lie on the lines AI, BI, CI and DI, respectively.

*Proof.* By symmetry it suffices to prove the claim for O_a. (See the figure to the right above.)

Notice first that the incircles of triangles ABC and ACD can be obtained from the incircle of the quadrilateral $ABCD$ with homothety centers B and D, respectively, and homothety factors less than 1, therefore the points I_b and I_d lie on the line segments BI and DI, respectively.

As is well-known, in every triangle the altitude and the diameter of the circumcircle starting from the same vertex are symmetric about the angle bisector. By Claim 1, in triangle AI_dI_b, the segment AT is the altitude starting from A. Since the foot T lies inside the segment I_bI_d, the circumcenter O_a of triangle AI_dI_b lies in the angle domain I_bAI_d in such a way that $\angle I_bAT = \angle O_aAI_d$. The points I_b and I_d are the incenters of triangles ABC and ACD, so the lines AI_b and AI_d bisect the angles $\angle BAC$ and $\angle CAD$, respectively. Then

$$\angle O_aAD = \angle O_aAI_d + \angle I_dAD = \angle I_bAT + \angle I_dAD = \tfrac{1}{2}\angle BAC + \tfrac{1}{2}\angle CAD = \tfrac{1}{2}\angle BAD,$$

so O_a lies on the angle bisector of $\angle BAD$, that is, on line AI. $\qquad \square$

The point X is the external similitude center of ω_a and ω_c; let U be their internal similitude center. The points O_a and O_c lie on the perpendicular bisector of the common chord I_bI_d of ω_a and ω_c, and the two similitude centers X and U lie on the same line; by Claim 2, that line is parallel to AC.
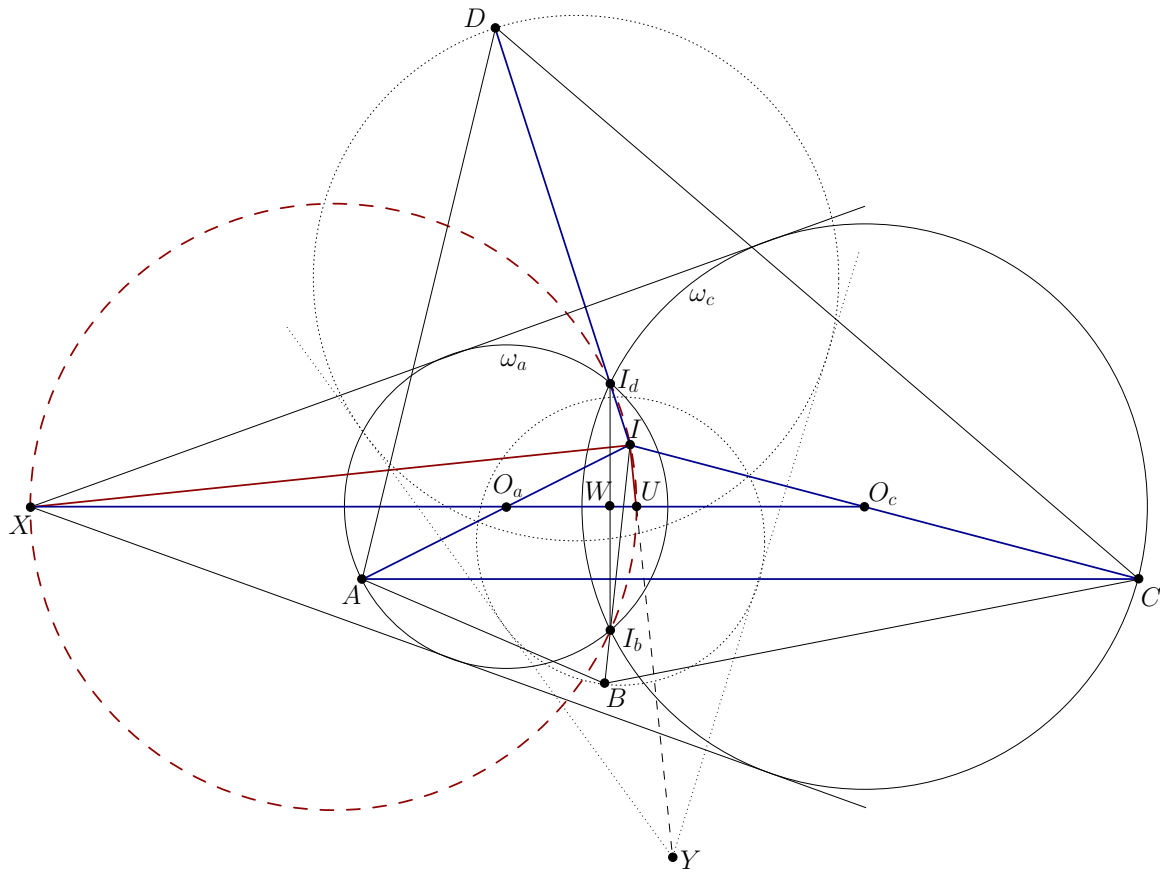
From the similarity of the circles ω_a and ω_c, from $O_aI_b = O_aI_d = O_aA = r_a$ and $O_cI_b = O_cI_d = O_cC = r_c$, and from $AC \parallel O_aO_c$ we can see that

$$\frac{O_aX}{O_cX} = \frac{O_aU}{O_cU} = \frac{r_a}{r_c} = \frac{O_aI_b}{O_cI_b} = \frac{O_aI_d}{O_cI_d} = \frac{O_aA}{O_cC} = \frac{O_aI}{O_cI}.$$

So the points X, U, I_b, I_d, I lie on the Apollonius circle of the points O_a, O_c with ratio $r_a : r_c$. In this Apollonius circle XU is a diameter, and the lines IU and IX are respectively the internal and external bisectors of $\angle O_aIO_c = \angle AIC$, according to the angle bisector theorem. Moreover, in the Apollonius circle the diameter UX is the perpendicular bisector of I_bI_d, so the lines IX and IU are the internal and external bisectors of $\angle I_bII_d = \angle BID$, respectively.

Repeating the same argument for the points B, D instead of A, C, we get that the line IY is the internal bisector of $\angle AIC$ and the external bisector of $\angle BID$. Therefore, the lines IX and IY respectively are the internal and external bisectors of $\angle BID$, so they are perpendicular.

Comment. In fact the points O_a, O_b, O_c and O_d lie on the *line segments AI, BI, CI* and DI, respectively. For the point O_a this can be shown for example by $\angle I_dO_aA + \angle AO_aI_b = (180° - 2\angle O_aAI_d) + (180° - 2\angle I_bAO_a) = 360° - \angle BAD = \angle ADI + \angle DIA + \angle AIB + \angle IBA > \angle I_dIA + \angle AII_b$.

The solution also shows that the line IY passes through the point U, and analogously, IX passes through the internal similitude center of ω_b and ω_d.

G8. There are 2017 mutually external circles drawn on a blackboard, such that no two are tangent and no three share a common tangent. A *tangent segment* is a line segment that is a common tangent to two circles, starting at one tangent point and ending at the other one. Luciano is drawing tangent segments on the blackboard, one at a time, so that no tangent segment intersects any other circles or previously drawn tangent segments. Luciano keeps drawing tangent segments until no more can be drawn. Find all possible numbers of tangent segments when he stops drawing.

(Australia)

Answer: If there were n circles, there would always be exactly $3(n-1)$ segments; so the only possible answer is $3 \cdot 2017 - 3 = 6048$.

Solution 1. First, consider a particular arrangement of circles $C_1, C_2, \ldots, C_n$ where all the centers are aligned and each C_i is eclipsed from the other circles by its neighbors – for example, taking C_i with center $(i^2, 0)$ and radius $i/2$ works. Then the only tangent segments that can be drawn are between adjacent circles C_i and C_{i+1}, and exactly three segments can be drawn for each pair. So Luciano will draw exactly $3(n-1)$ segments in this case.
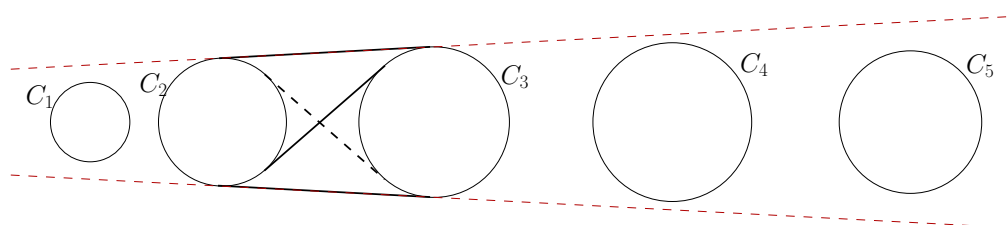
For the general case, start from a *final* configuration (that is, an arrangement of circles and segments in which no further segments can be drawn). The idea of the solution is to continuously resize and move the circles around the plane, one by one (in particular, making sure we never have 4 circles with a common tangent line), and show that the number of segments drawn remains constant as the picture changes. This way, we can reduce any circle/segment configuration to the particular one mentioned above, and the final number of segments must remain at $3n-3$.

Some preliminary considerations: look at all possible tangent segments joining any two circles. A segment that is tangent to a circle A can do so in two possible orientations — it may come out of A in clockwise or counterclockwise orientation. Two segments touching the same circle with the same orientation will never intersect each other. Each pair (A, B) of circles has 4 choices of tangent segments, which can be identified by their orientations — for example, $(A+, B-)$ would be the segment which comes out of A in clockwise orientation and comes out of B in counterclockwise orientation. In total, we have $2n(n-1)$ possible segments, disregarding intersections.

Now we pick a circle C and start to continuously move and resize it, maintaining all existing tangent segments according to their identifications, including those involving C. We can keep our choice of tangent segments until the configuration reaches a *transition*. We lose nothing if we assume that C is kept at least ε units away from any other circle, where ε is a positive, fixed constant; therefore at a transition either: (1) a currently drawn tangent segment t suddenly becomes obstructed; or (2) a currently absent tangent segment t suddenly becomes unobstructed and available.

Claim. A transition can only occur when three circles C_1, C_2, C_3 are tangent to a common line ℓ containing t, in a way such that the three tangent segments lying on ℓ (joining the three circles pairwise) are not obstructed by any other circles or tangent segments (other than C_1, C_2, C_3).

Proof. Since (2) is effectively the reverse of (1), it suffices to prove the claim for (1). Suppose t has suddenly become obstructed, and let us consider two cases.

Case 1: t becomes obstructed by a circle
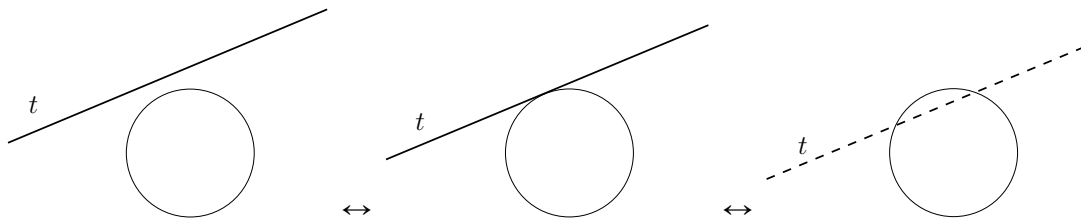
Then the new circle becomes the third circle tangent to ℓ, and no other circles or tangent segments are obstructing t.

Case 2: t becomes obstructed by another tangent segment t'

When two segments t and t' first intersect each other, they must do so at a vertex of one of them. But if a vertex of t' first crossed an interior point of t, the circle associated to this vertex was already blocking t (absurd), or is about to (we already took care of this in case 1). So we only have to analyze the possibility of t and t' suddenly having a common vertex. However, if that happens, this vertex must belong to a single circle (remember we are keeping different circles at least ε units apart from each other throughout the moving/resizing process), and therefore they must have different orientations with respect to that circle.
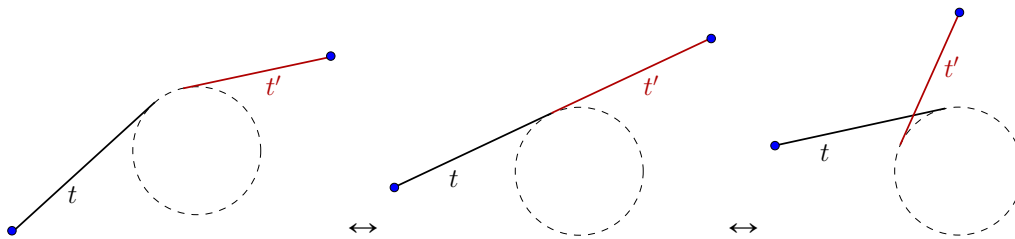
Thus, at the transition moment, both t and t' are tangent to the same circle at a common point, that is, they must be on the same line ℓ and hence we again have three circles simultaneously tangent to ℓ. Also no other circles or tangent segments are obstructing t or t' (otherwise, they would have disappeared before this transition). $\qquad\square$

Next, we focus on the maximality of a configuration immediately before and after a transition, where three circles share a common tangent line ℓ. Let the three circles be C_1, C_2, C_3, ordered by their tangent points. The only possibly affected segments are the ones lying on ℓ, namely t_{12}, t_{23} and t_{13}. Since C_2 is in the middle, t_{12} and t_{23} must have different orientations with respect to C_2. For C_1, t_{12} and t_{13} must have the same orientation, while for C_3, t_{13} and t_{23} must have the same orientation. The figure below summarizes the situation, showing alternative positions for C_1 (namely, C_1 and C_1') and for C_3 (C_3 and C_3').
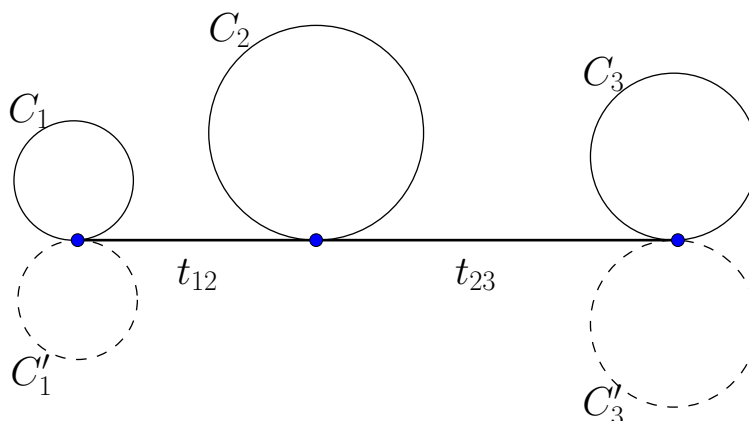
Now perturb the diagram slightly so the three circles no longer have a common tangent, while preserving the definition of t_{12}, t_{23} and t_{13} according to their identifications. First note that no other circles or tangent segments can obstruct any of these segments. Also recall that tangent segments joining the same circle at the same orientation will never obstruct each other.
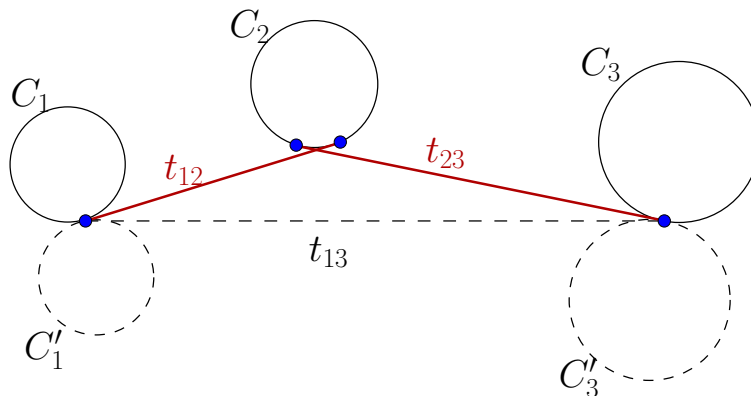
The availability of the tangent segments can now be checked using simple diagrams.

Case 1: t_{13} passes through C_2
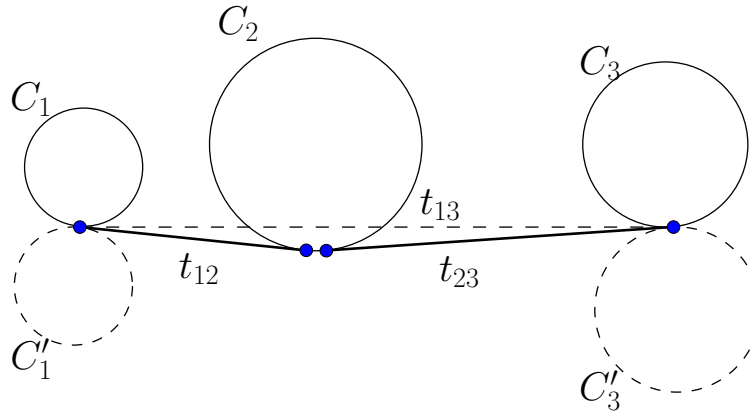
In this case, t_{13} is not available, but both t_{12} and t_{23} are.

*Case 2: t_{13} does not pass through C_2*

Now t_{13} is available, but t_{12} and t_{23} obstruct each other, so only one can be drawn.

In any case, exactly 2 out of these 3 segments can be drawn. Thus the maximal number of segments remains constant as we move or resize the circles, and we are done.

Solution 2. First note that all tangent segments lying on the boundary of the convex hull of the circles are always drawn since they do not intersect anything else. Now in the final picture, aside from the n circles, the blackboard is divided into regions. We can consider the picture as a plane (multi-)graph G in which the circles are the vertices and the tangent segments are the edges. The idea of this solution is to find a relation between the number of edges and the number of regions in G; then, once we prove that G is connected, we can use Euler's formula to finish the problem.

The boundary of each region consists of 1 or more (for now) simple closed curves, each made of arcs and tangent segments. The segment and the arc might meet smoothly (as in S_i, $i = 1, 2, \ldots, 6$ in the figure below) or not (as in P_1, P_2, P_3, P_4; call such points *sharp corners* of the boundary). In other words, if a person walks along the border, her direction would suddenly turn an angle of π at a sharp corner.
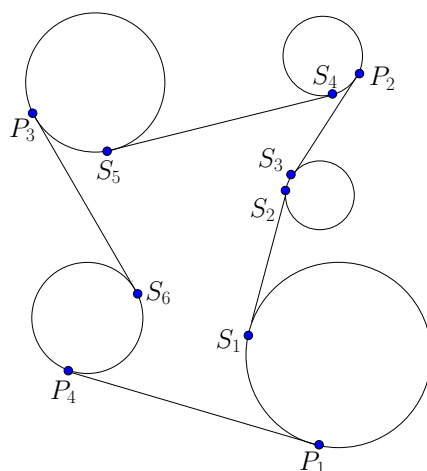
Claim 1. The outer boundary B_1 of any internal region has at least 3 sharp corners.

Proof. Let a person walk one lap along B_1 in the counterclockwise orientation. As she does so, she will turn *clockwise* as she moves along the circle arcs, and not turn at all when moving along the lines. On the other hand, her total rotation after one lap is 2π in the *counterclockwise* direction! Where could she be turning counterclockwise? She can only do so at sharp corners, and, even then, she turns only an angle of π there. But two sharp corners are not enough, since at least one arc must be present—so she must have gone through at least 3 sharp corners. □

Claim 2. Each internal region is simply connected, that is, has only one boundary curve.

Proof. Suppose, by contradiction, that some region has an outer boundary B_1 and inner boundaries $B_2, B_3, \ldots, B_m$ ($m \geqslant 2$). Let P_1 be one of the sharp corners of B_1.

Now consider a car starting at P_1 and traveling counterclockwise along B_1. It starts in reverse, i.e., it is initially facing the corner P_1. Due to the tangent conditions, the car may travel in a way so that its orientation only changes when it is moving along an arc. In particular, this means the car will sometimes travel forward. For example, if the car approaches a sharp corner when driving in reverse, it would continue travel forward after the corner, instead of making an immediate half-turn. This way, the orientation of the car only changes in a clockwise direction since the car always travels clockwise around each arc.

Now imagine there is a laser pointer at the front of the car, pointing directly ahead. Initially, the laser endpoint hits P_1, but, as soon as the car hits an arc, the endpoint moves clockwise around B_1. In fact, the laser endpoint must move continuously along B_1! Indeed, if the endpoint ever jumped (within B_1, or from B_1 to one of the inner boundaries), at the moment of the jump the interrupted laser would be a drawable tangent segment that Luciano missed (see figure below for an example).
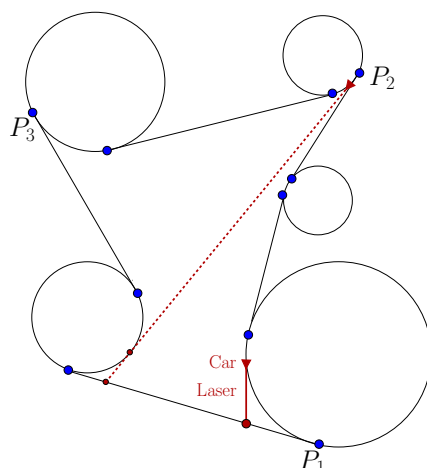
Now, let P_2 and P_3 be the next two sharp corners the car goes through, after P_1 (the previous lemma assures their existence). At P_2 the car starts moving forward, and at P_3 it will start to move in reverse again. So, at P_3, the laser endpoint is at P_3 itself. So while the car moved counterclockwise between P_1 and P_3, the laser endpoint moved clockwise between P_1 and P_3. That means the laser beam itself scanned the whole region within B_1, and it should have crossed some of the inner boundaries.   □

Claim 3. Each region has exactly 3 sharp corners.

Proof. Consider again the car of the previous claim, with its laser still firmly attached to its front, traveling the same way as before and going through the same *consecutive* sharp corners P_1, P_2 and P_3. As we have seen, as the car goes counterclockwise from P_1 to P_3, the laser endpoint goes clockwise from P_1 to P_3, so together they cover the whole boundary. If there were a fourth sharp corner P_4, at some moment the laser endpoint would pass through it. But, since P_4 is a sharp corner, this means the car must be on the extension of a tangent segment going through P_4. Since the car is not on that segment itself (the car never goes through P_4), we would have 3 circles with a common tangent line, which is not allowed.

                                                                                                   □
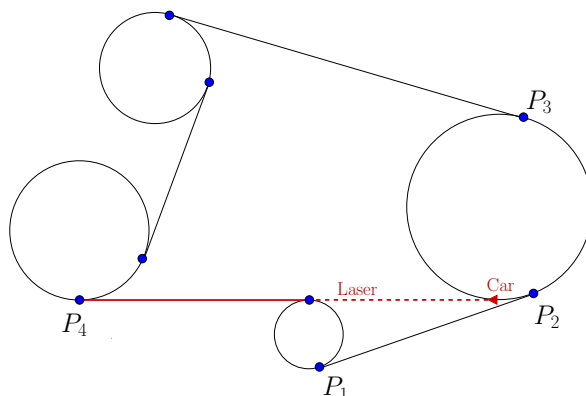
We are now ready to finish the solution. Let r be the number of internal regions, and s be the number of tangent segments. Since each tangent segment contributes exactly 2 sharp corners to the diagram, and each region has exactly 3 sharp corners, we must have $2s = 3r$. Since the graph corresponding to the diagram is connected, we can use Euler's formula $n - s + r = 1$ and find $s = 3n - 3$ and $r = 2n - 2$.

Number Theory

$\boxed{\textbf{N1.}}$ The sequence $a_0, a_1, a_2, \ldots$ of positive integers satisfies

$$a_{n+1} = \begin{cases} \sqrt{a_n}, & \text{if } \sqrt{a_n} \text{ is an integer} \\ a_n + 3, & \text{otherwise} \end{cases} \quad \text{for every } n \geqslant 0.$$

Determine all values of $a_0 > 1$ for which there is at least one number a such that $a_n = a$ for infinitely many values of n.

(South Africa)

Answer: All positive multiples of 3.

Solution. Since the value of a_{n+1} only depends on the value of a_n, if $a_n = a_m$ for two different indices n and m, then the sequence is eventually periodic. So we look for the values of a_0 for which the sequence is eventually periodic.

Claim 1. If $a_n \equiv -1 \pmod 3$, then, for all $m > n$, a_m is not a perfect square. It follows that the sequence is eventually strictly increasing, so it is not eventually periodic.

Proof. A square cannot be congruent to -1 modulo 3, so $a_n \equiv -1 \pmod 3$ implies that a_n is not a square, therefore $a_{n+1} = a_n + 3 > a_n$. As a consequence, $a_{n+1} \equiv a_n \equiv -1 \pmod 3$, so a_{n+1} is not a square either. By repeating the argument, we prove that, from a_n on, all terms of the sequence are not perfect squares and are greater than their predecessors, which completes the proof. $\square$

Claim 2. If $a_n \not\equiv -1 \pmod 3$ and $a_n > 9$ then there is an index $m > n$ such that $a_m < a_n$.

Proof. Let t^2 be the largest perfect square which is less than a_n. Since $a_n > 9$, t is at least 3. The first square in the sequence $a_n, a_n + 3, a_n + 6, \ldots$ will be $(t+1)^2$, $(t+2)^2$ or $(t+3)^2$, therefore there is an index $m > n$ such that $a_m \leqslant t + 3 < t^2 < a_n$, as claimed. $\square$

Claim 3. If $a_n \equiv 0 \pmod 3$, then there is an index $m > n$ such that $a_m = 3$.

Proof. First we notice that, by the definition of the sequence, a multiple of 3 is always followed by another multiple of 3. If $a_n \in \{3, 6, 9\}$ the sequence will eventually follow the periodic pattern $3, 6, 9, 3, 6, 9, \ldots$. If $a_n > 9$, let j be an index such that a_j is equal to the minimum value of the set $\{a_{n+1}, a_{n+2}, \ldots\}$. We must have $a_j \leqslant 9$, otherwise we could apply Claim 2 to a_j and get a contradiction on the minimality hypothesis. It follows that $a_j \in \{3, 6, 9\}$, and the proof is complete. $\square$

Claim 4. If $a_n \equiv 1 \pmod 3$, then there is an index $m > n$ such that $a_m \equiv -1 \pmod 3$.

Proof. In the sequence, 4 is always followed by $2 \equiv -1 \pmod 3$, so the claim is true for $a_n = 4$. If $a_n = 7$, the next terms will be $10, 13, 16, 4, 2, \ldots$ and the claim is also true. For $a_n \geqslant 10$, we again take an index $j > n$ such that a_j is equal to the minimum value of the set $\{a_{n+1}, a_{n+2}, \ldots\}$, which by the definition of the sequence consists of non-multiples of 3. Suppose $a_j \equiv 1 \pmod 3$. Then we must have $a_j \leqslant 9$ by Claim 2 and the minimality of a_j. It follows that $a_j \in \{4, 7\}$, so $a_m = 2 < a_j$ for some $m > j$, contradicting the minimality of a_j. Therefore, we must have $a_j \equiv -1 \pmod 3$. $\square$

It follows from the previous claims that if a_0 is a multiple of 3 the sequence will eventually reach the periodic pattern $3, 6, 9, 3, 6, 9, \ldots$; if $a_0 \equiv -1 \pmod 3$ the sequence will be strictly increasing; and if $a_0 \equiv 1 \pmod 3$ the sequence will be eventually strictly increasing.

So the sequence will be eventually periodic if, and only if, a_0 is a multiple of 3.

N2. Let $p \geqslant 2$ be a prime number. Eduardo and Fernando play the following game making moves alternately: in each move, the current player chooses an index i in the set $\{0, 1, \ldots, p-1\}$ that was not chosen before by either of the two players and then chooses an element a_i of the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Eduardo has the first move. The game ends after all the indices $i \in \{0, 1, \ldots, p-1\}$ have been chosen. Then the following number is computed:

$$M = a_0 + 10 \cdot a_1 + \cdots + 10^{p-1} \cdot a_{p-1} = \sum_{j=0}^{p-1} a_j \cdot 10^j.$$

The goal of Eduardo is to make the number M divisible by p, and the goal of Fernando is to prevent this.

Prove that Eduardo has a winning strategy.

(Morocco)

Solution. We say that a player makes the move (i, a_i) if he chooses the index i and then the element a_i of the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ in this move.

If $p = 2$ or $p = 5$ then Eduardo chooses $i = 0$ and $a_0 = 0$ in the first move, and wins, since, independently of the next moves, M will be a multiple of 10.

Now assume that the prime number p does not belong to $\{2, 5\}$. Eduardo chooses $i = p - 1$ and $a_{p-1} = 0$ in the first move. By Fermat's Little Theorem, $(10^{(p-1)/2})^2 = 10^{p-1} \equiv 1 \pmod{p}$, so $p \mid (10^{(p-1)/2})^2 - 1 = (10^{(p-1)/2} + 1)(10^{(p-1)/2} - 1)$. Since p is prime, either $p \mid 10^{(p-1)/2} + 1$ or $p \mid 10^{(p-1)/2} - 1$. Thus we have two cases:

Case a: $10^{(p-1)/2} \equiv -1 \pmod{p}$

In this case, for each move (i, a_i) of Fernando, Eduardo immediately makes the move $(j, a_j) = (i + \frac{p-1}{2}, a_i)$, if $0 \leqslant i \leqslant \frac{p-3}{2}$, or $(j, a_j) = (i - \frac{p-1}{2}, a_i)$, if $\frac{p-1}{2} \leqslant i \leqslant p-2$. We will have $10^j \equiv -10^i \pmod{p}$, and so $a_j \cdot 10^j = a_i \cdot 10^j \equiv -a_i \cdot 10^i \pmod{p}$. Notice that this move by Eduardo is always possible. Indeed, immediately before a move by Fernando, for any set of the type $\{r, r + (p-1)/2\}$ with $0 \leqslant r \leqslant (p-3)/2$, either no element of this set was chosen as an index by the players in the previous moves or else both elements of this set were chosen as indices by the players in the previous moves. Therefore, after each of his moves, Eduardo always makes the sum of the numbers $a_k \cdot 10^k$ corresponding to the already chosen pairs (k, a_k) divisible by p, and thus wins the game.

Case b: $10^{(p-1)/2} \equiv 1 \pmod{p}$

In this case, for each move (i, a_i) of Fernando, Eduardo immediately makes the move $(j, a_j) = (i + \frac{p-1}{2}, 9 - a_i)$, if $0 \leqslant i \leqslant \frac{p-3}{2}$, or $(j, a_j) = (i - \frac{p-1}{2}, 9 - a_i)$, if $\frac{p-1}{2} \leqslant i \leqslant p-2$. The same argument as above shows that Eduardo can always make such move. We will have $10^j \equiv 10^i \pmod{p}$, and so $a_j \cdot 10^j + a_i \cdot 10^i \equiv (a_i + a_j) \cdot 10^i = 9 \cdot 10^i \pmod{p}$. Therefore, at the end of the game, the sum of all terms $a_k \cdot 10^k$ will be congruent to

$$\sum_{i=0}^{\frac{p-3}{2}} 9 \cdot 10^i = 10^{(p-1)/2} - 1 \equiv 0 \pmod{p},$$

and Eduardo wins the game.

N3. Determine all integers $n \geqslant 2$ with the following property: for any integers $a_1, a_2, \ldots, a_n$ whose sum is not divisible by n, there exists an index $1 \leqslant i \leqslant n$ such that none of the numbers

$$a_i, a_i + a_{i+1}, \ldots, a_i + a_{i+1} + \cdots + a_{i+n-1}$$

is divisible by n. (We let $a_i = a_{i-n}$ when $i > n$.)

(Thailand)

Answer: These integers are exactly the prime numbers.

Solution. Let us first show that, if $n = ab$, with $a, b \geqslant 2$ integers, then the property in the statement of the problem does not hold. Indeed, in this case, let $a_k = a$ for $1 \leqslant k \leqslant n-1$ and $a_n = 0$. The sum $a_1 + a_2 + \cdots + a_n = a \cdot (n-1)$ is not divisible by n. Let i with $1 \leqslant i \leqslant n$ be an arbitrary index. Taking $j = b$ if $1 \leqslant i \leqslant n - b$, and $j = b + 1$ if $n - b < i \leqslant n$, we have

$$a_i + a_{i+1} + \cdots + a_{i+j-1} = a \cdot b = n \equiv 0 \pmod{n}.$$

It follows that the given example is indeed a counterexample to the property of the statement.

Now let n be a prime number. Suppose by contradiction that the property in the statement of the problem does not hold. Then there are integers $a_1, a_2, \ldots, a_n$ whose sum is not divisible by n such that for each i, $1 \leqslant i \leqslant n$, there is j, $1 \leqslant j \leqslant n$, for which the number $a_i + a_{i+1} + \cdots + a_{i+j-1}$ is divisible by n. Notice that, in any such case, we should have $1 \leqslant j \leqslant n - 1$, since $a_1 + a_2 + \cdots + a_n$ is not divisible by n. So we may construct recursively a finite sequence of integers $0 = i_0 < i_1 < i_2 < \cdots < i_n$ with $i_{s+1} - i_s \leqslant n - 1$ for $0 \leqslant s \leqslant n-1$ such that, for $0 \leqslant s \leqslant n - 1$,

$$a_{i_s+1} + a_{i_s+2} + \cdots + a_{i_{s+1}} \equiv 0 \pmod{n}$$

(where we take indices modulo n). Indeed, for $0 \leqslant s < n$, we apply the previous observation to $i = i_s + 1$ in order to define $i_{s+1} = i_s + j$.

In the sequence of $n + 1$ indices $i_0, i_1, i_2, \ldots, i_n$, by the pigeonhole principle, we have two distinct elements which are congruent modulo n. So there are indices r, s with $0 \leqslant r < s \leqslant n$ such that $i_s \equiv i_r \pmod{n}$ and

$$a_{i_r+1} + a_{i_r+2} + \cdots + a_{i_s} = \sum_{j=r}^{s-1} (a_{i_j+1} + a_{i_j+2} + \cdots + a_{i_{j+1}}) \equiv 0 \pmod{n}.$$

Since $i_s \equiv i_r \pmod{n}$, we have $i_s - i_r = k \cdot n$ for some positive integer k, and, since $i_{j+1} - i_j \leqslant n - 1$ for $0 \leqslant j \leqslant n - 1$, we have $i_s - i_r \leqslant (n-1) \cdot n$, so $k \leqslant n - 1$. But in this case

$$a_{i_r+1} + a_{i_r+2} + \cdots + a_{i_s} = k \cdot (a_1 + a_2 + \cdots + a_n)$$

cannot be a multiple of n, since n is prime and neither k nor $a_1 + a_2 + \cdots + a_n$ is a multiple of n. A contradiction.

N4. Call a rational number *short* if it has finitely many digits in its decimal expansion. For a positive integer m, we say that a positive integer t is *m-tastic* if there exists a number $c \in \{1, 2, 3, \ldots, 2017\}$ such that $\dfrac{10^t - 1}{c \cdot m}$ is short, and such that $\dfrac{10^k - 1}{c \cdot m}$ is not short for any $1 \leqslant k < t$. Let $S(m)$ be the set of m-tastic numbers. Consider $S(m)$ for $m = 1, 2, \ldots$. What is the maximum number of elements in $S(m)$?

(Turkey)

Answer: 807.

Solution. First notice that $x \in \mathbb{Q}$ is short if and only if there are exponents $a, b \geqslant 0$ such that $2^a \cdot 5^b \cdot x \in \mathbb{Z}$. In fact, if x is short, then $x = \frac{n}{10^k}$ for some k and we can take $a = b = k$; on the other hand, if $2^a \cdot 5^b \cdot x = q \in \mathbb{Z}$ then $x = \frac{2^b \cdot 5^a q}{10^{a+b}}$, so x is short.

If $m = 2^a \cdot 5^b \cdot s$, with $\gcd(s, 10) = 1$, then $\frac{10^t - 1}{m}$ is short if and only if s divides $10^t - 1$. So we may (and will) suppose without loss of generality that $\gcd(m, 10) = 1$. Define

$$C = \{1 \leqslant c \leqslant 2017 \colon \gcd(c, 10) = 1\}.$$

The m-tastic numbers are then precisely the smallest exponents $t > 0$ such that $10^t \equiv 1 \pmod{cm}$ for some integer $c \in C$, that is, the set of *orders of* 10 *modulo cm*. In other words,

$$S(m) = \{\operatorname{ord}_{cm}(10) \colon c \in C\}.$$

Since there are $4 \cdot 201 + 3 = 807$ numbers c with $1 \leqslant c \leqslant 2017$ and $\gcd(c, 10) = 1$, namely those such that $c \equiv 1, 3, 7, 9 \pmod{10}$,

$$|S(m)| \leqslant |C| = 807.$$

Now we find m such that $|S(m)| = 807$. Let

$$P = \{1 < p \leqslant 2017 \colon p \text{ is prime}, p \neq 2, 5\}$$

and choose a positive integer α such that every $p \in P$ divides $10^\alpha - 1$ (e.g. $\alpha = \varphi(T)$, T being the product of all primes in P), and let $m = 10^\alpha - 1$.

Claim. For every $c \in C$, we have

$$\operatorname{ord}_{cm}(10) = c\alpha.$$

As an immediate consequence, this implies $|S(m)| = |C| = 807$, finishing the problem.

Proof. Obviously $\operatorname{ord}_m(10) = \alpha$. Let $t = \operatorname{ord}_{cm}(10)$. Then

$$cm \mid 10^t - 1 \quad \Longrightarrow \quad m \mid 10^t - 1 \quad \Longrightarrow \quad \alpha \mid t.$$

Hence $t = k\alpha$ for some $k \in \mathbb{Z}_{>0}$. We will show that $k = c$.

Denote by $\nu_p(n)$ the number of prime factors p in n, that is, the maximum exponent β for which $p^\beta \mid n$. For every $\ell \geqslant 1$ and $p \in P$, the Lifting the Exponent Lemma provides

$$\nu_p(10^{\ell\alpha} - 1) = \nu_p((10^\alpha)^\ell - 1) = \nu_p(10^\alpha - 1) + \nu_p(\ell) = \nu_p(m) + \nu_p(\ell),$$

so

$$
\begin{aligned}
cm \mid 10^{k\alpha} - 1 &\iff \forall p \in P; \ \nu_p(cm) \leqslant \nu_p(10^{k\alpha} - 1) \\
&\iff \forall p \in P; \ \nu_p(m) + \nu_p(c) \leqslant \nu_p(m) + \nu_p(k) \\
&\iff \forall p \in P; \ \nu_p(c) \leqslant \nu_p(k) \\
&\iff c \mid k.
\end{aligned}
$$

The first such k is $k = c$, so $\operatorname{ord}_{cm}(10) = c\alpha$. $\qquad\square$

Comment. The Lifting the Exponent Lemma states that, for any odd prime p, any integers a, b coprime with p such that $p \mid a - b$, and any positive integer exponent n,

$$\nu_p(a^n - b^n) = \nu_p(a - b) + \nu_p(n),$$

and, for $p = 2$,

$$\nu_2(a^n - b^n) = \nu_2(a^2 - b^2) + \nu_p(n) - 1.$$

Both claims can be proved by induction on n.

N5. Find all pairs (p, q) of prime numbers with $p > q$ for which the number

$$\frac{(p + q)^{p+q}(p - q)^{p-q} - 1}{(p + q)^{p-q}(p - q)^{p+q} - 1}$$

is an integer.

(Japan)

Answer: The only such pair is $(3, 2)$.

Solution. Let $M = (p + q)^{p-q}(p - q)^{p+q} - 1$, which is relatively prime with both $p + q$ and $p - q$. Denote by $(p - q)^{-1}$ the multiplicative inverse of $(p - q)$ modulo M.

By eliminating the term -1 in the numerator,

$$(p + q)^{p+q}(p - q)^{p-q} - 1 \equiv (p + q)^{p-q}(p - q)^{p+q} - 1 \pmod{M}$$
$$(p + q)^{2q} \equiv (p - q)^{2q} \pmod{M} \tag{1}$$
$$\left((p + q) \cdot (p - q)^{-1}\right)^{2q} \equiv 1 \pmod{M}. \tag{2}$$

Case 1: $q \geqslant 5$.

Consider an arbitrary prime divisor r of M. Notice that M is odd, so $r \geqslant 3$. By (2), the multiplicative order of $\left((p + q) \cdot (p - q)^{-1}\right)$ modulo r is a divisor of the exponent $2q$ in (2), so it can be 1, 2, q or $2q$.

By Fermat's theorem, the order divides $r - 1$. So, if the order is q or $2q$ then $r \equiv 1 \pmod{q}$. If the order is 1 or 2 then $r \mid (p + q)^2 - (p - q)^2 = 4pq$, so $r = p$ or $r = q$. The case $r = p$ is not possible, because, by applying Fermat's theorem,

$$M = (p + q)^{p-q}(p - q)^{p+q} - 1 \equiv q^{p-q}(-q)^{p+q} - 1 = \left(q^2\right)^p - 1 \equiv q^2 - 1 = (q+1)(q-1) \pmod{p}$$

and the last factors $q - 1$ and $q + 1$ are less than p and thus $p \nmid M$. Hence, all prime divisors of M are either q or of the form $kq + 1$; it follows that all positive divisors of M are congruent to 0 or 1 modulo q.

Now notice that

$$M = \left((p + q)^{\frac{p-q}{2}}(p - q)^{\frac{p+q}{2}} - 1\right)\left((p + q)^{\frac{p-q}{2}}(p - q)^{\frac{p+q}{2}} + 1\right)$$

is the product of two consecutive positive odd numbers; both should be congruent to 0 or 1 modulo q. But this is impossible by the assumption $q \geqslant 5$. So, there is no solution in Case 1.

Case 2: $q = 2$.

By (1), we have $M \mid (p + q)^{2q} - (p - q)^{2q} = (p + 2)^4 - (p - 2)^4$, so

$$(p + 2)^{p-2}(p - 2)^{p+2} - 1 = M \leqslant (p + 2)^4 - (p - 2)^4 \leqslant (p + 2)^4 - 1,$$
$$(p + 2)^{p-6}(p - 2)^{p+2} \leqslant 1.$$

If $p \geqslant 7$ then the left-hand side is obviously greater than 1. For $p = 5$ we have $(p + 2)^{p-6}(p - 2)^{p+2} = 7^{-1} \cdot 3^7$ which is also too large.

There remains only one candidate, $p = 3$, which provides a solution:

$$\frac{(p + q)^{p+q}(p - q)^{p-q} - 1}{(p + q)^{p-q}(p - q)^{p+q} - 1} = \frac{5^5 \cdot 1^1 - 1}{5^1 \cdot 1^5 - 1} = \frac{3124}{4} = 781.$$

So in Case 2 the only solution is $(p, q) = (3, 2)$.

Case 3: q = 3.

Similarly to Case 2, we have

$$M \mid (p + q)^{2q} - (p - q)^{2q} = 64 \cdot \left(\left(\frac{p + 3}{2} \right)^6 - \left(\frac{p - 3}{2} \right)^6 \right).$$

Since M is odd, we conclude that

$$M \mid \left(\frac{p + 3}{2} \right)^6 - \left(\frac{p - 3}{2} \right)^6$$

and

$$(p + 3)^{p-3}(p - 3)^{p+3} - 1 = M \leqslant \left(\frac{p + 3}{2} \right)^6 - \left(\frac{p - 3}{2} \right)^6 \leqslant \left(\frac{p + 3}{2} \right)^6 - 1,$$
$$64(p + 3)^{p-9}(p - 3)^{p+3} \leqslant 1.$$

If $p \geqslant 11$ then the left-hand side is obviously greater than 1. If $p = 7$ then the left-hand side is $64 \cdot 10^{-2} \cdot 4^{10} > 1$. If $p = 5$ then the left-hand side is $64 \cdot 8^{-4} \cdot 2^8 = 2^2 > 1$. Therefore, there is no solution in Case 3.

N6. Find the smallest positive integer n, or show that no such n exists, with the following property: there are infinitely many distinct n-tuples of positive rational numbers $(a_1, a_2, \ldots, a_n)$ such that both

$$a_1 + a_2 + \cdots + a_n \qquad \text{and} \qquad \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}$$

are integers.

<div align="right">(Singapore)</div>

Answer: $n = 3$.

Solution 1. For $n = 1$, $a_1 \in \mathbb{Z}_{>0}$ and $\frac{1}{a_1} \in \mathbb{Z}_{>0}$ if and only if $a_1 = 1$. Next we show that

(i) *There are finitely many $(x, y) \in \mathbb{Q}_{>0}^2$ satisfying $x + y \in \mathbb{Z}$ and $\frac{1}{x} + \frac{1}{y} \in \mathbb{Z}$*

Write $x = \frac{a}{b}$ and $y = \frac{c}{d}$ with $a, b, c, d \in \mathbb{Z}_{>0}$ and $\gcd(a, b) = \gcd(c, d) = 1$. Then $x + y \in \mathbb{Z}$ and $\frac{1}{x} + \frac{1}{y} \in \mathbb{Z}$ is equivalent to the two divisibility conditions

$$bd \mid ad + bc \quad (1) \qquad \text{and} \qquad ac \mid ad + bc \quad (2)$$

Condition (1) implies that $d \mid ad + bc \iff d \mid bc \iff d \mid b$ since $\gcd(c, d) = 1$. Still from (1) we get $b \mid ad + bc \iff b \mid ad \iff b \mid d$ since $\gcd(a, b) = 1$. From $b \mid d$ and $d \mid b$ we have $b = d$.

An analogous reasoning with condition (2) shows that $a = c$. Hence $x = \frac{a}{b} = \frac{c}{d} = y$, i.e., the problem amounts to finding all $x \in \mathbb{Q}_{>0}$ such that $2x \in \mathbb{Z}_{>0}$ and $\frac{2}{x} \in \mathbb{Z}_{>0}$. Letting $n = 2x \in \mathbb{Z}_{>0}$, we have that $\frac{2}{x} \in \mathbb{Z}_{>0} \iff \frac{4}{n} \in \mathbb{Z}_{>0} \iff n = 1, 2$ or 4, and there are finitely many solutions, namely $(x, y) = (\frac{1}{2}, \frac{1}{2})$, $(1, 1)$ or $(2, 2)$.

(ii) *There are infinitely many triples $(x, y, z) \in \mathbb{Q}_{>0}^2$ such that $x + y + z \in \mathbb{Z}$ and $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} \in \mathbb{Z}$.* We will look for triples such that $x + y + z = 1$, so we may write them in the form

$$(x, y, z) = \left(\frac{a}{a + b + c}, \frac{b}{a + b + c}, \frac{c}{a + b + c} \right) \qquad \text{with } a, b, c \in \mathbb{Z}_{>0}$$

We want these to satisfy

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{a + b + c}{a} + \frac{a + b + c}{b} + \frac{a + b + c}{c} \in \mathbb{Z} \iff \frac{b + c}{a} + \frac{a + c}{b} + \frac{a + b}{c} \in \mathbb{Z}$$

Fixing $a = 1$, it suffices to find infinitely many pairs $(b, c) \in \mathbb{Z}_{>0}^2$ such that

$$\frac{1}{b} + \frac{1}{c} + \frac{c}{b} + \frac{b}{c} = 3 \iff b^2 + c^2 - 3bc + b + c = 0 \qquad (*)$$

To show that equation $(*)$ has infinitely many solutions, we use *Vieta jumping* (also known as *root flipping*): starting with $b = 2$, $c = 3$, the following algorithm generates infinitely many solutions. Let $c \geqslant b$, and view $(*)$ as a quadratic equation in b for c fixed:

$$b^2 - (3c - 1) \cdot b + (c^2 + c) = 0 \qquad (**)$$

Then there exists another root $b_0 \in \mathbb{Z}$ of $(**)$ which satisfies $b + b_0 = 3c - 1$ and $b \cdot b_0 = c^2 + c$. Since $c \geqslant b$ by assumption,

$$b_0 = \frac{c^2 + c}{b} \geqslant \frac{c^2 + c}{c} > c$$

Hence from the solution (b, c) we obtain another one (c, b_0) with $b_0 > c$, and we can then "jump" again, this time with c as the "variable" in the quadratic $(*)$. This algorithm will generate an infinite sequence of distinct solutions, whose first terms are

$$(2, 3), (3, 6), (6, 14), (14, 35), (35, 90), (90, 234), (234, 611), (611, 1598), (1598, 4182), \ldots$$

Comment. Although not needed for solving this problem, we may also explicitly solve the recursion given by the Vieta jumping. Define the sequence (x_n) as follows:

$$x_0 = 2, \quad x_1 = 3 \quad \text{and} \quad x_{n+2} = 3x_{n+1} - x_n - 1 \text{ for } n \geqslant 0$$

Then the triple

$$(x, y, z) = \left(\frac{1}{1 + x_n + x_{n+1}}, \frac{x_n}{1 + x_n + x_{n+1}}, \frac{x_{n+1}}{1 + x_n + x_{n+1}} \right)$$

satisfies the problem conditions for all $n \in \mathbb{N}$. It is easy to show that $x_n = F_{2n+1} + 1$, where F_n denotes the n-th term of the Fibonacci sequence ($F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for $n \geqslant 0$).

Solution 2. Call the n-tuples $(a_1, a_2, \ldots, a_n) \in \mathbb{Q}_{>0}^n$ satisfying the conditions of the problem statement *good*, and those for which

$$f(a_1, \ldots, a_n) \overset{\text{def}}{=} (a_1 + a_2 + \cdots + a_n) \left(\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} \right)$$

is an integer *pretty*. Then good n-tuples are pretty, and if $(b_1, \ldots, b_n)$ is pretty then

$$\left(\frac{b_1}{b_1 + b_2 + \cdots + b_n}, \frac{b_2}{b_1 + b_2 + \cdots + b_n}, \ldots, \frac{b_n}{b_1 + b_2 + \cdots + b_n} \right)$$

is good since the sum of its components is 1, and the sum of the reciprocals of its components equals $f(b_1, \ldots, b_n)$. We declare pretty n-tuples proportional to each other *equivalent* since they are precisely those which give rise to the same good n-tuple. Clearly, each such equivalence class contains exactly one n-tuple of positive integers having no common prime divisors. Call such n-tuple a *primitive* pretty tuple. Our task is to find infinitely many primitive pretty n-tuples.

For $n = 1$, there is clearly a single primitive 1-tuple. For $n = 2$, we have $f(a, b) = \frac{(a+b)^2}{ab}$, which can be integral (for coprime $a, b \in \mathbb{Z}_{>0}$) only if $a = b = 1$ (see for instance (i) in the first solution).

Now we construct infinitely many primitive pretty triples for $n = 3$. Fix $b, c, k \in \mathbb{Z}_{>0}$; we will try to find sufficient conditions for the existence of an $a \in \mathbb{Q}_{>0}$ such that $f(a, b, c) = k$. Write $\sigma = b + c$, $\tau = bc$. From $f(a, b, c) = k$, we have that a should satisfy the quadratic equation

$$a^2 \cdot \sigma + a \cdot (\sigma^2 - (k-1)\tau) + \sigma\tau = 0 \tag{1}$$

whose discriminant is

$$\Delta = (\sigma^2 - (k-1)\tau)^2 - 4\sigma^2\tau = ((k+1)\tau - \sigma^2)^2 - 4k\tau^2.$$

We need it to be a square of an integer, say, $\Delta = M^2$ for some $M \in \mathbb{Z}$, i.e., we want

$$((k+1)\tau - \sigma^2)^2 - M^2 = 2k \cdot 2\tau^2$$

so that it suffices to set

$$(k+1)\tau - \sigma^2 = \tau^2 + k, \qquad M = \tau^2 - k.$$

The first relation reads $\sigma^2 = (\tau - 1)(k - \tau)$, so if b and c satisfy

$$\tau - 1 \mid \sigma^2 \quad \text{i.e.} \quad bc - 1 \mid (b + c)^2 \tag{2}$$

then $k = \frac{\sigma^2}{\tau - 1} + \tau$ will be integral, and we find rational solutions to (1), namely

$$a = \frac{\sigma}{\tau - 1} = \frac{b + c}{bc - 1} \quad \text{or} \quad a = \frac{\tau^2 - \tau}{\sigma} = \frac{bc \cdot (bc - 1)}{b + c}$$

We can now find infinitely many pairs (b, c) satisfying (2) by Vieta jumping. For example, if we impose

$$(b + c)^2 = 5 \cdot (bc - 1)$$

then all pairs $(b, c) = (v_i, v_{i+1})$ satisfy the above condition, where

$$v_1 = 2, \ v_2 = 3, \qquad v_{i+2} = 3v_{i+1} - v_i \quad \text{for } i \geqslant 0$$

For $(b, c) = (v_i, v_{i+1})$, one of the solutions to (1) will be $a = (b + c)/(bc - 1) = 5/(b + c) = 5/(v_i + v_{i+1})$. Then the pretty triple (a, b, c) will be equivalent to the integral pretty triple

$$(5, v_i(v_i + v_{i+1}), v_{i+1}(v_i + v_{i+1}))$$

After possibly dividing by 5, we obtain infinitely many primitive pretty triples, as required.

Comment. There are many other infinite series of $(b, c) = (v_i, v_{i+1})$ with $bc - 1 \mid (b + c)^2$. Some of them are:

$$v_1 = 1, \qquad v_2 = 3, \qquad v_{i+1} = 6v_i - v_{i-1}, \qquad (v_i + v_{i+1})^2 = 8 \cdot (v_i v_{i+1} - 1);$$
$$v_1 = 1, \qquad v_2 = 2, \qquad v_{i+1} = 7v_i - v_{i-1}, \qquad (v_i + v_{i+1})^2 = 9 \cdot (v_i v_{i+1} - 1);$$
$$v_1 = 1, \qquad v_2 = 5, \qquad v_{i+1} = 7v_i - v_{i-1}, \qquad (v_i + v_{i+1})^2 = 9 \cdot (v_i v_{i+1} - 1)$$

(the last two are in fact one sequence prolonged in two possible directions).

N7. Say that an ordered pair (x, y) of integers is an *irreducible lattice point* if x and y are relatively prime. For any finite set S of irreducible lattice points, show that there is a homogenous polynomial in two variables, $f(x, y)$, with integer coefficients, of degree at least 1, such that $f(x, y) = 1$ for each (x, y) in the set S.

Note: A homogenous polynomial of degree n is any nonzero polynomial of the form

$$f(x, y) = a_0 x^n + a_1 x^{n-1} y + a_2 x^{n-2} y^2 + \cdots + a_{n-1} x y^{n-1} + a_n y^n.$$

(U.S.A.)

Solution 1. First of all, we note that finding a homogenous polynomial $f(x, y)$ such that $f(x, y) = \pm 1$ is enough, because we then have $f^2(x, y) = 1$. Label the irreducible lattice points (x_1, y_1) through (x_n, y_n). If any two of these lattice points (x_i, y_i) and (x_j, y_j) lie on the same line through the origin, then $(x_j, y_j) = (-x_i, -y_i)$ because both of the points are irreducible. We then have $f(x_j, y_j) = \pm f(x_i, y_i)$ whenever f is homogenous, so we can assume that no two of the lattice points are collinear with the origin by ignoring the extra lattice points.

Consider the homogenous polynomials $\ell_i(x, y) = y_i x - x_i y$ and define

$$g_i(x, y) = \prod_{j \neq i} \ell_j(x, y).$$

Then $\ell_i(x_j, y_j) = 0$ if and only if $j = i$, because there is only one lattice point on each line through the origin. Thus, $g_i(x_j, y_j) = 0$ for all $j \neq i$. Define $a_i = g_i(x_i, y_i)$, and note that $a_i \neq 0$.

Note that $g_i(x, y)$ is a degree $n - 1$ polynomial with the following two properties:

1. $g_i(x_j, y_j) = 0$ if $j \neq i$.

2. $g_i(x_i, y_i) = a_i$.

For any $N \geqslant n - 1$, there also exists a polynomial of degree N with the same two properties. Specifically, let $I_i(x, y)$ be a degree 1 homogenous polynomial such that $I_i(x_i, y_i) = 1$, which exists since (x_i, y_i) is irreducible. Then $I_i(x, y)^{N-(n-1)} g_i(x, y)$ satisfies both of the above properties and has degree N.

We may now reduce the problem to the following claim:

Claim: For each positive integer a, there is a homogenous polynomial $f_a(x, y)$, with integer coefficients, of degree at least 1, such that $f_a(x, y) \equiv 1 \pmod{a}$ for all relatively prime (x, y).

To see that this claim solves the problem, take a to be the least common multiple of the numbers a_i $(1 \leqslant i \leqslant n)$. Take f_a given by the claim, choose some power $f_a(x, y)^k$ that has degree at least $n - 1$, and subtract appropriate multiples of the g_i constructed above to obtain the desired polynomial.

We prove the claim by factoring a. First, if a is a power of a prime $(a = p^k)$, then we may choose either:

- $f_a(x, y) = (x^{p-1} + y^{p-1})^{\phi(a)}$ if p is odd;

- $f_a(x, y) = (x^2 + xy + y^2)^{\phi(a)}$ if $p = 2$.

Now suppose a is any positive integer, and let $a = q_1 q_2 \cdots q_k$, where the q_i are prime powers, pairwise relatively prime. Let f_{q_i} be the polynomials just constructed, and let F_{q_i} be powers of these that all have the same degree. Note that

$$\frac{a}{q_i} F_{q_i}(x, y) \equiv \frac{a}{q_i} \pmod{a}$$

for any relatively prime x, y. By Bézout's lemma, there is an integer linear combination of the $\frac{a}{q_i}$ that equals 1. Thus, there is a linear combination of the F_{q_i} such that $F_{q_i}(x, y) \equiv 1 \pmod{a}$ for any relatively prime (x, y); and this polynomial is homogenous because all the F_{q_i} have the same degree.

Solution 2. As in the previous solution, label the irreducible lattice points $(x_1, y_1), \ldots, (x_n, y_n)$ and assume without loss of generality that no two of the points are collinear with the origin. We induct on n to construct a homogenous polynomial $f(x, y)$ such that $f(x_i, y_i) = 1$ for all $1 \leqslant i \leqslant n$.

If $n = 1$: Since x_1 and y_1 are relatively prime, there exist some integers c, d such that $cx_1 + dy_1 = 1$. Then $f(x, y) = cx + dy$ is suitable.

If $n \geqslant 2$: By the induction hypothesis we already have a homogeneous polynomial $g(x, y)$ with $g(x_1, y_1) = \ldots = g(x_{n-1}, y_{n-1}) = 1$. Let $j = \deg g$,

$$g_n(x, y) = \prod_{k=1}^{n-1} (y_k x - x_k y),$$

and $a_n = g_n(x_n, y_n)$. By assumption, $a_n \neq 0$. Take some integers c, d such that $cx_n + dy_n = 1$. We will construct $f(x, y)$ in the form

$$f(x, y) = g(x, y)^K - C \cdot g_n(x, y) \cdot (cx + dy)^L,$$

where K and L are some positive integers and C is some integer. We assume that $L = Kj - n + 1$ so that f is homogenous.

Due to $g(x_1, y_1) = \ldots = g(x_{n-1}, y_{n-1}) = 1$ and $g_n(x_1, y_1) = \ldots = g_n(x_{n-1}, y_{n-1}) = 0$, the property $f(x_1, y_1) = \ldots = f(x_{n-1}, y_{n-1}) = 1$ is automatically satisfied with any choice of K, L, and C.

Furthermore,

$$f(x_n, y_n) = g(x_n, y_n)^K - C \cdot g_n(x_n, y_n) \cdot (cx_n + dy_n)^L = g(x_n, y_n)^K - Ca_n.$$

If we have an exponent K such that $g(x_n, y_n)^K \equiv 1 \pmod{a_n}$, then we may choose C such that $f(x_n, y_n) = 1$. We now choose such a K.

Consider an arbitrary prime divisor p of a_n. By

$$p \mid a_n = g_n(x_n, y_n) = \prod_{k=1}^{n-1} (y_k x_n - x_k y_n),$$

there is some $1 \leqslant k < n$ such that $x_k y_n \equiv x_n y_k \pmod{p}$. We first show that $x_k x_n$ or $y_k y_n$ is relatively prime with p. This is trivial in the case $x_k y_n \equiv x_n y_k \not\equiv 0 \pmod{p}$. In the other case, we have $x_k y_n \equiv x_n y_k \equiv 0 \pmod{p}$, If, say $p \mid x_k$, then $p \nmid y_k$ because (x_k, y_k) is irreducible, so $p \mid x_n$; then $p \nmid y_n$ because (x_k, y_k) is irreducible. In summary, $p \mid x_k$ implies $p \nmid y_k y_n$. Similarly, $p \mid y_n$ implies $p \nmid x_k x_n$.

By the homogeneity of g we have the congruences

$$x_k^d \cdot g(x_n, y_n) = g(x_k x_n, x_k y_n) \equiv g(x_k x_n, y_k x_n) = x_n^d \cdot g(x_k, y_k) = x_n^d \pmod{p} \tag{1.1}$$

and

$$y_k^d \cdot g(x_n, y_n) = g(y_k x_n, y_k y_n) \equiv g(x_k y_n, y_k y_n) = y_n^d \cdot g(x_k, y_k) = y_n^d \pmod{p}. \tag{1.2}$$

If $p \nmid x_k x_n$, then take the $(p-1)^{st}$ power of (1.1); otherwise take the $(p-1)^{st}$ power of (1.2); by Fermat's theorem, in both cases we get

$$g(x_n, y_n)^{p-1} \equiv 1 \pmod{p}.$$

If $p^\alpha \mid m$, then we have

$$g(x_n, y_n)^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^\alpha},$$

which implies that the exponent $K = n \cdot \varphi(a_n)$, which is a multiple of all $p^{\alpha-1}(p-1)$, is a suitable choice. (The factor n is added only so that $K \geqslant n$ and so $L > 0$.)

Comment. It is possible to show that there is no constant C for which, given any two irreducible lattice points, there is some homogenous polynomial f of degree at most C with integer coefficients that takes the value 1 on the two points. Indeed, if one of the points is $(1,0)$ and the other is (a,b), the polynomial $f(x,y) = a_0 x^n + a_1 x^{n-1} y + \cdots + a_n y^n$ should satisfy $a_0 = 1$, and so $a^n \equiv 1 \pmod{b}$. If $a = 3$ and $b = 2^k$ with $k \geqslant 3$, then $n \geqslant 2^{k-2}$. If we choose $2^{k-2} > C$, this gives a contradiction.

N8.   Let p be an odd prime number and $\mathbb{Z}_{>0}$ be the set of positive integers. Suppose that a function $f\colon \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \to \{0,1\}$ satisfies the following properties:

- $f(1,1) = 0$;

- $f(a,b) + f(b,a) = 1$ for any pair of relatively prime positive integers (a,b) not both equal to 1;

- $f(a + b, b) = f(a, b)$ for any pair of relatively prime positive integers (a, b).

Prove that

$$\sum_{n=1}^{p-1} f(n^2, p) \geqslant \sqrt{2p} - 2.$$

<div align="right">(Italy)</div>

Solution 1.   Denote by $\mathbb{A}$ the set of all pairs of coprime positive integers. Notice that for every $(a, b) \in \mathbb{A}$ there exists a pair $(u, v) \in \mathbb{Z}^2$ with $ua + vb = 1$. Moreover, if (u_0, v_0) is one such pair, then all such pairs are of the form $(u, v) = (u_0 + kb, v_0 - ka)$, where $k \in \mathbb{Z}$. So there exists a unique such pair (u, v) with $-b/2 < u \leqslant b/2$; we denote this pair by $(u, v) = g(a, b)$.

Lemma. Let $(a, b) \in \mathbb{A}$ and $(u, v) = g(a, b)$. Then $f(a, b) = 1 \iff u > 0$.

Proof. We induct on $a + b$. The base case is $a + b = 2$. In this case, we have that $a = b = 1$, $g(a, b) = g(1, 1) = (0, 1)$ and $f(1, 1) = 0$, so the claim holds.

Assume now that $a + b > 2$, and so $a \neq b$, since a and b are coprime. Two cases are possible.

Case 1: $a > b$.

Notice that $g(a - b, b) = (u, v + u)$, since $u(a - b) + (v + u)b = 1$ and $u \in (-b/2, b/2]$. Thus $f(a, b) = 1 \iff f(a - b, b) = 1 \iff u > 0$ by the induction hypothesis.

Case 2: $a < b$. (Then, clearly, $b \geqslant 2$.)

Now we estimate v. Since $vb = 1 - ua$, we have

$$1 + \frac{ab}{2} > vb \geqslant 1 - \frac{ab}{2}, \quad \text{so} \quad \frac{1 + a}{2} \geqslant \frac{1}{b} + \frac{a}{2} > v \geqslant \frac{1}{b} - \frac{a}{2} > -\frac{a}{2}.$$

Thus $1 + a > 2v > -a$, so $a \geqslant 2v > -a$, hence $a/2 \geqslant v > -a/2$, and thus $g(b, a) = (v, u)$.

Observe that $f(a, b) = 1 \iff f(b, a) = 0 \iff f(b - a, a) = 0$. We know from Case 1 that $g(b - a, a) = (v, u + v)$. We have $f(b - a, a) = 0 \iff v \leqslant 0$ by the inductive hypothesis. Then, since $b > a \geqslant 1$ and $ua + vb = 1$, we have $v \leqslant 0 \iff u > 0$, and we are done. $\square$

The Lemma proves that, for all $(a, b) \in \mathbb{A}$, $f(a, b) = 1$ if and only if the inverse of a modulo b, taken in $\{1, 2, \ldots, b - 1\}$, is at most $b/2$. Then, for any odd prime p and integer n such that $n \not\equiv 0 \pmod{p}$, $f(n^2, p) = 1$ iff the inverse of $n^2 \bmod p$ is less than $p/2$. Since $\{n^2 \bmod p\colon 1 \leqslant n \leqslant p - 1\} = \{n^{-2} \bmod p\colon 1 \leqslant n \leqslant p - 1\}$, including multiplicities (two for each quadratic residue in each set), we conclude that the desired sum is twice the number of quadratic residues that are less than $p/2$, i.e.,

$$\sum_{n=1}^{p-1} f(n^2, p) = 2\left|\left\{k\colon 1 \leqslant k \leqslant \frac{p-1}{2} \text{ and } k^2 \bmod p < \frac{p}{2}\right\}\right|. \tag{1}$$

Since the number of perfect squares in the interval $[1, p/2)$ is $\lfloor \sqrt{p/2} \rfloor > \sqrt{p/2} - 1$, we conclude that

$$\sum_{n=1}^{p-1} f(n^2, p) > 2\left(\sqrt{\frac{p}{2}} - 1\right) = \sqrt{2p} - 2.$$

Solution 2. We provide a different proof for the Lemma. For this purpose, we use continued fractions to find $g(a,b) = (u,v)$ explicitly.

The function f is completely determined on $\mathbb{A}$ by the following

Claim. Represent a/b as a continued fraction; that is, let a_0 be an integer and $a_1, \ldots, a_k$ be positive integers such that $a_k \geqslant 2$ and

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_k}}}} = [a_0; a_1, a_2, \ldots, a_k].$$

Then $f(a,b) = 0 \iff k$ is even.

Proof. We induct on b. If $b = 1$, then $a/b = [a]$ and $k = 0$. Then, for $a \geqslant 1$, an easy induction shows that $f(a,1) = f(1,1) = 0$.

Now consider the case $b > 1$. Perform the Euclidean division $a = qb + r$, with $0 \leqslant r < b$. We have $r \neq 0$ because $\gcd(a,b) = 1$. Hence

$$f(a,b) = f(r,b) = 1 - f(b,r), \quad \frac{a}{b} = [q; a_1, \ldots, a_k], \quad \text{and} \quad \frac{b}{r} = [a_1; a_2, \ldots, a_k].$$

Then the number of terms in the continued fraction representations of a/b and b/r differ by one. Since $r < b$, the inductive hypothesis yields

$$f(b,r) = 0 \iff k - 1 \text{ is even,}$$

and thus

$$f(a,b) = 0 \iff f(b,r) = 1 \iff k - 1 \text{ is odd} \iff k \text{ is even.} \qquad \square$$

Now we use the following well-known properties of continued fractions to prove the Lemma:

Let p_i and q_i be coprime positive integers with $[a_0; a_1, a_2, \ldots, a_i] = p_i/q_i$, with the notation borrowed from the Claim. In particular, $a/b = [a_0; a_1, a_2, \ldots, a_k] = p_k/q_k$. Assume that $k > 0$ and define $q_{-1} = 0$ if necessary. Then

- $q_k = a_k q_{k-1} + q_{k-2}$, and

- $a q_{k-1} - b p_{k-1} = p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$.

Assume that $k > 0$. Then $a_k \geqslant 2$, and

$$b = q_k = a_k q_{k-1} + q_{k-2} \geqslant a_k q_{k-1} \geqslant 2 q_{k-1} \implies q_{k-1} \leqslant \frac{b}{2},$$

with strict inequality for $k > 1$, and

$$(-1)^{k-1} q_{k-1} a + (-1)^k p_{k-1} b = 1.$$

Now we finish the proof of the Lemma. It is immediate for $k = 0$. If $k = 1$, then $(-1)^{k-1} = 1$, so

$$-b/2 < 0 \leqslant (-1)^{k-1} q_{k-1} \leqslant b/2.$$

If $k > 1$, we have $q_{k-1} < b/2$, so

$$-b/2 < (-1)^{k-1} q_{k-1} < b/2.$$

Thus, for any $k > 0$, we find that $g(a,b) = ((-1)^{k-1} q_{k-1}, (-1)^k p_{k-1})$, and so

$$f(a,b) = 1 \iff k \text{ is odd} \iff u = (-1)^{k-1} q_{k-1} > 0.$$

Comment 1. The Lemma can also be established by observing that f is uniquely defined on $\mathbb{A}$, defining $f_1(a,b) = 1$ if $u > 0$ in $g(a,b) = (u,v)$ and $f_1(a,b) = 0$ otherwise, and verifying that f_1 satisfies all the conditions from the statement.

It seems that the main difficulty of the problem is in conjecturing the Lemma.

Comment 2. The case $p \equiv 1 \pmod 4$ is, in fact, easier than the original problem. We have, in general, for $1 \leqslant a \leqslant p-1$,

$$f(a,p) = 1 - f(p,a) = 1 - f(p-a,a) = f(a,p-a) = f(a+(p-a),p-a) = f(p,p-a) = 1 - f(p-a,p).$$

If $p \equiv 1 \pmod 4$, then a is a quadratic residue modulo p if and only if $p - a$ is a quadratic residue modulo p. Therefore, denoting by r_k (with $1 \leqslant r_k \leqslant p-1$) the remainder of the division of k^2 by p, we get

$$\sum_{n=1}^{p-1} f(n^2, p) = \sum_{n=1}^{p-1} f(r_n, p) = \frac{1}{2} \sum_{n=1}^{p-1} (f(r_n, p) + f(p - r_n, p)) = \frac{p-1}{2}.$$

Comment 3. The estimate for the sum $\sum_{n=1}^{p} f(n^2, p)$ can be improved by refining the final argument in Solution 1. In fact, one can prove that

$$\sum_{n=1}^{p-1} f(n^2, p) \geqslant \frac{p-1}{16}.$$

By counting the number of perfect squares in the intervals $[kp, (k+1/2)p)$, we find that

$$\sum_{n=1}^{p-1} f(n^2, p) = \sum_{k=0}^{p-1} \left(\left\lfloor \sqrt{\left(k + \frac{1}{2}\right)p} \right\rfloor - \left\lfloor \sqrt{kp} \right\rfloor \right). \tag{2}$$

Each summand of (2) is non-negative. We now estimate the number of positive summands. Suppose that a summand is zero, i.e.,

$$\left\lfloor \sqrt{\left(k + \frac{1}{2}\right)p} \right\rfloor = \left\lfloor \sqrt{kp} \right\rfloor =: q.$$

Then both of the numbers kp and $kp + p/2$ lie within the interval $[q^2, (q+1)^2)$. Hence

$$\frac{p}{2} < (q+1)^2 - q^2,$$

which implies

$$q \geqslant \frac{p-1}{4}.$$

Since $q \leqslant \sqrt{kp}$, if the kth summand of (2) is zero, then

$$k \geqslant \frac{q^2}{p} \geqslant \frac{(p-1)^2}{16p} > \frac{p-2}{16} \implies k \geqslant \frac{p-1}{16}.$$

So at least the first $\lceil \frac{p-1}{16} \rceil$ summands (from $k = 0$ to $k = \lceil \frac{p-1}{16} \rceil - 1$) are positive, and the result follows.

Comment 4. The bound can be further improved by using different methods. In fact, we prove that

$$\sum_{n=1}^{p-1} f(n^2, p) \geqslant \frac{p-3}{4}.$$

To that end, we use the Legendre symbol

$$\left(\frac{a}{p} \right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a nonzero quadratic residue mod } p \\ -1 & \text{otherwise.} \end{cases}$$

We start with the following Claim, which tells us that there are not too many consecutive quadratic residues or consecutive quadratic non-residues.

Claim. $\sum_{n=1}^{p-1} \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = -1$.

Proof. We have $\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = \left(\frac{n(n+1)}{p}\right)$. For $1 \leqslant n \leqslant p-1$, we get that $n(n+1) \equiv n^2(1+n^{-1}) \pmod{p}$, hence $\left(\frac{n(n+1)}{p}\right) = \left(\frac{1+n^{-1}}{p}\right)$. Since $\{1 + n^{-1} \bmod p \colon 1 \leqslant n \leqslant p-1\} = \{0, 2, 3, \ldots, p-1 \bmod p\}$, we find

$$\sum_{n=1}^{p-1} \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = \sum_{n=1}^{p-1} \left(\frac{1+n^{-1}}{p}\right) = \sum_{n=1}^{p-1}\left(\frac{n}{p}\right) - 1 = -1,$$

because $\sum_{n=1}^{p}\left(\frac{n}{p}\right) = 0$. $\qquad\square$

Observe that (1) becomes

$$\sum_{n=1}^{p-1} f(n^2, p) = 2\,|S|, \quad S = \left\{r\colon 1 \leqslant r \leqslant \frac{p-1}{2} \text{ and } \left(\frac{r}{p}\right) = 1\right\}.$$

We connect S with the sum from the claim by pairing quadratic residues and quadratic non-residues. To that end, define

$$S' = \left\{r\colon 1 \leqslant r \leqslant \frac{p-1}{2} \text{ and } \left(\frac{r}{p}\right) = -1\right\}$$

$$T = \left\{r\colon \frac{p+1}{2} \leqslant r \leqslant p-1 \text{ and } \left(\frac{r}{p}\right) = 1\right\}$$

$$T' = \left\{r\colon \frac{p+1}{2} \leqslant r \leqslant p-1 \text{ and } \left(\frac{r}{p}\right) = -1\right\}$$

Since there are exactly $(p-1)/2$ nonzero quadratic residues modulo p, $|S| + |T| = (p-1)/2$. Also we obviously have $|T| + |T'| = (p-1)/2$. Then $|S| = |T'|$.

For the sake of brevity, define $t = |S| = |T'|$. If $\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = -1$, then exactly of one the numbers $\left(\frac{n}{p}\right)$ and $\left(\frac{n+1}{p}\right)$ is equal to 1, so

$$\left|\left\{n\colon 1 \leqslant n \leqslant \frac{p-3}{2} \text{ and } \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = -1\right\}\right| \leqslant |S| + |S-1| = 2t.$$

On the other hand, if $\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = -1$, then exactly one of $\left(\frac{n}{p}\right)$ and $\left(\frac{n+1}{p}\right)$ is equal to -1, and

$$\left|\left\{n\colon \frac{p+1}{2} \leqslant n \leqslant p-2 \text{ and } \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = -1\right\}\right| \leqslant |T'| + |T'-1| = 2t.$$

Thus, taking into account that the middle term $\left(\frac{(p-1)/2}{p}\right)\left(\frac{(p+1)/2}{p}\right)$ may happen to be -1,

$$\left|\left\{n\colon 1 \leqslant n \leqslant p-2 \text{ and } \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = -1\right\}\right| \leqslant 4t + 1.$$

This implies that

$$\left|\left\{n\colon 1 \leqslant n \leqslant p-2 \text{ and } \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = 1\right\}\right| \geqslant (p-2) - (4t+1) = p - 4t - 3,$$

and so

$$-1 = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) \geqslant p - 4t - 3 - (4t+1) = p - 8t - 4,$$

which implies $8t \geqslant p - 3$, and thus

$$\sum_{n=1}^{p-1} f(n^2, p) = 2t \geqslant \frac{p-3}{4}.$$

Comment 5. It is possible to prove that

$$\sum_{n=1}^{p-1} f(n^2, p) \geqslant \frac{p-1}{2}.$$

The case $p \equiv 1 \pmod 4$ was already mentioned, and it is the equality case. If $p \equiv 3 \pmod 4$, then, by a theorem of Dirichlet, we have

$$\left| \left\{ r \colon 1 \leqslant r \leqslant \frac{p-1}{2} \text{ and } \left(\frac{r}{p}\right) = 1 \right\} \right| > \frac{p-1}{4},$$

which implies the result.

See `https://en.wikipedia.org/wiki/Quadratic_residue#Dirichlet.27s_formulas` for the full statement of the theorem. It seems that no elementary proof of it is known; a proof using complex analysis is available, for instance, in Chapter 7 of the book *Quadratic Residues and Non-Residues: Selected Topics*, by Steve Wright, available in `https://arxiv.org/abs/1408.0235`.