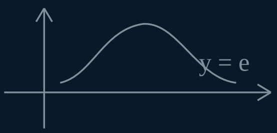
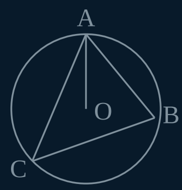
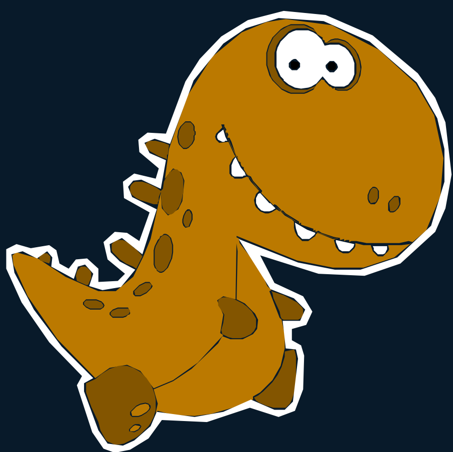




Selected Math Works

by Vladimir Barzov

$a^2 + b^2 = c^2$



$k = n(n+1)/2$

Selected Math Works

by Vladimir Barzov

Sofia, 2026

Printed by Bulged Ltd. – Bulgaria

Contents

Foreword

This collection of mathematical problems and articles includes some of my finer work from my high school days. It has been edited and translated into English to broaden its potential audience. I would like to share it with other math enthusiasts who also see math as more art than science.

Some say math is useful because it helps drive progress. Others claim it is practical because it advances their careers. I, for my part, always saw math as more like a glass of beer: it brings enjoyment to the person consuming it, but does little for anyone else. I invite all mathematicians to keep indulging in math without fear or guilt, and I hope this book will add to their enjoyment.

For her help in putting this book together, I would specifically like to thank my former math teacher Rumiana Karadzhova. But more importantly, I owe a debt of gratitude to Mrs. Karadzhova for encouraging and inspiring me during the early stages of my mathematical journey. True learning can only come from within, through trying and failing, rather than through instruction alone. A real teacher does not merely instruct; a real teacher inspires the pupil to do their very best on their own. Mrs. Karadzhova is a real teacher.

Problem selection

Abstract

This is a collection of original math problems and their solutions. The problems have been grouped into the standard IMO categories of algebra, combinatorics, number theory, and geometry. Some of them have appeared in various competitions and magazines. An attempt has been made to order the problems by difficulty, but this is subjective.

1 Problem statements

1.1 Algebra

Problem A1. Let $n > 1$ and

$$0 = a_1 < a_2 < \ldots < a_n,$$

$$0 = b_n < b_{n-1} < \ldots < b_1.$$

We set

$$\alpha_i = \sqrt{1 - \sqrt{\frac{1}{1 + \left(\frac{a_i b_{i+1} - b_i a_{i+1}}{a_i a_{i+1} + b_i b_{i+1}}\right)^2}}}$$

for $i = 1, 2, \ldots, n-1$. Prove that

$$\sum_{i=1}^{n-1} \alpha_i < 1.111.$$

Problem A2. A sequence of pairs of real numbers $(a_1, b_1), (a_2, b_2), \ldots, (a_{2001}, b_{2001})$ is given such that

$$(a_1, b_1) = (0, 1)$$

and for each $n = 1, 2, \ldots, 2000$,

$$(a_{n+1}, b_{n+1}) \in \left\{(-a_n, b_n),\ \left(\frac{5}{4}a_n + \frac{3}{4}b_n,\ \frac{5}{4}b_n + \frac{3}{4}a_n\right)\right\}.$$

Prove that

$$(a_1 + b_1)(a_2 + b_2) \cdots (a_{2001} + b_{2001}) \geq 1.$$

Problem A3. Let A_0 be a finite set of rational numbers. We define the sequence of sets

$$A_{k+1} = \left\{ \frac{x+y}{1+xy} \mid x, y \in A_k,\ xy \neq -1 \right\}, \quad k = 0, 1, \ldots$$

Prove that there exists a *rational* number which does not belong to any of the sets A_k, for $k = 0, 1, \ldots$

Problem A4. The lateral surface of a cylinder whose circumference is the odd prime p and whose height is a positive integer k is divided into unit squares. In each square a real number is written. For every square, the sum of the numbers written in its left and right neighbors equals the sum of the numbers written in its vertical neighbors (above and below), whenever these neighbors exist. Moreover, at least one of the numbers is nonzero. Prove that $k \geq p - 1$.

Problem A5. A sequence of polynomials is defined in the following way:

$$p_0(x) = x,$$

$$p_n(x) = 1 + p_0(x)p_1(x)\cdots p_{n-1}(x), \qquad n = 1, 2, \ldots$$

Prove that for $n > 0$ the number of odd coefficients of $p_n(x)$ is one more than some integer power of the number 2.

Problem A6. Prove that the following holds for every positive integer n:

$$\left| \left\{ \frac{n}{1} \right\} - \left\{ \frac{n}{2} \right\} + \left\{ \frac{n}{3} \right\} - \cdots + (-1)^{n-1} \left\{ \frac{n}{n} \right\} \right| < \sqrt{2n}.$$

Problem A7. Prove that
a) there does not exist a function $f : \mathbb{R}^+ \times \mathbb{R}^+ \to \mathbb{R}$,
b) there exists a function $f : \mathbb{Q}^+ \times \mathbb{Q}^+ \to \mathbb{Q}$,
such that for all $a < b < c$ in the domain of f, we have:

$$f(a, c) < f(a, b) < f(b, c).$$

1.2 Combinatorics

Problem C1. Let A, B be lattice points with positive coordinates such that $OA = OB$. Prove that the circles with diameters OA and OB contain the same number of lattice points with positive coordinates.

Problem C2. Given is a sequence $a_1, a_2, \ldots, a_n$ of distinct real numbers, such that there does not exist a decreasing subsequence of length $k+1$. Prove that the number of pairs $\{i, j\}$ for which $i < j$ and $a_i > a_j$ does not exceed

$$\frac{k-1}{2k} n^2.$$

Problem C3. There is a 6×21 table (a_{ij}) with a total of 18 zeros, 18 ones, ..., 18 sixes. For any $k, l \in \{1, 2, \ldots, 6\}$ and $p, q \in \{1, 2, \ldots 21\}$ we have

$$a_{k,p} - a_{l,p} \equiv a_{k,q} - a_{l,q} (\pmod 7).$$

Prove that every row contains 3 zeros, 3 ones, ..., 3 sixes.

Problem C4. We are given n switches and n lamps. We know that each switch connects to exactly one lamp, but not which switch connects to which lamp. At each move, we are allowed to flip simultaneously any switches and observe which lamps change state. Find the minimum number $f(n)$ of moves that guarantees we can switch all lamps OFF regardless of their original ON/OFF state.

Problem C5. Let there be several distinct words of p ones and q zeros ($p > q$). Prove that we can pick a 1 from each word and replace it with 0 so that the obtained words of $p - 1$ ones and $q + 1$ zeros are again distinct.

Problem C6. For every integer x, a, b, we shall say that $x \in ((a, b))$ if $x \neq b$ and

$$(x - a)(x - b)(a - b) \geq 0.$$

A "nice" partition of $\{1, 2, \ldots, 2n\}$ into pairs $(a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n)$ shall be one for which

- (i) $\exists p, 1 \leq p \leq 2n : p \in ((a_i, b_i))$ for $i = 1, 2, \ldots, n$;
- (ii) $\exists q, 1 \leq q \leq 2n : q \notin ((a_i, b_i))$ for $i = 1, 2, \ldots, n$.

Prove that the number of nice partitions is $2n \times n!$.

Problem C7. A 2002×2002 square is divided into unit squares. A straight line may be drawn, and every unit square whose interior it intersects is colored. Prove that at least 1173 lines are required to color the whole square.

Problem C8. There are $2n$ cards arranged in a row. The numbers $1, 2, \ldots, 2n$ are written on the two sides of the cards, each number appearing exactly twice in total. Initially only one side of each card is visible.

A move consists of flipping one card. The goal is to reach a configuration in which all visible numbers are distinct.

(i) Prove that $3n - 2$ moves always suffice.

(ii) Prove that $3n - 3$ moves do not always suffice.

1.3 Number Theory

Problem N1. Let $p > 2$ be prime. There are p numbers written in a circle. At each move, simultaneously each number is replaced by the number plus its right neighbor minus twice its left neighbor. Prove that after $p - 1$ moves all numbers will give equal remainders upon division by p.

Problem N2. Let d be the smallest positive integer for which $n \mid 2^d + 1$. If $n > 6d$, prove that there are more than $6d$ positive integers m, $m \leq n$, such that for some $x, y, z \in \mathbb{N}$,

$$n \mid (2^x + 2^y + 2^z + m).$$

Problem N3. Let p be prime and $a \neq b$ be positive integers less than p. Prove that the equation

$$am + bn = p$$

has a solution in positive integers m, n if and only if the sets

$$A = \left\{ \left\lfloor \frac{ip}{a} \right\rfloor : i = 1, 2, \ldots, a-1 \right\}, \qquad B = \left\{ \left\lfloor \frac{ip}{b} \right\rfloor : i = 1, 2, \ldots, b-1 \right\}$$

have no common element.

Problem N4. For which positive integers n can the divisors of 2001^n be partitioned into triples such that the product of the numbers in each triple is the same?

Problem N5. Let $p > 2$ be prime, and let $\underline{x}$ denote the least non-negative residue of x modulo p. For $0 \leq a < p$ define

$$f_a(m) = m + \underline{ma}.$$

Determine the number of integers a with $0 \leq a < p$ such that

$$f_a(m) > a \quad \text{for all } m = 1, 2, \ldots, p-1.$$

Problem N6. Let p be a prime and consider a regular $2p$-gon. Let A and B be opposite vertices. Among the remaining vertices, $k < p$ are marked. Draw all segments joining pairs of marked vertices that intersect AB, and assume that at least one such segment exists. Prove that at least $k-1$ of these segments can be chosen so that no two are parallel or perpendicular.

1.4 Geometry

Problem G1. Let $ABCD$ be an isosceles trapezoid with $AB \parallel CD$. A point T is taken on AB such that $DP \cdot DT = CQ \cdot CT$, where $P = AC \cap TD$ and $Q = BD \cap TC$. Prove that the circumcenter of $\triangle TPQ$ is equidistant from A and B.

Problem G2. From the center of the circle k a perpendicular is dropped to the line l, intersecting k at the point D. Let P, Q be arbitrary points of l, and

$$P' = (PD) \cap k, \qquad Q' = (QD) \cap k, \qquad P, Q \neq D.$$

Prove that the center of the circumcircle of $\triangle P'Q'P$ lies on k exactly when

$$PQ = P'Q'.$$

Problem G3. The excircles constructed on the sides AB, BC, CA of $\triangle ABC$ touch the lines CA, CB, AB, AC, BC, BA respectively at the points C_1, C_2, A_1, A_2, B_1, B_2. Let

$$P_C = B_1B_2 \cap A_1A_2, \qquad P_A = B_1B_2 \cap C_1C_2, \qquad P_B = A_1A_2 \cap C_1C_2.$$

Prove that P_CC, P_AA, P_BB pass through the center of the circumcircle of $\triangle P_AP_BP_C$.

Problem G4. Let P be a point inside the acute triangle ABC. X is such a point that the quadrilateral $PBXC$ is inscribed in a circle and is with perpendicular diagonals. Similarly the points Y, Z are defined with respect to CA and AB. Prove that if $PB \perp XZ$ and $PA \perp YZ$, then P is the center of the circumcircle of $\triangle ABC$.

Problem G5. Let C_1, A_1, B_1 be the touchpoints on the incircle $\Gamma(I, r)$ with the sides AB, BC, CA of $\triangle ABC$ respectively. Also let $\angle A = 60^\circ$ and $A_2 = \Gamma \cap AA_1$, $A_2 \neq A_1$. If $I \in BC$ and A, A_2, I, T lie on a circle, find $\angle TA_1C_1$.

Problem G6. Given is $\triangle ABC$ with $\angle B = 60^\circ$. Let T be the point of tangency of the incircle of $\triangle ABC$ with AB, and C' be such that T is the midpoint of CC'. If the perpendicular bisector of BC' intersects the angle bisector of $\angle A$ at A', prove that $\triangle A'BC'$ is equilateral.

Problem G7. Let Γ be a set of points $A_1, A_2, \ldots, A_n$, $n > 2$, which is symmetric with respect to point O. If no three points of Γ are collinear and

$$OA_1 + OA_2 + \cdots + OA_n > 7,$$

prove that we can choose points $P, Q \in \Gamma$ such that the circumradius of $\triangle OPQ$ is larger than 1.

Problem G8. Let P and Q be points inside an acute triangle $\triangle ABC$ such that

$$\angle PCA = \angle PAB = \angle PBC, \qquad \angle QBA = \angle QCB = \angle QAC.$$

(a) Prove that the feet of the perpendiculars from P and Q to the sides of $\triangle ABC$ lie on a circle whose center is the midpoint of PQ.

(b) If O is the circumcenter of $\triangle ABC$, prove that $OP = OQ$.

2 Solutions

2.1 Algebra

Solution A1. From $a_i^2 + b_i^2 > 0$, without loss of generality we may replace (a_i, b_i) by

$$\left(\frac{a_i}{\sqrt{a_i^2+b_i^2}}, \frac{b_i}{\sqrt{a_i^2+b_i^2}}\right)$$

without changing the values of $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ as the expression inside the innermost brackets is homogeneous in a_i and b_i, hence we can scale the a_i and b_i by the same factor to get $a_i^2 + b_i^2 = 1$. Now, the expression for α_i simplifies to:

$$\begin{aligned}\alpha_i &= \sqrt{1 - \frac{a_i a_{i+1} + b_i b_{i+1}}{\sqrt{(a_i^2+b_i^2)(a_{i+1}^2+b_{i+1}^2)}}} = \sqrt{1-(a_i a_{i+1} + b_i b_{i+1})} \\ &= \frac{1}{\sqrt{2}}\sqrt{1 - 2a_i a_{i+1} - 2b_i b_{i+1}} = \frac{1}{\sqrt{2}}\sqrt{(a_i - a_{i+1})^2 + (b_i - b_{i+1})^2}.\end{aligned}$$

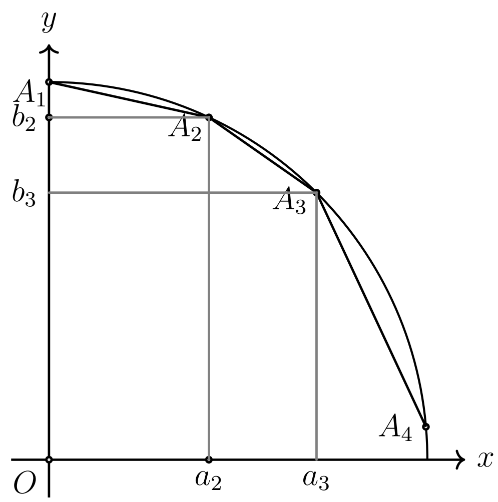
Consider a coordinate system and points with coordinates (a_i, b_i). They lie in the first quadrant of the circle $x^2 + y^2 = 1$. Since a_i increases and b_i decreases, the ratios a_i/b_i strictly increase, hence the angles $\angle A_i O x$ strictly decrease. Therefore the points are distinct and appear in clockwise order in the first quadrant, with A_1 lying exactly on the y-axis. Then

$$\sqrt{2}\sum_{i=1}^{n-1} \alpha_i$$

represents the length of the polygonal line $A_1 A_2 \cdots A_n$. Since each $|A_i A_{i+1}|$ is a chord in a circle and is strictly shorter than the arc $\overset{\frown}{A_i A_{i+1}}$, the length of this line is strictly shorter than the sum of the lengths of the arcs, which in turn is no greater than a quarter of the perimeter of the circle, namely $\pi/2$. It follows that

$$\sum_{i=1}^{n-1} \alpha_i < \frac{1}{\sqrt{2}} \cdot \frac{\pi}{2} = 1.1107 < 1.111.$$

Notice that the bound is quite sharp. $\square$



Solution A2. Let $\varepsilon = \ln 2$, so that $\sinh(\varepsilon) = 3/4$ and $\cosh(\varepsilon) = 5/4$. We claim that the representation

$$(a_n, b_n) = (\sinh(\alpha_n), \cosh(\alpha_n)) \tag{*}$$

holds for $\alpha_1 = 0$. Next, for $n \geq 1$, either

$$(a_{n+1}, b_{n+1}) = (-a_n, b_n) = (\sinh(-\alpha_n), \cosh(\alpha_n))$$

or

$$\begin{aligned}
(a_{n+1}, b_{n+1}) &= \left(\frac{5}{4}a_n + \frac{3}{4}b_n, \frac{5}{4}b_n + \frac{3}{4}a_n\right) \\
&= (\cosh\varepsilon \sinh\alpha_n + \sinh\varepsilon \cosh\alpha_n, \cosh\varepsilon \cosh\alpha_n + \sinh\varepsilon \sinh\alpha_n) \\
&= (\sinh(\alpha_n + \varepsilon), \cosh(\alpha_n + \varepsilon)).
\end{aligned}$$

Therefore, the identity (*) remains valid for all n where

$$\alpha_{n+1} = -\alpha_n \quad \text{or} \quad \alpha_{n+1} = \alpha_n + \varepsilon.$$

We shall prove the following

Lemma.

$$\alpha_1 + \alpha_2 + \ldots + \alpha_n \geq 0 \quad \text{for } n \geq 1.$$

Proof. Let us encode the given sequence satisfying the above properties by means of a symbolic string of x and y (whose length is one less than the length of the sequence), corresponding to the case $\alpha_{n+1} = -\alpha_n$ or $\alpha_{n+1} = \alpha_n + \varepsilon$. For example, for the sequence

$$0, \varepsilon, 2\varepsilon, -2\varepsilon, -\varepsilon, \varepsilon$$

the symbolic string representation is $yyxyx$. For completeness, let the empty string correspond to the single-term sequence α_1. For every such string A we define by $s(A)$ the sum of the members of the sequence. We shall make the following observations:

- Observation 1. For every symbolic sequence A,

  $$s(A) = s(Axx) = s(Ayx),$$

  because if α is the last term of the sequence encoded by A, the only difference with Axx is the last two terms $(-\alpha), \alpha$, and the only difference with Ayx is the last two terms $\alpha + \varepsilon, -(\alpha + \varepsilon)$. In both cases the terms sum to 0.

- Observation 2. A leading x replaces $\alpha_1 = 0$ with the pair $(0, 0)$. Therefore any number of leading x's simply inserts zeros into the sequence and does not change the sum, hence

  $$s(xA) = s(A).$$

- Observation 3. If α is the last term of the sequence encoded by A, the only difference between $AyxyB$ and AxB is the two terms following A, namely $\alpha + \varepsilon, -(\alpha + \varepsilon)$, after which point the two sequences continue with $-\alpha$ the same way. Therefore

  $$s(AyxyB) = s(AxB).$$

To prove that there is no sequence with negative sum, assume the contrary, and let's pick the shortest such symbolic string. We can assume it has more than 1 symbols, as the cases for 0 and 1 can easily be examined: the empty string gives rise to 0, and the one-symbol string sequences x and y give sums 0 and ε respectively. In any of these cases, the sums are non-negative. So the shortest sequence must have more than 1 symbols.

By the symbolic analogue of this sequence, the string does not begin with x (due to observation 2), as it could otherwise be reduced to a shorter one that still has negative sum. Furthermore, it does not end with x either due to observation 1, as we could otherwise chop the last two symbols regardless if they are xx or yx. Then it must begin and end with y, and according to observation 3, it must not contain x, else it would be reducible to a shorter one. So the string contains only y, and hence its corresponding α sequence is

$$0, \varepsilon, 2\varepsilon, \ldots, k\varepsilon$$

which has nonnegative sum – a contradiction. Thus the lemma is proved and so

$$\prod_{i=1}^{2001}(a_i + b_i) = \prod_{i=1}^{2001}(\sinh(\alpha_i) + \cosh(\alpha_i)) = \prod_{i=1}^{2001} e^{\alpha_i} = e^{\sum_{i=1}^{2001} \alpha_i} \geq 1.$$

Solution A3. If 1 is not in A_0, then it is not in any of the subsequent sets since

$$\frac{x+y}{1+xy} = 1 \Rightarrow x = 1 \text{ or } y = 1.$$

In such a case, 1 would be the rational number we are looking for. So from now on, we assume that $1 \in A_0$. Let

$$A_0 = \{1, a_1, a_2, \ldots, a_n\},$$

where $a_i \neq 1$. We define

$$v_k = \frac{1+a_k}{1-a_k}.$$

We shall prove by induction on k that every element $x \in A_k$, $x \neq 1$ is representable as

$$f(v_1^{\alpha_1} v_2^{\alpha_2} \ldots v_n^{\alpha_n}), \alpha_i \in \mathbb{N}_0,$$

where

$$f(x) = \frac{x-1}{x+1}.$$

Indeed:

$$f(v_k) = \frac{\frac{1+a_k}{1-a_k} - 1}{\frac{1+a_k}{1-a_k} + 1} = \frac{2a_k}{2} = a_k,$$

so the statement is true for all elements in A_0.
Next, observe that

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

So for every two elements x and y in A_k with $xy \neq 1$, the induction provides representations $f(v_1^{\alpha_1} v_2^{\alpha_2} \ldots v_n^{\alpha_n})$ and $f(v_1^{\beta_1} v_2^{\beta_2} \ldots v_n^{\beta_n})$, so we have

$$\frac{x+y}{1+xy} = f(v_1^{\alpha_1+\beta_1} v_2^{\alpha_2+\beta_2} \ldots v_n^{\alpha_n+\beta_n}).$$

That means all elements in A_{k+1} are representable in the desired form, which completes the induction. Thus

$$A_k \subseteq A \cup \{1\} \quad \text{for } k \geq 0, \tag{*}$$

where

$$A = \{f\left(v_1^{\alpha_1} v_2^{\alpha_2} \dots v_n^{\alpha_n}\right) \mid \alpha_i \in \mathbb{N}_0, \qquad i = 1, 2, \dots, n\}.$$

Let p be a prime number, greater than any prime number in the prime factorization of the numerators and denominators of the rational numbers v_i, $i = 1, 2, \dots, n$. Such a prime p exists since there are finitely many v_i, and it has no representation of the form

$$p = v_1^{\alpha_1} v_2^{\alpha_2} \dots v_n^{\alpha_n},$$

since none of the factorizations of the numerators and denominators of v_i contain the prime p. Furthermore, notice that $f(x)$ is a bijection

$$f : \mathbb{R} \setminus \{-1\} \to \mathbb{R} \setminus \{1\},$$

as it is defined for every real number different from -1, and for every number $y \neq 1$ there is a unique solution $x = (1 + y)/(1 - y)$ to $f(x) = y$. Since p cannot be expressed as $v_1^{\alpha_1} \cdots v_n^{\alpha_n}$, from the bijection we get that $f(p) \notin A$, and since $f(p) \neq 1$, it means the rational number $f(p)$ is not in any A_k, which completes the proof. $\square$

Solution A4. Let us choose one column and consider the rows as p–dimensional vectors whose first coordinate lies in the chosen column. Let us index the vectors as $a_1, a_2, \dots, a_k$. We also define $a_0 = a_{k+1} = \vec{0}$ for completeness. Let C be the cyclic $p \times p$ shift matrix that has ones on the first upper diagonal with its wraparound entry and zeros everywhere else, i.e. $C_{ij} = 1$ for $(i, j) = (1, 2), (2, 3), \dots, (p - 1, p), (p, 1)$. It is easy to see that C^m is the matrix with ones on the m–th upper cyclic diagonal. Hence $C^p = I$ (the identity matrix), so $C^{p-1} = C^{-1}$. The condition of the problem translates into the following relation for the vectors a_i:

$$a_{i-1} + a_{i+1} = (C + C^{-1})a_i, \qquad i = 1, 2, \dots, k - 1. \tag{*}$$

For the last k-th vector we have

$$a_{k-1} = (C + C^{-1})a_k,$$

and since we defined $a_{k+1} = \vec{0}$, the expression (*) can be extended to $i = k$. Then from (*) we have

$$\begin{aligned} a_{i+1} - Ca_i &= C^{-1}(a_i - Ca_{i-1}) \\ &= C^{-2}(a_{i-1} - Ca_{i-2}) \\ &\dots \\ &= C^{-i}(a_1 - Ca_0) = C^{-i}a_1. \end{aligned}$$

Hence by induction

$$a_{i+1} = (C^i + C^{i-2} + \dots + C^{-(i-2)} + C^{-i})a_1, \qquad i = 1, 2, \dots k.$$

Clearly $a_1 \neq \vec{0}$, otherwise the recurrence would imply $a_i = \vec{0}$ for all i, which would contradict the condition. Applying the above to $i = k$ and using $a_{k+1} = \vec{0}$, we get $Ba_1 = \vec{0}$, where

$$B = C^k + C^{k-2} + \cdots + C^{-k+2} + C^{-k}.$$

Now, using $Ba_1 = \vec{0}$ we get

$$\vec{0} = CBa_1 = (CB + B)a_1 = (C^{k+1} + C^k + \cdots + C^{-k+1} + C^{-k})a_1.$$

Multiplying both sides by C^k we get

$$Ta_1 = \vec{0},$$

where $T = C^0 + C^1 + \cdots + C^{2k+1}$.

If we suppose that $k < p - 1$, since p is odd, we have $(2k + 2, p) = 1$, so there exist positive integers m and r such that $m(2k + 2) = rp + 1$. From $Ta_1 = \vec{0}$ and $C^p = I$ we have

$$\begin{aligned}
\vec{0} = Ta_1 &= (I + C^{2k+2} + C^{2(2k+2)} + \cdots + C^{(m-1)(2k+2)})Ta_1 \\
&= (T + C^{2k+2}T + \cdots + C^{(m-1)(2k+2)}T)a_1 \\
&= (I + C + C^2 + \cdots + C^{rp})a_1 \\
&= rpDa_1 + Ia_1,
\end{aligned}$$

where D is the matrix with only 1 in all its entries. Let $a_1 = (x_1, x_2, \ldots, x_p)$. Then

$$rp(x_1 + x_2 + \cdots + x_p) + x_i = 0, \qquad i = 1, 2, \ldots, p.$$

Therefore

$$rp \sum_{j=1}^{p} x_j + x_i = 0 = rp \sum_{j=1}^{p} x_j + x_1$$

for all i, which means $x_i = x_1$ for all i. Now we have

$$\begin{aligned}
0 = rp \sum_{j=1}^{p} x_j + x_1 &= rp \sum_{j=1}^{p} x_1 + x_1 \\
&= rp^2 x_1 + x_1 = (rp^2 + 1)x_1.
\end{aligned}$$

Therefore $x_1 = 0$ and so $x_i = x_1 = 0$ for $i = 1, 2, \ldots, p$, implying that $a_1 = \vec{0}$, which is a contradiction. Thus $k \geq p - 1$. □

Solution A5. We have

$$p_1(x) = 1 + x$$

and

$$p_n(x) = 1 + (p_{n-1}(x) - 1)p_{n-1}(x) = p_{n-1}(x)^2 - p_{n-1}(x) + 1.$$

From now on, we work modulo 2. First, notice that for every polynomial $q(x)$ we have

$$\begin{aligned}
q(x)^2 &= (a_0 + a_1 x + \cdots + a_n x^n)^2 \\
&= a_0^2 + a_1^2 x^2 + \cdots + a_n^2 x^{2n} + 2 \sum_{i \neq j} a_i a_j x^{i+j} \\
&= a_0 + a_1 x^2 + \cdots + a_n x^{2n} = q(x^2).
\end{aligned}$$

Therefore, from the recursive relation for p_n, we have

$$p_n(x) = p_{n-1}(x)^2 - p_{n-1}(x) + 1 = p_{n-1}(x^2) + p_{n-1}(x) + 1. \tag{*}$$

By induction, it is seen that the degree of $p_n(x)$ is exactly 2^{n-1}, that it always has a constant term 1, and that besides x^0 it has nonzero coefficients only in front of x^{2^i} for some $i \geq 0$. Let the coefficient in front of x^{2^i} be $a_i^{(n)}$ for $i = 0, 1, \ldots, n-1$, i.e.

$$p_n(x) = 1 + a_0^{(n)} x^{2^0} + a_1^{(n)} x^{2^1} + a_2^{(n)} x^{2^2} + \cdots + a_{n-1}^{(n)} x^{2^{n-1}}.$$

From (*), we know that:

- the coefficient in front of $x = x^{2^0}$ in $p_n(x)$ is only contributed by $p_{n-1}(x)$, so $a_0^{(n)} = a_0^{(n-1)}$;
- the coefficient in front of $x^{2^{n-1}}$ in $p_n(x)$ is only contributed by $p_{n-1}(x^2)$, so $a_{n-1}^{(n)} = a_{n-2}^{(n-1)}$;
- for $1 \leq i \leq n-2$, the coefficient in front of x^{2^i} in $p_n(x)$ is the sum of $a_{i-1}^{(n-1)}$, owing to $p_{n-1}(x^2)$, and $a_i^{(n-1)}$, owing to $p_{n-1}(x)$, so $a_i^{(n)} = a_{i-1}^{(n-1)} + a_i^{(n-1)}$.

But that is the exact recurrence relation that the binomial coefficients satisfy, namely

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Therefore, by induction, we get

$$a_i^{(n)} = \binom{n-1}{i}.$$

Thus the number of odd coefficients of $p_n(x)$ is 1 plus the number of odd binomial coefficients of order $n-1$. But from Lucas' theorem, $\binom{n-1}{i}$ is odd exactly when every digit in the binary representation of $n-1$ is at least the corresponding digit in the binary representation of i. That means $a_i^{(n)} \neq 0$ for precisely those i that have 0 wherever $n-1$ has 0 and 0 or 1 whenever $n-1$ has 1. The number of such i is thus

$$2^{S(n-1)},$$

where $S(n-1)$ is the number of 1s in the binary representation of $n-1$. That completes the proof. $\square$

Solution A6. For $n = 1, 2, 3, 4$ we verify directly, so we can assume $n > 4$. Let us take an integer $k \in [\sqrt{n}, n]$. We know that $k > 2$. We shall split the sum in two parts and bound each part separately:

$$A_k = \left\{\frac{n}{1}\right\} - \left\{\frac{n}{2}\right\} + \left\{\frac{n}{3}\right\} - \cdots + (-1)^k \left\{\frac{n}{k-1}\right\}$$

and

$$B_k = \left\{\frac{n}{k}\right\} - \left\{\frac{n}{k+1}\right\} + \left\{\frac{n}{k+2}\right\} - \cdots + (-1)^{n-k} \left\{\frac{n}{n}\right\} = C_k - D_k,$$

where

$$C_k = \left(\frac{n}{k} - \frac{n}{k+1} + \cdots + (-1)^{n-k}\frac{n}{n}\right),$$

$$D_k = \left(\left\lfloor\frac{n}{k}\right\rfloor - \left\lfloor\frac{n}{k+1}\right\rfloor + \cdots + (-1)^{n-k}\left\lfloor\frac{n}{n}\right\rfloor\right).$$

With respect to C_k we have:

$$C_k = \frac{n}{k} - \left(\frac{n}{k+1} - \frac{n}{k+2}\right) - \cdots \leq \frac{n}{k},$$

since all the terms in the brackets are positive (no matter whether the last bracket contains one or two terms). Furthermore, equality holds only when $k = n$, when the bracketed terms are missing.

Furthermore,

$$C_k = \left(\frac{n}{k} - \frac{n}{k+1}\right) + \left(\frac{n}{k+2} - \frac{n}{k+3}\right) + \cdots > 0,$$

so we conclude $0 < C_k \leq \frac{n}{k}$.

For D_k we have

$$D_k = \left(\left\lfloor\frac{n}{k}\right\rfloor - \left\lfloor\frac{n}{k+1}\right\rfloor\right) + \left(\left\lfloor\frac{n}{k+2}\right\rfloor - \left\lfloor\frac{n}{k+3}\right\rfloor\right) + \cdots$$

For $k \geq \sqrt{n}$ and for $i = 0, 1, \ldots$ we have

$$\frac{n}{k+2i} - \frac{n}{k+2i+1} < \frac{n}{k(k+1)} < 1,$$

and so

$$\left\lfloor\frac{n}{k+2i}\right\rfloor - \left\lfloor\frac{n}{k+2i+1}\right\rfloor \in \{0, 1\}.$$

Notice that among the inequalities

$$\left\lfloor\frac{n}{k+i}\right\rfloor - \left\lfloor\frac{n}{k+i+1}\right\rfloor \leq 1$$

exactly $\left\lfloor\frac{n}{k}\right\rfloor - 1$ are strict, since the telescopic sum of all those terms for $i = 0, 1, \ldots n - k - 1$ is exactly

$$\left\lfloor\frac{n}{k+0}\right\rfloor - \left\lfloor\frac{n}{n}\right\rfloor = \left\lfloor\frac{n}{k}\right\rfloor - 1.$$

Then at most $\left\lfloor\frac{n}{k}\right\rfloor - 1$ of the inequalities

$$\left\lfloor\frac{n}{k+2i}\right\rfloor - \left\lfloor\frac{n}{k+2i+1}\right\rfloor \leq 1$$

are strict too (the even indices being a subset of all), and therefore

$$0 \leq D_k \leq \left\lfloor\frac{n}{k}\right\rfloor - 1 < \frac{n}{k},$$

where $D_k = 0$ is not possible for $k = n$, because then $D_k = 1$. Finally

$$|B_k| = |C_k - D_k| < \frac{n}{k}$$

and therefore the inequality is strict.

For A_k we have

$$-\left\{\frac{n}{2}\right\} - \left\{\frac{n}{4}\right\} - \cdots \le A_k \le \left\{\frac{n}{3}\right\} + \left\{\frac{n}{5}\right\} + \cdots$$

From

$$0 \le \left\{\frac{n}{i}\right\} \le \frac{i-1}{i} \le \frac{k-2}{k-1}$$

it follows

$$|A_k| \le \left\lceil \frac{k-2}{2} \right\rceil \frac{k-2}{k-1} \le \left(\frac{k-2}{2} + \frac{1}{2}\right) \frac{k-2}{k-1} = \frac{k-2}{2}.$$

Since the sum in the statement is equal to $A_k + (-1)^{k+1} B_k$ and

$$|A_k \pm B_k| \le |A_k| + |B_k| < \frac{k-2}{2} + \frac{n}{k},$$

to complete the proof we need to find some $k \in [\sqrt{n}, n]$ such that:

$$\frac{k-2}{2} + \frac{n}{k} \le \sqrt{2n}.$$

That last inequality is equivalent to

$$k^2 - (2 + \sqrt{8n})k + 2n \le 0,$$

and so k must lie between the roots of the quadratic equation, i.e. it must satisfy

$$k \in [\gamma - \delta, \gamma + \delta],$$

where $\gamma = \sqrt{2n} + 1$ and $\delta = \sqrt{\sqrt{8n} + 1}$.

We shall show that the choice of $k = \lceil \sqrt{2n} \rceil$ satisfies both requirements. First, $k < 1 + \sqrt{2n} = \gamma < \gamma + \delta$. Next, $k \ge \sqrt{2n} = \gamma - 1 > \gamma - \delta$, since $\delta > 1$. That gives us $k \in [\gamma - \delta, \gamma + \delta]$. That $k > \sqrt{n}$ follows directly from $k \ge \sqrt{2n} > \sqrt{n}$. And finally, since $k < \gamma$, to prove $k \le n$, it suffices to show that $\gamma < n$. But

$$\gamma < n \leftrightarrow 2n < (n-1)^2 \leftrightarrow 0 < n(n-4) + 1,$$

which is true for $n \ge 4$. Therefore $k \in [\sqrt{n},\, n]$ and all requirements are satisfied. $\square$

Solution A7. We proceed in order.

Proof a) Suppose that such a function exists. For every positive real number x, using $a = x, b = 2x, c = 3x$, we get

$$f(x, 3x) < f(x, 2x).$$

For every x, consider the interval $\Delta(x) = (f(x, 3x), f(x, 2x))$. We shall see that these intervals are pairwise disjoint. Let us take any $x < y$ and examine the three possibilities:

- Case 1. $y > 2x$. We have $x < 2x < y < 3y$. Taking $a = x, b = 2x, c = 3y$, we obtain $f(x, 2x) < f(2x, 3y)$; and taking $a = 2x, b = y, c = 3y$, we obtain $f(2x, 3y) < f(y, 3y)$. Combining the two inequalities gives $f(x, 2x) < f(2x, 3y) < f(y, 3y)$.

- Case 2. $y = 2x$. As in the previous case, we take $a = x, b = 2x, c = 3y$ to obtain $f(x, 2x) < f(2x, 3y)$, but this time $f(2x, 3y) = f(y, 3y)$, so now $f(x, 2x) < f(2x, 3y) = f(y, 3y)$.

- Case 3. $y < 2x$. We have $x < y < 2x < 3y$. Taking $a = x, b = y, c = 2x$, we obtain $f(x, 2x) < f(x, y)$; and taking $a = x, b = y, c = 3y$, we obtain $f(x, y) < f(y, 3y)$. Combining the two inequalities gives $f(x, 2x) < f(x, y) < f(y, 3y)$.

In all examined cases, we have $f(x, 2x) < f(y, 3y)$, and so the intervals $\Delta(x)$ and $\Delta(y)$ do not intersect. But each interval $\Delta(x)$ contains infinitely many rational numbers. Choose a rational number from each interval and denote it by $q(x)$. Since the intervals are pairwise disjoint, all $q(x)$ are different, which means q is an injection from $\mathbb{R}^+ \to \mathbb{Q}$. But, as is well known, this is impossible. Consequently, a function with the sought properties does not exist.

Proof b) Notice that it does not matter how we define $f(x, y)$ for $x \geq y$. Our goal is to construct a function f such that: (a) $f(a, x)$ is decreasing in x for every fixed a and all $x > a$; and (b), the image $F_a = \{f(a, x) : x > a\}$ is to the left of the image $F_b = \{f(b, x) : x > b\}$ for every $a < b$. The second condition is the hard one, and it requires us to do in $\mathbb{Q}$ what we could not do in $\mathbb{R}$ earlier, namely to construct a set of non-overlapping intervals where between every two intervals from the set there is a third one from the same set.

Part 1: Constructing the intervals. Consider all sequences $p_1, p_2, \ldots, p_{n-1}$ where $p_i \in \{0, 2\}$, and for each such sequence define l and r as follows:

$$l = (0.p_1 p_2 \cdots p_{n-1} 1)_3; \qquad r = (0.p_1 p_2 \cdots p_{n-1} 2)_3,$$

where the subscript 3 denotes *ternary representation*. In other words,

$$l = \sum_{i=1}^{n-1} \frac{p_i}{3^i} + \frac{1}{3^n}, \qquad r = \sum_{i=1}^{n-1} \frac{p_i}{3^i} + \frac{2}{3^n}.$$

Let C be the set of all intervals (l, r) for l and r defined in the above fashion. We shall show that between every two intervals in C there exists a third interval from C; therefore the intervals in C must be disjoint.

Let us take two different intervals (l_1, r_1) and (l_2, r_2). Clearly $r_1 \neq r_2$, else we would have $l_1 = l_2$ and the intervals would be the same. Without loss of generality, assume

$r_1 < r_2$. Then their ternary representations must differ in some digit, where the digit of r_2 is larger, and this digit cannot be the last one (as it is always 2). If r_2 is written with n symbols, then

$$r_2 - r_1 > \frac{2}{3^{n-1}} - (\frac{2}{3^n} + \frac{2}{3^{n+1}} + \cdots) = \frac{1}{3^{n-1}}.$$

Let

$$r_3 = r_2 - \frac{2}{3^n} + \frac{2}{3^{n+1}}, \qquad l_3 = r_2 - \frac{2}{3^n} + \frac{1}{3^{n+1}}.$$

Clearly (l_3, r_3) is from C, as the ternary representations of l_3 and r_3 are identical up to the last digit, which is 1 for l_3 and 2 for r_3. Therefore,

$$r_2 > l_2 = r_2 - \frac{1}{3^n} > r_3 > l_3 > r_2 - \frac{1}{3^{n-1}} > r_1 > l_1,$$

which shows that (l_3, r_3) sits between (l_1, r_1) and (l_2, r_2).

Furthermore, for every interval I in C, we could choose a sufficiently large n so that the following two intervals (also in C) sit to the left and right of I:

$$\left(\frac{1}{3^n}, \frac{2}{3^n}\right) \text{ and } \left(1 - \frac{2}{3^n}, 1 - \frac{1}{3^n}\right).$$

Now we define a map $\Delta : \mathbb{Q}^+ \to C$. Let us list the positive rational numbers as a sequence: $q_1, q_2, \ldots$ and define their corresponding intervals $\Delta(q_i)$ sequentially. First, we assign to q_1 an arbitrary interval $\Delta(q_1)$ from C. Thereafter, for every $m > 1$, we assign $\Delta(q_m) \in C$ as follows:

- if q_m is larger than all previously listed numbers, we choose an interval from C that is to the right of all intervals $\Delta(q_i)$ and assign it to q_m.
- if q_m is smaller than all previously listed numbers, we choose an interval from C that is to the left of all intervals $\Delta(q_i)$ and assign it to q_m.
- if q_m is neither the smallest nor the largest among the previously listed numbers, let $q_i < q_m < q_j$ be the two numbers among them immediately adjacent to q_m. In that case, we pick an interval from C that lies between $\Delta(q_i)$ and $\Delta(q_j)$ and assign it to q_m.

Part 2: Construction of f. Now that our map Δ is defined, we construct f as follows. For every $a \in \mathbb{Q}^+$ we take our $\Delta(a) = (l_a, r_a)$ and define $f(a, x)$ as follows:

$$f(a,x) = \begin{cases} 1983 & \text{if } x \le a \\ l_a + \frac{r_a - l_a}{x+1} & \text{if } x > a \end{cases}$$

Thus the function f is well defined for all $(a, x) \in \mathbb{Q}^+ \times \mathbb{Q}^+$ and its values lie in $\mathbb{Q}$, since l_a, r_a, x are positive rational numbers. We shall show that it satisfies the condition.

Let $a < b < c$ be any positive rational numbers. Since $f(a, x)$ is a decreasing function on $x > a$, we have $f(a, c) < f(a, b)$, so the first inequality is satisfied.

Next, notice that for all $x > a$, $l_a < f(a, x) < r_a$, so $f(a, x) \in \Delta(a)$, in particular $f(a, b) \in \Delta(a)$. Likewise, $f(b, c) \in \Delta(b)$. But since $a < b$, from the construction of the map Δ, we know that $\Delta(a)$ sits entirely to the left of $\Delta(b)$. Therefore $f(a, b) < f(b, c)$. The second inequality is also satisfied, and our construction is complete. □

2.2 Combinatorics

Solution C1. Let $A = (m, n)$ and $B = (a, b)$ and the two circles be k_1 and k_2 respectively. The condition $(x, y) \in k_1$ is equivalent to

$$x^2 + y^2 + (m-x)^2 + (n-y)^2 = m^2 + n^2$$
$$\iff (2x-m)^2 + (2y-n)^2 = m^2 + n^2.$$

Since

$$a^2 + b^2 = OB^2 = OA^2 = m^2 + n^2,$$

either (a) $m \equiv a,\ n \equiv b \pmod 2$ or (b) $m \equiv b,\ n \equiv a \pmod 2$. Indeed, if OA^2 is odd, then (a, b) and (m, n) are pairs of numbers of different parity, and if OA^2 is even, then a, b, m, n are of the same parity.

In the case (a) there is a bijection between the lattice points on the two circles:

$$f : \{(x, y) \mid (x, y) \in k_1\} \to \{(x', y') \mid (x', y') \in k_2\},$$

given by

$$f(x, y) = \left(x + \frac{a-m}{2},\ y + \frac{b-n}{2}\right).$$

Similarly, in case (b), we can define the bijection as follows:

$$f(x, y) = \left(y + \frac{a-n}{2},\ x + \frac{b-m}{2}\right).$$

Thus we proved that k_1 and k_2 have the same number N of integer points.

Let us take the positive integer points (x, y), $x, y > 0$, of k_1. We have

$$x^2 + y^2 = mx + ny.$$

If $x > m$, then

$$0 < (x-m)x = y(n-y) \Rightarrow y < n \quad \text{(type 1)}.$$

If $x < m$, then

$$y(y-n) = x(m-x) > 0 \Rightarrow y > n \quad \text{(type 2)}.$$

If $x = m$, then

$$y = n \quad \text{(type 3)}.$$

Clearly there are no points on k_1 with both negative coordinates, owing to $x^2 + y^2 = mx + ny$. The number of points $(u, v) \in k_1$ with positive u and negative v equals the number of positive points of type 2, since there is a bijection between the two sets given by $(u, v) \leftrightarrow (x, n - v)$. Likewise, the points $(u, v) \in k_1$ with positive v and negative u correspond to the positive points of type 1, as demonstrated by the bijection $(u, v) \leftrightarrow (m - x, y)$.

Including the points $(u, v) \in k_1$ with $uv = 0$, namely $(0, 0)$, $(m, 0)$, $(0, n)$, and the one point of type 3, we have:

$$N = 2(\#\text{type } 1) + 2(\#\text{type } 2) + 3 + 1.$$

Hence the number of positive points is

$$(\#\text{type } 1) + (\#\text{type } 2) + 1 = \frac{N-4}{2} + 1 = \frac{N}{2} - 1.$$

The same holds for the second circle, which completes the proof.

Geometrically the correspondence between the circles is a translation in case (a) and a reflection across the line $x = y$ followed by a translation in case (b). $\square$

Solution C2. A pair (i, j) with $i < j$ and $a_i > a_j$ is called an *inversion*. For every $i = 1, 2, \ldots, n$, define $r(i)$ as the maximal possible number r for which there exists a sequence

$$i_1 < i_2 < \ldots < i_{r-1} < i, \qquad a_{i_1} > a_{i_2} > \ldots > a_{i_{r-1}} > a_i.$$

From the condition we have $r(i) \leq k$. Let us take an arbitrary inversion (i, j) and let $r = r(j)$. We have

$$i_1 < i_2 < \ldots < i_{r-1} < j, \qquad a_{i_1} > a_{i_2} > \ldots > a_{i_{r-1}} > a_j,$$

which implies that $r(i) < r(j)$. Let us divide the indices into k sets $A(1), A(2), \ldots, A(k)$, where $i \in A(r(i))$. We have

$$|A(1)| + |A(2)| + \ldots + |A(k)| = n,$$

and for every two elements i and j from one and the same set $A(r)$ the pair (i, j) is not an inversion. Therefore the number of all pairs which are not inversions is at least

$$\binom{|A(1)|}{2} + \binom{|A(2)|}{2} + \cdots + \binom{|A(k)|}{2}.$$

Hence the number of inversions does not exceed

$$\binom{n}{2} - \left(\binom{|A(1)|}{2} + \binom{|A(2)|}{2} + \ldots + \binom{|A(k)|}{2}\right).$$

Finally, from the inequality of Cauchy, we obtain:

$$\binom{n}{2} - \sum_{r=1}^{k} \binom{|A(r)|}{2} \leq \frac{n(n-1) - \sum_{r=1}^{k} |A(r)|^2 + \sum_{r=1}^{k} |A(r)|}{2}$$
$$\leq \frac{n^2 - \frac{n^2}{k}}{2} = \frac{k-1}{2k} n^2.$$

Solution C3. Let us construct a new table (b_{ij}), where

$$b_{ij} = \omega^{a_{ij}}, \qquad \omega = \cos\frac{2\pi}{7} + i \sin\frac{2\pi}{7}.$$

Let the sum of the numbers in the k-th row be s_k, $k = 1, 2, \ldots, 6$. From the condition we have

$$a_{k,p} - a_{1,p} \equiv a_{k,1} - a_{1,1} \equiv m_k(\pmod 7)$$

for some integer m_k with $0 \leq m_k \leq 6$ and all $p = 1, 2, \ldots, 21$, and hence

$$s_k = s_1 \omega^{m_k}.$$

Let

$$q(x) = 1 + x + \ldots + x^6.$$

Since each of the numbers $0, 1, \ldots, 6$ appears 18 times in the entire table, summing over all rows we get

$$s_1(\omega^0 + \omega^1 + \ldots + \omega^6) = \sum_{k=1}^{6} s_k = 18q(\omega) = 0.$$

Let

$$p(x) = x^{m_1} + x^{m_2} + \ldots + x^{m_6}$$

and

$$s(x) = \sum_{i=1}^{21} x^{a_{1i}},$$

so

$$s(\omega) = s_1.$$

Thus

$$s(\omega)p(\omega) = 0,$$

i.e. ω is a root of either $s(x)$ or $p(x)$.

Now we use the well-known fact that the polynomial $q(x)$ is the 7th cyclotomic polynomial and is irreducible over $\mathbb{Q}$.

If we assume that $p(\omega) = 0 = q(\omega)$, then from the irreducibility of $q(x)$ it follows that $q(x)$ divides $p(x)$. From $\deg p(x) \leq 6 = \deg q(x)$ it follows that $p(x) = kq(x)$ for some integer k. But then

$$7k = q(1)k = p(1) = 6,$$

which is impossible. Consequently $p(\omega) \neq 0$ and so it must be the case that $s(\omega) = 0$.

Since $s(\omega) = 0$ and $q(x)$ is the minimal polynomial of ω over $\mathbb{Q}$, it follows that $q(x)|s(x)$, and since $\deg s \leq 6 = \deg q$, we must have

$$s(x) = kq(x)$$

for some integer k. Evaluating at $x = 1$, we obtain

$$21 = s(1) = kq(1) = 7k,$$

i.e. $k = 3$ and therefore

$$s(x) = 3 + 3x + 3x^2 + 3x^3 + 3x^4 + 3x^5 + 3x^6.$$

This proves that in the first row of the table there are 3 zeros, 3 ones, etc.. The same holds for the remaining rows, which completes the proof. $\square$

Solution C4. The general idea is to show that after each move, there is always the possibility that at least half of the work remains undone, with slightly more ON lamps than OFF lamps remaining until the end, when we will need one extra move to turn off the last lamp.

Let $t_c = \lceil \log_2 n \rceil$. Suppose that at the start exactly $\lceil n/2 \rceil$ (half or slightly more when n is odd) of the lamps are ON. We shall prove the following lemma:

Lemma. After any $0 \leq t \leq t_c$ moves, regardless of how we play, it may still be possible that there exist sets L_t of lamps and S_t of switches such that:

1. $|S_t| \geq |L_t| = n_t \geq \lceil n/2^t \rceil \geq 1$;
2. on every move, either all switches in S_t were flipped together or none were flipped; and
3. $k_t = \lceil n_t/2 \rceil \geq 1$ of the n_t lamps in L_t are ON.

Proof. For $t = 0$, all requirements are true with S_0 and L_0 consisting of all switches and all lamps respectively. By induction on t, consider $1 \le t \le t_c$. We have $|L_{t-1}| = n_{t-1} \ge 2$. Suppose after our t-th move we observe exactly m of the lamps in L_{t-1} change state. Consider two cases:

Case 1. $m < k_{t-1}$, so less than half of the lamps in L_{t-1} changed state. Let $L_t \subseteq L_{t-1}$ be the set of $n_t = n_{t-1} - m$ lamps that *did not change state*, and let $S_t \subseteq S_{t-1}$ be the switches we did not flip. Each lamp in L_t must necessarily connect to a switch in S_t, so $|S_t| \ge |L_t| = n_t$. Since $n_t \ge n_{t-1}/2 \ge n/2^t$, requirement 1 is satisfied. Furthermore, none of the switches in S_t were flipped at the t-th move, and since they are a subset of S_{t-1}, requirement 2 is satisfied as well.

Finally, to satisfy the third requirement, notice that since all switches in S_{t-1} were always flipped together or not flipped on every move, all lamps in L_{t-1} have exhibited exactly the same history on the first $t-1$ moves, because their controlling switches all lie in S_{t-1} and were treated identically on every previous move. From the observations so far, any matching of those lamps to distinct switches in S_{t-1} remains consistent with what we have seen. So L_t could consist of any n_t lamps from L_{t-1}. As a result, we may get exactly k_t lamps from among the k_{t-1} in L_{t-1} that were ON (and still are) and $n_t - k_t$ from the set of $n_{t-1} - k_{t-1}$ lamps that were OFF (and still are). Since $n_{t-1} \ge n_t$, this is feasible since $k_t \le \lceil n_{t-1}/2 \rceil = k_{t-1}$ and $n_t - k_t = \lfloor n_t/2 \rfloor \le \lfloor n_{t-1}/2 \rfloor = n_{t-1} - k_{t-1}$.

Case 2. $m \ge k_{t-1}$, so at least half of the lamps in L_{t-1} changed state. Let L_t be a set of $n_t = k_{t-1} < n_{t-1}$ chosen from the lamps of L_{t-1} that *did change state*. That $k_{t-1} < n_{t-1}$ follows from $t \le t_c$ and $n_{t-1} \ge 2$. Let $S_t \subseteq S_{t-1}$ be the switches we flipped. Since all switches in S_t were flipped on the t-th move and since $S_t \subseteq S_{t-1}$, requirement 2 holds. Since $n_t = k_{t-1} = \lceil n_{t-1}/2 \rceil \ge \lceil n/2^t \rceil$, requirement 1 holds too.

Again, to satisfy the third requirement, notice that under the same argument as before, L_t could comprise any n_t lamps from L_{t-1}. As a result we may get exactly k_t from among the $n_{t-1} - k_{t-1}$ lamps that were OFF (and are now ON) and $n_t - k_t$ lamps from the k_{t-1} that were ON and are now OFF. From the strict inequality $n_{t-1} > k_{t-1} = n_t$, this is feasible since $k_t = \lceil n_t/2 \rceil = \lfloor (n_t+1)/2 \rfloor \le \lfloor n_{t-1}/2 \rfloor = n_{t-1} - k_{t-1}$ and $n_t - k_t = \lfloor n_t/2 \rfloor \le \lfloor n_{t-1}/2 \rfloor \le k_{t-1}$.

That shows that in both cases we can continue the induction, and the lemma is proved.

Using $t = t_c$ we see that there will still exist a set L_{t_c} containing at least one lamp that is still ON, and so we need at least one more move to turn it off, hence $f(n) \ge 1 + t_c$.

To prove the reverse inequality, namely that $1 + t_c$ moves always suffice, let's number the switches from 0 to $n-1$ and consider their binary representation, which uses at most t_c digits. At every move $t = 1, 2, \ldots, t_c$, we flip the switches that have 1 in their t-th digit. Each lamp will flip exactly in the pattern corresponding to the binary code of its switch, so after t_c moves we know which switch controls which lamp. We may need one last move to switch off any lamps that remain ON. So finally, $f(n) \le 1 + t_c$ $\square$

Solution C5. We apply induction on $p + q$. If $p + q = 1$, then $p = 1$, $q = 0$. There is only one such word, 1, and replacing the one with zero results in a single word, so the statement is correct. Let us now assume that $p + q > 1$ and that we have proved the statement for all shorter words. Consider two cases:

Case 1. $p > q + 1$. Divide the given words into two groups: those beginning with 1 and those beginning with 0.

Consider the first group and remove the first symbol from each word. The resulting shortened words contain $p-1$ ones and q zeros. Because $p > q+1$, we have $p-1 > q$, so the induction hypothesis applies to these shortened words: we can replace a one in each of them so that they remain distinct. Restoring the initial symbol 1 to each shortened word yields words that are still distinct.

The same argument applies to the second group. After removing the first symbol, the shortened words contain p ones and $q-1$ zeros, and since $p > q-1$, the induction hypothesis again applies. Restoring the initial symbol 0 yields distinct words within this group as well.

Finally, every word obtained from the first group begins with 1, while every word obtained from the second group begins with 0. Hence the resulting words from the two groups are distinct from each other.

Case 2. $p = q+1$. In this case, the given words are a subset of the set A of all words with $q+1$ ones and q zeros. We shall prove the statement for the entire set A.

Let B be the set of all words with q ones and $q+1$ zeros. Changing any of the $q+1$ ones to zero for any given word in A results in a word from B, so each word $x \in A$ maps to a set $\Gamma(x) \subseteq B$ of size $q+1$. Vice versa, switching any of the $q+1$ zeros in B to one for any word $y \in B$ results in a distinct word $x \in A$ with $y \in \Gamma(x)$. Therefore, each word in B belongs to exactly $q+1$ of the sets $\Gamma(x)$. Let us take an arbitrary k-element subset $X = \{x_1, x_2, \ldots, x_k\}$ of A and consider the union

$$\Gamma(X) = \Gamma(x_1) \cup \Gamma(x_2) \cup \ldots \cup \Gamma(x_k).$$

Let the number of pairs $\{x, y\}$, $x \in X$, $y \in \Gamma(X)$ be $u(X)$. On one hand,

$$u(X) = |X|(q+1) = k(q+1).$$

On the other hand, every element of $\Gamma(X)$ participates in at most $q+1$ such pairs, whence $|\Gamma(X)|(q+1) \geq u(X) = k(q+1)$, and therefore $|\Gamma(X)| \geq k$.

By Hall's theorem, the family $\{\Gamma(x) : x \in A\}$ has a system of distinct representatives. Thus there exists an injective map $f : A \to B$ such that $f(x) \in \Gamma(x)$ for every $x \in A$. This completes the proof. $\square$

Solution C6. Let us arrange the numbers $1, 2, \ldots, 2n$ on a circle clockwise. From here onward, we consider the indices modulo $2n$, i.e. by point $2n+1$ we will mean point 1, point $2n+2$ will be point 2, point 0 will be $2n$ etc.

We draw an arrow from a_i to b_i for each i and call it arrow i. We define the "right" side of arrow i as the set $\{b_i, b_i+1, \ldots, a_i-1\}$, i.e. all the numbers that lie on the clockwise arc from b_i to a_i, including b_i but excluding a_i. Analogously, we define "left" side for every arrow as the complementary set $\{a_i, a_i+1, \ldots, b_i-1\}$.

We shall make use of the following lemma:

Lemma. $x \in ((a, b))$ is equivalent to x being to the left of the arrow from a to b.

Proof. Examine two cases: $a < b$ and $b < a$.

- Case 1. $1 \leq a < b \leq 2n$. The points to the left of the arrow from a to b are $a, a+1, \ldots b-1$. For each of those points x, either $x = a$ or x is strictly in between a and b, so $(x-a)(x-b) \leq 0$. With $a-b < 0$, that gives us $x \in ((a, b))$. Conversely, if $x \in ((a,b))$, then $x \neq b$ and $(x-a)(x-b) \leq 0$, so either $x = a$ or x is between a and b. But that is precisely the set of points to the left of the arrow.

- Case 2. $1 \leq b < a \leq 2n$. The points to the left of the arrow from a to b are $a, a+1, 2n, 1, 2, \dots, b-1$. For each of those points x, either $x < b$ or $x \geq a$. That means that $(x-a)(x-b) \geq 0$, and with $a - b > 0$, we get $x \in ((a,b))$. Conversely, if $x \in ((a,b))$, then $x \neq b$ and $(x-a)(x-b) \geq 0$, so either $x = a$ or $x > a > b$ or $x < b < a$, and all those points are to the left of the arrow.

That completes the proof of the lemma. Notice that (i) and (ii) in the condition are equivalent to $f(p) = n$ and $f(q) = 0$.

For each point x on the circle, define $f(x)$ as the number of arrows that have x to their left.

Now let us consider any two neighboring numbers $a = x$, and $b = x + 1$.

If there is an arrow connecting a and b, then for every other arrow they are simultaneously to the left or simultaneously to the right. Now, with respect to the arrow connecting them, exactly one of a and b (the one where the arrow originates) is to the left of it, and therefore

$$f(a) - f(b) = \pm 1.$$

Likewise, if there is no arrow connecting a and b, then a and b are simultaneously to the left or right of any arrow not incident with either a or b. Let us see that the same holds for the arrow incident with a. If it originates from a, then both a and b are to its left; and if it ends in a, then neither a nor b are to its left. In either case, that arrow contributes equally to $f(a)$ and $f(b)$.

The only difference between $f(a)$ and $f(b)$ comes from the arrow incident with b. If it originates in b, then a is to its right and b is to its left, so it contributes $+1$ to $f(b)$ only. And if it ends in b, then a is to its left and b to its right, so it contributes to $+1$ to $f(a)$ only. That means that

$$f(a) - f(b) = \pm 1,$$

where the sign is determined by whether the arrow incident with b originates or ends in b.

Let $\Delta(x) = f(x+1) - f(x) = \pm 1$. From the above observations, we see that if the path from one number a to another number b along the circle (in either direction) is of length m, then $|f(a) - f(b)| \leq m$ since it is a sum of m deltas, each equal to ± 1.

Thus from $f(p) = n$ and $f(q) = 0$ it follows that the path from p to q cannot be shorter than n, so they must be opposite points on the circle. Furthermore, since

$$n = f(p) - f(q) = \Delta(q) + \Delta(q+1) + \cdots + \Delta(p-1),$$

and all those n deltas are ± 1, then they must necessarily be all $+1$. Therefore

$$f(q+i) = f(q) + \Delta(q) + \Delta(q+1) + \cdots + \Delta(q+i-1) = i$$

for $i = 1, 2, \dots, n-1$. Similarly, we can see that $f(p+i) = n - i$ for $i = 1, 2, \dots, n-1$. That means that for $x \neq p, x \neq q$ we have $0 < f(x) < n$. One consequence is that p is the only point x for which $f(x) = n$ and q is the only point x for which $f(x) = 0$.

Furthermore, since $f(p) = n$ and $f(q) = 0$, it means that for each of the n arrows, p must be to its left and q to its right. That means all arrows must originate in

$$P = \{p+1, p+2, \dots, q\}$$

and end in

$$Q = \{q+1, q+2, \dots, p\}.$$

Conversely, any choice of two opposite points p and q and any bijection from P to Q produce a nice partition. To see why, observe that the arrows representing the bijection originate in P and end in Q, so they have p on their left and q on their right, which means p satisfies (i) and q satisfies (ii), implying the partition is nice.

There are $2n$ ways in which the ordered pair of opposite points (p, q) can be chosen and $n!$ ways in which arrows can be drawn from P to Q. Each combination produces a distinct nice partition, so the number of nice partitions is $2n \times n!$. $\square$

Solution C7. Let $n = 2002$. We index the unit squares with double coordinates, with $(1, 1)$ being in the bottom-left corner. We shall call "left chain" the sequence of squares

$$(i_1, j_1), (i_2, j_2), \dots, (i_{2n-1}, j_{2n-1}),$$

where $(i_1, j_1) = (1, 1)$ and either $(i_{k+1}, j_{k+1}) \equiv (i_k + 1, j_k)$ or $(i_{k+1}, j_{k+1}) \equiv (i_k, j_k + 1)$ for $k = 1, 2, \dots, 2n-2$. Similarly, a "right chain" is defined as a sequence that starts at $(i_1, j_1) = (1, n)$ and either $(i_{k+1}, j_{k+1}) \equiv (i_k + 1, j_k)$ or $(i_{k+1}, j_{k+1}) \equiv (i_k, j_k - 1)$ for $k = 1, 2, \dots, 2n-2$.

Observe that the squares intersected by any line form a subset of either a left chain or a right chain. Indeed, consider the segment in which the line intersects the big square. Traverse this segment from its lower endpoint to its upper endpoint. As we move along the segment, the y-coordinate never decreases. If the slope of the line is nonnegative, then the x-coordinate also never decreases. Consequently, each new square intersected by the segment lies either to the right of the previous one, above it, or diagonally above-right (when the segment passes through a grid vertex). Thus the colored squares appear in a monotone order and can be embedded in a left chain, although some squares of the chain may be skipped if the segment passes through a vertex. If the slope of the line is negative, then x never increases while y never decreases, and the same reasoning shows that the colored squares form a subset of a right chain.

We shall prove that at least $(2-\sqrt{2})n$ chains are needed to cover the big square.

Let us assume the contrary, and suppose that there exist s chains, $s < (2-\sqrt{2})n$ that cover the big square. We order the chains arbitrarily and take the first one. In each of its squares, we write its ordinal number in the chain, i.e. in the square (i_m, j_m) we write m. Then we take the second chain and, again, write in each of its squares its ordinal number in the chain, unless it already contains a number written by a previous chain. We proceed the same way for all chains, so after s steps each square will have a number.

Let $c(m)$ denote the number of times that the number m is written in the entire table. We note that each square (i, j) contains either the number $i + j - 1$, if it was written by a left chain, or the number $i + n - j$, if it was written by a right chain, so for m to be written in a square, the pair (i, j) must satisfy one of the equations $i + j - 1 = m$ or $i + n - j = m$.

For $m \le n$, there are $2m$ possible solutions to the above equations, and they are given by the diagonals $(1, m), (2, m-1), \dots, (m, 1)$, and $(m, n), (m-1, n-1), \dots, (1, n-m+1)$, so $c(m) \le 2m \le 2(2n-m)$.

Similarly, for $m > n$, there are $2(2n-m)$ possible solutions given by the diagonals $(m-n, n), (m-n+1, n-1), \dots, (n, m-n)$, and $(m-n+1, 1), (m-n+2, 2), \dots, (n, 2n-m)$, so $c(m) \le 2(2n-m) \le 2m$.

Therefore, in all cases we have

$$c(m) \leq 2m \text{ and } c(m) \leq 2(2n-m).$$

On the other hand, $c(m) \leq s$, since the number m can occur in a given chain at most once. Combining with the earlier upper bound on $c(m)$, we get

$$c(m) \leq \min(2m, 2(2n-m), s).$$

Since the maximum possible count of occurrences depends on whether s is even or odd, consider the two cases separately.

Case 1: $s = 2p$. Then the numbers

$$1, 2, \ldots, p, p+1, \ldots, n, n+1, \ldots, 2n-p, 2n-p+1, \ldots, 2n-1$$

occur respectively at most

$$2, 4, \ldots, 2p, 2p, \ldots, 2p, 2p, \ldots, 2p, 2p-2, \ldots, 2$$

times. We have at most

$$2(1+2+\cdots+p)+(2n-1-2p)2p+2(1+2+\cdots+p) = 2p(p+1)+(2n-1)2p-p^2 = 4np-2p^2$$

numbered squares, hence $n^2 \leq 4np - 2p^2$. That gives us

$$p \geq \left(1 - \frac{\sqrt{2}}{2}\right) n,$$

whence $s = 2p \geq (2-\sqrt{2})n > 1172$.

Case 2: $s = 2p-1$. Then the numbers

$$1, 2, \ldots, p-1, p, \ldots, n, n+1, \ldots, 2n-p, \ldots, 2n-1$$

occur respectively at most

$$2, 4, \ldots, 2p-2, s, \ldots, s, 2p-2, \ldots, 2$$

times. We have at most

$$2(1+2+\cdots+p-1)+(2n-1-2(p-1))s+2(1+2+\cdots+p-1) = 2p(p-1)+(2n-s)s$$

numbered squares, hence

$$n^2 \leq (s-1)(s+1)/2 + 2ns - s^2,$$

which gives us $s \geq 2n - \sqrt{2n^2-1} > 1172$. In either case, we have $s \geq 1173$. $\square$

Solution C8. Without loss of generality, we can treat the numbers as simply any $2n$ distinct numbers.

(i) We shall prove the statement by induction. For $n = 1$, either the two numbers shown are equal, so we turn either card, or they are different and there is nothing to do. So $3n - 2 = 1$ moves suffice.

Now, assume that the statement holds for $1, 2, \ldots, n-1$. If all shown numbers are different, we are done. If they are not, assume without loss of generality that the number appearing twice is 1. Let those two cards be called "starting" and the remaining $2n - 2$ cards be called "remaining". We flip both starting cards and let the uncovered numbers be a and b.

Define $N = \{1, 2, \ldots, 2n\}$.

- If $a = b$, then $a, b \neq 1$, so the numbers 1 and a are used twice across the starting cards and the other $2n-2$ numbers $N \setminus \{1, a\}$ are used twice across the remaining $2n - 2$ cards. That means the induction hypothesis applies to the remaining cards and we need at most $3(n - 1) - 2$ moves to display all numbers in $N \setminus \{1, a\}$ in the remaining cards. In the end, we flip back one of the starting cards to uncover the 1 on its back, and we are done with a total of $2 + 3(n - 1) - 2 + 1 = 3n - 2$ moves.

- If $a \neq b$, then each of the numbers a and b is used once more in the remaining cards. We temporarily relabel those two occurrences of a and b in the remaining cards with some arbitrary number $x \notin N$. The $2n-2$ remaining cards now contain $2n - 2$ distinct numbers $N \setminus \{1, x\}$, each used twice, so the induction hypothesis applies and we need at most $3(n-1)-2$ moves to display all those numbers exactly once. The x that now appears was originally either a or b, so depending on which one it was, we flip back one of the starting cards to uncover the 1 on its back. Again, we are done with a total of $2 + 3(n - 1) - 2 + 1 = 3n - 2$ moves.

(ii) Consider a starting configuration where the numbers $1, 2, \ldots, n$ appear twice on the front and the numbers $n+1, n+2, \ldots, 2n$ are written twice on the back of the cards. No matter what strategy we choose, sooner or later there must be a move that uncovers the number $2n$. At any move, we shall call a card "primary" if it has not been flipped yet and "secondary" if it has been flipped already.

Notice that (a) swapping two moves does not change the resulting configuration; and (b) flipping a secondary card carries no new information, since we know what is on its back. Combining (a) and (b), we can assume that any move flipping a secondary card is postponed until after there are no more primary cards.

We know that the number $2n$ is written twice on the back of two cards, but we do not know which ones those are. In the worst case, the two cards containing $2n$ may be the last two primary cards flipped. Thus it may take $2n - 1$ moves before the first $2n$ is revealed. Let i, $1 \leq i \leq n$ be the number on the front of the last remaining primary card..

Each of the $2n - 2$ cards originally displaying

$$1, 1, 2, 2, \ldots, i-1, i-1, i+1, i+1, \ldots, n, n$$

is now flipped, so from each pair of cards with j written on their back, $1 \leq j \leq n, j \neq i$, at least one must be flipped again. That means we need at least a total of $(2n-1)+(n-1) = 3n - 2$ moves, which completes the proof of (ii). □

2.3 Number Theory

Solution N1. We shall consider the numbers modulo p. Define two operators $d(x)$ and $f(x)$ on any vector $x = (x_1, x_2, \dots, x_p)$ as follows:

$$d(x) = (x_1 - x_2, x_2 - x_3, \dots, x_p - x_1),$$

$$f(x) = (x_1 + x_2 - 2x_p, x_2 + x_3 - 2x_1, \dots, x_p + x_1 - 2x_{p-1}).$$

The operator f corresponds exactly to the move applied to the vector of the p numbers.

Define $\vec{0} = (0, 0, \dots, 0)$ and call a vector *uniform* if all its entries are the same. We shall list the following properties of d and f:

- For any uniform vector x, $f(x) = \vec{0}$ and $d(x) = \vec{0}$. (*)
- If $d(x) = \vec{0}$, then $x_1 - x_2 = x_2 - x_3 = \cdots = 0$, so all x_i are the same and hence x is uniform. (**)
- Direct computation shows that

  $$d(f(x)) = (3x_1 - 2x_p - x_3, 3x_2 - 2x_1 - x_4, \dots, 3x_p - 2x_{p-1} - x_2),$$

  which coincides with $f(d(x))$. Hence d and f commute. (***)

Next, we show by induction that

$$d^k(x) = \left(\sum_{i=0}^{k} \binom{k}{i} (-1)^i x_{1+i}, \sum_{i=0}^{k} \binom{k}{i} (-1)^i x_{2+i}, \dots, \sum_{i=0}^{k} \binom{k}{i} (-1)^i x_{p+i} \right),$$

where the indices are taken cyclically modulo p (i.e. $x_{p+1} = x_1$, and so on). The statement is obvious for $k = 1$. If we assume that it holds for k, then

$$d^{k+1}(x) = d \left(\sum_{i=0}^{k} \binom{k}{i} (-1)^i x_{1+i}, \sum_{i=0}^{k} \binom{k}{i} (-1)^i x_{2+i}, \dots, \sum_{i=0}^{k} \binom{k}{i} (-1)^i x_{p+i} \right).$$

The r-th term of $d^{k+1}(x)$ is then

$$\sum_{i=0}^{k} \binom{k}{i} (-1)^i x_{r+i} - \sum_{i=0}^{k} \binom{k}{i} (-1)^i x_{r+i+1}$$

$$= \binom{k}{0} (-1)^0 x_{r+0} + \sum_{i=1}^{k} \left(\binom{k}{i} (-1)^i - \binom{k}{i-1} (-1)^{i-1} \right) x_{r+i} - \binom{k}{k} (-1)^k x_{r+k+1}$$

$$= \binom{k}{0} x_r + \sum_{i=1}^{k} \left(\binom{k}{i} + \binom{k}{i-1} \right) (-1)^i x_{r+i} + \binom{k+1}{k+1} (-1)^{k+1} x_{r+k+1}$$

$$= \sum_{i=0}^{k+1} \binom{k+1}{i} (-1)^i x_{r+i},$$

and the induction step is complete. Applying the formula with $k = p$ and working modulo p, since $p \mid \binom{p}{i}$ for $0 < i < p$, we have

$$d^p(x) = (x_1 - x_1, x_2 - x_2, \dots, x_p - x_p) = \vec{0}.$$

From (**) we have that $d^{p-1}(x)$ is uniform, so using (*) we have $f(d^{p-1}(x)) = \vec{0}$. Using (***), that gives us $d^{p-1}(f(x)) = \vec{0}$.

Again, from (**) we have that $d^{p-2}(f(x))$ is uniform, so using (*) we have $f(d^{p-2}(f(x))) = \vec{0}$. Using (***), that gives us $d^{p-2}(f^2(x)) = \vec{0}$.

Continuing this argument inductively, we obtain that $d^{p-1-i}(f^i(x))$ is uniform for $i = 0, 1, \ldots, p-1$. Using $i = p-1$ and setting x to the vector of the numbers on the circle, we get that $f^{p-1}(x)$ is uniform, which completes the proof. $\square$

Solution N2. From $n \mid 2^d + 1$ it follows that n is odd and greater than 6. We shall consider the numbers as residues modulo n.

Let X, Y, Z be the sets of all *nonzero* residues modulo n representable as 2^x, $2^x + 2^y$, and $2^x + 2^y + 2^z$ respectively. Notice that $X \subseteq Y$, since $2^x \equiv 2^{x+2d-1} + 2^{x+2d-1} \in Y$ and that $Y \subseteq Z$, since $2^x + 2^y \equiv 2^{x+2d-1} + 2^{x+2d-1} + 2^y \in Z$. In view of the fact that $2^d + 2^d + 2^1 + n \equiv 0$, we see that n is an admissible m, and since $n \equiv 0 \notin Z$, the remaining admissible values of m correspond to the nonzero residues in Z. Thus it suffices to prove that $|Z| \geq 6d$.

Since $2^{2d} \equiv (-1)^2 = 1$, there exists a *minimal* j such that $2^j \equiv 1$ and $j \mid 2d$. Notice that $j \neq d$, otherwise $1 \equiv -1$, which is impossible for $n > 6$. At the same time, it cannot be that $j < d$, otherwise $2^{d-j} \equiv -1$ would contradict the minimality of d. Therefore $j > d$.

Since $j > d$ and $j \mid 2d$, we must have $j = 2d$. Thus $X = \{2^i\}, i = 1, 2, \ldots 2d$, so $|X| = 2d$.

Consider first the case where $X = Y$. In that case, for every $a \in X$, from $2^{2d} \equiv 1$ we have $a + 1 \equiv a + 2^{2d} \in Y = X$, hence recursively we get $a, a+1, a+2, \ldots, n-1 \in X$. From $n - 1 + 2^1 \in Y = X$ we get that $n + 1 \equiv 1 \in X$, and again recursively we get that $2, 3, \ldots a-1 \in X$. So X contains all $n-1$ nonzero residues. Therefore $|X| = n-1$, and so $|Z| \geq |X| = 6d$ and the condition is proved.

So from now on, we assume that $X \subset Y$. We choose an arbitrary $a \in Y$. Since n is odd and $a \not\equiv 0$, we have $2a \not\equiv 0$ and so $2a \in Y$. Consider a bijection $f : Y \to Y$ defined by $f(a) = 2a$. It is an injection, since $2a \equiv 2b \Rightarrow a = b$, and hence it is a bijection, since it is an injection of one set into itself. For any $a \in Y$, consider its orbit in f of length k, so k is the minimal number such that $f^k(a) = a$. We have $a2^k \equiv a \Rightarrow 2^k \equiv 1$, since $a \not\equiv 0$. By the minimality of $2d$ we get $2d \mid k$, and from $k \leq 2d$ we get $k = 2d$. That means all orbits are of length $2d$, hence $2d \mid |Y|$.

Similarly to the earlier case $X = Y$, if $Y = Z$ we end up with $|Y| = n-1$ and $|Z| \geq 6d$, so we can consider $Y \subset Z$. Like before, we conclude $2d \mid |Z|$.

Therefore we have that

$$\frac{|X|}{2d} < \frac{|Y|}{2d} < \frac{|Z|}{2d},$$

are three distinct integers. So $\dfrac{|Z|}{2d} \geq 3$ and $|Z| \geq 6d$, which completes the proof. $\square$

Solution N3. We shall prove each direction in turn.

Forward direction. We have $am + bn = p$ and want to show that $A \cap B = \emptyset$. Suppose the contrary, and let k be an element of $A \cap B$, so

$$k = \left\lfloor \frac{ip}{a} \right\rfloor = \left\lfloor \frac{jp}{b} \right\rfloor \qquad (*)$$

for some $1 \leq i \leq a-1$ and $1 \leq j \leq b-1$. That gives us

$$\frac{ip}{a} > k > \frac{ip}{a} - 1 \text{ and } \frac{jp}{b} > k > \frac{jp}{b} - 1,$$

where the strictness of the inequalities comes from the fact that the elements inside the floor brackets in (*) are non-integer. Multiply the first inequality by am and the second by bn, then add them to obtain

$$ipm + jpn > kam + kbn > ipm - am + jpn - bn.$$

Using $am + bn = p$ and dividing by p, we get

$$im + jn > k > im + jn - 1,$$

which is impossible. So $k \in A \cap B$ cannot exist and we are done.

Backward direction. We have $A \cap B = \emptyset$ and want to prove that $am + bn = p$ for some positive integers m, n. If $d = \gcd(a, b) > 1$, we have $a = a_1 d$ and $b = b_1 d$ for some $a_1 < a$ and $b_1 < b$, hence

$$\left\lfloor \frac{a_1 p}{a} \right\rfloor = \left\lfloor \frac{p}{d} \right\rfloor = \left\lfloor \frac{b_1 p}{b} \right\rfloor,$$

and so $\left\lfloor \frac{p}{d} \right\rfloor \in A \cap B$, contradicting $A \cap B \neq \emptyset$. Therefore, $d = 1$, so there exists $m' \in \{1, 2, \ldots, b-1\}$ such that $am' \equiv 1 \pmod{b}$. Writing $am' - 1 = n'b$ yields

$$m'a - n'b = 1$$

with $n' \in \{1, 2, \ldots, a-1\}$. Next,

$$\frac{m'p}{b} - \frac{n'p}{a} = \frac{p}{ab} > 0 \Rightarrow \left\lfloor \frac{m'p}{b} \right\rfloor \geq \left\lfloor \frac{n'p}{a} \right\rfloor,$$

where equality is not possible, otherwise A and B would have a common element, contradicting $A \cap B \neq \emptyset$. Thus

$$\left\lfloor \frac{m'p}{b} \right\rfloor = \left\lfloor \frac{n'p}{a} \right\rfloor + k$$

for some integer $k \geq 1$. Therefore,

$$\frac{p}{ab} = \frac{m'p}{b} - \frac{n'p}{a} = \left\lfloor \frac{m'p}{b} \right\rfloor - \left\lfloor \frac{n'p}{a} \right\rfloor + \left\{ \frac{m'p}{b} \right\} - \left\{ \frac{n'p}{a} \right\} = k + \left\{ \frac{m'p}{b} \right\} - \left\{ \frac{n'p}{a} \right\}.$$

Multiplying both sides by ab and rearranging, we get

$$p = \left\{ \frac{m'p}{b} \right\} ab + \left(k - \left\{ \frac{n'p}{a} \right\} \right) ab = am + bn,$$

where

$$m = b \left\{ \frac{m'p}{b} \right\} = m'p - b \left\lfloor \frac{m'p}{b} \right\rfloor$$

and

$$n = a \left(k - \left\{ \frac{n'p}{a} \right\} \right) = ak - n'p + a \left\lfloor \frac{n'p}{a} \right\rfloor$$

are positive integers, so the statement is proved. □

Solution N4. Observe that $2001 = pqr$ for the primes $p = 3, q = 23, r = 29$. Since the total number of divisors of $(pqr)^n$ is $(n+1)^3$, the number of triples is $(n+1)^3/3$ and so $3 \mid (n+1)$. Let the product of the numbers in each triple be a. If we multiply all these triples, we obtain

$$a^{(n+1)^3/3} = (pqr)^{(n+1)^2(0+1+\cdots+n)} = (pqr)^{(n+1)^3 n/2},$$

hence $a = 2001^{3n/2}$, so n is even. Combining with $3 \mid n+1$, a necessary condition for n becomes $n \equiv 2 \pmod 6$. We shall prove that this condition is also sufficient.

Let $n = 6m + 2$ for some integer $m \geq 0$, and let A denote the set of $2m+1$ vectors α_k defined as

$$\alpha_k = (k, m+k, 2m-2k)\,, \quad k = 0, 1, \ldots, m$$

and

$$\alpha_k = (k, k-m-1, 4m+1-2k)\,, \quad k = m+1, \ldots, 2m.$$

For each α, observe that the sum of its coordinates is $3m$. Furthermore, observe that each coordinate assumes every value $0, 1, \ldots, 2m$ exactly once as k iterates from 0 to $2m$. Indeed, the first coordinate takes the values $0, 1, \ldots, m, m+1, \ldots, 2m$; the second coordinate takes the values $m, m+1, \ldots, 2m, 0, 1, \ldots, m-1$; and the third coordinate takes the values $2m, 2m-2, \ldots, 0, 2m-1, 2m-3, \ldots, 1$.

Define the transformation f by

$$f(x, y, z) = (3x, 3y+1, 3z+2)$$

and the set F as:

$$F = \bigcup_{\alpha \in A} f(\alpha).$$

Notice that F has the following properties:

- (i) all coordinates of its vectors are in the interval $[0, n]$, since $x, y, z \in [0, 2m]$;
- (ii) every integer in $\{0, 1, \ldots, n\}$ appears as one of the coordinates in exactly one vector from F, since $3x$ iterates over all numbers congruent to $0 \pmod 3$, $3y+1$ over all numbers congruent to $1 \pmod 3$, and $3z+2$ over all numbers congruent to $2 \pmod 3$;
- (iii) the sum of coordinates of each vector in F is exactly $3(x+y+z)+3 = 9m+3$.

Similarly, define

$$f'(x, y, z) = (3x+2, 3y, 3z+1), \qquad f''(x, y, z) = (3x+1, 3y+2, 3z)$$

and

$$F' = \bigcup_{\alpha \in A} f'(\alpha), \qquad F'' = \bigcup_{\alpha \in A} f''(\alpha).$$

Analogously, properties (i), (ii), and (iii) apply to F' and F''. Furthermore, the sets F, F', F'' are disjoint, since the first coordinates have different residues modulo 3. Let $U = F \cup F' \cup F''$. Note that by property (ii), every integer in $\{0, 1, \ldots, n\}$ appears exactly once as a coordinate of a vector in F, and exactly three times among the vectors in U, once in each coordinate position.

We construct the partitioning of the triples as follows: for every element

$$(x_1, y_1, z_1) \in F, \qquad (x_2, y_2, z_2), (x_3, y_3, z_3) \in U,$$

define the triple

$$\left(p^{x_1}q^{x_2}r^{x_3}, p^{y_1}q^{y_2}r^{y_3}, p^{z_1}q^{z_2}r^{z_3}\right).$$

For every given triple, from (i), each number is a divisor of $p^n q^n r^n = 2001^n$, and from (iii), the product of these numbers is the constant

$$p^{x_1+y_1+z_1}q^{x_2+y_2+z_2}r^{x_3+y_3+z_3} = (pqr)^{9m+3}.$$

Furthermore, the numbers in each triple are different, since x_1, y_1, z_1 are congruent to $0, 1, 2 \pmod 3$, the exponent vectors differ in at least one coordinate.

What remains is to show that this set of triples constitutes an actual *partition* of the divisors of 2001^n. Consider any one of these divisors $p^{u_1}q^{u_2}r^{u_3}$. We need to show that it appears in exactly one of the triples.

From (ii), we know that u_1 appears exactly once as a coordinate of exactly one vector of F. Let that vector be $\mu_1 = (x_1, y_1, z_1)$, and let $l \in \{1, 2, 3\}$ denote the coordinate position of u_1 in it.

Again from (ii), among the vectors in U, there are exactly 3 vectors that contain u_2 as a coordinate, each in a different position. Let the one that has u_2 in position l be $\mu_2 = (x_2, y_2, z_2)$. Similarly, $\mu_3 = (x_3, y_3, z_3)$ is determined. Notice that the triple corresponding to $\mu_1 \in F, \mu_2, \mu_3 \in U$ contains $p^{u_1}q^{u_2}r^{u_3}$ in position l. Finally, all desired n are given by $n = 2 + 6m, \quad m = 0, 1, \ldots$. □

Solution N5. We divide the proof into three parts. The first proposes a set of numbers that work; the second shows that those are the only numbers that work; and the third part counts them. Define $a_k = \left\lfloor \frac{p}{k} \right\rfloor$ for all $k \geq 1$ and let

$$A = \{a_k \mid k = 2, 3, \ldots, p\}.$$

We call a number $a \in [0, p-1]$ *good* if $f_a(m) > a$ for all $m \in [1, p-1]$. Our goal is to count the good numbers.

Lemma 1. We shall prove that every $a \in A \cup \{0, p-1\}$ is a good number.

Proof. If $a = 0$, then $f_a(m) = m > 0 = a$; and if $a = p-1$, then $f_a(m) = m + \underline{ma} = m + \underline{-m} = m + p - m = p > p - 1 = a$. So 0 and $p-1$ are good numbers. Next, let $a \in A$. We shall prove by contradiction that there cannot exist $m_0 \in [1, p-1]$ such that $a \geq f_a(m_0)$. Assume the contrary, and let m_0 be the number minimizing $f_a(m)$, i.e.

$$a \geq f_a(m_0) = \min_{1 \leq m \leq p-1} f_a(m).$$

From $f_a(1) = 1 + a > a$, we see that $m_0 \neq 1$, so $a \geq f_a(m_0) \geq m_0 > 1$, thus $a > 1$. Let $v = \underline{m_0 a} > 0$ and $m_0 a = lp + v$ for some $l \geq 0$. From $m_0 > 1$ and the minimality of m_0, we have

$$m_0 + v = f_a(m_0) \leq f_a(m_0 - 1) = (m_0 - 1) + \underline{(m_0 - 1)a},$$

so $v < \underline{(m_0-1)a}$. It must be that $v < a$, otherwise $\underline{(m_0-1)a} = \underline{v-a} = v - a \le 0$, which would contradict $v < \underline{(m_0-1)a}$. Hence $0 \le v < a$, and thus

$$\frac{lp}{a} < m_0 < \frac{lp}{a} + 1 \Rightarrow m_0 = \left\lceil \frac{lp}{a} \right\rceil.$$

Since $a \in A$, there exist integers $k, k' : 0 < k' < k$ for which $a = a_k$ and $p = ak + k'$, so

$$m_0 = \left\lceil \frac{lp}{a} \right\rceil = \left\lceil \frac{l(ak+k')}{a} \right\rceil = lk + \left\lceil \frac{lk'}{a} \right\rceil.$$

From $a \ge f_a(m_0) > m_0 \ge lk > lk'$ we get

$$\left\lceil \frac{lk'}{a} \right\rceil = 1 \Rightarrow m_0 = lk + 1.$$

Using again $a > lk'$ and $ak = p - k'$, we have

$$f_a(m_0) = f_a(lk+1) = lk + 1 + \underline{lka + a} = lk + 1 + \underline{a - lk'}.$$

But as $0 \le a - lk' < a < p$, we have $\underline{a - lk'} = a - lk'$, so

$$f_a(m_0) = lk + 1 + (a - lk') = (a+1) + l(k - k') \ge a + 1 > a,$$

which contradicts the choice of m_0, and Lemma 1 is proved.

Lemma 2. We shall prove that if $a \notin A$ and $0 < a < p - 1$, then $f_a(m) \le a$ for some m.

Proof. Since $a \notin A$ and $a_p = 1 < a < p = a_1$, there must exist $k \in [1, p-1]$ such that

$$a_{k+1} < a < a_k.$$

For $p > 2$ we have $a_{p-1} = a_p = 1$, so $k \ne p - 1$ and hence $k \in [1, p-2]$. From the upper bound, we get

$$a + 1 \le a_k \le \frac{p}{k},$$

where at least one of the two inequalities is strict, except when $k = 1$ and $a = p - 1$, which contradicts $a < p - 1$. From the lower bound, we have

$$a \ge a_{k+1} > \frac{p}{k+1}.$$

From $p < ak + a < p + a < 2p$ we have $\underline{ak + a} = (ak + a) - p$, so

$$ak + k < p < ak + a \Rightarrow f_a(k+1) = k + 1 + \underline{ak + a} = k + 1 + ak + a - p < a + 1,$$

thus $f_a(k+1) \le a$ and Lemma 2 is proved.

Lemmas 1 and 2 tell us that all the good numbers are $0, p-1$ and the elements of A. All it remains then is to count $|A|$ and add 2. Intuitively, for small k, the numbers a_k are widely spaced, so they are all different; and for large k, a_k are thinly spaced, so they assume every integer value from some point onward.

Let k_0 be the largest $k \in [2, p-1]$ for which $\dfrac{p}{k-1} - \dfrac{p}{k} > 1$. Such a number necessarily exists, since $k = 2$ satisfies the inequality for $p > 2$. If the gap between two rational numbers is > 1, their floors differ by at least 1. Applying this observation to our case yields $a_k < a_{k-1}$ for $2 \le k \le k_0$, hence $a_2, a_3, \ldots, a_{k_0}$ are $k_0 - 1$ distinct elements of A. On the other hand, when the gap between two rational numbers is ≤ 1, their floors differ by at most 1. Applying this to our case, for $k > k_0$ we have $a_{k-1} - a_k \le 1$, so all positive numbers less than a_{k_0} also belong to A. Therefore

$$|A| = k_0 - 1 + a_{k_0} - 1 = k_0 + \left\lfloor \frac{p}{k_0} \right\rfloor - 2.$$

We just need to find the k_0 and compute the above expression. So k_0 must satisfy the inequalities:

$$\frac{p}{k-1} - \frac{p}{k} > 1 \ge \frac{p}{k} - \frac{p}{k+1}$$
$$\Rightarrow k(k+1) > p > k(k-1).$$

Notice that $s = \sqrt{p}$ is irrational. Consider two cases:

Case 1. $p > k^2$, so $k(k+1) > p > k^2$. We have

$$(2k+1)^2 > 4(k+1)k > 4p > 4k^2 \Rightarrow s \in (k, k+1/2),$$

so $k = \lfloor s \rfloor$. From $k + 1 > p/k > k$ we obtain $a_k = k$, and hence $|A| = a_k + k - 2 = 2k - 2 = 2\lfloor s \rfloor - 2 = \lfloor 2s \rfloor - 2$.

Case 2. $p < k^2$, so $k^2 > p \ge k(k-1) + 1$. We have

$$4k^2 > 4p \ge 4k(k-1) + 4 > (2k-1)^2 \Rightarrow s \in (k - 1/2, k),$$

so $k = \lfloor s \rfloor + 1$. From $k > p/k > k - 1$ we obtain $a_k = k - 1$, and so $|A| = a_k + k - 2 = 2k - 3 = 2\lfloor s \rfloor - 2 = \lfloor 2s \rfloor - 2$.

The case $p = k^2$ need not be examined, since s is irrational. Therefore $|A| = \lfloor 2\sqrt{p} \rfloor - 2$, and adding back the 2 good numbers 0 and $p - 1$, the final count becomes $\lfloor 2\sqrt{p} \rfloor$. $\square$

Solution N6. Number the p vertices from A to B along one side with $0, 1, \ldots, p-1$ and call this set L. Likewise, number the p vertices from B to A on the other side and call this set R. Every segment crosses AB, so it must have one endpoint numbered $a \in L$ and the other $b \in R$ due to the convexity of the polygon. Since vertex k corresponds to angle $k\pi/p$, the direction of chord ab depends only on the midpoint angle $(a+b)\pi/(2p)$. Hence two chords are parallel iff these midpoint angles are equal, and perpendicular iff they differ by $\pi/2$. Therefore,

$$a_1b_1 \parallel a_2b_2 \Leftrightarrow a_1 + b_1 = a_2 + b_2,$$

$$a_1b_1 \perp a_2b_2 \Leftrightarrow a_1 + b_1 = a_2 + b_2 \pm p.$$

In either case, the statement that a_1b_1 is either parallel or perpendicular to a_2b_2 is equivalent to $a_1 + b_1 \equiv a_2 + b_2 \pmod{p}$. So all we need to do is prove the following Lemma:

Lemma. Let A, B be sets of residues modulo p and $|A| + |B| < p$. Define their "sum" by

$$A + B = \{a + b \mid a \in A,\ b \in B\}.$$

Then

$$|A + B| \geq |A| + |B| - 1.$$

Proof. Let $|A| = m$, $|B| = n$, and assume without loss of generality that $m \leq n$.

Define "translation" t on the set C as follows:

$$t + C = \{t + c \mid c \in C\}.$$

Observe that $(t + A) + B = t + (A + B)$, hence $|(t + A) + B| = |A + B|$. If $m = 1$, then $|A + B| = |B| = |A| + |B| - 1$ and we are done, so hereafter assume $m > 1$ and let a_1, a_2 be two elements of A. Furthermore, $m \leq n < p$, hence $\exists c : c \notin B$. Now, as the sequence

$$c + t(a_2 - a_1), \quad t = 1, 2, \ldots, p - 1$$

runs through all residues modulo p except c, there exists a minimal t such that for $b = c + t(a_2 - a_1) \in B$. Then

$$A' = (b - a_2) + A$$

contains the element $b + (a_1 - a_2) \in B$ and $b + (a_2 - a_2) = b \notin B$. Since A' is just a translation of A, we only need to prove the lemma for A' and B. Let

$$F = A' \cap B, \quad G = A' \cup B.$$

We have

$$\emptyset \neq F \subset A', \qquad B \subset G,$$

hence

$$0 < |F| < m, n < |G|.$$

Observe that $|F| + |G| = |A| + |B|$, since every element $f \in F$ is counted exactly twice on each side, and every element $x \in (A' \cup B)\backslash F$ is counted exactly once on each side. We shall show that

$$F + G \subseteq A + B.$$

Indeed, if $f \in F$, $g \in G$, then depending on whether $g \in A'$ or $g \in B$ we have $(f, g) \in A' \times B$ or $(f, g) \in B \times A'$. In either case, $f + g \in A' + B$. Thus

$$|A' + B| \geq |F + G|,$$

so it suffices to prove the lemma for F and G instead of A' and B. Thus we replace the pair A, B (with $|A| \leq |B|$) in the original statement by the pair F, G, for which $|F| < |A|$ and $|G| > |B|$. Repeating this reduction decreases the size of the smaller set each time, so eventually that set has size 1, which was already handled. Thus the lemma is proved. Applying the lemma to the original problem, each segment corresponds to the residue $a + b \pmod{p}$. Since parallel or perpendicular segments correspond to the same residue, selecting segments with distinct residues yields a family of at least $k - 1$ segments no two of which are parallel or perpendicular. $\square$

2.4 Geometry

Solution G1. Let

$$\angle DCA = \alpha, \qquad \angle DCT = y, \qquad \angle CDT = x.$$

Since $ABCD$ is an isosceles trapezoid, we have $\alpha = \angle DCA = \angle CDB = \angle CDQ$. From the sine rule in $\triangle CDP$ and $\triangle CDT$, we get

$$DP \cdot DT = \frac{CD \sin\alpha}{\sin(x+\alpha)} \cdot \frac{CD \sin y}{\sin(x+y)}.$$

From the sine rule in $\triangle CDQ$ and $\triangle CDT$, we get

$$CQ \cdot CT = \frac{CD \sin\alpha}{\sin(y+\alpha)} \cdot \frac{CD \sin x}{\sin(x+y)}.$$

Therefore

$$\begin{aligned} \frac{CD^2 \sin\alpha \sin y}{\sin(x+\alpha)\sin(x+y)} &= DP \cdot DT = CQ \cdot CT = \frac{CD^2 \sin\alpha \sin x}{\sin(y+\alpha)\sin(x+y)} \\ &\Rightarrow \frac{\sin y}{\sin(x+\alpha)} = \frac{\sin x}{\sin(y+\alpha)}. \end{aligned}$$

Therefore,

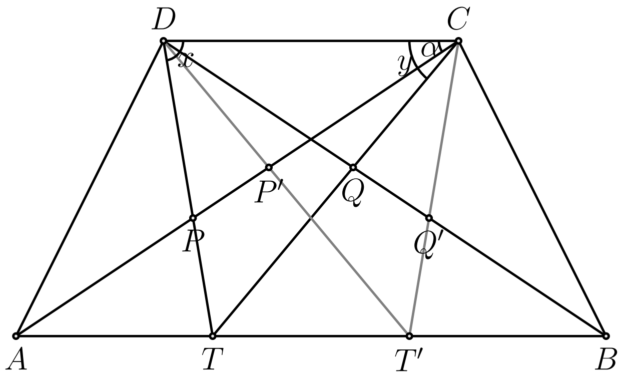
$$\begin{aligned} \sin y\big(\sin y \cos\alpha + \sin\alpha \cos y\big) &= \sin x\big(\sin x \cos\alpha + \sin\alpha \cos x\big), \\ \cos\alpha\big(\sin^2 y - \sin^2 x\big) &= \sin\alpha\big(\sin x \cos x - \sin y \cos y\big), \\ \cos\alpha \sin(x+y)\sin(y-x) &= -\sin\alpha \cos(x+y)\sin(y-x), \\ \sin(x+y+\alpha)\sin(y-x) &= 0. \end{aligned}$$

Thus

$$x = y \qquad \text{or} \qquad x + y + \alpha = 180^\circ.$$

In the first case, $\triangle DTC$ is isosceles and symmetric with respect to the perpendicular bisector of AB and of DC (hereafter called just *symmetric* for simplicity). So T is the midpoint of AB, and P and Q are symmetric, thus the circumcenter of $\triangle TPQ$ is on the line of symmetry, and we are done.

In the second case, $\angle DTC = 180^\circ - x - y = \alpha$. Let T' be the point symmetric to T, $P' = AC \cap T'D$, and $Q' = BD \cap T'C$. Notice that P' and Q' are symmetric to Q and P respectively, so $PQ' \parallel DC$ and therefore $\angle PQ'Q = \alpha = \angle PTQ$. That means PQ is seen at the same angle from Q' and T and so $TPQQ'$ are concyclic. Hence point T (and therefore also T') lies on the circumcircle of the isosceles trapezoid $PQ'QP'$. Again due to symmetry, the circumcenter of $\triangle TPQ$ is on the line of symmetry and so equidistant from A and B. $\square$



Solution G2 Obviously l is external to k. An inversion with center D which maps k onto l (and vice versa) sends P into P' and Q into Q', hence P, P', Q, Q' lie on a circle.

Let the positive direction of rotation about D be counterclockwise. If

$$H = (OD) \cap l,$$

we define

$$OH = h, \quad \angle PDH = x, \quad \angle QDH = y, \quad k(O, R).$$

We have

$$x, y \in (-90^\circ, 90^\circ).$$

If $x = -y$, then $PQP'Q'$ is an isosceles trapezoid and the condition that the center of its circumcircle lies on k is equivalent to

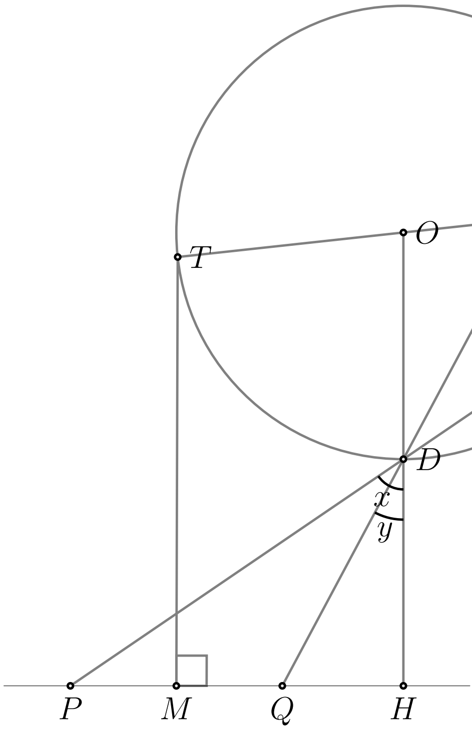
$$PQP'Q' \text{ is a rectangle } \Leftrightarrow PQ = P'Q'.$$

Now let $x + y \neq 0^\circ$. Then if the center of the circumcircle of $PQP'Q'$ lies on k, we have that the perpendicular bisectors of PQ and $P'Q'$ intersect on k. Let that point be T. From the first bisector, T's projection M onto l must be the midpoint of PQ, hence $HM = h(\tan x + \tan y)/2$ (the distance being signed and depending on the signs of x and y). From the second bisector, it follows that T is the midpoint of either the major or minor arc of $P'Q'$, so it forms with OD angles $x + y$ or $180^\circ + x + y$ around O. Therefore, its distance from OH is $\pm R \sin(x + y)$, depending on which arc midpoint T is. Therefore

$$\frac{1}{2}h(\tan x + \tan y) = \pm R \sin(x + y) \Leftrightarrow$$
$$\frac{h}{\cos x \cos y} = \pm 2R \Leftrightarrow$$
$$\frac{1}{2}h(\tan x - \tan y) = \pm R \sin(x - y) \Leftrightarrow$$
$$P'Q' = \pm PQ,$$

where exactly one of the $+$ or $-$ must be true.

The converse direction does not need consideration of cases, since $\sin(x - y) \neq 0$ and therefore the argument flows backward.



Solution G3. Let the radius of the circumcircle of $\triangle ABC$ be $R = 1/2$, and the angles of the triangle be 2α, 2β, 2γ. Let A_1A_2 intersect the altitude through C at point P', and let the foot of this altitude be C_H. We have

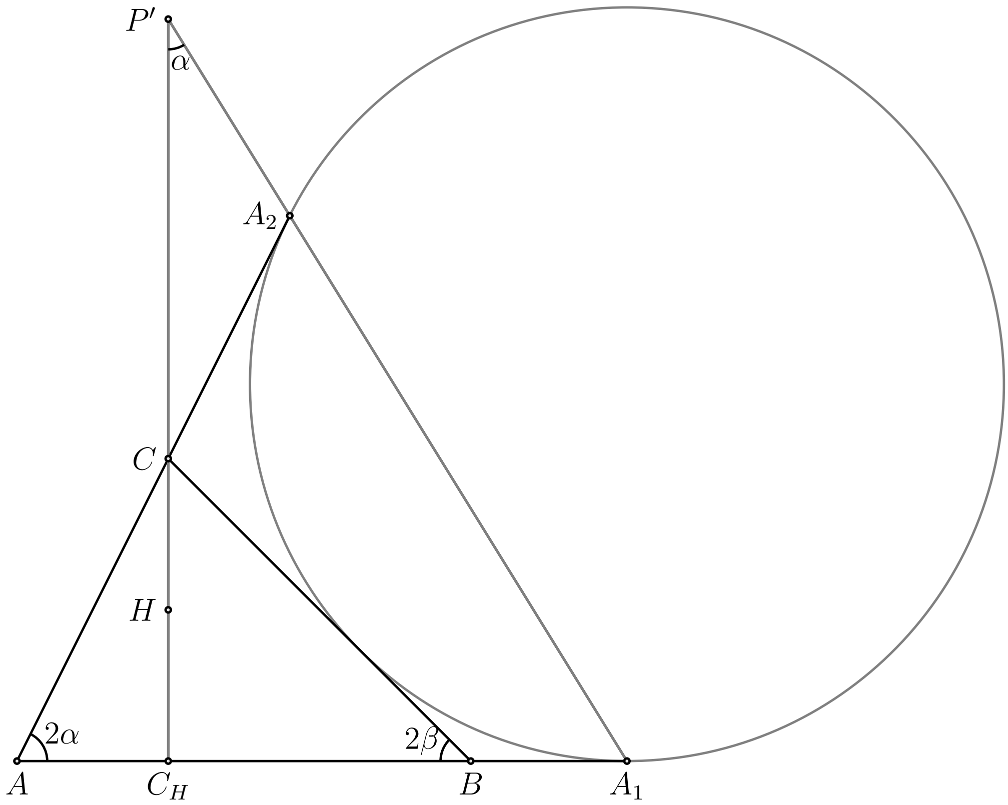
$$\begin{aligned}
P'C_H &= C_HA_1 \cot\alpha = (AA_1 - AC_H)\cot\alpha \\
&= (2\cos\alpha\cos\beta\cos\gamma - \sin 2\beta\cos 2\alpha)\cot\alpha \\
&= 2\cos\beta(\cos\alpha\sin(\alpha+\beta) - \sin\beta\cos 2\alpha)\cot\alpha \\
&= 2\cos\beta(\sin\alpha\cos\alpha\cos\beta + \sin\beta\sin^2\alpha)\cot\alpha \\
&= 2\cos\beta\sin\alpha\cos\alpha\cos(\alpha-\beta)\cot\alpha \\
&= 2\cos\beta\cos\alpha\cos(\alpha-\beta)
\end{aligned}$$

which is a symmetric expression in α and β. Then B_1B_2 intersects the altitude CC_H in the same point P', i.e. $P \equiv P_C$. Therefore, $P_CC \perp AB$ and $H \in P_CC$. Analogously $H \in P_BB$ and $H \in P_AA$.

We shall show that H is the circumcenter of $\triangle P_AP_BP_C$. We have

$$\begin{aligned}
P_CH &= 2\cos\alpha\cos\beta\cos(\alpha-\beta) - \cos(2\alpha)\cos(2\beta) \\
&= (\cos(\alpha-\beta) + \cos(\alpha+\beta))\cos(\alpha-\beta) - \frac{\cos(2\alpha-2\beta)+\cos(2\alpha+2\beta)}{2} \\
&= \cos^2(\alpha-\beta) + \cos(\alpha-\beta)\cos(\alpha+\beta) - \frac{2\cos^2(\alpha-\beta)-1}{2} + \frac{\cos(2\gamma)}{2} \\
&= \frac{1+\cos(2\alpha)+\cos(2\beta)+\cos(2\gamma)}{2},
\end{aligned}$$

which is a symmetric expression in α, β, γ, so we conclude that $P_CH = P_AH = P_BH$ and the statement is proved. $\square$



Solution G4. Let

$$M = PX \cap BC, \quad N = PY \cap AC, \quad L = PZ \cap AB.$$

Let the lengths of the sides of the triangle be $2a, 2b, 2c$, and let x, y, z be the directed distances (clockwise) from the midpoints on BC, CA, AB to M, N, L respectively.

From ABC acute and P interior it follows that

$$-1 < \frac{x}{a}, \frac{y}{b}, \frac{z}{c} < 1,$$

so

$$a \pm x > 0, b \pm y > 0, c \pm z > 0. \quad (a)$$

From $PB \perp XZ$ and Pythagorean theorem to $\triangle PBZ$ and $\triangle PBX$ it follows that

$$\begin{aligned}
BZ^2 - BX^2 &= PZ^2 - PX^2 \\
\Rightarrow BL^2 + LZ^2 - BM^2 - MX^2 &= (PL + LZ)^2 - (PM + MX)^2 \\
&= PL^2 + LZ^2 + 2PL \cdot LZ \\
&\quad - PM^2 - MX^2 - 2PM \cdot MX \\
\Rightarrow BL^2 - BM^2 &= (PB^2 - BL^2) + 2PL \cdot LZ \\
&\quad - (PB^2 - BM^2) - 2PM \cdot MX \\
&= -BL^2 + 2BL \cdot LA + BM^2 - 2BM \cdot MC
\end{aligned}$$

since $PL \cdot LZ = BL \cdot LA$ and $PM \cdot MX = BM \cdot MC$. From here:

$$BL^2 - BM^2 = BL \cdot LA - BM \cdot MC$$

$$\Rightarrow BL(BL-AL) = BM(BM-MC)$$
$$\Rightarrow (c-z)2z = -(a+x)2x$$
$$\Rightarrow x(x+a) = z(z-c). \tag{*}$$

Analogously we obtain
$$z(c+z) = y(b-y). \tag{**}$$

From
$$0 = PA^2 - PB^2 + PB^2 - PC^2 + PC^2 - PA^2$$
$$= AL^2 - LB^2 + BM^2 - MC^2 + CN^2 - NA^2$$
$$\Rightarrow ax + by + cz = 0.$$

Using that and adding the equalities (*) and (**), we obtain

$$ax + x^2 + z^2 + cz = z^2 - cz + y^2 - by$$

$$\Rightarrow x^2 + cz = y^2 = y^2 + ax + by + cz$$
$$\Rightarrow y(b+y) = x(x-a), \tag{***}$$

i.e. the third equality of the form (*) is true, which also proves that $PC \perp YX$. Now, multiply the three equalities to get:

$$xyz(a+x)(b+y)(c+z) = xyz(x-a)(y-b)(z-c)$$

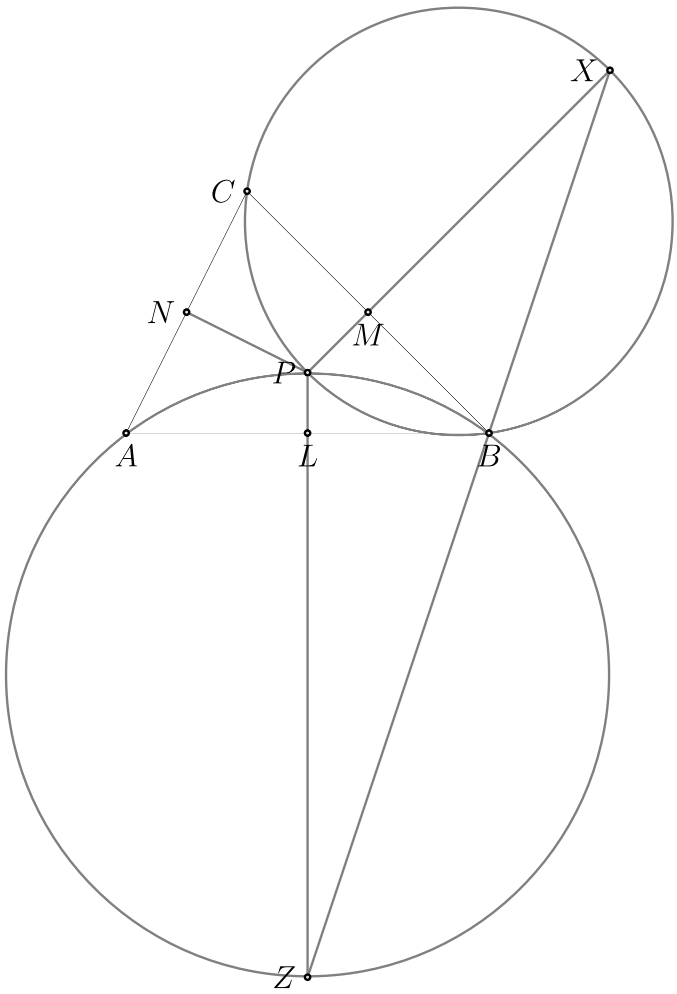
$$\Rightarrow xyz\big((a+x)(b+y)(c+z) + (a-x)(b-y)(c-z)\big) = 0.$$

Since the expressions in parentheses are sums of positive numbers due to (a), it follows that $xyz = 0$, so one of x, y, z is 0. Without loss of generality, let $x = 0$.

Then from (***) and (*) with $x = 0$ we get

$$y(b+y) = 0, \quad z(z-c) = 0,$$

which, owing to (a), implies $y = z = 0$. That means that P projects to the midpoints of the sides of the triangle, hence it is the center of its circumcircle.



Solution G5. If there were two distinct points T_1, T_2 on B_1C_1 such that A, A_2, T_1, T_2, I lie on a circle, then we would have

$$\angle AT_1I + \angle AT_2I = 180^\circ,$$

which would be impossible since both $\angle AT_1I$ and $\angle AT_2I$ would need to be obtuse (being larger than the rectangles $\angle AB_1I$ and $\angle AC_1I$). Thus the point in question is exactly one, and we will construct it.

Let M be the midpoint of the arc $B_1A_1C_1$ in Γ, and $T' = MA_2 \cap BC$, then A_2T' is the angular bisector of $\angle B_1A_2C_1$ and hence

$$\frac{B_1T'}{T'C_1} = \frac{B_1A_2}{A_2C_1} = \frac{\frac{B_1A_1}{AA_1}AB_1}{\frac{A_1C_1}{AA_1}AC_1} = \frac{B_1A_1}{A_1C_1}$$

Therefore A_1T' is the angular bisector of $\angle B_1A_1C_1$ and $\angle T'A_1C_1 = 30^\circ$.

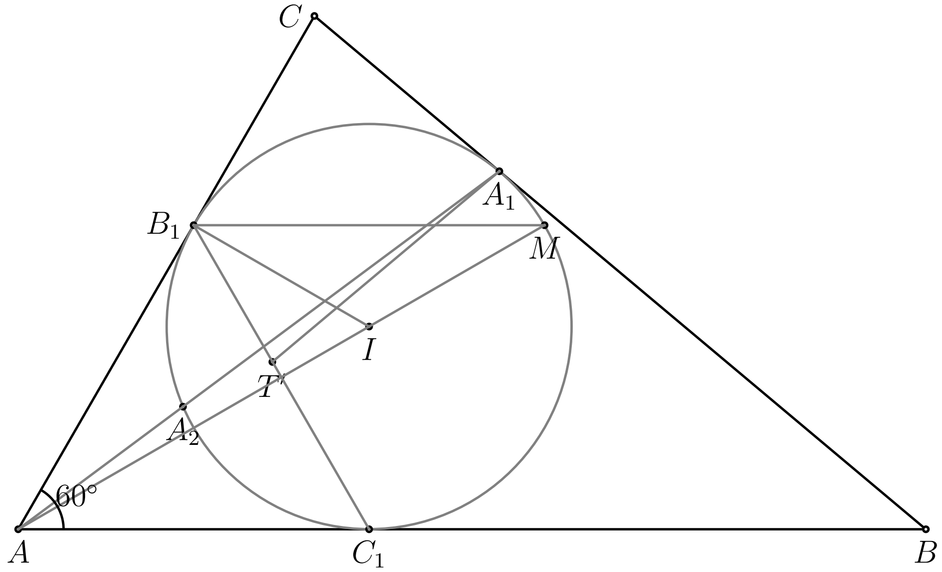
We shall show that $T' \equiv T$ and the problem is solved. We have

$$\angle B_1A_2M = \angle MA_2C_1 = \angle T'B_1M \Rightarrow$$
$$\triangle MB_1A_2 \sim \triangle MTB_1 \Rightarrow$$
$$\frac{MB_1}{MT'} = \frac{MA_2}{MB_1} \Rightarrow MB_1^2 = MT' \cdot MA_2.$$

Since $I \in AM$, then from $\angle IB_1M = \angle IMB_1 = 30^\circ = \angle B_1AM$ it follows

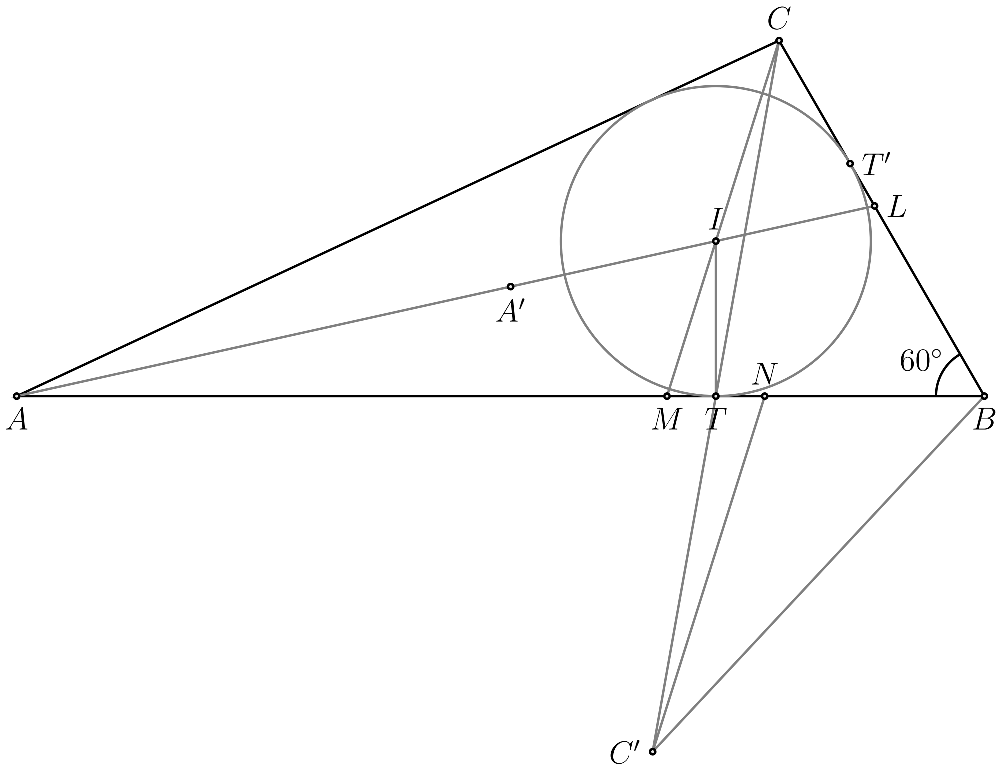
$$\triangle MB_1I \sim \triangle MAB_1 \Rightarrow MI \cdot MA = MB_1^2 = MT' \cdot MA_2$$

and therefore A, A_2, I, T' lie on a circle, from where $T' \equiv T$. Final answer: 30° $\square$



Solution G6. Let I be the center of the inscribed circle in $\triangle ABC$, and let it touch BC at T'. Let $L = AI \cap BC$ and $M = CI \cap AB$. Then we shall show that $BL + BM = 2BT$. Indeed, $\angle IMB + \angle ILB = \angle A + \frac{1}{2}\angle C + \angle C + \frac{1}{2}\angle A = \frac{3}{2}(\angle A + \angle C) = 180^\circ$ since $\angle A + \angle C = 180^\circ - \angle B = 120^\circ$. Furthermore, $BM > BT \iff BL < BT' = BT$. Then the right triangles $\triangle IMT$ and $\triangle ILT'$ are identical, since they have the same angles and since $IT = IT'$ (being the radius of the incircle). Now from $MT = LT'$ it follows that $BL + BM = 2BT$.

Let N be obtained from L by rotation by 60° about B, i.e. $N \in AB$ and $BN = BL$. Then $MT = TN$ and $CMCN$ is a parallelogram. So $\angle BNC = 180^\circ - \angle BMC = \angle BLA$. Then under rotation by -60° about B the ray NC' goes into LA, hence C' goes into a point B' on AL. It is easy to see that $\triangle BC'B'$ is equilateral, hence B' lies on the perpendicular bisector of BC'. That means $B' = A'$ and so $\triangle A'BC'$ is equilateral.



Solution G7. From the noncollinearity it follows $O \notin \Gamma$, hence $n = 2m, m > 1$. Without loss of generality, we may consider that $\arg(a_i) < \arg(a_j)$ for $i < j$, where a_i is the affix of A_i, and 0 is the affix of O in the complex plane. We have $a_i + a_{i+m} = 0$, $i = 1, 2, \ldots, m$. All indices below shall be considered cyclically, i.e. $a_{-1} = a_{n-1}, a_0 = a_n, a_1 = a_{n+1}$ etc..

Consider the polygon

$$\beta = B_1 B_2 \ldots B_{2m}$$

such that $b_i = a_1 + a_2 + \cdots + a_i$. Since $B_i B_{i+1} = a_{i+1}$, the directions of the consecutive sides of β are $\arg(a_i)$ listed in increasing order. Hence at each vertex the direction changes by an angle strictly between $0°$ and $180°$. Therefore every interior angle of β is less than $180°$, so β is convex. The sides of β have lengths $OA_1, OA_2, \ldots, OA_n$, and therefore its perimeter c is larger than 7.

Let $\gamma(i, j, k)$ denote the circumcircle of $\triangle B_i B_j B_k$ for any three distinct vertices B_i, B_j, B_k of β. We shall say that a circle $\beta \subset \gamma$ when all vertices of β lie on or inside of γ. Since β is convex, that also means that the entire polygon β lies inside γ. We shall prove there is i such that $\beta \subset \gamma(i-1, i, i+1)$.

Let $i' \in [3, n]$ be the index i that minimizes $\angle B_1 B_i B_2$. Then $\beta \subset \gamma(1, i', 2)$, otherwise there would be another $i'' \in [3, n], i'' \neq i'$ for which $B_{i''}$ is outside $\gamma(1, i', 2)$, and we would have $\angle B_1 B_{i''} B_2 < \angle B_1 B_{i'} B_2$ in contradiction to the minimality of $\angle B_1 B_{i'} B_2$.

Let us consider the set Φ of all triples (i, p, q) where $\beta \subset \gamma(i-p, i, i+q)$ with $1 \le i \le n$, $1 \le p, q$, and $p + q \le n - 1$. We saw earlier that $(2, 1, i' - 2) \in \Phi$, so $\Phi \neq \emptyset$. Let us assume that we have chosen the $(i, p, q) \in \Phi$ for which $p + q$ is minimal (or one of them if there are several).

We shall prove that $p + q \le 2$. Assume the contrary, so $p + q \ge 3$, hence either $p \ge 2$ or $q \ge 2$, i.e. there are points either between $i - p$ and i or between i and $i + q$. The two cases are symmetrical, so we only need to consider the first one, namely $p \geq 2$.

Let

$$S = \{i-p+1, i-p+2, \dots, i-1\},$$
$$T = \{i+1, i+2, \dots, i+q, \dots, i-p-1\},$$

where both intervals are understood cyclically. Thus S and T are precisely the two sets of vertices lying on the two sides of the chord $B_{i-p}B_i$ and $i+q \in T$.

Since $p \geq 2$, we have $S \neq \emptyset$. Denote

$$\gamma = \gamma(i-p, i, i+q), \qquad \alpha = \angle B_{i-p}B_{i+q}B_i.$$

For every $s \in S$ we know that B_s and B_{i+q} are on the opposite sides of line $B_{i-p}B_i$, and since $B_s \in \beta \subset \gamma$, we have $\angle B_{i-p}B_sB_i \geq 180^\circ - \alpha$, or equivalently

$$\alpha \geq 180^\circ - \angle B_{i-p}B_sB_i. \tag{*}$$

Similarly, for every $t \in T$, we know that B_t and B_{i+q} are on the same side of the line $B_{i-p}B_i$, and since $B_t \in \beta \subset \gamma$, we have

$$\angle B_{i-p}B_tB_i \geq \alpha. \tag{**}$$

Let $s' \in S$ be the s that minimizes $\angle B_{i-p}B_sB_i$. We shall show that $\beta \subset \gamma(i-p, s', i)$. Indeed, the choice of s' guarantees that

$$\angle B_{i-p}B_sB_i \geq \angle B_{i-p}B_{s'}B_i,$$

and since B_s and $B_{s'}$ are on the same side of the line $B_{i-p}B_i$, it follows that B_s is on or inside of $\gamma(i-p, s', i)$.

Likewise, for every $t \in T$, we know that B_t and $B_{s'}$ are on opposite sides of the line $B_{i-p}B_i$, and from (**) for t and (*) for s' we get

$$\angle B_{i-p}B_tB_i \geq \alpha \geq 180^\circ - \angle B_{i-p}B_{s'}B_i.$$

Therefore B_t is on or inside of $\gamma(i-p, s', i)$. That means all vertices of β lie on or inside of $\gamma(i-p, s', i)$, hence $(s', s'-(i-p), i-s') \in \Phi$. But from $s'-(i-p)+(i-s') = p < p+q$ we have obtained a new triple in Φ that contradicts the optimality of the original (i, p, q). The contradiction shows that $p \geq 2$ (and similarly $q \geq 2$) is not possible, hence $p+q \geq 3$ is not possible.

Therefore $p+q \leq 2$, hence $p = q = 1$ and $\beta \subset \gamma = \gamma(i-1, i, i+1)$.

Next, observe that the circumference of γ is greater than c. For each side B_iB_{i+1}, draw the two rays

$$B_iD_i \perp B_iB_{i+1}, \qquad B_{i+1}C_{i+1} \perp B_iB_{i+1},$$

both pointing to the exterior of β.

Since $\beta \subset \gamma$, the circle γ meets these two rays at points N_i and M_{i+1}, and the arc of γ between them is contained in the strip-like region $D_iB_iB_{i+1}C_{i+1}$.
Since β is convex, these regions are pairwise disjoint except possibly at their boundary rays, so the corresponding arcs are pairwise non-overlapping. Therefore, if r is the radius of γ,

$$2\pi r \geq \sum_{i=1}^{n} \operatorname{arc}(M_{i+1}N_i) > \sum_{i=1}^{n} M_{i+1}N_i \geq \sum_{i=1}^{n} B_iB_{i+1} = c > 7 > 2\pi.$$

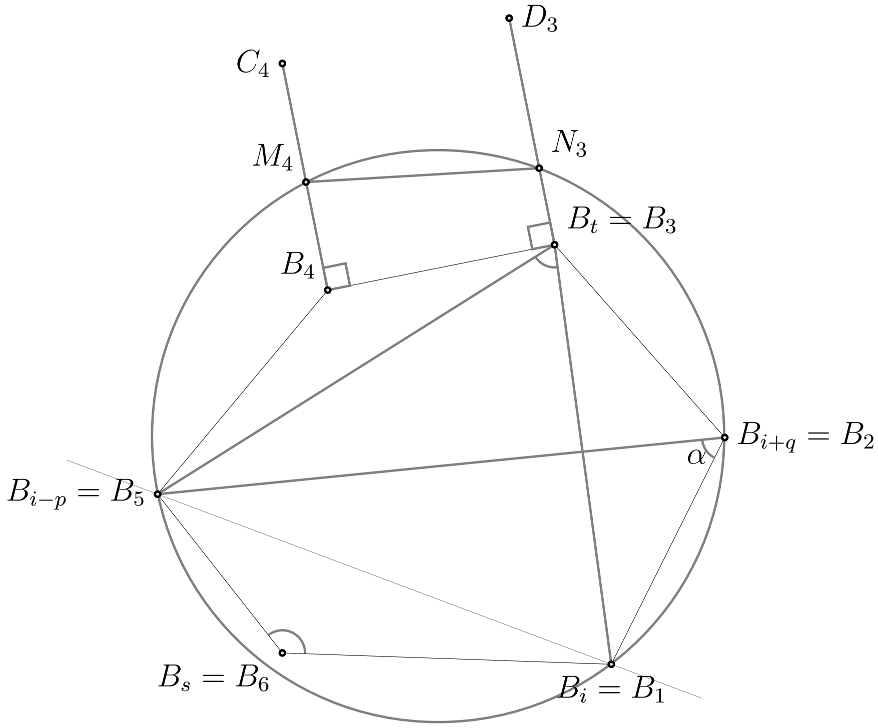
Hence $r > 1$.

Finally, for $\triangle B_{i-1}B_iB_{i+1}$ and $\triangle OA_iA_{i+m+1}$ we have

$$B_{i-1}B_i = |a_i| = OA_i,$$

$$B_iB_{i+1} = |a_{i+1}| = |a_{i+m+1}| = OA_{i+m+1},$$
$$B_{i-1}B_{i+1} = |a_i + a_{i+1}| = |a_i - a_{i+m+1}| = A_iA_{i+m+1},$$

hence the $\triangle B_{i-1}B_iB_{i+1} \equiv \triangle OA_iA_{i+m+1}$ by SSS.
Therefore the circumradius of $\triangle OA_iA_{i+m+1}$ equals $r > 1$ and the problem is solved by choosing $P = A_i, Q = A_{i+m+1}$. □



Example with $n = 6, (i, p, q) = (1, 2, 1), S = \{6\}, T = \{2, 3, 4\}, s = 6, t = 3$

Solution G8. Let $\triangle A_1B_1C_1$ denote the pedal triangle of P with respect to $\triangle ABC$, where $A_1 \in BC$, $B_1 \in CA$, $C_1 \in AB$. By the sine law, we have

$$\frac{\sin\angle PAC}{\sin\angle PCA}\cdot\frac{\sin\angle PCB}{\sin\angle PBC}\cdot\frac{\sin\angle PBA}{\sin\angle PAB} = 1 = \frac{\sin\angle QCA}{\sin\angle QAC}\cdot\frac{\sin\angle QBC}{\sin\angle QCB}\cdot\frac{\sin\angle QAB}{\sin\angle QBA}.$$

Let $x = \angle PCA = \angle PAB = \angle PBC$ and $y = \angle QBA = \angle QCB = \angle QAC$. Also, let $\alpha = \angle BAC, \beta = \angle CBA, \gamma = \angle ACB < 90°$ be the angles of $\triangle ABC$. Then x and y are two solutions to the equation $f(x) = 0$, where

$$f(x) = \sin^3 x - \sin(\alpha - x)\sin(\beta - x)\sin(\gamma - x). \qquad (*)$$

If $\mu = \min(\alpha, \beta, \gamma)$, then $f(x)$ is a continuous, strictly increasing function on $(0, \mu) \subset (0, 90°)$ and its values range from $-\sin\alpha\sin\beta\sin\gamma$ to $\sin^3\mu$. Therefore f has a unique root, so $x = y$.

Observe that the quadrilaterals PB_1AC_1 and PB_1CA_1 are cyclic, since each quadrilateral has two opposite right angles. Then

$$\angle PB_1C_1 = \angle PAC_1 = x, \qquad \angle PB_1A_1 = \angle PCB = \gamma - x,$$

hence $\angle C_1B_1A_1 = \gamma = \angle ACB$. Similarly, $\angle A_1C_1B_1 = \angle BAC = \alpha$, so the triangles $\triangle ABC$ and $\triangle C_1A_1B_1$ are similar and similarly oriented. Then there exists a spiral similarity ρ_1 centered at P mapping $A_1 \to B$, $B_1 \to C$, $C_1 \to A$ respectively. Since $\rho_1(B_1) = C$, we see that the angle of ρ_1 is $\angle B_1PC = 90° - x$ and its coefficient is $CP/B_1P = 1/\sin x$.

Analogously, let $\triangle A_2B_2C_2$ be the pedal triangle of Q with respect to $\triangle ABC$, where $A_2 \in BC$, $B_2 \in CA$, $C_2 \in AB$. By the earlier argument, there exists a spiral similarity ρ_2 with center Q, angle $90° - x$ and coefficient $\sin(x)$, mapping $\triangle ABC$ to $\triangle B_2C_2A_2$.

Since the coefficient of $\rho_2\rho_1$ equals the product of the coefficients of ρ_1 and ρ_2, which is 1, it follows that $\rho = \rho_2\rho_1$ is a rotation that maps $\triangle C_1A_1B_1$ to $\triangle B_2C_2A_2$.

Let O' be the midpoint of PQ and $S = \rho_1(O')$. Since ρ_1 has center P, coefficient $1/\sin(x)$, and angle $90° - x$, we have $PS = PO'/\sin(x)$ and $\angle O'PS = 90° - x$. If K is the projection of S onto PQ, we have $\angle O'PS = 90° - x$, so

$$PK = PS\cos(90° - x) = PS\sin x = PO'.$$

Hence $K = O'$, so $SO' \perp PQ$. Therefore S lies on the perpendicular bisector of PQ, and thus $PS = QS$. Therefore $\rho_2(S) = O'$, consequently $\rho(O') = O'$ and O' is the center of ρ. Since

$$\rho(C_1) = B_2, \qquad \rho(A_1) = C_2, \qquad \rho(B_1) = A_2,$$

then

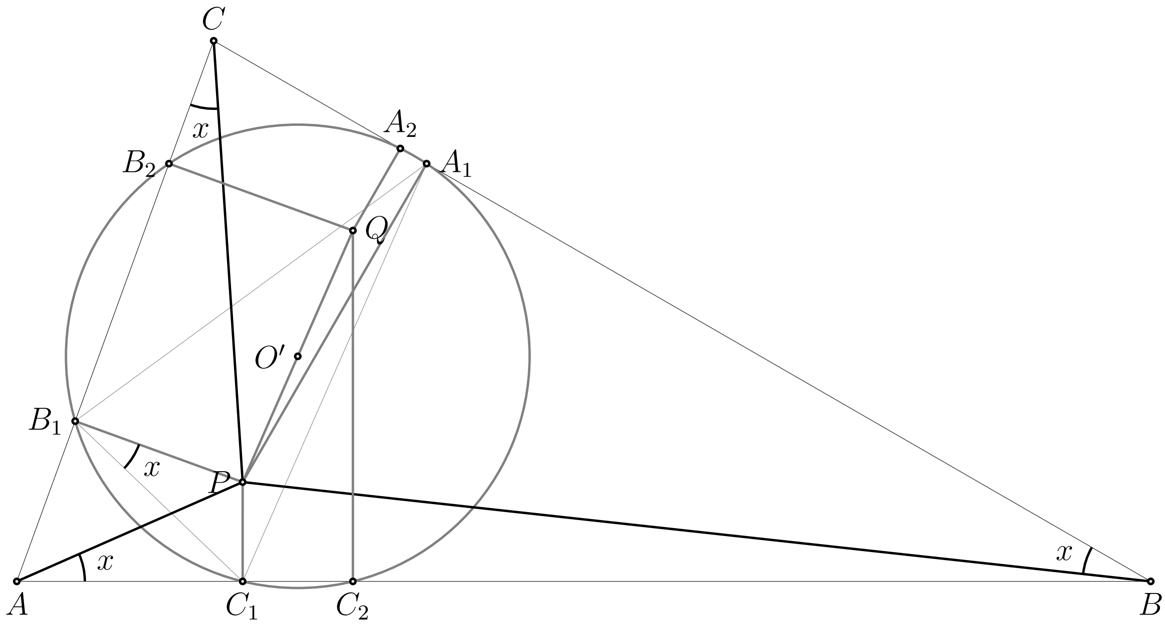
$$O'C_1 = O'B_2, \qquad O'A_1 = O'C_2, \qquad O'B_1 = O'A_2. \tag{**}$$

At the same time, since $PC_1 \perp AB$ and $QC_2 \perp AB$, both P and Q project onto AB at C_1 and C_2 respectively. Hence the midpoint O' of PQ lies on the perpendicular bisector of C_1C_2 and so $O'C_1 = O'C_2$. Analogously, $O'A_1 = O'A_2$. Combined with (**), that yields

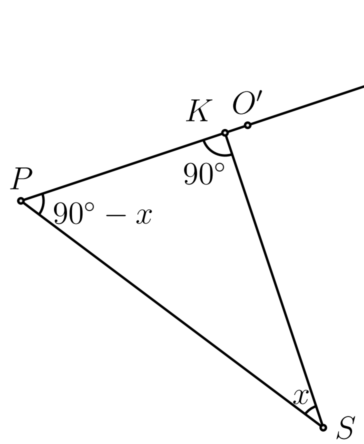
$$O'B_2 = O'C_1 = O'C_2 = O'A_1 = O'A_2 = O'B_1,$$

hence O' is the circumcenter of the hexagon $C_1A_1B_2C_2B_1A_2$ and (a) is proved.

To prove (b), let us note that since O' is the circumcenter of $\triangle C_1A_1B_1$, its image under ρ_1 is the circumcenter of $\triangle ABC$, hence $S = \rho_1(O') = O$. From $PS = QS$ we obtain $PO = QO$ and the problem is solved. $\square$



C
x
A_2
B_2
A_1
Q
O'
B_1
x
P
x
x
A
C_1
C_2
B



Q
K
O'
P
90°
90° − x
x
S

Various problems

Abstract

These are problems that are not suitable for competitions for one reason or another, yet they are interesting in their own right.

1 Problem statements

Problem 1. Let

$$x_n = \underbrace{\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}}_{n \text{ square roots}},$$

for $n \geq 1$. Prove that

$$\lim_{n\to\infty} 4^{n+1}(2-x_n) = \pi^2.$$

Problem 2. Does there exist a coloring of the vertices of a regular polygon in more than one color such that:

1. each color class is the vertex set of a regular polygon; and
2. the union of any two or more congruent monochromatic polygons is *not* the vertex set of a regular polygon?

For clarity, a pair of opposite vertices is regarded as a regular 2-gon, whereas a single vertex is not permitted as a regular 1-gon.

Problem 3. Given $2n$ distinct numbers, we want to partition them into n pairs so that the largest pair sum is as small as possible. Prove that the following pairing provides an optimal solution (though not necessarily the unique one): pair the smallest with the largest, the second smallest with the second largest, etc.

Problem 4. Let $n \geq 3$, and let $A_1A_2\cdots A_n$ be a regular polygon of side length 1. Prove that, for any subset of

$$\left\{\overrightarrow{A_1A_2}, \overrightarrow{A_2A_3}, \ldots, \overrightarrow{A_{n-1}A_n}\right\},$$

the length of the sum of its vectors is less than

$$\frac{\pi}{n} + \frac{n}{\pi}.$$

Problem 5. Let $\triangle ABC$ be a triangle. Let M be the midpoint of AB, H the foot of the perpendicular from C to AB, T the point of tangency of the incircle with AB, and I the incenter. If

$$AT \cdot BT = 3IT^2,$$

prove that T is the midpoint of MH.

Problem 6. Let $ABCD$ be a convex quadrilateral circumscribed about a circle with center O. Prove that

$$\frac{AB}{AO} \cdot \frac{BC}{BO} \cdot \frac{CD}{CO} \cdot \frac{DA}{DO} \geq 4.$$

Determine when equality occurs.

2 Solutions

Solution 1. For convenience, define $x_0 = 0$. Then

$$x_{n+1} = \sqrt{2 + x_n}$$

for $n \geq 0$. Define

$$\alpha_n = \frac{\pi}{2^{n+2}}.$$

We claim that

$$x_n = 2 - 4\sin^2 \alpha_n$$

for all $n \geq 0$. For $n = 0$,

$$x_0 = 0 = 2 - 4\sin^2 \frac{\pi}{4} = 2 - 4\sin^2 \alpha_0.$$

Now assume the formula holds for some n. Then

$$\begin{aligned} x_{n+1} &= \sqrt{2 + x_n} = \sqrt{2 + 2 - 4\sin^2(\alpha_n)} = 2\cos\alpha_n \\ &= 2\cos(2\alpha_{n+1}) = 2\left(\cos^2\alpha_{n+1} - \sin^2\alpha_{n+1}\right) \\ &= 2 - 4\sin^2\alpha_{n+1}, \end{aligned}$$

which completes the induction. Therefore,

$$\begin{aligned} 4^{n+1}(2 - x_n) = 2^{2n+2}4\sin^2(\alpha_n) &= \frac{\pi^2}{\alpha_n^2}\sin^2\alpha_n \\ &= \pi^2\left(\frac{\sin\alpha_n}{\alpha_n}\right)^2 \to \pi^2 \end{aligned}$$

as $n \to \infty$ and $\alpha_n \to 0$. $\square$

Solution 2. Yes, such a coloring exists. Let $n = 60$ and consider a regular n-gon with vertices labeled $0, 1, \ldots, n-1$. The vertices of any regular d-gon among the vertices of this regular n-gon can be described as

$$\{a + (n/d)i \mid 0 \leq i \leq d-1\}$$

for some $0 \leq a \leq n/d - 1$. A necessary condition is $d \mid n$.

Now let us color the n vertices so that the color classes are exactly the following sets.

- Decagons: $P_j = \{a_j + 6i \mid 0 \leq i \leq 9\}$ for $a_j = 0, 2$.
- Hexagons: $P_j = \{a_j + 10i \mid 0 \leq i \leq 5\}$ for $a_j = 1, 3, 5, 7$.
- Squares: $P_j = \{a_j + 15i \mid 0 \leq i \leq 3\}$ for $a_j = 4$.
- 2-gons: $P_j = \{a_j + 30i \mid i = 0, 1\}$ for $a_j = 9, 10, 16, 22, 28, 29$.

It is tedious but straightforward to verify that these sets form a partition of the n vertices, so the first condition is satisfied. What remains is to show that the second condition is satisfied.

Observe the following: if the union of m d-gons described as

$$P_j = \{a_j + (n/d)i \mid 0 \le i \le d-1\}, j = 0, 1, \ldots, m-1$$

is a regular polygon, it must be a md-gon described as

$$\{a + (n/md)i \mid 0 \le i \le md - 1\}$$

for some $0 \le a \le n/md - 1$. Since both $\{a_0, a_1, \ldots, a_{m-1}\}$ and $\{a + (n/md)i \mid 0 \le i \le m-1\}$ are sets of m distinct integers between 0 and $n/d - 1$, we must have

$$\{a_0, a_1, \ldots, a_{m-1}\} = \{a + (n/md)i \mid 0 \le i \le m-1\}.$$

In other words, the set $\{a_0, a_1, \ldots, a_{m-1}\}$ must be an arithmetic progression with common difference n/md.

Now, consider each congruence class with more than one member:

First, consider the two decagons with $d = 10$. Their union has $m = 2$, and $\{a_0, a_1\} = \{0, 2\}$ which is not an arithmetic progression with common difference $n/md = 3$, hence it is not a regular polygon.

Next, consider the four hexagons with $d = 6$. If a union of m of them were a regular md-gon, we would have $m \mid n/d = 10$ and $2 \le m \le 4$, hence $m = 2$. Furthermore, the a_j would need to be an arithmetic progression with common difference $n/md = 5$, but no two elements of $\{1, 3, 5, 7\}$ have a difference of 5. Therefore, the union could not be a regular polygon.

Finally, consider the six 2-gons with $d = 2$. If a union of m of them were a regular md-gon, we would need $m \mid n/d = 30$ and $2 \le m \le 6$, so $m \in \{2, 3, 5, 6\}$. Examine each possibility.

- For $m = 2$, we would need two a_j among $9, 10, 16, 22, 28, 29$ with common difference $n/md = 15$, but no such exist.
- For $m = 3$, we would need three a_j with common difference $n/md = 10$, but no such exist.
- For $m = 5$, we would need five a_j with common difference $n/md = 6$, but no such set exists (though there is a set of 4 such a_j).
- For $m = 6$, we would need all six a_j to be an arithmetic progression with common difference $n/md = 5$, which is not the case.

That shows that the union of any two or more monochromatic polygons from the same congruence class is not a regular polygon, hence condition 2 is also satisfied. $\square$

Solution 3. Let the $2n$ numbers be

$$a_1 < a_2 < \cdots < a_{2n}.$$

For every partition G into pairs

$$(a_{i_1}, a_{j_1}), (a_{i_2}, a_{j_2}), \ldots, (a_{i_n}, a_{j_n}),$$

define

$$f(G) = \max_{1\le k\le n}(a_{i_k} + a_{j_k}), \qquad s(G) = \sum_{k=1}^{n} i_k j_k.$$

Let G^* be the pairing described in the statement, i.e.

$$G^* = (a_1, a_{2n}), (a_2, a_{2n-1}), \ldots, (a_n, a_{n+1}).$$

We shall show that, starting from any pairing $G_0 \neq G^*$, we can successively swap two numbers from two pairs at each step, so that the resulting sequence of pairings $G_1, G_2, \ldots, G_m = G^*$ satisfies:

$$f(G_0) \ge f(G_1) \ge \cdots \ge f(G_m) = f(G^*),$$

$$s(G_0) > s(G_1) > \cdots > s(G_m).$$

This automatically proves the optimality of $f(G^*)$.

Let k be the minimal positive integer for which a_k is not paired with a_{2n+1-k}. Such k necessarily exists, since $G_0 \neq G^*$. For brevity, let $u = 2n + 1 - k$. Given that $a_1, a_2, \ldots, a_{k-1}$ are already paired with $a_{2n}, a_{2n-1}, \ldots, a_{u+1}$, and that a_k is not paired with a_u, two things follow:

- a_k is paired with some a_j where $k < j < u$;
- a_u is paired with some a_i where $k < i < u$.

Let us take the pairs (a_k, a_j) and (a_i, a_u) and swap a_j with a_u, obtaining the pairs (a_k, a_u) and (a_i, a_j). This new pairing G_1 differs from G_0 in only those two pairs, so we only need to examine how f and s change for these two pairs. From $a_i > a_k$ and $a_u > a_j$ we have

$$a_i + a_u > \begin{cases} a_k + a_u \\ a_i + a_j \end{cases},$$

so

$$\max(a_k + a_j, a_i + a_u) = a_i + a_u > \max(a_k + a_u, a_i + a_j),$$

hence $f(G_0) \ge f(G_1)$, since outside those two pairs, nothing changes. At the same time,

$$s(G_0) - s(G_1) = (kj + iu) - (ku + ij) = (u - j)(i - k) > 0.$$

Similarly, if $G_1 \neq G^*$, we repeat the procedure and get G_2 with $f(G_1) \ge f(G_2)$ and $s(G_1) > s(G_2)$ and so on. Now, $s(G_0), s(G_1), \ldots$ is a strictly decreasing sequence of positive integers, so the process terminates after finitely many steps. But the only way for it to terminate is if $G_m = G^*$. This completes the proof. $\square$

Solution 4. Let $k = \lfloor n/2 \rfloor$, and let γ, R, O be the circumcircle, circumradius, and circumcenter of the polygon. If $\alpha = \pi/n$, from $\triangle OA_1A_2$ with $\angle A_1OA_2 = 2\alpha$, we have

$$R = \frac{1}{2\sin\alpha}.$$

Let

$$A = \{a_i = \overrightarrow{A_iA_{i+1}} \mid i = 1, 2, \ldots, n\},$$

where the index i runs cyclically on n. For any set of vectors, we call the length of its sum the sum-length. The objective is to determine the maximum sum-length among subsets of A. Though the problem statement explicitly excludes a_n, we can include it for symmetry without changing the result. Indeed, the sum-length of A is 0 and for any $A' \subseteq A$ with $a_n \in A'$ its complement $A'' = A \setminus A'$ has the same sum-length.

First, we shall show that

$$A_1A_{k+1} < \frac{\pi}{n} + \frac{n}{\pi},$$

and then we shall prove that the set

$$\{a_1, a_2, \dots, a_k\},$$

whose sum-length is A_1A_{k+1}, has the maximal sum-length. These two claims together complete the proof.

To prove the upper bound for A_1A_{k+1}, consider $\triangle A_1OA_{k+1}$, where

$$A_1A_{k+1} = 2R\sin(\angle A_1OA_{k+1}/2) = 2R\cos(\angle A_1A_{k+1}O).$$

We have

$$\angle A_1A_{k+1}O = \begin{cases} 0 & \text{for even } n \\ \alpha/2 & \text{for odd } n \end{cases}.$$

Therefore, for even n:

$$A_1A_{k+1} = 2R = \frac{1}{\sin\alpha},$$

and for odd n:

$$A_1A_{k+1} = 2R\cos(\alpha/2) = \frac{\cos(\alpha/2)}{\sin\alpha}.$$

Since $\cos(\alpha/2) \le 1$, in either case,

$$A_1A_{k+1} \le \frac{1}{\sin\alpha}.$$

Notice that A_1A_{k+1} has maximal possible length among the chords determined by the vertices of the polygon, as $\angle A_1OA_{k+1}$ is maximal among the central angles subtending such chords.

Now, using the Taylor expansion for $\sin\alpha$, and since $\alpha = \pi/n \in (0,2)$, we have

$$\sin\alpha = \alpha - \frac{\alpha^3}{3!} + \sum_{i\ge 3}\left(\frac{\alpha^{2i-1}}{(2i-1)!} - \frac{\alpha^{2i+1}}{(2i+1)!}\right) > \alpha - \frac{\alpha^3}{6},$$

since for $\alpha \in (0,2)$ each bracketed summand is positive. Therefore, using $\alpha^2 < 5$,

$$A_1A_{k+1} \le \frac{1}{\sin\alpha} < \frac{1}{\alpha - \alpha^3/6} < \alpha + \frac{1}{\alpha} = \frac{\pi}{n} + \frac{n}{\pi},$$

which is what we wanted.

What remains is to prove that A_1A_{k+1} is the maximum obtainable sum-length. Assume the contrary, and let $B \subseteq A$ be a subset with maximal sum-length. If $b = \sum_{a\in B} a$, then

$$|b| > A_1A_{k+1}.$$

Let ϕ_i be the angle between a_i and b for $i = 1, 2, \dots, n$ and

$$\Phi = (\phi_i \mid 1 \leq i \leq n) = (\xi + 2i\alpha \mid 1 \leq i \leq n)$$

where $\xi = \phi_n$, and each $\xi + 2i\alpha$ is taken modulo 2π.

Now, observe that for every $a_i \in B$ we must have $|b| \geq |b - a_i|$, else we could remove a_i from B and get an even longer sum-length. Thus

$$|b|^2 \geq |b - a_i|^2 = |a_i|^2 - 2a_i \cdot b + |b|^2 = 1 - 2|b|\cos\phi_i + |b|^2$$

$$\Rightarrow 2|b|\cos\phi_i \geq 1 \Rightarrow \cos\phi_i \geq \frac{1}{2|b|} > 0$$

$$\Rightarrow \phi_i \notin \Delta_1 = \left[\frac{\pi}{2}, \frac{3\pi}{2}\right].$$

Therefore, for any $1 \leq i \leq n$, we must have

$$\phi_i \in \Delta_1 \Rightarrow a_i \notin B. \tag{*}$$

Likewise, for any $a_i \in A \setminus B$ we must have $|b| \geq |b + a_i|$, else we could add a_i to B and get a strictly larger sum-length. Thus

$$|b|^2 \geq |b + a_i|^2 = |a_i|^2 + 2a_i \cdot b + |b|^2 = 1 + 2|b|\cos\phi_i + |b|^2$$

$$\Rightarrow -1 \geq 2|b|\cos\phi_i \Rightarrow \cos\phi_i \leq \frac{-1}{2|b|} < 0$$

$$\Rightarrow \phi_i \notin \Delta_2 = \left[0, \frac{\pi}{2}\right] \cup \left[\frac{3\pi}{2}, 2\pi\right).$$

Therefore, for any $1 \leq i \leq n$, we must have

$$\phi_i \in \Delta_2 \Rightarrow a_i \in B. \tag{**}$$

When viewed modulo 2π, both Δ_1 and Δ_2 are connected arcs on the circle. Since $\Delta_1 \cup \Delta_2 = [0, 2\pi)$, every element $\phi_i \in \Phi$ must fall in either Δ_1 or Δ_2. No element ϕ_i can belong to both, otherwise its corresponding a_i would have to both belong to B and not belong to B, which is impossible. Since the ϕ_i are cyclically ordered, the elements of Φ lying in each of the arcs Δ_1 and Δ_2 form a cyclically consecutive block. Thus:

- the elements $\phi_i \in \Delta_1$ form a cyclically consecutive block, and by (*) their corresponding vectors satisfy $a_i \notin B$;
- the elements $\phi_i \in \Delta_2$ form a cyclically consecutive block, and by (**) their corresponding vectors satisfy $a_i \in B$.

Since every element of Φ lies in exactly one of Δ_1 and Δ_2, these two blocks together exhaust all elements of Φ. Hence the elements of B form one cyclically consecutive block, and therefore b is a chord, i.e.

$$b = \overrightarrow{A_i A_j}$$

for some i and j. But as $A_1 A_{k+1}$ is the longest of all chords, we get $|b| \leq A_1 A_{k+1}$, a contradiction with the assumption that $A_1 A_{k+1}$ is not the maximal sum-length. $\square$

Solution 5. In $\triangle ABC$, let $\alpha = \frac{\angle A}{2}, \beta = \frac{\angle B}{2}, \gamma = \frac{\angle C}{2}$. Let R and $r = IT$ be the circumradius and inradius respectively. From the right triangles $\triangle AIT$ and $\triangle BIT$ we have

$$\frac{1}{3} = \frac{IT}{AT} \cdot \frac{IT}{BT} = \tan\alpha\tan\beta,$$

and our objective is to prove that $AT = (AM + AH)/2$, where AM, AH, AT denote directed lengths along the oriented line AB from A toward B. Using the fact that each side equals $2R$ times the sine of its opposite angle and that the ratio of r to R is $4\sin\alpha\sin\beta\sin\gamma$, we have

$$\begin{aligned} AM &= \frac{AB}{2} = R\sin(2\gamma) = R\sin(2\alpha+2\beta), \\ AH &= AC\cos(2\alpha) = 2R\sin(2\beta)\cos(2\alpha), \\ AT &= r\cot\alpha = 4R\cos\alpha\sin\beta\sin\gamma. \end{aligned}$$

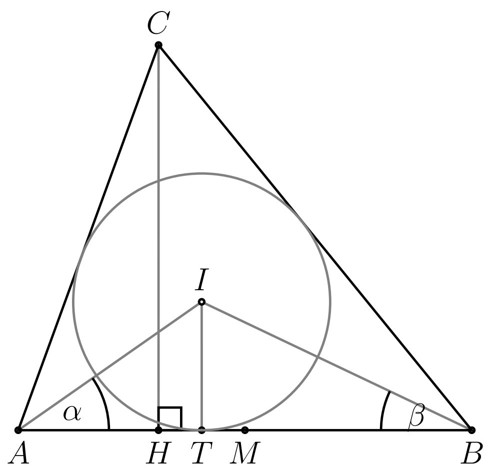
Substituting the expressions above into $AT = \frac{AM+AH}{2}$, we need to prove that

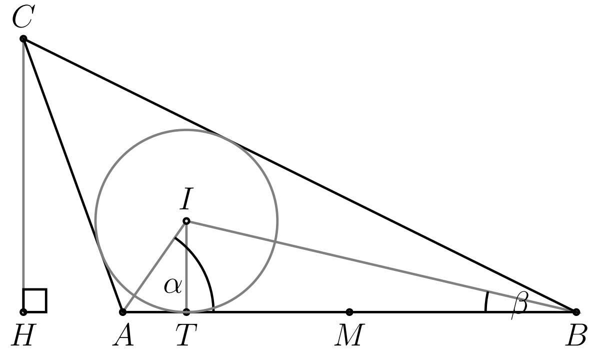
$$4R\cos\alpha\sin\beta\sin\gamma = \frac{R\sin(2\alpha+2\beta) + 2R\sin(2\beta)\cos(2\alpha)}{2}.$$

After cancelling R, it remains to prove that

$$\begin{aligned} 0 &= 4\cos\alpha\sin\beta\sin\gamma - \frac{\sin(2\alpha+2\beta) + 2\sin(2\beta)\cos(2\alpha)}{2} \\ &= 4\cos\alpha\sin\beta\cos(\alpha+\beta) - \sin(\alpha+\beta)\cos(\alpha+\beta) - \sin(2\beta)\cos(2\alpha) \\ &= \cos(\alpha+\beta)\big(4\cos\alpha\sin\beta - \sin(\alpha+\beta)\big) - \sin(2\beta)\cos(2\alpha) \\ &= \cos(\alpha+\beta)\big(3\cos\alpha\sin\beta - \sin\alpha\cos\beta\big) - 2\sin\beta\cos\beta\cos(2\alpha) \\ &= \cos^2\alpha\cos^2\beta\left((1-\tan\alpha\tan\beta)(3\tan\beta-\tan\alpha) - 2\tan\beta\left(1-\tan^2\alpha\right)\right) \\ &= \cos^2\alpha\cos^2\beta\left(\tan\beta - \tan\alpha + 3\tan\alpha\tan\beta(\tan\alpha-\tan\beta)\right) \\ &= \cos^2\alpha\cos^2\beta(\tan\beta-\tan\alpha)(1-3\tan\alpha\tan\beta) \\ &= 0 \end{aligned}$$

using the fact that $\tan\alpha\tan\beta = \dfrac{1}{3}$. Thus $AT = \dfrac{AM+AH}{2}$ so T is the midpoint of MH. $\square$





Solution 6. Let $\alpha = \frac{\angle A}{2}, \beta = \frac{\angle B}{2}, \gamma = \frac{\angle C}{2}, \delta = \frac{\angle D}{2}$, so that $\alpha + \beta + \gamma + \delta = 180°$. Let $\Omega = (0°, 90°)$. Since $ABCD$ is convex, we have

$$\alpha, \beta, \gamma, \delta \in \Omega.$$

Conversely, any four numbers $\alpha, \beta, \gamma, \delta \in \Omega$ that sum to $180°$ produce a circumscribed convex quadrilateral $ABCD$ with angles $2\alpha, 2\beta, 2\gamma, 2\delta$, obtained from the intersections of four lines tangent to the circle at four points such that consecutive pairs subtend the central angles $180° - 2\alpha, 180° - 2\beta, 180° - 2\gamma, 180° - 2\delta$. This observation will be used later when we consider the equality case.

Since OA and OB are angle bisectors of $\angle A$ and $\angle B$, we have $\angle OAB = \alpha$ and $\angle OBA = \beta$. Hence, by the sine rule in $\triangle AOB$, we get

$$\frac{AB}{AO} = \frac{\sin(\alpha + \beta)}{\sin \beta},$$

and cyclically

$$\frac{BC}{BO} = \frac{\sin(\beta + \gamma)}{\sin \gamma}, \quad \frac{CD}{CO} = \frac{\sin(\gamma + \delta)}{\sin \delta}, \quad \frac{DA}{DO} = \frac{\sin(\delta + \alpha)}{\sin \alpha}.$$

Thus it remains to prove that

$$\frac{AB}{AO} \cdot \frac{BC}{BO} \cdot \frac{CD}{CO} \cdot \frac{DA}{DO} = \frac{\sin(\alpha + \beta)}{\sin \beta} \frac{\sin(\beta + \gamma)}{\sin \gamma} \frac{\sin(\gamma + \delta)}{\sin \delta} \frac{\sin(\delta + \alpha)}{\sin \alpha} \geq 4. \tag{*}$$

Notice that all the sines are positive owing to the fact that $\alpha, \beta, \gamma, \delta$ are in Ω.

Next, on an auxiliary circle with diameter d and center Q, choose four consecutive points A', B', C', D' so that

$$\angle A'QB' = 2\alpha, \quad \angle B'QC' = 2\beta, \quad \angle C'QD' = 2\gamma, \quad \angle D'QA' = 2\delta.$$

This is possible because $2\alpha + 2\beta + 2\gamma + 2\delta = 360°$. Since a chord subtending a central angle 2θ has length $d \sin \theta$, we have

$$A'B' = d \sin \alpha, \quad B'C' = d \sin \beta, \quad C'D' = d \sin \gamma, \quad D'A' = d \sin \delta.$$

Similarly, the diagonals have lengths

$$A'C' = d \sin(\alpha + \beta), \quad B'D' = d \sin(\beta + \gamma).$$

Applying Ptolemy's theorem to the cyclic quadrilateral $A'B'C'D'$, we get

$$A'C' \cdot B'D' = A'B' \cdot C'D' + B'C' \cdot D'A'.$$

Substituting the chord lengths and cancelling d^2, we obtain

$$\sin(\alpha + \beta) \sin(\beta + \gamma) = \sin \alpha \sin \gamma + \sin \beta \sin \delta \geq 2\sqrt{\sin \alpha \sin \gamma \sin \beta \sin \delta},$$

with equality if and only if

$$\sin \alpha \sin \gamma = \sin \beta \sin \delta. \tag{**}$$

By the same argument, after a cyclic permutation of $\alpha, \beta, \gamma, \delta$, we have

$$\sin(\gamma + \delta) \sin(\delta + \alpha) = \sin \gamma \sin \alpha + \sin \delta \sin \beta \geq 2\sqrt{\sin \gamma \sin \alpha \sin \delta \sin \beta},$$

with equality if and only if $\sin\alpha\sin\gamma = \sin\beta\sin\delta$. Thus the equality condition here is exactly the same as (**), so no additional restriction is imposed.

Multiplying the last two inequalities, we get

$$\sin(\alpha+\beta)\sin(\beta+\gamma)\sin(\gamma+\delta)\sin(\delta+\alpha) \geq 4\sin\alpha\sin\beta\sin\gamma\sin\delta,$$

which is exactly (*). Hence

$$\frac{AB}{AO}\cdot\frac{BC}{BO}\cdot\frac{CD}{CO}\cdot\frac{DA}{DO} \geq 4.$$

Equality condition Equality holds if and only if (**) holds. Using the sine rule again in $\triangle AOB$ and $\triangle COD$, we have

$$\frac{BO}{AO} = \frac{\sin\alpha}{\sin\beta}, \qquad \frac{DO}{CO} = \frac{\sin\gamma}{\sin\delta}.$$

Therefore

$$(**) \iff \frac{\sin\alpha}{\sin\beta}\frac{\sin\gamma}{\sin\delta} = 1 \iff \frac{BO}{AO}\cdot\frac{DO}{CO} = 1 \iff AO\cdot CO = BO\cdot DO.$$

This gives a convenient geometric description of the equality condition, but to explore the family of solutions, we return to the trigonometric expression. We have

$$\begin{aligned}
\sin\alpha\sin\gamma &= \sin\beta\sin\delta = \sin\beta\sin(\alpha+\beta+\gamma)\\
&= \sin\beta(\sin(\alpha+\beta)\cos\gamma + \cos(\alpha+\beta)\sin\gamma)\\
\Leftrightarrow \sin\alpha &= \sin\beta(\sin(\alpha+\beta)\cot\gamma + \cos(\alpha+\beta))\\
\Leftrightarrow \frac{\sin\alpha}{\sin\beta} &= \sin(\alpha+\beta)\cot\gamma + \cos(\alpha+\beta)\\
\Leftrightarrow \cot\gamma &= \frac{\frac{\sin\alpha}{\sin\beta} - \cos(\alpha+\beta)}{\sin(\alpha+\beta)} \qquad (***)
\end{aligned}$$

Since cot is a bijection from Ω to $(0,\infty)$, the equation (***) has a solution $\gamma\in\Omega$ for every $\alpha,\beta\in\Omega$ such that the right-hand side is positive. Since $\sin(\alpha+\beta) > 0$, this is equivalent to

$$\begin{aligned}
&\frac{\sin\alpha}{\sin\beta} - \cos(\alpha+\beta) > 0\\
&\Leftrightarrow \sin\alpha > \sin\beta(\cos\alpha\cos\beta - \sin\alpha\sin\beta)\\
&\Leftrightarrow 1 > \sin\beta\cos\beta\cot\alpha - \sin^2\beta\\
&\Leftrightarrow \frac{\cos^2\beta + 2\sin^2\beta}{\sin\beta\cos\beta} > \cot\alpha\\
&\Leftrightarrow \alpha > \operatorname{arccot}(\cot\beta + 2\tan\beta),
\end{aligned}$$

since cot is a decreasing function on Ω. Here arccot denotes the inverse of cot on Ω. This is the lower bound on α in terms of β. The last angle δ is given by $180^\circ - (\alpha+\beta+\gamma)$.

Next, in (***) we interchange α and β, and γ and δ to get

$$\cot\delta = \frac{\frac{\sin\beta}{\sin\alpha} - \cos(\beta+\alpha)}{\sin(\beta+\alpha)}. \qquad (****)$$

As before, $\delta \in \Omega$ translates to a lower bound on β in terms of α:

$$\beta > \operatorname{arccot}(\cot \alpha + 2 \tan \alpha).$$

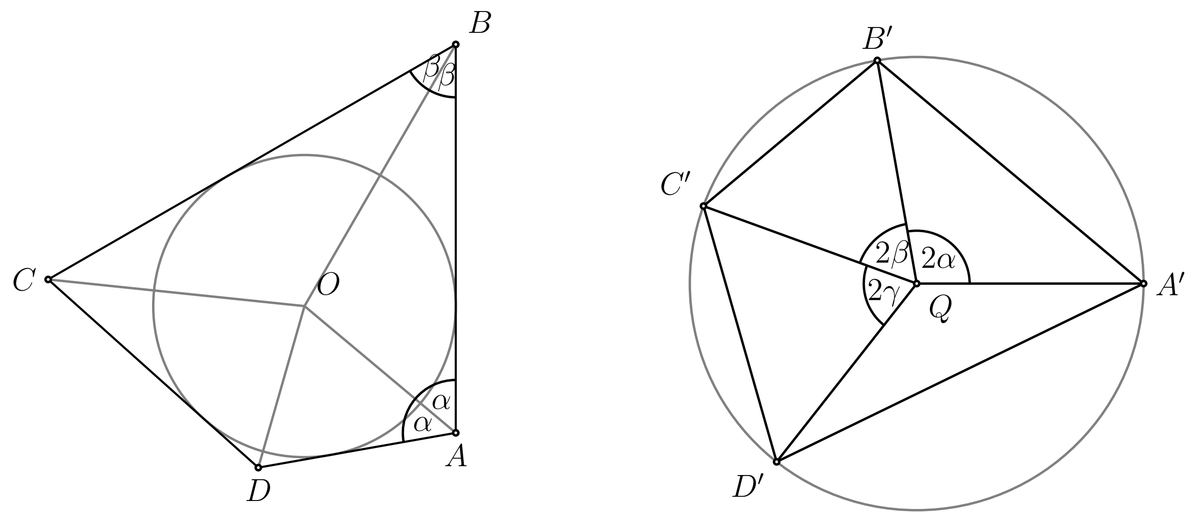
We are ready to describe the entire collection of quadrilaterals for which equality is achieved. Remember that the necessary and sufficient conditions are $\alpha, \beta, \gamma, \delta \in \Omega$ and $\alpha + \beta + \gamma + \delta = 180°$.

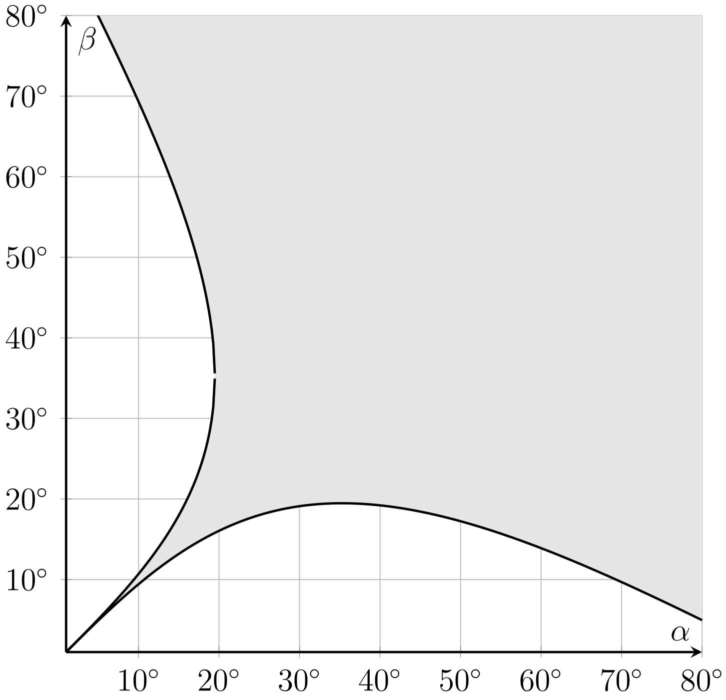
- Take any $\alpha, \beta \in \Omega$ for which $\alpha > \operatorname{arccot}(\cot \beta + 2 \tan \beta)$ and $\beta > \operatorname{arccot}(\cot \alpha + 2 \tan \alpha)$. See the graph at the end for a visual representation of that region.
- Compute γ from (***) and set $\delta = 180° - (\alpha + \beta + \gamma)$ (or compute δ from (****) and define $\gamma = 180° - (\alpha + \beta + \delta)$).

The resulting quadruple meets the required conditions to form a convex circumscribed quadrilateral for which

$$\frac{AB}{AO} \cdot \frac{BC}{BO} \cdot \frac{CD}{CO} \cdot \frac{DA}{DO} = 4.$$

Since all these conditions are necessary and sufficient, this construction exhausts all possible cases. Some notable examples of quadrilaterals in that family include the trapezoids corresponding to $(\alpha, \alpha, 90° - \alpha, 90° - \alpha)$ for any $\alpha \in \Omega$, one example of which is the square $(45°, 45°, 45°, 45°)$. $\square$




80°
70°
60°
50°
40°
30°
20°
10°
β
α
10°
20°
30°
40°
50°
60°
70°
80°

Sums of sets

Abstract

This article is based on a problem from number theory. We present several generalizations and corollaries. The paper studies residues modulo a prime, sets of such residues, and a special type of summing sets. The examples are taken from past mathematical competitions.

1 Background

During the preparation of the US team for the 2001 IMO, the following problem was proposed:

Problem 1 Let d and n be positive integers, and let p be a prime. Prove that there exist integers $x_1, x_2, \ldots, x_d$ such that

$$x_1^d + x_2^d + \cdots + x_d^d \equiv n \pmod{p}.$$

This problem can be solved combinatorially by using a bijection between sets of remainders, or algebraically, by using a minimal polynomial. However, both approaches may not work in a different setting. We will define several new concepts and show that they have interesting properties. Some of these properties can be formulated as separate problems. In addition, the article also gives a refinement of the conclusion of the problem above.

2 Sum of sets

Fix a prime p. For any two nonempty sets A and B of elements of $\mathbb{Z}_p$, define their sum as follows:

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

We can also define translation and multiplication by elements from $\mathbb{Z}_p$ in the following way:

$$t + A = \{t + a \mid a \in A\} \qquad cA = \{ca \mid a \in A\}, \quad c \neq 0.$$

For convenience, define $-A$ to be the set $\{-a : a \in A\}$. A nonempty set $A \subseteq \mathbb{Z}_p$ is called an arithmetic series if there exist elements $a, d \in \mathbb{Z}_p, d \neq 0$ such that

$$A = \{a, a + d, \ldots, a + (|A| - 1)d\}.$$

Also, for any two $A, B \subseteq \mathbb{Z}_p$ we will write $A \sim B$ if and only if there exist elements $a, b, d \in \mathbb{Z}_p$, such that

$$A = \{a, a + d, \ldots, a + (|A| - 1)d\} \quad \text{and} \quad B = \{b, b + d, \ldots, b + (|B| - 1)d\}.$$

Note that the statement $A \sim B$ implies that both A and B are arithmetic series. Let us list some useful properties of arithmetic series.
(i) For every $c, t \in \mathbb{Z}_p$ with $c \neq 0$ and $A, B \subseteq \mathbb{Z}_p$ holds

$$(t + A) + B = t + (A + B), \qquad cA + cB = c(A + B).$$

(ii) For any $c \neq 0$, $A \sim B$ implies $cA \sim cB$ and also the chain of relations:

$$B \sim A \sim t + A \sim -A.$$

(iii) Translation and multiplication do not change the number of elements:

$$|A| = |t + A| = |cA|.$$

Our goal is to find a lower bound for the number of elements in a set which is a sum of two other sets. We will formulate this in the next theorem:

Theorem 1 *For all nonempty subsets $A, B \subseteq \mathbb{Z}_p$,*

$$|A + B| \geq \min(|A| + |B| - 1, p).$$

Proof. Let $|A| = m, |B| = n$. We will consider two possibilities.
Case 1: $m + n > p$. Suppose $|A + B| < p$. Then there exists $t \notin A + B$, hence

$$\begin{cases} (t + (-B)) \cap A = \emptyset \\ |t + (-B)| + |A| = m + n > p \end{cases}$$

which is impossible. Therefore

$$|A + B| = p = \min(m + n - 1,\ p).$$

Case 2: $m + n \leq p$. We will conduct an induction on $\min(m, n)$. Without loss of generality, assume $m \leq n \leq p$. If $m = 1$, then

$$|A + B| = |B| = |A| + |B| - 1 \tag{1}$$

and the statement holds.

Now, suppose that $1 < m \leq n < p$ and take an arbitrary element u of $\mathbb{Z}_p \setminus B$ and two distinct elements a_1, a_2 of A. Since the series

$$u + i(a_2 - a_1), \quad i = 1, 2, \ldots, p - 1$$

runs through all elements of $\mathbb{Z}_p \setminus \{u\}$, there exists a smallest i_0 for which the element $b = u + i_0(a_2 - a_1) \in B$. From properties (i) and (iii), we can replace A by the set $(b - a_2) + A$, which now contains $b + (a_1 - a_2) \notin B$ and $b \in B$. Let

$$F = A \cap B, \quad G = A \cup B, \tag{2}$$

with $0 < |F| < m \leq n < |G|$. We have

$$|F| + |G| = |A| + |B| = m + n. \tag{3}$$

At the same time, if $f \in F$ and $g \in G$, then, depending on whether $g \in A$ or $g \in B$, either $(g, f) \in A \times B$ or $(f, g) \in A \times B$. Indeed, if $g \in A$ then $(g, f) \in A \times B$, while if $g \in B$ then $(f, g) \in A \times B$. Both possibilities lead to $f + g \in A + B$. This means that

$$F + G \subseteq A + B \tag{4}$$

and therefore

$$|A + B| \geq |F + G|. \tag{5}$$

Taking into account (3), it remains to prove the statement for the couple F and G. Since $|F| < |A|$, we can apply the induction and the proof is complete. $\square$

Corollary 1

$$|A_1 + A_2 + \cdots + A_k| \geq \min(|A_1| + |A_2| + \cdots + |A_k| - (k-1),\ p).$$

Now we shall establish when equality does hold in the statement of Theorem 1.

Theorem 2 *Let $A, B \subseteq \mathbb{Z}_p$ with $|A|, |B| > 1$ and $|A| + |B| < p$, then*

$$|A + B| = |A| + |B| - 1 \iff A \sim B.$$

Proof. Let $m = |A|, n = |B|$, where $m > 1, n > 1$ and $m + n < p$. Without loss of generality, we can assume that $m \leq n$.

The backward direction is straightforward: if $A \sim B$ and

$$A = \{a, a + d, \ldots, a + (m-1)d\}, \qquad B = \{b, b + d, \ldots, b + (n-1)d\},$$

then from $m + n < p$ we have

$$A + B = \{a + b, a + b + d, \ldots, a + b + (m + n - 2)d\},$$

hence $|A + B| = m + n - 1 = |A| + |B| - 1$.

To prove the forward direction, let $|A + B| = |A| + |B| - 1$. We want to prove that $A \sim B$. Observe that from properties (ii) and (iii) it suffices to prove the statement for any translations of A or B or for the sets cA and cB for some $c \neq 0$.

If $a_1 \neq a_2 \in A$ are two arbitrary elements, replace A and B by $c(-a_1 + A)$ and cB respectively, where $c = (a_2 - a_1)^{-1}$. Now we have the convenient fact that

$$0, 1 \in A. \tag{6}$$

We will prove the theorem by induction on m, the size of the smaller set.

If $m = 2$, from (6) we get $A = \{0, 1\}$. Notice that if there existed more than one element $b \in B$ with $b + 1 \notin B$, we would have

$$|A + B| \geq |B| + 2 > |A| + |B| - 1,$$

contradicting the assumption. Therefore B must be a set of consecutive elements, i.e. of the form $x, x+1, x+2, \ldots$. Obviously, in this case $A \sim B$ and the statement is proved.

Now, let $3 \le m \le n$. We want to apply the earlier idea of replacing A and B with their union and intersection, but this time the induction hypothesis has a stronger requirement, namely $|A \cap B| > 1$. We examine the following cases:

Case 1: There exists a translation of A whose intersection with B has between 2 and $m-1$ elements, i.e.

$$\exists t \in \mathbb{Z}_p : 2 \le |(t+A) \cap B| \le m-1.$$

Replace A by $t+A$ and define

$$F = A \cap B, \quad G = A \cup B.$$

From the choice of t we have

$$2 \le |F| \le m-1. \tag{7}$$

As in the proof of Theorem 1, from (3) and (5) we have

$$|F| + |G| - 1 \le |F+G| \le |A+B| = |A| + |B| - 1 = |F| + |G| - 1,$$

so all the inequalities must be equalities, hence

$$|F+G| = |F| + |G| - 1 = |A+B| \tag{8}$$

From (7), the induction hypothesis applies to F and G, yielding $F \sim G$. Furthermore, $|G| = |A \cup B| \le |A| + |B| = m+n < p$, so $G \ne \mathbb{Z}_p$. Therefore if $k = |F|, r = |G|$, we have $1 < k < m \le n \le r < p$ and

$$F = \{f, f+d, \dots, f+(k-1)d\}, \qquad G = \{g, g+d, \dots, g+(r-1)d\}.$$

where $f-d \notin F, f+kd \notin F, g-d \notin G, g+rd \notin G$. From $F \subset G$ it follows that

$$f = g + qd \tag{9}$$

for some $q \ge 0$, and since $g + rd \notin G$, it must be that $q \le r-k$. We can now represent G as $G = L \cup F \cup R$, where

$$L = \{g, g+d, \dots, g+(q-1)d\},$$

$$F = \{g+qd, g+(q+1)d \dots, g+(q+k-1)d\},$$

$$R = \{g+(q+k)d, g+(q+k+1)d, \dots, g+(r-1)d\}.$$

Basically L and R consist of the first q and the last $r-k-q$ elements of G respectively. Notice that $L, R \subseteq G \setminus F$, so each of the elements in L and R belongs to either A or B but not to both A and B at the same time.

We shall show that all elements of L (and similarly of R) belong entirely either to A or to B.

If $|L| \le 1$ there is nothing to prove, so assume $|L| = q > 1$.

First, we shall show that for any two indices $i, j \in [0, q-1]$ with $i+j \in \{q-2, q-1\}$ holds

$$g+id, g+jd \in A \text{ or } g+id, g+jd \in B. \qquad (*)$$

Assume the contrary, and let $g + id \in A, g + jd \in B$ without loss of generality. Again, as in the proof of Theorem 1, we have $F + G \subseteq A + B$ as in (4). From (8) we obtain $A + B = F + G$, hence

$$(g + id) + (g + jd) = (f + i'd) + (g + j'd)$$

for some $i' \in [0, k-1]$ and $j' \in [0, r-1]$. Then, from (9) and $d \neq 0$, we obtain:

$$i + j \equiv i' + j' + q \pmod{p}. \tag{10}$$

Now, using (8), from $m+n < p$ we have $k+r = m+n < p$, and from $i+j \in [q-2, q-1]$ we obtain

$$\begin{aligned} i + j &\leq q - 1 \\ &< i' + j' + q \leq (k-1) + (r-1) + q \\ &< p + q - 2 \leq p + (i + j). \end{aligned}$$

Subtracting $i + j$, we have

$$0 < i' + j' + q - (i + j) < p,$$

which contradicts (10) and completes the proof of $(*)$.

Consider the elements of L arranged in the following order:

$$g + (q-1)d, g, g + (q-2)d, g + d, g + (q-3)d, g + 2d, g + (q-4)d, g + 3d, \ldots$$

Observe that each two consecutive elements are of the form $g+id, g+jd$ where $i+j = q-1$ or $i + j = q - 2$, so according to $(*)$ they must belong to either A or B. Therefore all elements of L belong simultaneously to either A or to B, which is what we wanted. The proof for R is analogous to the proof of L.

Now, we have $L \subseteq A$ or $L \subseteq B$ and $R \subseteq A$ or $R \subseteq B$. Examine the four possible cases:

- $L, R \subseteq A \Rightarrow (A, B) = (L \cup F \cup R, F)$;
- $L \subseteq A, R \subseteq B \Rightarrow (A, B) = (L \cup F, F \cup R)$;
- $L \subseteq B, R \subseteq A \Rightarrow (A, B) = (F \cup R, L \cup F)$;
- $L, R \subseteq B \Rightarrow (A, B) = (F, L \cup F \cup R)$.

In all examined cases, A and B consist of consecutive elements in G, and therefore $A \sim B$.

Case 2: There *is no* translation of A whose intersection with B has between 2 and $m-1$ elements. Therefore, any translation that has at least two elements in common with B must have all m elements in B. Formally,

$$|(t + A) \cap B| \geq 2 \Rightarrow |(t + A) \cap B| \geq m = |t + A| \Rightarrow (t + A) \subseteq B. \tag{11}$$

The idea is to remove an element from A so as to use the induction hypothesis.
Let k, $1 \leq k \leq n < p$ be the maximum length of a block of consecutive elements in B, i.e.

$$w, w + 1, \ldots, w + k - 1 \in B \text{ and } w - 1, w + k \notin B$$

for some $w \in \mathbb{Z}_p$. Next, replace B by its translation $-w + B$ so that now

$$0, 1, \ldots, k-1 \in B, \qquad -1, k \notin B. \tag{12}$$

Suppose first that there exists an element $q \neq 0$ in $\mathbb{Z}_p$ with

$$q \in A, \qquad -q \in B, \tag{13}$$

and let $A_1 = -q + A$. From (6), (12), and (13) we have

$$\{-q, -q+1, 0\} \subseteq A_1, \qquad \{-q, 0\} \subseteq B. \tag{14}$$

Then, $|A_1 \cap B| \geq 2$, and from (11) we get $A_1 \subseteq B$, thus $-q+1 \in B$.
Next, let $A_2 = -q + 1 + A$, so

$$\{-q+1, -q+2, 1\} \subseteq A_2, \qquad \{-q+1, 1\} \subseteq B.$$

Again, $|A_2 \cap B| \geq 2$ hence $A_2 \subseteq B$, thus $-q+2 \in B$.
We proceed the same way with $A_3, A_4, \ldots$ until we reach $A_k = -q + k - 1 + A$ with

$$\{-q+k-1, -q+k, k-1\} \subseteq A_k, \qquad \{-q+k-1, k-1\} \subseteq B.$$

One last time, $|A_k \cap B| \geq 2$, and from (11) we get $A_k \subseteq B$, thus $-q+k \in B$. Now, we have found $k+1$ consecutive elements in B, namely $-q, -q+1, \ldots, -q+k$, which contradicts the maximality choice of k. Therefore, the existence of q in (13) is not possible, and from (6) and (12)

$$A \cap (-B) \quad = \quad \{0\} \tag{15}$$

Define

$$A^* = A \setminus \{0\},$$

where $|A^*| = |A| - 1 = m - 1 > 1$ since $m \geq 3$. Notice that from $0 \notin A^*$ and (15) we get

$$0 \notin A^* + B, \tag{16}$$

else there would exist a nonzero element in both A and $-B$ in contradiction to (15).

We know that $0 \in A$ and $0 \in B$, so $0 \in A + B$, while at the same time $0 \notin A^* + B$. Therefore

$$A^* + B \subseteq A + B \setminus \{0\}. \tag{17}$$

From Theorem 1, we have

$$(m-1) + n - 1 \leq |A^* + B| < |A + B| = m + n - 1,$$

whence

$$|A^* + B| = m + n - 2 = |A^*| + |B| - 1 = |A + B| - 1. \tag{18}$$

Applying the induction hypothesis to A^* and B yields $A^* \sim B$. Let

$$A^* = \{a, a+d, \ldots, a+(m-2)d\}, \quad B = \{b, b+d, \ldots, b+(n-1)d\} \tag{19}$$

for some $a, b, d \in \mathbb{Z}_p$ where $d \neq 0$. We have

$$A^* + B = \{a + b + id \mid i = 0, 1, \ldots, (m+n-3)\}. \tag{20}$$

From (17) and (18) we know that $A^* + B \subseteq A + B \setminus \{0\}$ and $|A^* + B| = |A + B \setminus \{0\}| = m + n - 2$, hence

$$A^* + B = A + B \setminus \{0\}. \tag{21}$$

From (6) we have $0 \in A$, so $B = 0 + B \subseteq A + B$, and together with (21) we get

$$B \setminus \{0\} \subseteq (A + B) \setminus \{0\} = A^* + B. \tag{22}$$

From (12) we have $0 \in B$, so from (16) and (19) there exists $r \in [0, n-1]$ such that

$$b + rd = 0 \notin A^* + B \tag{23}$$

We shall show that $r = 0$ or $r = n - 1$. Assume the contrary, so $0 < r < n - 1$. In that case, from (19) and (23) the elements $b + (r-1)d = -d$ and $b + (r+1)d = d$ are nonzero and belong to B, so using (22) we obtain

$$-d, d \in A^* + B. \tag{24}$$

From $d \in A^* + B$ and (20) there must be $i \in [0, m+n-3]$ such that $a + b + id = d$. But if $i > 0$, we would have $a + b + (i-1)d = 0 \in A^* + B$ in contradiction to (16). Therefore $i = 0$, hence $a = d - b = (r+1)d$ owing to (23). Similarly, from $-d \in A^* + B$ and (20), there must be $j \in [0, m+n-3]$ such that $a + b + jd = -d$. But if $j < m + n - 3$, we would have $a + b + (j+1)d = 0 \in A^* + B$ in contradiction to (16). Therefore $j = m + n - 3$, hence $a = -b - (m+n-2)d = (r - m - n + 2)d$ owing to (23). Finally, coupling $a = (r - m - n + 2)d$ with $a = (r+1)d$ and $d \neq 0$ we get $m + n \equiv 1 \pmod{p}$, contradicting $2 \leq m + n < p$.

Consequently, $r = 0$ or $r = n - 1$.

Consider first the case $r = 0$, so $b = 0$ due to (23). Since $n \geq 2$ and $d \neq 0$, using (19) we have $d = b + d \in B \setminus \{0\}$. From (22) we now have

$$d \in A^* + B.$$

Therefore, from (20) there must be $i \in [0, m+n-3]$ such that $a + b + id = d$. But if $i > 0$, we would have $a + b + (i-1)d = 0 \in A^* + B$ in contradiction to (16). Therefore $i = 0$, hence $a = d - b = d$. Now, using (19) and $A = A^* \cup \{0\} = A^* \cup \{a - d\}$, we obtain

$$A = \{a - d, a, a + d, \ldots, a + (m-2)d\},$$

hence $A \sim B$.

Similarly, we consider the case $r = n - 1$, where $b = -(n-1)d$. Since $n \geq 2$ and $d \neq 0$, using (19) we have $-d = b + (n-2)d \in B \setminus \{0\}$. From (22) we now have

$$-d \in A^* + B.$$

Therefore, from (20) there must be $j \in [0, m+n-3]$ such that $a + b + jd = -d$. But if $j < m + n - 3$, we would have $a + b + (j+1)d = 0 \in A^* + B$ in contradiction to (16). Therefore $j = m + n - 3$, hence $a = -(m-1)d$. Again, using (19) and $A = A^* \cup \{0\} = A^* \cup \{a + (m-1)d\}$, we obtain

$$A = \{a, a + d, \ldots, a + (m-2)d, a + (m-1)d\},$$

and again $A \sim B$.

This completes the proof of the theorem. $\square$

Here is a question to explore: describe all non-empty $A, B \subseteq \mathbb{Z}_p$ such that

$$|A + B| = |A| + |B| - 1. \qquad (**)$$

- If $|A| = 1$, then $|A + B| = |B| = |A| + |B| - 1$, so $(**)$ holds for any $B \subseteq \mathbb{Z}_p$. Likewise, $(**)$ holds for any A and any B with $|B| = 1$.
- If $|A| + |B| > p + 1$, from $|A + B| \le p < |A| + |B| - 1$ we see that $(**)$ never holds.
- If $|A| + |B| = p + 1$, then Theorem 1 gives us $|A + B| \ge p$, so $|A + B| = p = |A| + |B| - 1$, and hence $(**)$ is true for any $A, B \subseteq \mathbb{Z}_p$ with $|A| + |B| = p + 1$.
- If $|A| > 1$ and $|B| > 1$ and $|A| + |B| < p$, then Theorem 2 tells us that $(**)$ iff $A \sim B$.
- Finally, if $|A| + |B| = p$, then $(**)$ is equivalent to $|A + B| = p - 1$, i.e. $A + B = \mathbb{Z}_p \setminus \{t\}$ for some $t \in \mathbb{Z}_p$, which in turn is equivalent to

  $$A \cap (t + (-B)) = \emptyset. \tag{25}$$

  Since $|t + (-B)| = |B| = p - |A|$, then (25) implies that A and $t - B$ are complementary sets. Therefore

  $$t - B = (\mathbb{Z}_p \setminus A) \Rightarrow B = t - (\mathbb{Z}_p \setminus A).$$

  Conversely, we shall see that every $A \subset \mathbb{Z}_p$ and $B = t - (\mathbb{Z}_p \setminus A)$ satisfy $(**)$. Indeed, in this case $p - 1 = |A| + |B| - 1 \le |A + B|$. At the same time, $t = a + b$ does not have a solution in $a \in A$ and $b = t - a' \in B$, otherwise we would have $t = a + (t - a') \leftrightarrow a = a'$ for some $a' \in \mathbb{Z}_p \setminus A$, a contradiction. Therefore $t \notin A + B$, hence $|A + B| < p$, and so $|A + B| = p - 1 = |A| + |B| - 1$, satisfying $(**)$.

3 Applications

We are ready to solve the problem we formulated in the beginning.
Solution: Let $A_d = \{0, 1^d, 2^d, \dots, (p-1)^d\}$. Since the equation $x^d - c = 0, c \ne 0$ has no more than d roots in $\mathbb{Z}_p$, among the $p - 1$ numbers $1^d, 2^d, \dots, (p-1)^d$ at least $\dfrac{p-1}{d}$ are distinct, whence $|A_d| \ge 1 + \dfrac{p-1}{d}$. Now, from the corollary of Theorem 1 we have

$$|\underbrace{A_d + A_d + \cdots + A_d}_{d\text{-times}}| \ge \min(d|A_d| - (d-1), p) = p.$$

In particular, $n \in (A_d + A_d + \cdots + A_d)$ and we are done. $\square$

Here are several more problems for practice.

Problem[1] **2** Let p be a prime and consider a regular $2p$-gon. Let A and B be opposite vertices. Among the remaining vertices, $k < p$ are marked. Draw all segments joining pairs of marked vertices that intersect AB, and assume that at least one such segment exists. Prove that at least $k - 1$ of these segments can be chosen so that no two are parallel or perpendicular.

Solution Let us number the points clockwise from A inclusive to B respectively by $0, 1, \dots, p - 1$ and call them "left" points. We do the same with the "right" points, i.e. from B to A in the same direction. Let us take one of the mentioned diagonals with left

[1]This and the next problems are equivalent to Theorem 1

end a_1 and right end b_1. It is parallel to another diagonal with ends a_2 and b_2 whenever $a_1 + b_1 = a_2 + b_2$, and it is perpendicular to it iff $a_1 + b_1 = a_2 + b_2 \pm p$. In order to find $k - 1$ diagonals with the desired property we need at least $k - 1$ incongruent modulo p sums of the type $a + b$, which is actually the result of Theorem 1. $\square$

Problem 3 Let $p > 2$ be prime and let $a(x)$, $b(x)$, and $c(x)$, be three nonzero polynomials of degree less than p having all coefficients in $\{0, 1\}$.

Prove that if $a(1) + b(1) + c(1) = p + 2$, then

$$\sum_{j=0}^{p-1} a(\omega^j)b(\omega^j)c(\omega^j) > 0,$$

where ω is a primitive p-th root of 1.

Solution: Since

$$\sum_{j=0}^{p-1} \omega^{jr} = \begin{cases} p, & p \mid r, \\ 0, & p \nmid r, \end{cases}$$

the sum in the problem statement equals $p\times$ the sum of the coefficients of those monomials in $s(x) = a(x)b(x)c(x)$ whose exponents are divisible by p. Since all coefficients of $s(x)$ are nonnegative coefficients, we just need to show that one of the monomials $x^{jp}, j \geq 0$ appears in $s(x)$.

Let A be the set of exponents n such that the monomial x^n appears in $a(x)$. Same for B and C. From $a(1)+b(1)+c(1) = p+2$ it follows that $|A|+|B|+|C| = p+2$. Then, from the corollary of Theorem 1, we get $A+B+C = \mathbb{Z}_p$, and in particular $0 \in A+B+C$. That means there exist exponents $\alpha \in A, \beta \in B$, and $\gamma \in C$ such that

$$\alpha + \beta + \gamma \equiv 0 \pmod{p}.$$

Since $0 \leq \alpha, \beta, \gamma \leq p - 1$, it follows that $\alpha + \beta + \gamma = kp$ for some integer $k \in [0, 2]$. Therefore the polynomial $s(x)$, contains $x^{\alpha+\beta+\gamma} = x^{kp}$ and the proof is complete. $\square$

Problem 4 (Selection test for JBMO 1998) Given are seven integers not divisible by seven. Prove that all their sums represent all seven remainders modulo seven.

Hint: If the numbers are a_i, consider the sets $A_i = \{0, a_i\}$.

Problem 5 Find all prime numbers p with the property: There exists only one element among $\{0, 1, \ldots, p - 1\}$ which is not a sum of a quadratic residue and a non-quadratic residue modulo p.

4 Special cases

4.1 Geometric series

We will examine the sets $A_d = \{0, 1^d, 2^d, \ldots, (p-1)^d\}$ from the first problem more closely. Let ξ be a primitive root in $\mathbb{Z}_p$ and define

$$S_n = \underbrace{A_d + A_d + \cdots + A_d}_{n\text{-times}}.$$

Next, define

$$h(d) = \min n : S_n = \mathbb{Z}_p.$$

We want to find an upper bound on $h(d)$.

If $\delta = (p-1, d)$, we shall see that $A_d = A_\delta$. There exist integers a and b, such that $(p-1)a + db = \delta$. Therefore, for every $x \in \mathbb{Z}_p \setminus \{0\}$ and some u we have

$$x^\delta = (\xi^u)^\delta = \xi^{(p-1)au+dbu} = (\xi^{bu})^d = y^d,$$

hence every non-zero element in A_δ is also in A_d.

Conversely, $x^d = (x^{d/\delta})^\delta = y^\delta$, so every non-zero element in A_d is also in A_δ. Finally, given that $0 \in A_d$ and $0 \in A_\delta$, we have $A_\delta = A_d$. Therefore it suffices to examine only those d that divide $p-1$. Let

$$m = \frac{p-1}{d}.$$

Notice that

$$A_d = \{0, \xi^d, \xi^{2d}, \ldots, \xi^{md}\}. \tag{26}$$

There are several possibilities for d and m where either $d \leq 2$ or $m \leq 2$:

- $m = 1, d = p-1 \Rightarrow A_d \equiv \{0, 1\} \Rightarrow h(d) = p-1$;
- $m = 2, d = \dfrac{p-1}{2} \Rightarrow A_d = \{-1, 0, 1\} \Rightarrow h(d) = \dfrac{p-1}{2}$;
- $d = 1 \Rightarrow A_d = \mathbb{Z}_p \Rightarrow h(d) = 1$;
- $d = 2 \Rightarrow |A_d| = m + 1 = \dfrac{p+1}{2} \Rightarrow h(d) = 2$.

In all four cases we have $h(d) = d$. Now, consider $m, d > 2$, i.e.

$$3 \leq d \leq \frac{p-1}{3}, \qquad 3 \leq m \leq \frac{p-1}{3}. \tag{27}$$

We shall show that A_d is *not* an arithmetic series. Assume the contrary, and let

$$\{a, a+t, \ldots, a+mt\} = A_d = \{0, \xi^d, \xi^{2d}, \ldots, \xi^{md}\} \tag{28}$$

for some $a, t \in \mathbb{Z}_p$. From (27) we have $\xi^d \neq \pm 1$. Operating in $\mathbb{Z}_p$ and using (28) we obtain:

$$0 = \sum_{i=1}^{m} \xi^{id} = \sum_{i=0}^{m} (a + it) = (m+1)a + \frac{m(m+1)}{2} t, \tag{29}$$

$$0 = \sum_{i=1}^{m} (\xi^{id})^2 = \sum_{i=0}^{m} (a+it)^2 = (m+1)a^2 + \frac{m(m+1)(2m+1)}{6} t^2 + m(m+1)at. \tag{30}$$

Since $m + 1 \neq 0$, from (29) it follows $a = -mt/2$, which we plug into (30) to obtain

$$0 = -\frac{m^2}{4} + \frac{m(2m+1)}{6}$$

after dividing by $(m+1)t^2 \neq 0$. From $m \neq 0$, this leads to $m \equiv -2 \pmod{p}$, hence $m = p - 2$, which is a contradiction with (27). Consequently the equivalence (28) is not possible, and we can conclude that A_d is not an arithmetic series.

We know that $|S_k| < p$ for $k = 1, 2, \ldots, h(d) - 1$ by the definition of $h(d)$. Consider the bijection $g : (S_k \setminus \{0\}) \to (S_k \setminus \{0\})$, defined by $g(x) = \xi^d x$. Each orbit in this bijection has length m, therefore

$$m \mid |S_k| - 1. \tag{31}$$

We will prove by induction on k that $|S_k| \geq (2k-1)m + 1$ for $k = 1, 2, \ldots, h(d) - 1$.

For $k = 1$, we get $|S_k| - 1 \geq m$ from (31), hence the start of the induction is established.
From now on, assume $1 < k < h(d)$ and $|S_{k-1}| \geq (2k-3)m + 1$. From Theorem 1 we have

$$|S_1| + |S_{k-1}| - 1 \leq |S_1 + S_{k-1}| = |S_k| \leq p - 1,$$

so

$$|S_1| + |S_{k-1}| \leq p. \tag{32}$$

Next, from (31), we have $|S_i| \equiv 1 \pmod{m}$, so $|S_1| + |S_{k-1}| \equiv 2 \pmod{m}$, where $m > 2$ owing to (27). At the same time, $p \equiv 1 \pmod{m}$, hence $|S_1| + |S_{k-1}| \neq p$, which means the inequality in (32) is strict.

Now we have $|S_1| + |S_{k-1}| < p$, and from $|S_1| > 1, |S_{k-1}| > 1$ we can apply Theorem 2 to these two sets. We already know that $S_1 = A_d$ is not an arithmetic series, hence

$$|S_k| \geq |S_1| + |S_{k-1}| \geq m + 1 + (2k-3)m + 1 = (2k-2)m + 2.$$

Now, from (31) we conclude $|S_k| \geq (2k-1)m + 1$ and the induction is complete.

Now, applying the result of the induction to $k = h(d) - 1$,

$$p > |S_k| \geq (2k-1)m + 1 = (2k-1)\frac{p-1}{d} + 1$$
$$\Rightarrow d > 2k - 1 \Rightarrow d \geq 2k = 2(h(d) - 1)$$
$$\Rightarrow h(d) \leq \frac{d}{2} + 1 \Rightarrow h(d) \leq \left\lfloor \frac{d}{2} \right\rfloor + 1.$$

Since we used the limits on d specified in (27), this result is not guaranteed for the 4 cases $d \leq 2$ and $m \leq 2$ that we examined earlier. However, we can verify manually that it also holds for $d = 1, 2$, where $h(1) = 1$ and $h(2) = 2$.
We summarize this result in a theorem:

Theorem 3 *For every positive integer d,*

$$h(d) \leq \left\lfloor \frac{(p-1,d)}{2} \right\rfloor + 1,$$

with the exception of $(p-1,d) = \dfrac{p-1}{2}, p-1$, *where* $h(d) = (p-1,d)$.

Comment The sets $A_d \setminus \{0\}$ are the subgroups of $\mathbb{Z}_p^*$.
The next problem illustrates the result achieved.
Problem 6 Let n be the smallest positive integer for which $2^n - 1$ is divisible by the prime $p > 3$. Prove that for every integer d, there exists an integer $m, 1 \leq m \leq 2^n$ such

that p divides $d+m$ and the binary representation of m has no more than $\left\lfloor \frac{p-1}{2n} \right\rfloor + 1$ units.

Comment. If we change $\left\lfloor \frac{p-1}{2n} \right\rfloor + 1$ to $\frac{p-1}{n}$, the problem becomes much easier and the solution requires only Theorem 1.

4.2 Arithmetic series

The arithmetic series sets A are easily described by complex numbers. Let ω be a primitive p-th root of 1. Define the function $\tau(A) : \{A : A \subset \mathbb{Z}_p\} \to \mathbb{C}$ by

$$\tau(A) = \sum_{a \in A} \omega^a.$$

It can be shown that the minimal polynomial of $\tau(A_d)$ over $\mathbb{Q}$ has degree $m = (p-1, d)$, which allows us to solve the first problem without using the theorems. Unfortunately, in the general case $h(A) < \deg_{\mathbb{Q}} \tau(A)$. We know that the polynomial $\Phi_p(x) = 1 + x + \cdots + x^{p-1}$ is irreducible over $\mathbb{Q}$. Therefore, we are able to identify the sets by their τ-values, namely $A = B \iff \tau(A) = \tau(B)$. Consequently, the assertion that A is an arithmetic series implies that there exist $a \in [0, p-1]$ and $d \in [1, p-1]$ with

$$\tau(A) = \omega^a + \omega^{a+d} + \omega^{a+2d} + \cdots + \omega^{a+(m-1)d} = \frac{\omega^{a+md} - \omega^a}{\omega^d - 1},$$

where $m = |A|$. When $m = 1$ or $m = p-1$ everything is clear. Assume now $1 < m < p-1$. We will prove that there exist exactly two couples $\{a, d\}$ generating the arithmetic series A. Let

$$\frac{\omega^{a+md} - \omega^a}{\omega^d - 1} = \tau(A) = \frac{\omega^{a'+md'} - \omega^{a'}}{\omega^{d'} - 1}.$$

Move everything to the left and notice that every term with sign "+" needs to be cancelled by the *same* term with sign "-":

$$\omega^{a+md+d'} + \omega^a - \omega^{a+md} - \omega^{a+d'} - \omega^{a'+md'+d} - \omega^{a'} + \omega^{a'+md'} + \omega^{a'+d} = 0.$$

Since $\omega^a \neq \omega^{a+md}, \omega^{a+d'}$ and $\omega^{a+md+d'} \neq \omega^{a+md}, \omega^{a+d'}$, then either

$$\left(\omega^{a+md+d'}, \omega^a\right) = \left(\omega^{a'+md'+d}, \omega^{a'}\right),$$

or

$$\left(\omega^{a+md+d'}, \omega^a\right) = \left(\omega^{a'}, \omega^{a'+md'+d}\right),$$

where the pairs are ordered. The first case leads to $\omega^{(m-1)(d-d')} = 1$, hence $d = d'$ and $a = a'$; and the second case leads to $\omega^{(m+1)(d+d')} = 1$, hence $d' = p-d$ and $a' \equiv a+(m-1)d \pmod{p}$. This shows that each arithmetic series A with $1 < |A| < p-1$ is given by the pairs (a, d) and $(a', p-d)$.

Corollary 2 *If $A, B, C \subset \mathbb{Z}_p$ and $1 < |B| < p-1$, then*

$$A \sim B \sim C \quad \Rightarrow \quad A \sim C.$$

Corollary 3 *For a given p, the number of all arithmetic series except $\mathbb{Z}_p$ is*

$$p + \frac{p(p-1)(p-3)}{2} + p = \frac{p(p^2-4p+7)}{2}.$$

We can define arithmetic series for every positive integer p, not necessarily prime. However, when $p = mn$ for $m, n > 1$ all theorems become false, as shown by the following example:

$$A = \{0, n, 2n, \ldots, (m-1)n\}.$$

We have $A + A = A$ and $m = |A| = |A + A| < |A| + |A| - 1$, but $A + A \neq \mathbb{Z}_p$. On the other hand, the first two theorems remain true when we remove p from the stem and consider instead the numbers in $\mathbb{Z}$:

Theorem 4 *For every two sets A and B of integers holds*

$$|A + B| \geq |A| + |B| - 1,$$

with equality holding for $|A|, |B| > 1$ whenever A and B are arithmetic series with the same common difference.

We conclude with a nice problem about arithmetic series in $\mathbb{Z}_p$.

Problem 7 Let $p > 5$ be prime, and a, d, n be integers for which $2 \leq d \leq p-2$ and $3 \leq n \leq p-3$. It is known that for each $j = 1, 2, \ldots, n$ there exists an integer $b_j \in [0, n]$ with $b_j \equiv a + jd \pmod{p}$. Prove that $n = p - 3$.

Hint Consider the numbers $a + jd$ geometrically as points on a circle.

Similar triangles inscribed in one another

In collaboration with Nikolay Nikolov

Abstract

The use of complex numbers in geometry is often regarded as less elegant than purely geometric methods. Yet, despite its lack of aesthetics, a bit of algebra can lead to surprisingly interesting geometric results. In this article, we examine families of triangles inscribed in one another.

Definition 1. We shall call two triangles $\triangle XYZ$ and $\triangle X'Y'Z'$ *similar* and denote this by $\triangle XYZ \sim \triangle X'Y'Z'$ if they have the same orientation and $XY : YZ : ZX = X'Y' : Y'Z' : Z'X'$. (Notice that, under this definition, $\triangle XYZ \not\sim \triangle XZY$ because the orientation is different.)

Definition 2. We shall say that $\triangle X'Y'Z'$ is inscribed in $\triangle ABC$ if

$$X' \in BC, \quad Y' \in CA, \quad Z' \in AB,$$

where AB, BC, CA denote the lines and not just the segments.

1 General form of the transformation

Consider two arbitrary triangles $\triangle ABC$ and $\triangle XYZ$ inscribed in the unit circle in the complex plane. Let $\Phi_{\triangle ABC}(\triangle XYZ) = \Phi$ be the set of all triangles inscribed in $\triangle ABC$ and similar to $\triangle XYZ$.

For every triangle $\triangle X'Y'Z' \in \Phi$, there is a similarity transformation that sends $\triangle XYZ$ into $\triangle X'Y'Z'$, which can be described as an affine map $\rho(w) = uw + v$ in the complex plane. We have

$$\begin{aligned}\rho(x) &= ux + v = x' \\ \rho(y) &= uy + v = y' \\ \rho(z) &= uz + v = z'\end{aligned}$$

From $X' \in BC$, we have

$$\frac{x'-b}{b-c} = \frac{\overline{x'-b}}{\overline{b-c}} \Rightarrow \frac{ux+v-b}{b-c} = bc\frac{\overline{ux}+\overline{v}-\overline{b}}{c-b} \Rightarrow$$

$$ux + \overline{u}\frac{bc}{x} + v + \overline{v}bc = b + c \tag{1}$$

Similarly, from $Y' \in CA$ it follows that

$$uy + \overline{u}\frac{ca}{y} + v + \overline{v}ca = c + a.$$

Subtracting from (1), we get

$$u(x-y)+\overline{u}\left(\frac{bc}{x}-\frac{ca}{y}\right)+\overline{v}c(b-a)=b-a \tag{2}$$

In the same way, we derive

$$u(y-z)+\overline{u}\left(\frac{ca}{y}-\frac{ab}{z}\right)+\overline{v}a(c-b)=c-b \tag{3}$$

Dividing (2) and (3) by $c(b-a)$ and $a(c-b)$ respectively and subtracting from one another, we get

$$u\left(\frac{ax(c-b)+by(a-c)+cz(b-a)}{ac(b-a)(c-b)}\right)+$$
$$\overline{u}\left(b\frac{xy(a-b)+yz(b-c)+zx(c-a)}{xyz(a-b)(b-c)}\right)=\frac{a-c}{ac},$$

which simplifies to

$$ut+\overline{ut}=-1, \tag{4}$$

where

$$t=\frac{ax(c-b)+by(a-c)+cz(b-a)}{(a-b)(b-c)(c-a)}. \tag{5}$$

A necessary condition for $\Phi\neq\emptyset$ is $t\neq 0$.

Now, if we conjugate both sides of (2), we get

$$\overline{u}\frac{abc(y-x)}{xy(a-b)}+u\frac{ax-by}{a-b}+v=c.$$

Plugging in $\overline{u}=\dfrac{-1-ut}{\overline{t}}$ from (4) into the previous equation and after simplifying, we get

$$up+v=q, \tag{6}$$

where

$$p=\frac{ax-by}{a-b}-\frac{t}{\overline{t}}\frac{(y-x)abc}{(a-b)xy}, \tag{7}$$

$$q=c+\frac{1}{\overline{t}}\frac{(y-x)abc}{(a-b)xy}. \tag{8}$$

After simplifying (7) and (8), we get

$$p=\frac{ax^2(z-y)+by^2(x-z)+cz^2(y-x)}{yz(c-b)+zx(a-c)+xy(b-a)}, \tag{9}$$

$$q=\frac{xyc(b-a)+yza(c-b)+zxb(a-c)}{yz(c-b)+zx(a-c)+xy(b-a)}. \tag{10}$$

Therefore, from (4) and (6), we get

$$\rho(w)=\frac{\mu}{t}(w-p)+q, \tag{11}$$

where μ is a complex number with $\Re(\mu)=-1/2$. It is easy to see that the image of any given point under ρ is a line passing through $q-\dfrac{w-p}{2t}$ and perpendicular to the vector $\dfrac{w-p}{t}$.

2 Examining the set Φ

Proposition 1. The set Φ

(i) is the empty set when $\triangle XYZ$ is similar to the mirror image of $\triangle ABC$.

(ii) contains infinitely many triangles, namely the images of $\triangle XYZ$ under the transformation (11) for all μ with $\Re(\mu) = -1/2$ when $\triangle XYZ$ is not similar to the mirror image of $\triangle ABC$.

Proof. We shall show first that $t = 0$ is equivalent to $(x, y, z) = \lambda(\bar{a}, \bar{b}, \bar{c})$ for some $\lambda \neq 0$, which in turn is equivalent to $\triangle XYZ$ being similar to the mirror image of $\triangle ABC$.

The reverse implication is easy to verify by plugging in $x = \lambda\bar{a}, y = \lambda\bar{b}$, and $z = \lambda\bar{c}$ into (5).

Now, consider $t = 0$. From (5), we get

$$x(\bar{c} - \bar{b}) + y(\bar{a} - \bar{c}) + z(\bar{b} - \bar{a}) = t\frac{(a-b)(b-c)(c-a)}{abc} = 0,$$

which can be re-written as

$$\begin{vmatrix} x & y & z \\ 1 & 1 & 1 \\ \bar{a} & \bar{b} & \bar{c} \end{vmatrix} = 0. \tag{12}$$

As the vectors $(1, 1, 1)$ and $(\bar{a}, \bar{b}, \bar{c})$ are linearly independent, the last equation is equivalent to

$$(x, y, z) = \lambda_1(1, 1, 1) + \lambda_2(\bar{a}, \bar{b}, \bar{c})$$

for some complex λ_1 and λ_2. From here and $|a| = |b| = |c| = 1$, we get

$$|x - \lambda_1| = |y - \lambda_1| = |z - \lambda_1| = |\lambda_2|,$$

whence the three different points X, Y, Z must lie on a circle centered at λ_1 with radius $|\lambda_2|$ and at the same time lie on the unit circle. The two circles can have three points in common only when they coincide, i.e. when $\lambda_1 = 0$ and $|\lambda_2| = 1$, from where $(x, y, z) = \lambda(\bar{a}, \bar{b}, \bar{c})$.

Now, we want to show that if $t \neq 0$, every transformation (11) with $\Re(\mu) = -1/2$ sends $\triangle XYZ$ into a similar $\triangle X'Y'Z'$ inscribed in $\triangle ABC$. We shall only show that $X' \in BC$, as the other two conditions follow analogously. The condition $X' \in BC$ is equivalent to

$$\frac{x' - b}{b - c} = \frac{\overline{x' - b}}{\overline{b - c}},$$

where $x' = \rho(x) = \dfrac{\mu}{t}(x - p) + q$ and $\mu + \bar{\mu} = -1$. Simplifying the last equation and replacing $\bar{\mu}$ by $-1 - \mu$, it remains to prove that

$$\mu\left(\frac{x - p}{t} - \frac{\bar{x} - \bar{p}}{\bar{t}}bc\right) + \left(q + \bar{q}bc - b - c - \frac{\bar{x} - \bar{p}}{\bar{t}}bc\right) = 0. \tag{13}$$

We shall show first that

$$q + \bar{q}bc - b - c = \frac{x - p}{t}. \tag{14}$$

From (8) and (7), we have

$$\begin{aligned}
q + \bar{q}bc - b - c &= (q - c) + bc(\overline{q - c}) \\
&= \frac{1}{\bar{t}} \frac{(y - x)abc}{(a - b)xy} + bc\frac{1}{t} \frac{(y - x)}{(a - b)c} \\
&= \frac{1}{t} \left(x - \frac{ax - by}{a - b} + \frac{t}{\bar{t}} \frac{(y - x)abc}{(a - b)xy} \right) \\
&= \frac{x - p}{t},
\end{aligned}$$

which proves (14). Therefore,

$$\frac{\bar{x} - \bar{p}}{\bar{t}} bc = (\bar{q} + q\overline{bc} - \bar{b} - \bar{c})bc = \bar{q}bc + q - b - c = \frac{x - p}{t},$$

which shows that both expressions in the brackets in (13) are 0 and completes the proof. □

3 Geometric observations

We shall prove several facts.

Proposition 2. The feet of the perpendiculars from point Q, whose complex coordinate is given by (10), to the sides of $\triangle ABC$ form the smallest triangle of the set Φ.

Proof. The similarity ratio between $\triangle X'Y'Z'$ and $\triangle XYZ$ is $\frac{|\mu|}{|t|}$, and it becomes smallest when $|\mu|$ is smallest, that is, when $\mu = -1/2$. Consider this minimal triangle for the set Φ. Using (14), we have

$$\begin{aligned}
x' = \rho(x) &= -\frac{x - p}{2t} + q \\
&= -\frac{q + \bar{q}bc - b - c}{2} + q \\
&= \frac{q + b + c - \bar{q}bc}{2},
\end{aligned}$$

hence X' is the foot of the perpendicular from Q to BC. Similarly for Y' and Z'. □

Observe that Q, as the image of P under all affine maps ρ, is stationary for the whole set Φ, and that all triangles in Φ can be obtained from each other by direct similarity centered at Q. If

$$\mu = -\frac{1 + i\tan(\phi)}{2},$$

with $\Re(\mu) = -1/2$ and $\arg(\mu) = 180^\circ + \phi$, the corresponding triangle under $\rho(w) = \frac{\mu}{t}(w - p) + q$ is obtained from the minimal one through direct similarity with angle ϕ and coefficient $\sec(\phi)$.

We shall prove the following statement about the stationary point Q for the family Φ.

Proposition 3. The point Q for Φ satisfies

$$\begin{aligned}\angle AQB &= \angle C + \angle Z,\\ \angle BQC &= \angle A + \angle X,\\ \angle CQA &= \angle B + \angle Y,\end{aligned}$$

where the angles above are directed. Furthermore,

$$AQ : BQ : CQ = \frac{YZ}{BC} : \frac{ZX}{CA} : \frac{XY}{AB}.$$

Proof. Consider the ratio

$$s = \frac{b-q}{a-q} \cdot \frac{x-z}{y-z} \cdot \frac{a-c}{b-c}, \tag{15}$$

whose argument is $\angle AQB - \angle C - \angle Z$ (where the angles are directed).

From (10), we have

$$\begin{aligned} s &= \frac{byz(c-b) + bxy(b-a) - xyc(b-a) - yza(c-b)}{azx(a-c) + axy(b-a) - xyc(b-a) - zxb(a-c)} \cdot \frac{x-z}{y-z} \cdot \frac{a-c}{b-c} \\ &= \frac{yz(b-a)(c-b) + xy(b-c)(b-a)}{zx(a-b)(a-c) + xy(a-c)(b-a)} \cdot \frac{x-z}{y-z} \cdot \frac{a-c}{b-c} \\ &= \frac{y(z-x)(b-a)(c-b)}{x(z-y)(a-b)(a-c)} \cdot \frac{x-z}{y-z} \cdot \frac{a-c}{b-c} \\ &= \frac{y}{x}\frac{(x-z)^2}{(y-z)^2} = \frac{(x-z)(\bar{x}-\bar{z})}{(y-z)(\bar{y}-\bar{z})} = \frac{|x-z|^2}{|y-z|^2} > 0 \end{aligned}$$

Therefore, $s \in \mathbb{R}^+$ with $\arg(s) = 0$, hence the first of the angular identities holds (the other two follow similarly). At the same time,

$$|s| = \frac{BQ}{AQ} \cdot \frac{XZ}{YZ} \cdot \frac{AC}{BC},$$

hence

$$\frac{BQ}{AQ} \cdot \frac{XZ}{YZ} \cdot \frac{AC}{BC} = \frac{XZ^2}{YZ^2},$$

That proves the second part of the proposition. $\square$

The minimal triangle in the family is therefore the pedal triangle of Q. All other triangles in Φ are obtained from it by direct similarities centered at Q.

4 Special cases

We saw that if $\triangle XYZ$ is similar to the mirror image of $\triangle ABC$, the set Φ is empty. More interesting are the cases where $\triangle XYZ$ is similar to one of the triangles $\triangle ABC, \triangle BCA$, or $\triangle CAB$. Consider the sets $\Phi_1 = \Phi_{\triangle ABC}(\triangle BCA)$ and $\Phi_2 = \Phi_{\triangle ABC}(\triangle CAB)$. Using

(9), (10), and (5), we can show that

$$
\begin{aligned}
t_1 &= \frac{3abc - ab^2 - bc^2 - ca^2}{(a-b)(b-c)(c-a)},\\
t_2 &= \frac{ac^2 + cb^2 + ba^2 - 3abc}{(a-b)(b-c)(c-a)},\\
p_1 = q_1 &= \frac{a^2b^2 + b^2c^2 + c^2a^2 - abc(a+b+c)}{ac^2 + cb^2 + ba^2 - 3abc},\\
p_2 = q_2 &= \frac{a^2b^2 + b^2c^2 + c^2a^2 - abc(a+b+c)}{ab^2 + bc^2 + ca^2 - 3abc}
\end{aligned}
$$

Notice that

$$
\begin{gathered}
|t_1| = |t_2|,\\
|p_1| = |q_1| = |p_2| = |q_2|.
\end{gathered}
$$

The equality $|t_1| = |t_2|$ implies that the feet of the perpendiculars from Q_1 and Q_2 onto the sides of $\triangle ABC$ form congruent triangles, as both are minimal for Φ_1 and Φ_2 and obtained from $\triangle ABC$ through direct similarities with magnitude $\dfrac{1}{2|t|}$. The fact that $|q_1| = |q_2|$ shows the stationary points for Φ_1 and Φ_2 are equidistant from the circumcenter of $\triangle ABC$.

Proposition 4. The points Q_1 and Q_2 are internal for $\triangle ABC$ and satisfy the following identities:

$$
\begin{aligned}
\angle Q_1AB = \angle Q_1BC = \angle Q_1CA &= \theta,\\
\angle Q_2BA = \angle Q_2CB = \angle Q_2AC &= \theta,\\
\angle Q_1OQ_2 &= 2\theta
\end{aligned}
$$

where $\theta \leq 30^\circ$ is the solution of the equation

$$
\tan(\theta) = \frac{\sin(\angle A)\sin(\angle B)\sin(\angle C)}{\cos(\angle A)\cos(\angle B)\cos(\angle C) + 1}.
$$

Proof. Consider Q_1 first. From Proposition 3, it follows that the directed angles $\angle AQ_1B, \angle BQ_1C$, and $\angle CQ_1A$ are $\angle C + \angle A$, $\angle A + \angle B$, and $\angle B + \angle C$ respectively. Those are less than 180°, hence Q_1 is internal for $\triangle ABC$. Now, if $\theta = \angle Q_1AB$, we get $\angle Q_1BA = \angle B - \theta$ so $\angle Q_1BC = \theta$. Similarly, $\angle Q_1CA = \theta$.

Next, to determine θ, consider the argument of the following complex number, whose argument is $-\theta$:

$$
\begin{aligned}
\frac{b-a}{q_1-a} &= \frac{(ac^2 + cb^2 + ba^2 - 3abc)(b-a)}{a^2b^2 + b^2c^2 + c^2a^2 - abc(a+b+c) - a(ac^2 + cb^2 + ba^2 - 3abc)}\\
&= \frac{(ac^2 + cb^2 + ba^2 - 3abc)(b-a)}{b(a^2 + c^2 - 2ac)(b-a)} = \frac{(ac^2 + cb^2 + ba^2 - 3abc)}{b(a^2 + c^2 - 2ac)}\\
&= \frac{c/b + b/a + a/c - 3}{a/c + c/a - 2} = \frac{3 - (c/b + b/a + a/c)}{|a-c|^2}\\
&= \frac{3 - (\cos(2\angle A) + \cos(2\angle B) + \cos(2\angle C))}{|a-c|^2}\\
&\quad - i\,\frac{\sin(2\angle A) + \sin(2\angle B) + \sin(2\angle C)}{|a-c|^2}
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
\tan(-\theta) &= -\frac{\sin(2\angle A)+\sin(2\angle B)+\sin(2\angle C)}{3-\cos(2\angle A)-\cos(2\angle B)-\cos(2\angle C)} \\
&= -\frac{4\sin(\angle A)\sin(\angle B)\sin(\angle C)}{2\sin^2(\angle A)+2\sin^2(\angle B)+2\sin^2(\angle C)} \\
&= -\frac{\sin(\angle A)\sin(\angle B)\sin(\angle C)}{\cos(\angle A)\cos(\angle B)\cos(\angle C)+1}
\end{aligned}
$$

The proof for Q_2 is analogous and yields the same θ, since the solution of the equation is unique. Next, to prove that $\angle Q_1OQ_2 = 2\theta$, consider the ratio

$$
\frac{q_2}{q_1} = \frac{ac^2+cb^2+ba^2-3abc}{ab^2+bc^2+ca^2-3abc} = \frac{3-(c/b+b/a+a/c)}{3-(b/c+c/a+a/b)},
$$

whose argument, as we saw earlier, is $-\theta-\theta=-2\theta$.

To prove the last bit, namely that $\theta \le 30^\circ$, consider Sine Ceva's theorem for Q_1:

$$
\sin^3(\theta) = \sin(\angle A-\theta)\sin(\angle B-\theta)\sin(\angle C-\theta).
$$

Taking logarithms on both sides and observing that the function $\ln(\sin(x))$ is concave for $x \in (0,\pi)$, we have

$$
\begin{aligned}
3\ln(\sin(\theta)) &= \ln(\sin(\angle A-\theta))+\ln(\sin(\angle B-\theta))+\ln(\sin(\angle C-\theta)) \\
&\le 3\ln\left(\sin\left(\frac{\angle A-\theta+\angle B-\theta+\angle C-\theta)}{3}\right)\right) \\
&= 3\ln(\sin(60^\circ-\theta))
\end{aligned}
$$

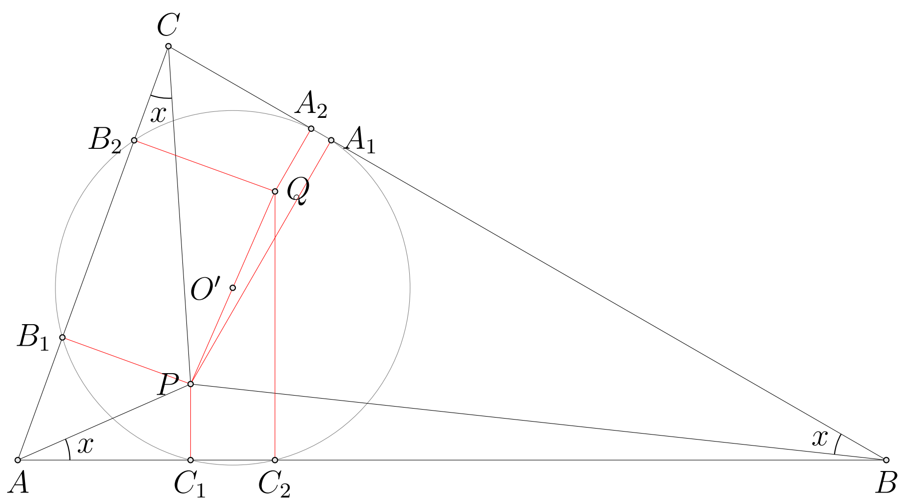
Notice that $\theta \le \angle A, \angle B, \angle C$, hence $\theta \in (0, 60^\circ)$, where $\ln(\sin(x))$ is increasing, hence $\theta \le 60^\circ - \theta$ and the proof is complete. $\square$

All these results can be nicely formulated as a problem.

Problem 1. Points P and Q inside an acute-angled $\triangle ABC$ are such that $\angle PCA = \angle PAB = \angle PBC$ and $\angle QAC = \angle QBA = \angle QCB$. Prove that

(i) the feet of the perpendiculars from P and Q to the sides of $\triangle ABC$ lie on a circle whose center is the midpoint of PQ.

(ii) if O is the circumcenter of $\triangle ABC$, then $PO = QO$.



5 Outscribed triangles

Consider again $\triangle ABC$ and $\triangle XYZ$ inscribed in the unit circle, and let $\Sigma_{\triangle ABC}(\triangle XYZ) = \Sigma$ denote all triangles similar to $\triangle XYZ$ such that $\triangle ABC$ is inscribed in them. We shall find the general form of the affine maps sending $\triangle XYZ$ into triangles $\triangle X''Y''Z''$ from Σ.

Consider such a transform σ and let $\sigma(w) = uw + v$. We have $\sigma(\triangle XYZ) = \triangle X''Y''Z''$, hence $\sigma^{-1}(\triangle X''Y''Z'') = \triangle XYZ$. As $\triangle ABC$ is inscribed in $\triangle X''Y''Z''$, it follows that $\triangle A'B'C' = \sigma^{-1}(\triangle ABC)$ is inscribed in

$$\sigma^{-1}(\triangle X''Y''Z'') = \triangle XYZ,$$

hence $\triangle A'B'C' \in \Phi_{\triangle XYZ}(\triangle ABC)$. Using the formula (11), we get

$$\sigma^{-1}(w) = \frac{1}{u}w - \frac{v}{u} = \frac{\mu}{t^*}(w - p^*) + q^*,$$

where p^*, q^*, t^* are obtained from the same formulas as p, q, t in (5),(9),(10) but with the triples x, y, z and a, b, c interchanged. Thus,

$$\sigma(w) = uw + v = \frac{t^*}{\mu}(w - q^*) + p^*. \tag{16}$$

We shall examine the image of any given point $W \neq Q^*$ under the various transforms σ. Let its complex coordinate be w, and let $w' = \sigma(w)$. From (16), we have

$$w' = p^* + \frac{t^*(w - q^*)}{\mu}.$$

Set

$$\alpha = t^*(w - q^*), \qquad \xi = \frac{1}{\mu}.$$

Then

$$w' = p^* + \alpha\xi.$$

Now $\Re(\mu) = -1/2$, so if $\xi = u + iv$, then

$$\Re\left(\frac{1}{\xi}\right) = \Re(\mu) = -\frac{1}{2}.$$

Since

$$\frac{1}{\xi} = \frac{\bar{\xi}}{|\xi|^2} = \frac{u - iv}{u^2 + v^2},$$

it follows that

$$\frac{u}{u^2 + v^2} = -\frac{1}{2} \Rightarrow u^2 + v^2 + 2u = 0 \Leftrightarrow (u + 1)^2 + v^2 = 1.$$

Therefore ξ runs over the circle with diameter endpoints 0 and -2. Multiplying by α and translating by p^*, we conclude that w' runs over the circle with diameter endpoints

$$p^* \qquad \text{and} \qquad p^* - 2t^*(w - q^*).$$

If $w = q^*$, then $\alpha = 0$ and the image degenerates to the single point p^*.

We conclude that the whole family of transforms has the common point P^*, and for every point $W \neq Q^*$ its image is a circle passing through P^*.

6 Hyperbola

Consider the special case $\triangle XYZ \sim \triangle ABC$ and the families Φ and Σ of inscribed and outscribed triangles to $\triangle ABC$ similar to it.

Notice that in that case $t = t^* = 1$, $p = p^* = h$ (where H is the orthocenter of $\triangle ABC$), and $q = q^* = 0$.

For every $\phi \in (-90°, 90°)$, consider

$$\mu_1 = -\frac{1 + i\tan(\phi)}{2}, \mu_2 = -\frac{1 - i\tan(\phi)}{2},$$

The corresponding transforms ρ and σ as defined in (11) and (16) become

$$\rho(w) = \mu_1(w - h),$$
$$\sigma(w) = \frac{1}{\mu_2}w + h$$

The corresponding triangles from Φ and Σ under (11) and (16) are obtained from the same triangle by direct similarities with coefficients μ_1 and $\frac{1}{\mu_2}$ respectively. The ratio of those coefficients, $\mu_1\mu_2$, is real for every ϕ, hence the two triangles are homothetic. We shall examine this homothety as ϕ varies between $-90°$ and $90°$. Suppose its center is s and its coefficient is λ, both functions of ϕ. We have

$$\frac{\rho(a) - s}{\sigma(a) - s} = \lambda = \mu_1\mu_2,$$

Plugging in the values for $\rho(a)$ and $\sigma(a)$, we solve the linear equation for s to get

$$s = h\frac{\mu_1 + \mu_1\mu_2}{\mu_1\mu_2 - 1},$$

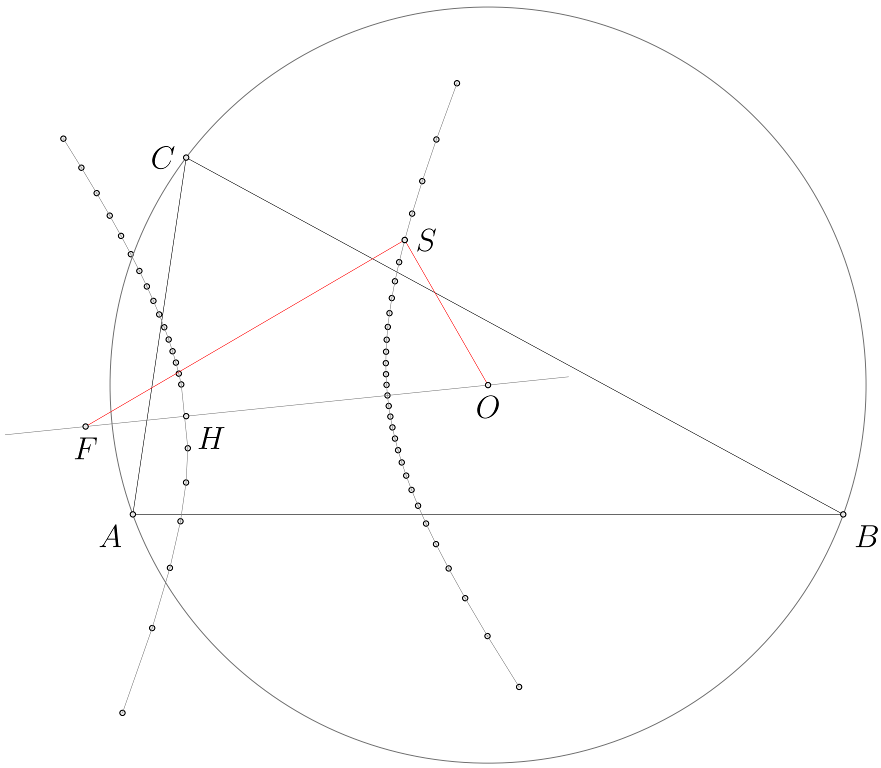
hence, if we set $\tan(\phi) = r$,

$$\frac{s}{h} = \frac{1 - r^2}{3 - r^2} + i\frac{2r}{3 - r^2}.$$

We can show that

$$\left|s - \frac{4}{3}h\right| - |s| = \pm\left|\frac{2}{3}h\right|,$$

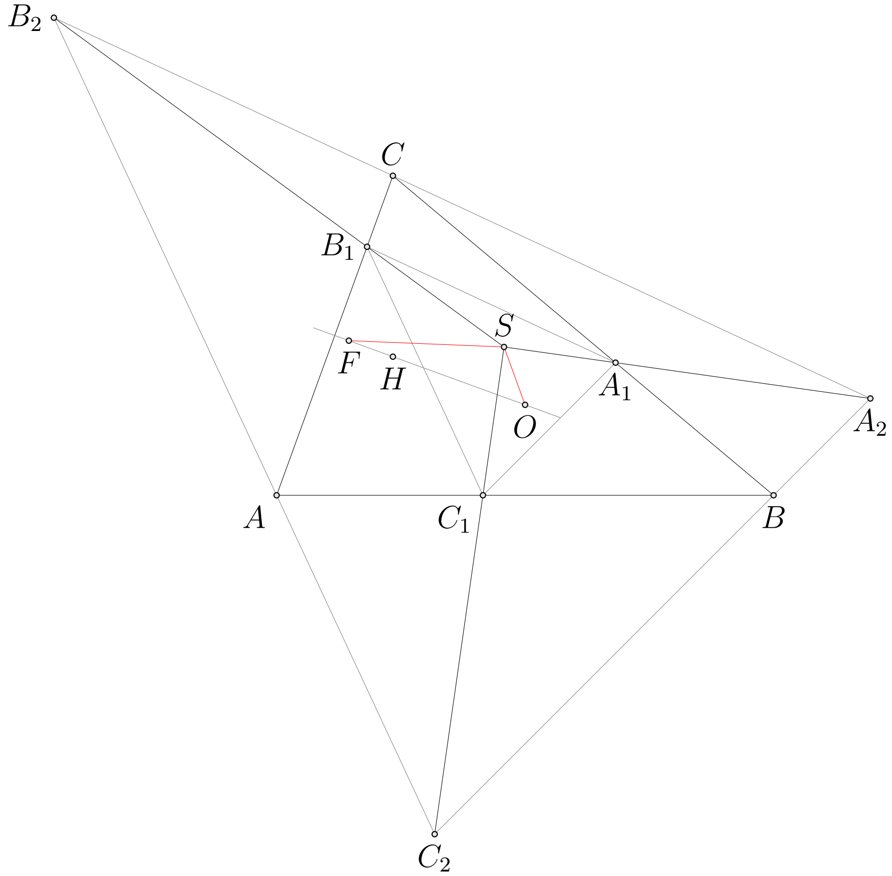
where we take sign $+$ when $r^2 < 3$ and sign $-$ when $r^2 > 3$. The case $r^2 = 3$ corresponds to the case when the inscribed and outscribed triangles are the same, hence the homothety is a translation and its center is a point at infinity. In all other cases, s lies on a hyperbola with foci O and the point symmetric to O across the midpoint of GH, both lying on the Euler line. Which leg of the hyperbola s lies on is determined by whether $r^2 < 3$ or $r^2 > 3$, equivalently whether $|\phi| < 60°$ or $|\phi| > 60°$.



This last result can be stated as a problem.

Problem 2. Let $\triangle ABC$ be a non-equilateral triangle with circumcenter O and orthocenter H. Let F lie on ray $\overrightarrow{OH}$ such that $OF : OH = 4 : 3$.
Points A_1, B_1, C_1 lie on BC, CA, AB respectively such that $\triangle A_1B_1C_1 \sim \triangle ABC$. The lines through A, B, C parallel to B_1C_1, C_1A_1, A_1B_1 intersect pairwise at C_2, A_2, B_2, respectively.
Prove that the lines A_1A_2, B_1B_2, and C_1C_2 concur at a point S satisfying

$$SF - SO = \frac{2}{3}OH.$$


B_2
C
B_1
S
F
H
A_1
O
A_2
A
C_1
B
C_2

Certain applications of the roots of unity

Abstract

The objective of this article is to illustrate the use of the roots of unity for solving problems from various mathematical areas, like combinatorics, algebra, number theory. The selected examples are either original or from national and international mathematical competitions.

It is well known that for every natural number n the equation

$$x^n - 1 = 0$$

has n distinct complex roots $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}$, where

$$\varepsilon_j = \cos\left(\frac{2\pi j}{n}\right) + i \sin\left(\frac{2\pi j}{n}\right), \quad j = 0, 1, \ldots, n-1.$$

The complex numbers ε_j have modulus 1 and if we set

$$\varepsilon = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right),$$

then from De Moivre's formula it follows that $\varepsilon_j = \varepsilon^j$. Furthermore $\varepsilon^k = \varepsilon^l$ for integers k and l if and only if $k \equiv l \pmod{n}$.

The following property of roots of unity is frequently used and therefore we isolate it as:

Lemma. For every positive integer n,

$$\sum_{j=0}^{n-1} \varepsilon_j^k = \begin{cases} n, & \text{if } k \equiv 0 \pmod{n} \\ 0, & \text{if } k \not\equiv 0 \pmod{n} \end{cases} \tag{*}$$

Proof. Notice that $\varepsilon^k = 1$ if and only if $k \equiv 0 \pmod{n}$. Therefore

$$\sum_{j=0}^{n-1} \varepsilon_j^k = \sum_{j=0}^{n-1} (\varepsilon^k)^j = \begin{cases} \frac{\varepsilon^{kn}-1}{\varepsilon^k - 1} = \frac{1-1}{\varepsilon^k-1} = 0, & \text{if } k \not\equiv 0 \pmod{n}, \\ 1 + 1 + \cdots + 1 = n, & \text{if } k \equiv 0 \pmod{n}. \end{cases}$$

Let us note that roots of unity can be represented geometrically as the vertices of a regular n-gon inscribed in the unit circle.

We begin with two problems where exactly this geometric interpretation is used.

Problem 1. (USSR Olympiad 1970) The vertices of a regular n-gon are colored in some colors (each vertex in one color) such that the points of one and the same color are vertices of regular polygons. Prove that among these polygons there are two identical ones.

Solution. Without loss of generality we may consider the vertices of the n-gon as n-th roots of unity. Suppose that no two monochromatic polygons are identical and let them have respectively $d_1 < d_2 < \cdots < d_m$ vertices.

Let us sum the d_1-th powers of the "vertices" of these polygons. From $n > d_1$ it follows that n does not divide d_1, and from (*) we conclude that this sum is 0.

But if we compute this sum separately for each of the monochromatic polygons, then from $d_j > d_1$ for $j = 2, 3, \dots, m$ and $d_1 \mid d_1$ it follows by (*) that it equals

$$\varepsilon^k d_1 + 0 + \cdots + 0 = d_1 \varepsilon^k \neq 0$$

for some integer k. The obtained contradiction proves the statement. □

Problem 2. (USAMO) Points $A_1, A_2, \dots, A_n$ are chosen on the unit circle. Prove that if

$$|MA_1| \cdot |MA_2| \cdots |MA_n| \leq 2$$

for every point M on the circle, then $A_1, A_2, \dots, A_n$ are vertices of a regular n-gon.

Solution. Consider the polynomial

$$f(z) = (z - a_1)(z - a_2) \cdots (z - a_n),$$

where a_j is the affix of point A_j. Notice that if M has affix z on the unit circle, then

$$|MA_1| \cdot |MA_2| \cdots |MA_n| = |f(z)|.$$

Let

$$a = (-1)^n (a_1 a_2 \cdots a_n)^{-1}, \quad \tau = a^{1/n}, \quad |a| = |\tau| = 1.$$

Set

$$g(z) = af\left(\frac{z}{\tau}\right) = z^n + A_{n-1} z^{n-1} + \cdots + A_1 z + 1.$$

If we assume $|f(z)| \leq 2$ for every $z : |z| = 1$, then also $|g(z)| \leq 2$ for every $z : |z| = 1$. Then we obtain

$$2n = \left| \sum_{j=0}^{n-1} g(\varepsilon_j) \right| \leq \sum_{j=0}^{n-1} |g(\varepsilon_j)| \leq 2n.$$

This is possible only when $g(\varepsilon_j) = 2$ for $j = 0, 1, \dots, n-1$.

This means that $g(z) - 2 = z^n - 1$ and therefore the equation $f(z) = 0$ has roots

$$\frac{1}{\tau}\left(\cos\left(\frac{(2j-1)\pi}{n}\right) + i \sin\left(\frac{(2j-1)\pi}{n}\right)\right),$$

for $j = 1, 2, \dots, n$, which are vertices of a regular n-gon. □

Problem 3. (MOM'95 Canada) For a given prime $p > 2$ determine the number of p-element subsets of $\{1, 2, \dots, 2p\}$ such that the sum of their elements is divisible by p.

Solution. Consider the polynomial

$$f(x, y) = (1 + yx)(1 + yx^2)(1 + yx^3) \cdots (1 + yx^{2p}).$$

It can be written in the form

$$f(x,y)=q_0(x)+q_1(x)y+\cdots+q_{2p}(x)y^{2p},$$

with $q_k(x)=\sum x^{\alpha_1+\cdots+\alpha_k}$, where the sums are taken over all k-element subsets of $\{1,2,\ldots,2p\}$. Now let

$$q_p(x)=A_0+A_1x+A_2x^2+\cdots,$$

then the sought number is

$$A=A_0+A_p+A_{2p}+\cdots.$$

From (*) we have

$$\sum_{j=0}^{p-1} f(x,\varepsilon_j)=p(q_0(x)+q_p(x)+q_{2p}(x))=p(1+x^{p(2p+1)})+pq_p(x).$$

But

$$\sum_{j=0}^{p-1} q_p(\varepsilon_j)=p(A_0+A_p+\cdots)=pA,$$

so

$$\sum_{j,k=0}^{p-1} f(\varepsilon_j,\varepsilon_k)=p(p+p)+p^2A=p^2(A+2).$$

We compute the same sum:

$$\sum_{j,k=0}^{p-1} f(\varepsilon_j,\varepsilon_k)=\sum_{k=0}^{p-1} f(1,\varepsilon_k)+\sum_{j=1}^{p-1}\sum_{k=0}^{p-1} f(\varepsilon_j,\varepsilon_k)$$

$$=\sum_{k=0}^{p-1}(1+\varepsilon_k)^{2p}+p(p-1)\prod_{j=0}^{p-1}(1+\varepsilon_j)^2.$$

We know that

$$g(x)=x^p-1=\prod_{j=0}^{p-1}(x-\varepsilon_j),$$

thus

$$4=g^2(-1)=\prod_{j=0}^{p-1}(1+\varepsilon_j)^2,$$

and from (*) we have

$$\sum_{j=0}^{p-1}(1+\varepsilon_j)^{2p}=p\binom{2p}{0}+p\binom{2p}{p}+p\binom{2p}{2p}=p\left(2+\binom{2p}{p}\right).$$

Thus

$$p^2(A+2)=4p^2-2p+p\binom{2p}{p}$$

and

$$A = \frac{\binom{2p}{p} - 2}{p} + 2.$$

Problem 4. (Author) In a table (a_{kl}) of size 6×21 are written 18 zeros, 18 ones, ..., 18 sixes. For arbitrary $k, l \in [1, 6]$ and $p, q \in [1, 21]$ it holds

$$a_{kp} - a_{lp} \equiv a_{kq} - a_{lq} \pmod 7.$$

Show that in each row there are exactly 3 zeros, 3 ones, ..., 3 sixes.

Solution. Construct a new table (b_{kp}) where

$$b_{kp} = \varepsilon^{a_{kp}}, \quad \varepsilon = \cos\left(\frac{2\pi}{7}\right) + i \sin\left(\frac{2\pi}{7}\right).$$

Let the sum of numbers in the k-th row be s_k. From the condition we have $s_k = s_1 \varepsilon^{m_k}$ for some integers m_k, which we may consider to be integers between 0 and 6. Let

$$q(x) = 1 + x + \cdots + x^6.$$

Then

$$s_1(\varepsilon^{m_1} + \varepsilon^{m_2} + \cdots + \varepsilon^{m_6}) = \sum_{k=1}^{6} s_k = 18q(\varepsilon) = 0.$$

Let

$$p(x) = x^{m_1} + x^{m_2} + \cdots + x^{m_6}$$

and

$$s(x) = \sum_{p=1}^{21} x^{a_{1p}}.$$

Then $s(\varepsilon) = s_1$. Hence $s(\varepsilon)p(\varepsilon) = 0$, hence ε is a root of either $s(x)$ or $p(x)$. We shall use the well-known fact that $q(x)$ is irreducible over $\mathbb{Q}$.

If $p(\varepsilon) = q(\varepsilon) = 0$, it follows that $q(x) \mid p(x)$. Since $\deg(p) \le 6 = \deg(q)$, we get $p(x) = kq(x)$ for some integer k. But then $7k = kq(1) = p(1) = 6$, which is impossible.

Therefore, $s(\varepsilon) = q(\varepsilon) = 0$. Using the irreducibility of q we get $s(x) = kq(x)$. From $21 = s(1) = kq(1) = 7k$ we get $k = 3$, hence

$$s(x) = 3 + 3x + \cdots + 3x^6,$$

which shows that the first row of the table contains 3 zeros, 3 ones, $\dots$, 3 sixes. The same holds true for each of the other rows, with which the problem is solved. $\square$

Problem 5. (Leningrad Olympiad 1991) A sequence $a_0, a_1, \dots, a_{n-1}$ is called p-balanced if all sums of the form

$$a_k + a_{k+p} + a_{k+2p} + \cdots$$

for $k = 0, 1, \dots, p-1$ are equal.

Prove that if a sequence of 50 terms is p-balanced for $p = 3, 5, 7, 11, 13, 17$, then all terms are equal to 0.

Solution. Let the sequence be $a_0, a_1, \dots, a_{49}$. Form the polynomial

$$q(x) = \sum_{j=0}^{49} a_j x^j.$$

Take the prime $p = 13$ for starters and let $\varepsilon = \cos\left(\frac{2\pi}{p}\right) + i\sin\left(\frac{2\pi}{p}\right)$. Then for $k = 1, 2, \dots, p-1$ we have

$$\begin{aligned} q(\varepsilon^k) &= (a_0 + a_p + \cdots) + (a_1 + a_{p+1} + \cdots)\varepsilon^k + (a_2 + a_{p+2} + \cdots)\varepsilon^{2k} + \cdots \\ &= (a_0 + a_p + \cdots)\left(1 + \varepsilon^k + \varepsilon^{2k} + \cdots + \varepsilon^{(p-1)k}\right) \\ &= 0 \end{aligned}$$

owing to (*), so $\varepsilon^k, k = 1, 2, \dots, p-1$ gives us $p-1 = 12$ distinct roots of $q(x)$. Similarly, using the other primes $3, 5, 7, 11, 17$ we obtain that $q(x)$ has $(3-1) + (5-1) + (7-1) + (11-1) + (13-1) + (17-1) = 50$ distinct roots, since different primes give rise to disjoint sets of ε_k. From $\deg q = 49$, it follows that $q(x) \equiv 0$. Thus

$$a_0 = a_1 = \cdots = a_{49} = 0$$

and the proof is complete. □

Problem 6. (IMO 1999 shortlist) Let $p > 5$ be a prime number. Denote by $E(0, 1, 2)$ the number of all sums of the form

$$x_1 + 2x_2 + \cdots + (p-1)x_{p-1},$$

which are divisible by p, where $x_i \in \{0, 1, 2\}$. Analogously define the number $E(0, 1, 3)$. Prove that

$$E(0, 1, 2) < E(0, 1, 3).$$

Solution: Let us consider the polynomial

$$f(x) = (1 + x + x^2)(1 + x^2 + x^4) \cdots \left(1 + x^{p-1} + x^{2(p-1)}\right).$$

This can be written in the form

$$f(x) = \frac{(x^3 - 1)(x^6 - 1) \cdots (x^{3(p-1)} - 1)}{(x - 1)(x^2 - 1) \cdots (x^{p-1} - 1)}.$$

As usual, we set

$$\varepsilon_j = \cos\left(\frac{2\pi j}{p}\right) + i\sin\left(\frac{2\pi j}{p}\right), \quad j = 0, 1, \dots, p-1$$

and denote $\varepsilon = \varepsilon_1$. From (*) it follows that

$$pE(0, 1, 2) = \sum_{j=0}^{p-1} f(\varepsilon_j).$$

Observe that the following two sets are the same:

$$\{\varepsilon_0^3, \varepsilon_1^3, \dots, \varepsilon_{p-1}^3\} = \{\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{p-1}\}.$$

Then for $j = 1, 2, \dots, p-1$ we have:

$$f(\varepsilon_j) = \frac{(\varepsilon_j^3 - 1)(\varepsilon_j^6 - 1)\cdots(\varepsilon_j^{3(p-1)} - 1)}{(\varepsilon_j - 1)(\varepsilon_j^2 - 1)\cdots(\varepsilon_j^{p-1} - 1)} = 1.$$

Therefore

$$pE(0,1,2) = 3^{p-1} + p - 1.$$

Analogously we consider the polynomial

$$g(x) = (1 + x + x^3)(1 + x^2 + x^6)\cdots(1 + x^{p-1} + x^{3(p-1)}).$$

Again

$$pE(0,1,3) = \sum_{j=0}^{p-1} g(\varepsilon_j) = g(1) + \sum_{j=1}^{p-1} g(\varepsilon_j) = 3^{p-1} + (p-1)g(\varepsilon),$$

since $g(\varepsilon) = g(\varepsilon_1) = g(\varepsilon_2) = \dots = g(\varepsilon_{p-1})$. It remains to prove that

$$g(\varepsilon) > f(\varepsilon) = 1.$$

We have

$$\begin{aligned} g(\varepsilon) &= \prod_{j=1}^{p-1}(1 + \varepsilon^j + \varepsilon^{3j}) = \prod_{j=1}^{\frac{p-1}{2}}(1 + \varepsilon^j + \varepsilon^{3j})(\overline{1} + \overline{\varepsilon^j} + \overline{\varepsilon^{3j}}) = \\ &= \prod_{j=1}^{\frac{p-1}{2}} \left(3 + (\varepsilon^j + \overline{\varepsilon^j}) + (\varepsilon^{2j} + \overline{\varepsilon^{2j}}) + (\varepsilon^{3j} + \overline{\varepsilon^{3j}})\right) \\ &= \prod_{j=1}^{\frac{p-1}{2}} \left(3 + 2\cos\left(\frac{2\pi j}{p}\right) + 2\cos\left(\frac{4\pi j}{p}\right) + 2\cos\left(\frac{6\pi j}{p}\right)\right) \\ &= \prod_{j=1}^{\frac{p-1}{2}} q\left(\cos(\alpha_j)\right), \end{aligned}$$

where

$$\alpha_j = \frac{2\pi j}{p}$$

and

$$q(x) = 3 + 2x + 2(2x^2 - 1) + 2(4x^3 - 3x) = 8x^3 + 4x^2 - 4x + 1.$$

More detailed investigation of $q(x) = q(\cos(\alpha))$ and its extrema shows that:

1. $q(x) > 1, \quad$ for $x \in (-1, 0) \leftrightarrow \alpha \in \left(\frac{\pi}{2}, \pi\right)$;
2. $q(x) \geq \frac{47 - 14\sqrt{7}}{27} > \frac{1}{3}, \quad$ for $x \in \left[0, \frac{1}{2}\right] \leftrightarrow \alpha \in \left[\frac{\pi}{3}, \frac{\pi}{2}\right]$;

3. $q(x) \geq 1, \quad$ for $x \in \left[\frac{1}{2}, \frac{\sqrt{2}}{2}\right] \leftrightarrow \alpha \in \left[\frac{\pi}{4}, \frac{\pi}{3}\right]$;

4. $q(x) \geq 3, \quad$ for $x \in \left[\frac{\sqrt{2}}{2}, 1\right] \leftrightarrow \alpha \in \left[0, \frac{\pi}{4}\right]$.

Consider those four intervals for α_j. When α_j lies in the first or third interval, $q(\cos(\alpha_j)) \geq 1$; when it lies in the second interval, $q(\cos(\alpha_j)) > \frac{1}{3}$; and when it lies in the fourth interval, $q(\cos(\alpha_j)) \geq 3$. There is at least one α_j in the first interval where $q(\cos(\alpha_j)) > 1$, e.g. for $j = \frac{p-1}{2}$ as long as $p > 2$. So to prove the strict inequality $g(\varepsilon) > 1$, it remains to prove that the number of the α_j in the second interval does not exceed the number of the α_j in the fourth interval. Those counts are respectively

$$\left\lfloor \frac{p}{4} \right\rfloor - \left\lfloor \frac{p}{6} \right\rfloor \quad \text{and} \quad \left\lfloor \frac{p}{8} \right\rfloor .$$

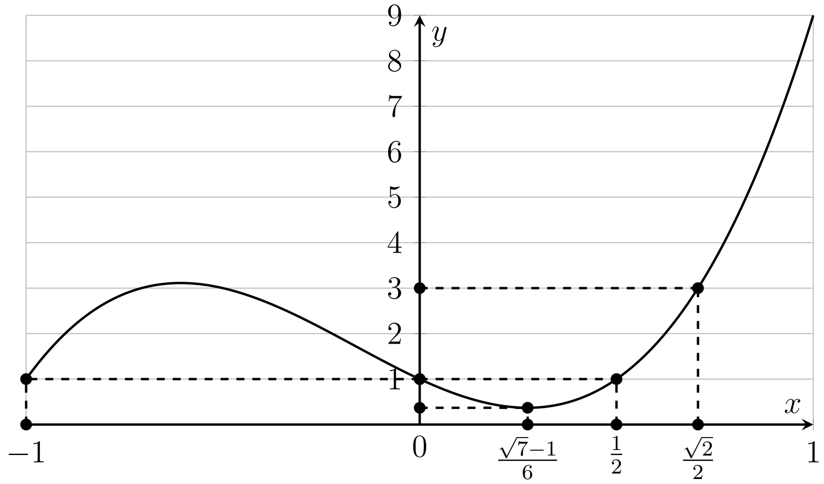
We need to show that for every prime $p > 5$

$$\left\lfloor \frac{p}{8} \right\rfloor \geq \left\lfloor \frac{p}{4} \right\rfloor - \left\lfloor \frac{p}{6} \right\rfloor .$$

For $p = 7, 11, 13, 17, 19, 23, 29, 31$ this is checked directly. For $p \geq 35$ we have

$$\left\lfloor \frac{p}{8} \right\rfloor \geq \frac{p-7}{8} \geq \frac{p-1}{4} - \frac{p-5}{6} \geq \left\lfloor \frac{p}{4} \right\rfloor - \left\lfloor \frac{p}{6} \right\rfloor$$

and the proof is complete. □



The next problem is original. It was not in the first version of the article from 2002, as the number 2026 gives it away, but I added it here as it fits nicely with the topic.

Problem 7. Let $n = 2026$. Given a regular n-gon $A_1 A_2 \cdots A_n$ with side length 1, prove that one can choose a subset of the vectors

$$\overrightarrow{A_1A_2}, \overrightarrow{A_2A_3}, \ldots, \overrightarrow{A_nA_1}$$

whose sum is a nonzero vector of length less than

$$\frac{2n}{5\left(2^{\frac{n-2}{4}}-1\right)}.$$

Solution. Write $n = 2p$, where $p = 1013$ is an odd prime. Identify the plane of the polygon with the complex plane in such a way that the side vectors

$$\overrightarrow{A_1A_2}, \overrightarrow{A_2A_3}, \ldots, \overrightarrow{A_nA_1}$$

correspond to

$$1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1},$$

where

$$\varepsilon = e^{2\alpha i}, \qquad \alpha = \frac{\pi}{n}.$$

It suffices to find a nonempty subset of $\{1, \varepsilon, \ldots, \varepsilon^{n-1}\}$ whose sum is nonzero and suitably small. Let $m = \dfrac{p-1}{2}$, and for $j = 0, 1, \ldots, m-1$, define

$$q_j = \{\varepsilon^j, \varepsilon^{p-j-1}\}, \qquad t_j = \{\varepsilon^{p+j}, \varepsilon^{2p-j-1}\}.$$

These $2m = p - 1$ groups are pairwise disjoint. Also, each element of q_j is opposite to the corresponding element of t_j, since

$$\varepsilon^j = -\varepsilon^{p+j}, \qquad \varepsilon^{p-j-1} = -\varepsilon^{2p-j-1}.$$

For each integer j, let B_j be the point on the unit circle corresponding to the complex number ε^j, and let O be the origin. Then each triangle $\triangle B_jOB_{p-j-1}$ is isosceles, and

$$\angle OB_jB_{p-j-1} = \angle OB_{p-j-1}B_j = (2j+1)\alpha.$$

The internal angle bisector of $\angle B_jOB_{p-j-1}$ is the same ray for every j; denote it by $\overrightarrow{OU}$, where U is the point on the unit circle such that

$$\angle UOB_0 = \frac{\pi}{2} - \alpha.$$

Hence

$$\overrightarrow{OB_j} + \overrightarrow{OB_{p-j-1}} = 2\sin\left((2j+1)\alpha\right)\overrightarrow{OU}.$$

Equivalently, if s_j denotes the sum of the elements in q_j, then

$$s_j = 2\sin((2j+1)\alpha)u,$$

where u is the unit vector in the direction of $\overrightarrow{OU}$.

Let $M = \{0, 1, \ldots, m-1\}$. We shall show that the 2^m subset sums

$$\sum_{j\in A} s_j, \qquad A \subseteq M,$$

are all distinct. Suppose, to the contrary, that

$$\sum_{j\in A'} s_j = \sum_{j\in A''} s_j$$

for two distinct subsets $A', A'' \subseteq M$. Removing common elements if necessary, we may assume that A' and A'' are disjoint. Then ε is a root of the polynomial

$$a(x) = \sum_{j \in A'} (x^j + x^{p-1-j}) - \sum_{j \in A''} (x^j + x^{p-1-j}).$$

The minimal polynomial of ε over $\mathbb{Q}$ is

$$b(x) = x^{p-1} - x^{p-2} + \cdots - x + 1.$$

Indeed,

$$b(\varepsilon)(1 + \varepsilon) = \varepsilon^p + 1 = 0,$$

and since $\varepsilon \neq -1$, we get $b(\varepsilon) = 0$. Also, $b(x)$ is irreducible over $\mathbb{Q}$ because

$$b(-x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \Phi_p(x),$$

the pth cyclotomic polynomial. Hence $b(x)$ is the minimal polynomial of ε, so

$$b(x) \mid a(x).$$

Therefore $\deg a \geq \deg b = p - 1$. On the other hand, since $0 \leq j \leq m - 1$, we have $\deg a \leq p - 1$, with equality only if $0 \in A'$ or $0 \in A''$. Without loss of generality, assume $0 \in A'$. Then

$$a(x) = (1 + x^{p-1}) + c(x) = b(x) + d(x) + c(x),$$

where

$$c(x) = \sum_{j \in A' \setminus \{0\}} (x^j + x^{p-1-j}) - \sum_{j \in A''} (x^j + x^{p-1-j}),$$

and

$$d(x) = x^{p-2} - x^{p-3} + \cdots + x.$$

Both $c(x)$ and $d(x)$ have degree at most $p - 2$. Since $b(x) \mid a(x)$, we have

$$b(x) \mid (c(x) + d(x)).$$

But $\deg(c + d) \leq p - 2$, so this forces $c(x) + d(x) \equiv 0$, which is impossible because $c(1) = 2(|A'| - 1) - 2|A''|$ is even, while $d(1) = 1$ is odd. Contradiction.

Thus the 2^m subset sums $\sum_{j \in A} s_j$ are all distinct. Each has the form λu, where

$$0 \leq \lambda \leq 2 \sum_{j=0}^{m-1} \sin((2j + 1)\alpha) < 2 \sum_{j=0}^{m-1} (2j + 1)\alpha = 2m^2\alpha.$$

Hence these 2^m distinct points all lie on a segment of length less than $2m^2\alpha$. By the pigeonhole principle, two of them must be at distance less than

$$\Delta = \frac{2m^2\alpha}{2^m - 1}.$$

So there exist distinct subsets $A', A'' \subseteq M$ such that

$$\left| \sum_{j \in A'} s_j - \sum_{j \in A''} s_j \right| \in (0, \Delta).$$

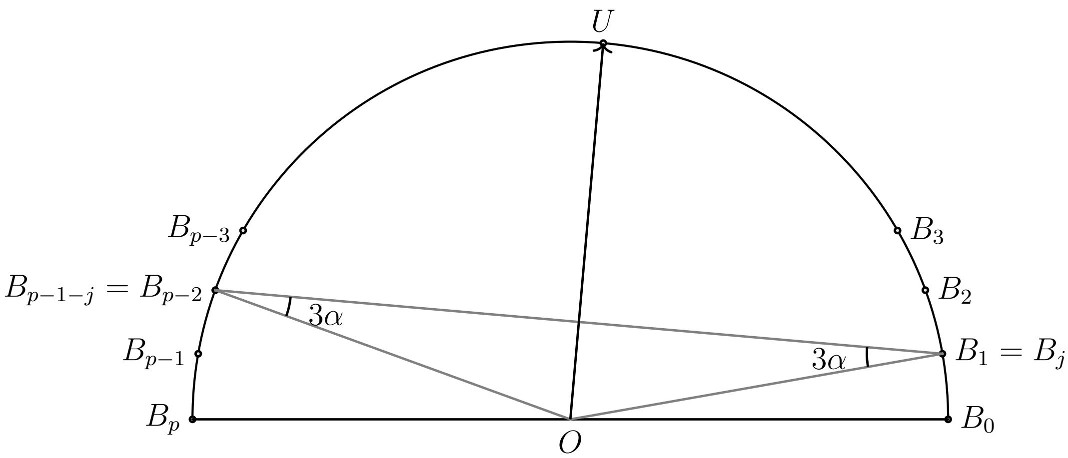
Therefore

$$\left|\sum_{j\in A'}\sum_{x\in q_j} x + \sum_{j\in A''}\sum_{x\in t_j} x\right| = \left|\sum_{j\in A'} s_j - \sum_{j\in A''} s_j\right| \in (0,\Delta).$$

This is the sum of a subset of the original n vectors. Finally,

$$\Delta = \frac{\pi}{n}\left(\frac{n-2}{4}\right)^2 \frac{2}{2^{(n-2)/4}-1} = \frac{\pi(n-2)^2}{8n\left(2^{(n-2)/4}-1\right)} < \frac{2n}{5\left(2^{(n-2)/4}-1\right)},$$

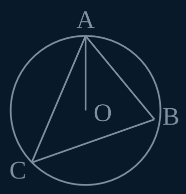
since $\pi < 16/5$ and $(n-2)^2 < n^2$. This completes the proof. $\square$



Example with $j = 1$

We shall conclude the article by leaving one last problem for exercise.

Problem 8. Given is a regular 2001-gon $A_0A_1\ldots A_{2000}$ inscribed in the unit circle. Prove that $|A_0A_1|\cdot|A_0A_2|\cdots|A_0A_{2000}| = 2001$.



$a^2 + b^2 = c^2$

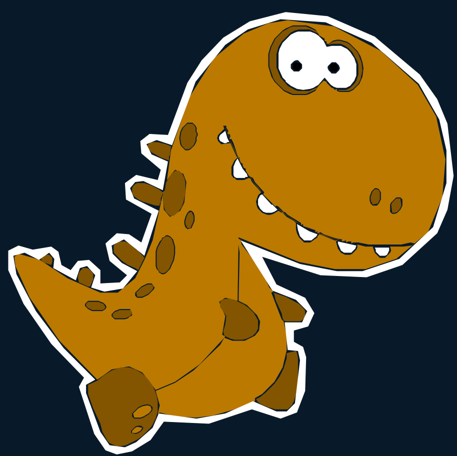
Selected Math Works

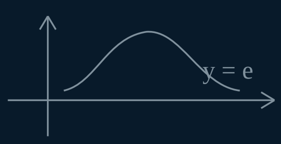
Math is more art than science

Selected Math Works brings together two collections of original problems and three articles I wrote during my high-school years, spanning algebra, combinatorics, number theory, and geometry.

Written for students who enjoy olympiad mathematics, as well as readers who appreciate elegant arguments, experimentation, and the pleasure of solving difficult problems, this collection presents mathematics not merely as a useful tool, but as a creative pursuit.

Vladimir Barzov





$k = n(n+1)/2$