The 15^{th} Romanian Master of Mathematics Competition

Day 1: Wednesday, February 28^{th}, 2024, Bucharest

Language: English

Problem 1. Let n be a positive integer. Initially, a bishop is placed in each square of the top row of a $2^n \times 2^n$ chessboard; those bishops are numbered from 1 to 2^n, from left to right. A *jump* is a simultaneous move made by all bishops such that the following conditions are satisfied:

- each bishop moves diagonally, in a straight line, some number of squares, and
- at the end of the jump, the bishops all stand in different squares of the same row.

Find the total number of permutations σ of the numbers $1, 2, \ldots, 2^n$ with the following property: There exists a sequence of jumps such that all bishops end up on the bottom row arranged in the order $\sigma(1), \sigma(2), \ldots, \sigma(2^n)$, from left to right.

Problem 2. Consider an odd prime p and a positive integer $N < 50p$. Let $a_1, a_2, \ldots, a_N$ be a list of positive integers less than p such that any specific value occurs at most $\frac{51}{100}N$ times and $a_1 + a_2 + \cdots + a_N$ is not divisible by p. Prove that there exists a permutation $b_1, b_2, \ldots, b_N$ of the a_i such that, for all $k = 1, 2, \ldots, N$, the sum $b_1 + b_2 + \cdots + b_k$ is not divisible by p.

Problem 3. Given a positive integer n, a set $\mathcal{S}$ is *n-admissible* if

- each element of $\mathcal{S}$ is an unordered triple of integers in $\{1, 2, \ldots, n\}$,
- $|\mathcal{S}| = n - 2$, and
- for each $1 \leq k \leq n-2$ and each choice of k distinct $A_1, A_2, \ldots, A_k \in \mathcal{S}$,

$$|A_1 \cup A_2 \cup \cdots \cup A_k| \geq k + 2.$$

Is it true that, for all $n > 3$ and for each n-admissible set $\mathcal{S}$, there exist pairwise distinct points $P_1, \ldots, P_n$ in the plane such that the angles of the triangle $P_iP_jP_k$ are all less than 61° for any triple $\{i, j, k\}$ in $\mathcal{S}$?

Each problem is worth 7 marks.
Time allowed: $4\frac{1}{2}$ hours.

The 15^{th} Romanian Master of Mathematics Competition

Day 2: Thursday, February 29^{th}, 2024, Bucharest

Language: English

Problem 4. Fix integers a and b greater than 1. For any positive integer n, let r_n be the (non-negative) remainder that b^n leaves upon division by a^n. Assume there exists a positive integer N such that $r_n < 2^n/n$ for all integers $n \geq N$. Prove that a divides b.

Problem 5. Let BC be a fixed segment in the plane, and let A be a variable point in the plane not on the line BC. Distinct points X and Y are chosen on the rays $\overrightarrow{CA}$ and $\overrightarrow{BA}$, respectively, such that $\angle CBX = \angle YCB = \angle BAC$. Assume that the tangents to the circumcircle of ABC at B and C meet line XY at P and Q, respectively, such that the points X, P, Y, and Q are pairwise distinct and lie on the same side of BC. Let Ω_1 be the circle through X and P centred on BC. Similarly, let Ω_2 be the circle through Y and Q centred on BC. Prove that Ω_1 and Ω_2 intersect at two fixed points as A varies.

Problem 6. A polynomial P with integer coefficients is *square-free* if it is not expressible in the form $P = Q^2R$, where Q and R are polynomials with integer coefficients and Q is not constant. For a positive integer n, let $\mathcal{P}_n$ be the set of polynomials of the form

$$1 + a_1x + a_2x^2 + \cdots + a_nx^n$$

with $a_1, a_2, \ldots, a_n \in \{0, 1\}$. Prove that there exists an integer N so that, for all integers $n \geq N$, more than 99% of the polynomials in $\mathcal{P}_n$ are square-free.

Each problem is worth 7 marks.
Time allowed: $4\frac{1}{2}$ hours.

The 15^{th} Romanian Master of Mathematics Competition

Day 1 — Solutions

Problem 1. Let n be a positive integer. Initially, in each square of the top row on the $2^n \times 2^n$ chessboard, a bishop is placed; those bishops are numbered from 1 to 2^n, from left to right. A *jump* is a simultaneous move made by all bishops such that the following conditions are satisfied:

Each bishop moves diagonally any number of squares; and

At the end of the jump, the bishops all stand in different squares of the same row.

Find the total number of permutations σ (of numbers $1, 2, \ldots, 2^n$) with the following property: There exists a sequence of jumps such that all bishops end up on the bottom row arranged in the order $\sigma(1)$, $\sigma(2)$, $\ldots$, $\sigma(2^n)$, from left to right.

Israel

Solution 1. The required number is 2^{n-1}. On a jump, every bishop moves the same number of rows up or down; call this number of rows the *length* of the jump.

Step 1. We show that the length of any jump is of the form 2^d for some integer $d \leq n-1$. Assign each bishop the number of the column it is situated on before the jump. Let k be the length of the jump; then each bishop's column number either increases by k, or decreases by k in the jump.

Thus, bishops $1, 2, \ldots, k$ should move to columns $k+1, k+2, \ldots, 2k$, as they cannot move leftwards. On the other hand, after the jump columns $1, 2, \ldots, k$ should be filled by the bishops $k+1, k+2, \ldots, 2k$. So the leftmost $2k$ bishops still fill the columns $1, 2, \ldots, 2k$ after the jump.

Repeating the argument shows that the next k bishops move rightwards, and the next k bishops beyond move leftwards, and so on and so forth. Finally, the bishops all split into contiguous groups of length $2k$, and in each group the leftmost k bishops move rightwards, whereas the rightmost k bishops move leftwards. Hence $2k \mid 2^n$, so k is indeed of the form 2^d with $d \leq n-1$.

Step 2. To make a more explicit description of the column change during the jump, assign each column the n-digit binary expansion of less 1 its number, augmented with zeroes leftwards if necessary. It is then easily seen that a jump of length 2^d just switches the d-th digit from the left, 0 to 1 and vice versa.

Thus, the resulting permutation also has the following form: For every $d = 0, 1, \ldots, n-1$, the d-th digit is either swapped for all bishops, or it is preserved for them all.

Moreover, notice that the total length of all jumps is odd, so there will be an odd number of jumps of length 1. Hence the 0-th (the rightmost) digit will be switched anyway. This leaves the room for 2^{n-1} possible permutations.

Step 3. It remains to show that all 2^{n-1} permutations are indeed possible. Let us show how to reach any of them.

Start by getting to the bottom row by downward jumps of lengths $1, 2, 4, \ldots, 2^{n-1}$ that will switch all n digits.

Now, if we want to switch the i-th digit back, $1 \leq i \leq n-1$, make two upward jumps of length 2^{i-1}, followed by a downward jump of length 2^i. Combine such modifications for all possible digit combinations to get all desired permutations.

Solution 2. Proceed until the end of Step 1 just like in the first solution. Then extend the board to a vertical strip of width 2^n, this will not affect the result, as it will be seen at the end of the proof.

We will show that any two jumps commute. Consider two jumps of length p and q with $p < q$, and call them the p-jump and the q-jump. As described in the first step, the bishops will be split in contiguous groups. For the p-jump, we look at groups of length p, call these p-groups; for the q-jump, we look at groups of length q, call these q-groups.

Since $2p$ divides q, any p-group is fully contained in a single q-group, and a q-group contains an even number of p-groups. First, let's look at the first two q-groups, and denote by $g_1, \ldots, g_{2k}$ the $p-$groups contained in the first q-group, and $g'_1, \ldots, g'_{2k}$ the p-groups contained in the second q-group, where $2k = q/p$. The p-jump will swap any g_{2i-1} with g_{2i}, and same for their g' counterparts, whereas a q-jump will swap g_j with g'_j. When putting these together, it follows that applying both jumps in either order gives the same result: g_{2i-1} is swapped with g'_{2i} and g_{2i} is swapped with g'_{2i-1}.

Repeat now the same argument for the next two q-groups, and so on and so forth, until the entire row will be accounted for.

We will now establish a bijection from the odd numbers between 1 and $2^n - 1$ to the desired permutations. Let $x = \sum 2^k a_k$ be an odd number between 1 and $2^n - 1$, where each a_k is either 0 or 1, in particular $a_0 = 1$. Perform a_k jumps of length 2^k in increasing order of k, then perform $2^n - 1 - x$ additional jumps of length 1 in order to reach the final row. This will result in a permutation σ, and set $f(x) = \sigma$. This provides a well defined function f.

To prove f injective, it suffices to look at bishop numbered 1 and show that it will end up in position $x + 1$. For any of jump of length 2^k, this bishop will move rightwards, as its position just before the jump was $1 + a_0 + 2a_1 + \ldots + 2^{k-1}a_{k-1} \leq 2^k$. Therefore, before the additional jumps of length 1, this bishop will reach position $x + 1$. Any two jumps of same length cancel each other out, and there is an even number of additional jumps of length 1, so the final position will also be $x + 1$. Consequently, f is injective.

To prove f surjective, consider a σ with the desired property, let b_k be the number of jumps of length 2^k, and let a_k be the remainder of b_k modulo 2. Since the total length of all jumps is odd, there has to be an odd number of jumps of length 1, so $a_0 = 1$. Let $x = \sum 2^k a_k$, and note that this is an odd number between 1 and $2^n - 1$. From Step 2 in Solution 1, the order of the jumps does not matter. Since two consecutive jumps of same length cancel each other out, performing a_k jumps of length 2^k is the same as performing b_k jumps of length 2^k. So $f(x) = \sigma$, as the $2^n - 1 - x$ additional jumps of length 1 at the end also cancel each other out.

Solution 3. Run again Step 1 through in Solution 1.

Look at the two *halves* $1, \ldots, 2^{n-1}$ and $2^{n-1} + 1, \ldots, 2^n$ and let $h(i) = i \pm 2^{n-1}$ be the counterpart of i in the other half, where the sign is chosen appropriately. A jump of length 2^{n-1} will swap the halves between themselves, so i will be swapped with $h(i)$. From Step 1, it follows that any shorter jump will only perform swaps inside a single half, and will act the same way on the other half; specifically, if a jump swaps i with j, it will also swap $h(i)$ with $h(j)$.

Furthermore, applying two jumps of 2^{n-1} will just cancel each other out, regardless of any other jumps in between, because we swapped i with $h(i)$ twice, and the inner configuration of each half is changed in the same way.

Induct now on n. There are 2^{n-2} possible permutations for the $2^{n-1} \times 2^{n-1}$ board. Performing jumps of the same length on a $2^n \times 2^n$ board gives the same configuration in each of the two halves. Now we can either apply a jump of length 2^{n-1}, which will swap the halves, or we can apply two jumps of length 2^{n-2}, which will cancel each other. This provides a construction for 2^{n-1} permutations in the $2^n \times 2^n$ board.

To show that these are the only ones, consider now a valid permutation for the $2^n \times 2^n$ board which is obtained from some jumps. First, discard the jumps of length 2^{n-1}, then attempt to apply the rest on the $2^{n-1} \times 2^{n-1}$ board. If a jump would exit the board, then make the jump of the same length in the opposite direction instead, which will stay on the board because its length is at most 2^{n-2}. Since the length is the same, the resulting bishop configuration is also the same. Since the total length of the moves executed so far is odd, we can make an even number of moves of length 1 in order to reach the final row of the $2^{n-1} \times 2^{n-1}$ board, and this will not change the configuration in the end. Therefore, we obtain a corresponding permutation for the $n-1$ case which describes the configuration in each of the halves. From there, the only variations are whether the halves are swapped or not, depending on whether the number of jumps of length 2^{n-1} was odd or even. So this valid permutation corresponds to one constructed in the earlier paragraph, which completes the induction.

Problem 2. Consider an odd prime p and an integer $N < 50p$. Let $a_1, a_2, \ldots, a_N$ be a list of positive integers less than p such that any specific value occurs at most $\frac{51}{100}N$ times and $a_1 + a_2 + \cdots + a_N$ is not divisible by p. Prove that there exists a permutation $b_1, b_2, \ldots, b_N$ of the a_i such that $b_1 + b_2 + \cdots + b_k$ is not divisible by p for all $k = 1, 2, \ldots, N$.

United Kingdom, Will Steinberg

Solution 1. The argument hinges on the lemma below.

Lemma. *Let n be a positive integer and let $c_1, c_2, \ldots, c_n$ be a list of positive integers less than p such that each specific value occurs at most $\frac{1}{2}(n+1)$ times. Fix a residue $r \not\equiv c_1 + c_2 + \cdots + c_n \pmod p$. Then there exists a permutation $d_1, d_2, \ldots, d_n$ of the c_i such that $r \not\equiv d_1 + d_2 + \cdots + d_k \pmod p$ for all $k = 1, 2, \ldots, n$.*

Proof. Induct on n. The base case, $n = 1$, is clear, so let $n \geq 2$. Consider the residue a that occurs the most times amongst the c_i.

If $a \not\equiv r \pmod p$, set $d_1 = a$ and complete the rest of the list using the inductive hypothesis with r replaced by $r - a$, as any residue will occur amongst the remaining c_i at most $\frac{1}{2}\big((n-1)+1\big)$ times. Indeed, if no other residue occurs as many times as a, then the number of occurrences of any residue amongst the remaining c_i is at most $\frac{1}{2}(n+1) - 1 = \frac{1}{2}(n-1) < \frac{1}{2}\big((n-1)+1\big)$. Otherwise, if there is another residue that occurs as many times as a, their number of occurrences has to be at most $\frac{1}{2}n = \frac{1}{2}\big((n-1)+1\big)$.

If $a \equiv r \pmod p$, choose a residue $b \not\equiv a \pmod p$ amongst the c_i; the choice is possible, as $\frac{1}{2}(n+1) < n$. Set $d_1 = b$ and $d_2 = a$, noting that $d_1 + d_2 = b + a \equiv r + b \not\equiv r \pmod p$. If no other residue occurs as many times as a, then each residue occurs amongst the remaining c_i at most $\frac{1}{2}(n+1) - 1 = \frac{1}{2}(n-1) = \frac{1}{2}\big((n-2)+1\big)$ times. If a occurs at most $\frac{1}{2}(n-1)$ times, then clearly the same will hold for any residue in the remaining c_i. The remaining possibility is that a and another residue both occur $\frac{1}{2}n$ times and n is even, meaning that that the other residue has to be b, and there are no other residues; it is clear that the occurrences in the remaining c_i are precisely $\frac{1}{2}(n-2) < \frac{1}{2}\big((n-2)+1\big)$. The inductive hypothesis then applies with r replaced by $-b$ to complete the list. This establishes the lemma.

Back to the problem, if each residue occurs at most $\frac{1}{2}(N+1)$ times, the conclusion follows by the Lemma.

Otherwise, there is exactly one residue a that occurs $M > \frac{1}{2}(N+1)$ times amongst the a_i. Note that $2M - N > (N+1) - N = 1$, to set $b_i = a$, $i = 1, 2, \ldots, 2M - N$. Letting $\alpha = 50$, note also that $2M - N \leq 2 \cdot \frac{\alpha+1}{2\alpha}N - N = \frac{1}{\alpha}N < p$, so none of the first $2M - N$ partial sums is divisible by p, as p is prime.

To complete the proof, apply the Lemma with $r = (N - 2M)a$ to the remaining a_i. There are left $N - (2M - N) = 2(N - M)$ such, a occurs $M - (2M - N) = N - M$ times amongst these and any other residue occurs at most $N - M$ times, both of which do not exceed $\frac{1}{2}\big(2(N-M)+1\big)$.

Solution 2. The permutation will be constructed step by step, first choosing b_1, then b_2, and so on. At every step, sort the remaining values by their number of appearances from most frequent to least frequent, and from largest to smallest for the situations where the number of appearances is the same. After that, attempt to select the first value from the sorted list; if this results in a partial sum that is divisible by p, then attempt to select the second value from the list, which will result in a partial sum that is not divisible by p as the first and second values are different modulo p. Label the step as type (I) if the first value has been selected and as type (II) if the second value has been selected.

Lemma. Any step of type (II) is followed by a step of type (I).

Proof. Suppose that step j is of type (II). Denote the first two values according to the sorting order with a and b, and let s be the partial sum until this step. Since step j is type (II), $s + a \equiv 0$

(mod p). At step $j+1$, the first value according to the sorting order will still be a. Since $s+b+a \not\equiv 0 \pmod{p}$, a can be selected for step $j+1$, so step $j+1$ is of type (I).

Now suppose, for the sake of contradiction, that this procedure fails. Let $k+1 < N$ be the first step when neither (I) nor (II) is possible. In particular, this means that there is a single value a remaining, and it occurs $N-k$ times. Let j be the smallest number with the following property: at *every* step between j and $k+1$, the value a is the first one according to the sorting order; in particular, a is the most frequently occurring one. Such a j exists because $k+1$ satisfies this property.

If $j > 1$, then at step $j-1$ there is another value b that comes before a in the sorted order. Suppose that at step $j-1$ there are q values of a remaining; then there are at least q values of b remaining. According to the lemma, at least half of the steps $j, j+1, \ldots, k$ are of type (I), which means that a is selected in them. Denote $\ell = k-j+1$, then a has been selected at least $\lfloor \ell/2 \rfloor$ steps between j and k. Since at step $k+1$, there are $N-k \geq 2$ values of a remaining, it means that $q \geq \lfloor \ell/2 \rfloor + 2$. At the same time, at step $k+1$ there are no values of b remaining, so between steps j and k all the remaining b values have been selected, and this can happen at most $\ell - \lfloor \ell/2 \rfloor$ times. Combining these two leads to $\ell - \lfloor \ell/2 \rfloor \geq q \geq \lfloor \ell/2 \rfloor + 2$, or $\ell \geq 2\lfloor \ell/2 \rfloor + 2$, a contradiction.

If $j = 1$, then a is always the first in the sorted order. Therefore, the first $p-1$ steps are of type (I), and step p is of type (II). If $k \geq p$, from steps $p+1$ to k, at least every other step is of type (I), meaning that a is selected. Once step k is done, there are $N-k$ remaining values of a. Therefore, in the beginning, there were at least

$$(p-1) + \frac{k-p}{2} + N - k = N - \frac{k}{2} + \frac{p}{2} - 1 > N - \frac{N-2}{2} + \frac{N}{2\alpha} - 1 = \frac{\alpha+1}{2\alpha} N$$

values of a, contradiction. In the situation when $k < p$, there are at least $N-1$ values of a, which is also a contradiction.

Problem 3. Fix an integer $n > 3$ and let $N = \{1, 2, \ldots, n\}$. Let $\mathcal{S}$ be a set of $n - 2$ pairwise distinct 3-element subsets of N such that $|A_1 \cup A_2 \cup \cdots \cup A_k| \geq k + 2$ for any $A_1, A_2, \ldots, A_k$ in $\mathcal{S}$ and any $k = 1, 2, \ldots, n - 2$. Are there n pairwise distinct points $p_1, p_2, \ldots, p_n$ in the plane such that the angles of the triangle $p_i p_j p_k$ are all less than $61°$ for any set $\{i, j, k\}$ in $\mathcal{S}$?

Russia, Ivan Frolov

Solution. The answer is in the affirmative. Note that the condition on $\mathcal{S}$ may be rephrased as follows: For any subset M of N of size $|M| \geq 2$, there are at most $|M| - 2$ sets in $\mathcal{S} \cap \mathcal{P}_3(M)$, where $\mathcal{P}_3(M)$ is the set of 3-element subsets of M.

Extend the problem to $n \geq 1$ and proceed by induction on n; for formal correctness, assume that $|\mathcal{S}| \leq \max(0, n - 2)$. The cases $n = 1$, 2 are both trivial.

Look upon points in the plane as complex numbers. Begin by considering a collection of points $q_1, q_2, \ldots, q_n$, not necessarily distinct, yet not all identical. Fix $q_n = 0$ and associate with each $\{i, j, k\}$ in $\mathcal{S}$ an equation $q_j - q_i = \omega \cdot (q_k - q_i)$, where $\omega = e^{i2\pi/3}$. This equation ensures that q_i,, q_j, q_k either are the vertices of a clockwise oriented non-degenerate equilateral triangle or they all coincide.

We then get a system of $n - 2$ linear equations with $n - 1$ complex variables $q_1, q_2, \ldots, q_{n-1}$. It is well-known that such a system has a non-trivial solution $(q_1, q_2, \ldots, q_{n-1}, q_n = 0)$. However, some of the q_i may coincide. So N splits into some classes, $N = N_1 \sqcup \cdots \sqcup N_m$, such that the points q_i and q_j coincide if and only if i and j share the same class and the size of each class is less than n. Note that the elements of any triple in $\mathcal{S}$ either all lie in the same class or no two lie in the same class.

Clearly, each $\mathcal{S}_i = \mathcal{S} \cap \mathcal{P}_3(N_i)$ satisfies the conditions in the statement relative to N_i of size less than n. By the inductive hypothesis, for each $i = 1, 2, \ldots, m$, there exists a point-configuration $\{r_{ij} \colon j \in N_i\}$ satisfying the corresponding requirements. For each $j = 1, 2, \ldots, n$, choose the index i of the class N_i containing j, and let $p_j = q_j + \varepsilon r_{ij}$, where ε is small enough.

If the elements of a triple $\{i, j, k\}$ in $\mathcal{S}$ lie in three different classes, then the angles of triangle $p_i p_j p_k$ are close to those of triangle $q_i q_j q_k$, provided that ε is small enough, so the triangle satisfies the required angle-condition. Otherwise, the three elements all lie in some class N_ℓ, and the angles of $p_i p_j p_k$ equal those of $r_{\ell i} r_{\ell j} r_{\ell k}$, so they satisfy the requirements by the inductive hypothesis.

The 15$^{\text{th}}$ Romanian Master of Mathematics Competition

Day 2 — Solutions

Problem 4. Fix integers a and b greater than 1. For any positive integer n, let r_n be the (non-negative) remainder b^n leaves upon division by a^n. Assume that there exists a positive integer N such that $r_n < 2^n/n$ for all integers $n \geq N$. Prove that a divides b.

Iran, Pouria Mahmoudkhan Shirazi

Solution 1. Arguing indirectly, assume that $a \nmid b$, so $r_n \neq 0$ for all n. Let $M = \max(b, N)$.

We now prove that $r_{n+1} \geq br_n$ for all $n \geq M$. Indeed, as $r_n < 2^n/b \leq a^n/b$, it follows that $br_n < a^n$ and $b^{n+1} \equiv br_n \pmod{a^n}$. Therefore, br_n is the remainder b^{n+1} leaves upon division by a^n, i.e., br_n is the smallest non-negative integer r such that $a^n \mid b^{n+1} - r$. This implies $br_n \leq r_{n+1}$, as $a^{n+1} \mid b^{n+1} - r_{n+1}$.

To complete the solution, note that $r_M \geq 1$, so $r_{M+k} \geq b^k r_M \geq 2^k$ for all $k \geq 0$. On the other hand, $r_{M+k} < 2^{M+k}/(M+k) < 2^k$ for k sufficiently large. This is a contradiction.

Solution 2. The argument hinges on the lemma below:

Lemma. *Consider two integers $b > a > 1$. If a does not divide b, then $\{b^n/a^n\} > 1/b$ for infinitely many positive integers n; as usual, $\{x\}$ denotes the fractional part of the real number x.*

Proof. For every positive integer n, write $x_n = \lfloor b^n/a^n \rfloor$ and $y_n = \{b^n/a^n\}$ and note that $by_n - ay_{n+1} = ax_{n+1} - bx_n$ is an integer.

Suppose now, if possible, that $y_n \leq 1/b$ for all $n \geq M$. Consider any such n and note that $y_n > 0$, as a does not divide b, so $-1 < -a/b < by_n - b/a \leq by_n - ay_{n+1} \leq 1 - ay_{n+1} < 1$. Hence the integer $by_n - ay_{n+1} = 0$, so $y_{n+1} = (b/a)y_n$.

Consequently, $y_n = (b/a)^{n-M} y_M$ for all $n \geq M$. As $b > a$, it then follows that $y_n \geq 1$ for all large enough n, contradicting the fact that $y_n < 1$ whatever n. This establishes the lemma.

Back to the problem, suppose a does not divide b. Then $b > a$; otherwise $2^n/n > r_n = b^n \geq 2^n$ which is impossible. Note that $a^n\{b^n/a^n\} = r_n < 2^n/n$ for all large enough n. The lemma then implies $1/b < \{b^n/a^n\} < (1/n)(2/a)^n \leq 1/n$ for infinitely many n which is clearly a contradiction.

Remark. The conclusion holds under the more general assumption that $r_n < 2^n/f(n)$, where f is any given function satisfying $\lim_{n\to\infty} f(n) = \infty$.

Problem 5. Let BC be a fixed segment in the plane, and let A be a variable point in that plane outside the line BC. Points X and Y are chosen on the rays CA (emanating from C) and BA (emanating from B), respectively, such that $\angle CBX = \angle YCB = \angle BAC$. Assume that the tangents to the circumcircle of ABC at B and C cross XY at$P$ and Q, respectively. Let Ω_1 be the circle through X and P centred on BC. Similarly, let Ω_2 be the circle through Y and Q centred on BC. Prove that Ω_1 and Ω_2 intersect at two fixed points as A varies.

Denmark, Daniel Pham Nguyen

Solution 1. All angles in the solution are oriented. We will prove that the two intersection points are points D and D' such that the triangles BCD and BCD' are equilateral.

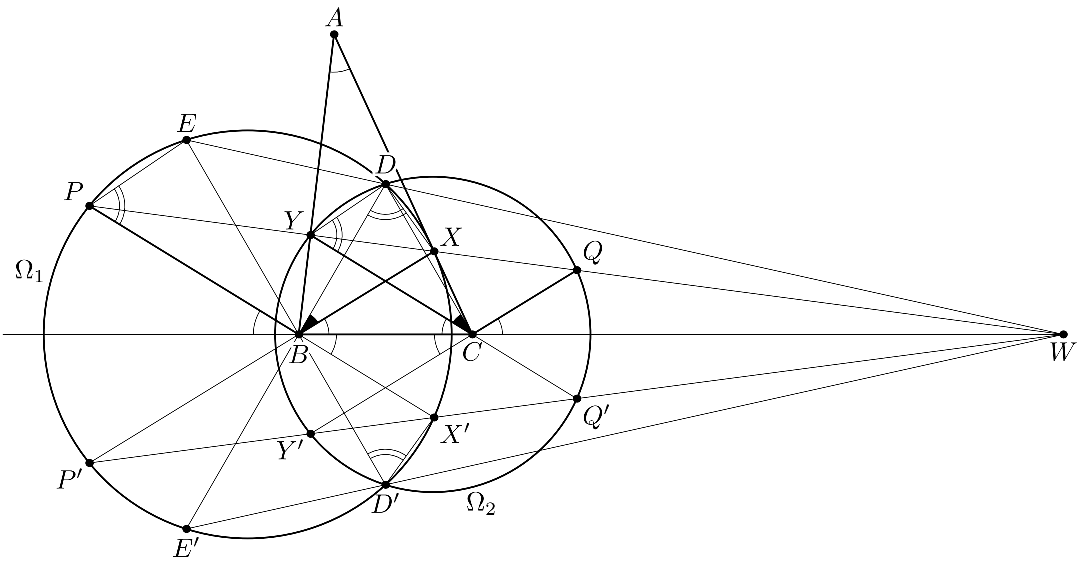
Let X', Y', P', and Q' be the reflections across BC of X, Y, P, and Q, respectively. Then Ω_1 and Ω_2 are just the circles $PXX'P'$ and $QYY'Q'$, respectively.

Denote $\alpha = \angle BAC = \angle CBX = \angle YCB$. Let XY cross BC at W; the case $XY \parallel BC$ may be treated as a limit case. The symmetry yields that W also lies on the line $X'Y'$. The same symmetry, along with tangency of PB and QC to the circle ABC, yields

$$\alpha = \angle X'BC = \angle PBW = \angle WCQ = \angle BCY'. \tag{$*$}$$

This yields that each of the triples (P, B, X'), (Q, C, Y'), (P', B, X), and (Q', C, Y) is the collinear, and, moreover, that $PBX' \parallel Q'CY$ and $P'BX \parallel QCY'$. It follows now that quadrilaterals $PXX'P'$ and $YQQ'Y'$ are homothetic at W. Therefore, so are Ω_1 and Ω_2.

Let now Ω_1 nd Ω_2 cross at D and D'. Let WD and WD' meet Ω_1 again at E and E'. Since $W = PX \cap P'X'$ and $B = PX' \cap P'X$, the point B lies on the polar of W with respect to Ω_1. In other words, W and B are inverse with respect to that circle. This yields that the lines DE' and $D'E$ also cross at B.



Now, we have $\angle BDX = \angle E'DX = \angle X'D'E = \angle X'PE = \angle BPE = \angle CYD$ (the last equality holds by means of homothety). Similarly, we have $\angle DXB = \angle DXP' = \angle PX'D' = \angle PED' = \angle PEB = \angle YDC$. Therefore, the triangles BDX and CYD are similar. Firstly, this yields that $\angle DBC = \angle DBX + \angle XBC = \angle YCD + \angle BCY = \angle BCD$, whence $BD = CD$. Secondly, this also implies that $BD/BX = CY/CD$, or $BX \cdot CY = BD \cdot CD = BD^2$. But the triangles BXC and CBY are also similar (as both are similar to ABC), so $BX/BC = BC/CY$, ot $BX \cdot CY = BC^2$. Thus, $BC = BD = CD$, and the triangle BCD is equilateral. This finishes the solution.

Remark. The fact that B and W are inverse to each other with respect to Ω_1 can be obtained (and implemented) in different ways. Two useful conditions equivalent to this fact are: the points P, B, and X are concyclic with the centre O_1 of Ω_1; and Ω_1 is the Apollonius circle with respect to the segment BW; the details follow below.

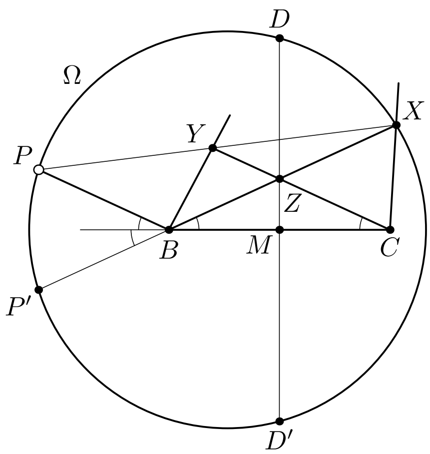
In particular, one may argue as follows. If O_1 is the centre of Ω_1, then O_1 lies on an (external or internal) bisector of $\angle PBX$, as well as on the perpendicular bisector of XP. This yields that O_1 is the midpoint of one of the arcs PX of the circle PBX. That, in turn, implies that the circle Ω_1 contains two of the four points: the incentre, and the three excentres of $\triangle PBX$. It follows that Ω_1 is an Apollonius circle of the segment BW.

So, if D is a point such that the triangle BCD is equilateral, it suffices to show that $BD/DW = BX/XW$ (so D lies on the same Apollonius circle). This can be done by a computation using the cosine law, although not very quickly.

Solution 2. All angles in the solution are directed. All segment lengths on lines BX and CY (and parallel to them) are also oriented; we assume that the directions $\overrightarrow{BX}$ and $\overrightarrow{CY}$ are positive. As in the solution above, we prove that $BP \parallel CY$.

Assume that ABC is oriented anti-clockwise. Let D and D' be the points such that the triangles DBC and $D'CB$ are equilateral, and oriented anti-clockwise. We will show that D and D' lie on the circle Ω_1; similarly, they lie on Ω_2.

Notice that $\alpha = \angle BAC = \angle CBX = \angle YCB = \pi - \angle CBP$; moreover, each of the triangles XBC and BCY is similar to BAC and oriented differently than BAC; hence those two triangles are equi-oriented. Let Ω denote the circle $(DD'X)$; clearly, its center lies on the perpendicular bisector of DD', i.e., on BC. We aim to prove that Ω passes through P; that will yield that $\Omega = \Omega_1$, which establishes what we are aimed to prove.



Denote $Z = XB \cap YC$. Since $\angle CBZ = \angle BAC = \angle ZCB$, we have $ZB = ZC$, and hence Z lies on the perpendicular bisector DD' of BC. By similarity, we get $BX/BC = BC/CY$, or $BC^2 = BX \cdot CY = BX \cdot (ZY + CZ)$. Since $CY \parallel BP$, the triangles XZY and XBP are similar, so $BX \cdot ZY = ZX \cdot BP$. Therefore,

$$BD^2 = BC^2 = BX \cdot ZY + BX \cdot CZ = ZX \cdot BP + (BZ + ZX) \cdot BZ = ZX \cdot (BP + BZ) + BZ^2.$$

On the other hand, let M be the midpoint of BC, and let XB cross Ω again at P'. Write the power of point Z with respect to Ω as

$$XZ \cdot (P'B + BZ) = XZ \cdot P'Z = ZD \cdot ZD' = MZ^2 - DM^2 = BZ^2 - MB^2 - DM^2 = BZ^2 - BD^2.$$

The two obtained relations yield

$$ZX \cdot (BP + BZ) = BD^2 - BZ^2 = ZX \cdot (P'B + BZ),$$

so $BP = P'B$, and so P and P' are reflections of one another in the line BC. Thus, P lies on Ω, as desired.

Remark. It is also possible to solve the problem via the *moving points* method. Introduce the points D and D' as in Solution 2, and introduce the reflections X', Y', P', and Q' of X. Y, P, and Q in the line BC, respectively, as in Solution 1 to read Ω_1 and Ω_2 as the circles $PXX'P'$ and $QYY'Q'$, respectively.

We need to show that D lies on Ω_2 (the other incidences are similar). To this end, it suffices to check that $\angle YDQ = \angle YY'Q = 90^\circ - \angle Y'CB = 90^\circ - \angle BAC$.

Fix B, C, and the circle ABC. As A varies over that circle, the lines BX, CY, BP, and CQ remain constant, and X and Y depend projectively on A. Choosing Q_1 on CQ such that $\angle YDQ_1 = 90^\circ - \angle BAC$, we need to show that $Q_1 = Q$, or that X, Y, and Q_1 are collinear. The point Q_1 also depends projectively on A, so it suffices to check that the points Q_1, X, and Y are collinear for four specific positions of A.

Problem 6. A polynomial P with integer coefficients is *square-free* if it is not expressible in the form $P = Q^2R$, where Q and R are polynomials with integer coefficients and Q is not constant. A polynomial is *suitable* if its constant term and all other non-zero coefficients are equal to 1. Prove that, for all but finitely many integers $n \geq 1$, more than 99% of the suitable polynomials of degree at most n are square-free.

Iran, Navid Safaei

Solution 1. Let $\mathcal{P}_n$ be the set of all suitable polynomials of degree at most n. Clearly, $|\mathcal{P}_n| = 2^n$. Alternatively, but equivalently, we prove that less than $\frac{1}{100} \cdot 2^n$ of the polynomials in $\mathcal{P}_n$ are not square-free for all but finitely many n. Throughout the solution n is always assumed to be sufficiently large to allow room for as large integers $r \leq n$ as the different stages of the argument require. Also, all polynomials have integer coefficients and divisibility is always understood in $\mathbb{Z}[X]$. The proof consists of three parts:

(1) Upper bounding the number of polynomials in $\mathcal{P}_n$ divisible by the square of a non-constant polynomial of degree at most r;

(2) Upper bounding the number of polynomials in $\mathcal{P}_n$ divisible by the square of a polynomial of degree greater than r; and

(3) Choosing a suitable r.

Before dealing with the three parts above, we prove a useful lemma.

Lemma. *The zeroes of any polynomial in $\mathcal{P}_n$ all lie in the open disc $|z| < 2$ and their real parts are all less than $C = \frac{1}{2}(1 + \sqrt{5})$.*

Proof. Let P be a degree m polynomial in $\mathcal{P}_n$. Leaving aside the trivial case $m = 0$, let $m \geq 1$. Write $P = \sum_{k=0}^{m} a_k X^k$ and consider a complex number z of absolute value $|z| \geq 2$. Then

$$|P(z)| \geq |z|^m - \sum_{k=0}^{m-1} |z|^k = \frac{(|z|-2)||z|^m + 1}{|z| - 1} \geq \frac{1}{|z|-1} > 0,$$

and the first part follows.

To prove the second part, let z have a real part $\Re z \geq C > 1$. Clearly, $|z| \geq \Re z \geq C > 1$. Leaving aside the trivial cases $m = 0$ and $m = 1$, let $m \geq 2$ to write

$$\begin{aligned}\left|\frac{P(z)}{z^m}\right| &\geq \left|a_m + \frac{a_{m-1}}{z}\right| - \frac{1}{|z|^2} - \cdots - \frac{1}{|z|^m} \geq \left|a_m + \frac{a_{m-1}}{z}\right| - \frac{1}{|z|^2} \\ &> \left|a_m + \frac{a_{m-1}}{z}\right| - \frac{1}{|z|^2 - |z|} \geq \left|a_m + \frac{a_{m-1}}{z}\right| - 1, \qquad \text{as } |z| \geq C, \\ &\geq \Re\left(a_m + \frac{a_{m-1}}{z}\right) - 1 \geq a_m - 1 \geq 0.\end{aligned}$$

This establishes the second part and completes the proof. (The argument in the second part shows in fact that, if $\Re z > 0$ and $|z| \geq C$, then $P(z) \neq 0$. Hence the zeroes of P with a positive real part all lie in the open disc $|z| < C$.)

To deal with **(1)**, consider a polynomial P in $\mathcal{P}_n$ divisible by the square of a non-constant polynomial Q of degree $q \leq r$. We first show that there are at most $(2^{2r+1} - 1)^{r+1}$ such Q's.

Clearly, the leading coefficient of Q is ± 1. The zeroes $z_1, \ldots, z_q$ of Q are amongst those of P, so $|z_k| < 2$, by the lemma. The absolute value of the coefficient of X^{q-k} in Q is then $\left|\sum z_{i_1} \cdots z_{i_k}\right| < \binom{q}{k} \cdot 2^k < 2^{q+k} \leq 2^{2q} \leq 2^{2r}$. Hence each coefficient of Q takes on at most $2 \cdot 2^{2r} - 1 = 2^{2r+1} - 1$ values, so there are at most $(2^{2r+1} - 1)^{r+1}$ such Q's, as stated.

Next, upper bound the number of P's in $\mathcal{P}_n$ that are divisible by the same Q^2. Consider such a $P = a_0 + \cdots + a_n X^n$ and let $\mathcal{S}_n(P)$ be the set of all polynomials $R = b_0 + \cdots + b_n X^n$ in $\mathcal{P}_n$ such that $b_k \neq a_k$ for exactly one k; note that $k \geq 1$, as $b_0 = a_0 = 1$. Alternatively, but equivalently, there exists a $k \geq 1$ such that $b_\ell = a_\ell$ for $\ell \neq k$ and $b_k + a_k = 1$. Hence $|\mathcal{S}_n(P)| = n$. Note further that $P - R = \pm X^k$ vanishes at 0, whereas Q does not, as $Q(0)^2$ divides $P(0) \neq 0$. Hence R is not divisible by Q^2, showing that none of the n polynomials in $\mathcal{S}_n(P)$ is.

Consider now distinct P_1 and P_2 in $\mathcal{P}_n$, both divisible by Q^2, to show that $\mathcal{S}_n(P_1)$ and $\mathcal{S}_n(P_2)$ are disjoint: If they shared some R, then $P_1 - R = \pm X^{k_1}$ and $P_2 - R = \pm X^{k_2}$ for some distinct k_1, $k_2 \geq 1$, so $P_1 - P_2 = \pm X^{k_1} \pm X^{k_2}$ would be divisible by Q^2, which is clearly not the case.

By the two paragraphs above, there are then at most $2^n/(n+1)$ polynomials in $\mathcal{P}_n$ that are divisible by the same Q^2.

As there are at most $(2^{2r+1} - 1)^{r+1}$ such Q's of degree at most r, there are at most

$$\frac{(2^{2r+1} - 1)^{r+1}}{n+1} \cdot 2^n$$

polynomials in $\mathcal{P}_n$ divisible by the square of a non-constant polynomial of degree at most r. For a fixed r this upper bound is clearly of order $o(2^n)$.

To deal with **(2)**, consider a polynomial P in $\mathcal{P}_n$ divisible by the square of a non-constant polynomial Q of degree $q > r$.

The zeroes $z_1, \ldots, z_q$ of Q are amongst those of P, so $|z_k| < 2$ and $\Re z_k < C$, by the lemma. As the leading coefficient of Q is clearly ± 1,

$$|Q(3)| = |(3 - z_1) \cdots (3 - z_q)| \geq (3 - \Re z_1) \cdots (3 - \Re z_q) > (3 - C)^q > (3 - C)^r.$$

As $3 - C > 1$, letting r be large enough, $P(3)$ is then divisible by d^2 for some large enough $d > (3 - C)^r$.

Consider the largest integer $s = s_d$ satisfying $3^s < d^2 \leq 3^{s+1}$. Clearly, $s \geq 1$. Write $P = \sum_{k=0}^{n} a_k X^k$. Then $1 = a_0 \leq \sum_{k=0}^{s-1} 3^k a_k \leq \sum_{k=0}^{s-1} 3^k = \frac{1}{2}(3^s - 1) < \frac{1}{2}(d^2 - 1) < d^2$. As for distinct choices of $a_1, \ldots, a_{s-1}$ from $\{0, 1\}$ the sums $\sum_{k=0}^{s-1} 3^k a_k$ are pairwise distinct, they are also pairwise distinct modulo d^2. Noting that these sums are all positive, it follows that there are at most 2^{n-s+1} polynomials P in $\mathcal{P}_n$ such that $P(3)$ is divisible by d^2.

If r is sufficiently large, then so is $d > (3 - C)^r$. Thus, if d is large enough, then $2^s > d^{5/4}$, as $d^2 \leq 3^{s+1}$ and $\log_2 3 < \frac{8}{5}$, so there are at most $2^{n-s+1} \leq 2^{n+1} d^{-5/4}$ polynomials P in $\mathcal{P}_n$ such that $P(3)$ is divisible by d^2. Hence, if d_0 is large enough, then the number of such P's is at most $2^{n+1} \sum_{d > d_0} d^{-5/4}$.

Now, as $\sum_{d \geq 1} d^{-5/4}$ converges, given any $c > 0$, the remainder $\sum_{d > d_0} d^{-5/4} < c$ for some large enough d_0 depending on c, of course. For any such d_0, the number of P's in $\mathcal{P}_n$ such that $P(3)$ is divisible by d^2 is then less than $2c \cdot 2^n$.

Consequently, so is the number of polynomials in $\mathcal{P}_n$ divisible by the square of a polynomial of degree greater than r.

Finally, we deal with **(3)**. Fix any $c > 0$. Then choose r large enough so that the remainder $\sum_{d > (3-C)^r} d^{-5/4} < c$. At this stage $n > r$. Let further $n > \frac{1}{c}(2^{2r+1} - 1)^{r+1}$. By **(1)** and **(2)**, the number of non-square-free polynomials in $\mathcal{P}_n$ is then less than $3c \cdot 2^n$. Setting $c = \frac{1}{300}$ provides the answer to the problem at hand.

Solution 2. We present an alternative approach to parts **(1)** and **(2)**.

To deal with **(1)**, use the first part of the lemma to bound the number of possible polynomials Q by some constant. For every such Q, we then prove that few polynomials in $\mathcal{P}_n$ are divisible by Q. This follows from the clam below:

Claim. *Given a non-constant polynomial Q, the number of polynomials in $\mathcal{P}_n$ that are divisible by Q does not exceed $\binom{n}{\lfloor n/2 \rfloor}$.*

Proof. Let ζ be a non-zero complex root of Q (if there are no such, then no polynomial in $\mathcal{P}_n$ is divisible by Q). Then each polynomial $P = p_n X^n + \cdots + p_1 X + p_0$ in $\mathcal{P}_n$ divisible by Q satisfies

$\sum_{i=0}^{n} p_i \cdot c\zeta^i = 0$, for any complex c. Choose a suitable c so that the $a_i = \operatorname{Re} c\zeta^i$ are all non-zero. Then $\sum_{i=0}^{n} a_i p_i = 0$.

Partially order the (binary) tuples of coefficients by letting $(p_1, p_2, \ldots, p_n) \preceq (p'_1, p'_2, \ldots, p'_n)$ if and only if the non-zero $a_i(p'_i - p_i)$ are all positive. The tuples corresponding to polynomials divisible by Q then form an independent set (anti-chain) in the $\preceq$-partially ordered n-cube.

Assign each tuple $(p_1, p_2, \ldots, p_n)$ the tuple $(\sigma p_1, \sigma p_2, \ldots, \sigma p_n)$, where $\sigma p_i = p_i$, if $a_i > 0$, and $\sigma p_i = 1 - p_i$, otherwise. This assignment shows $\preceq$ isomorphic to the (index) set-inclusion partial order on the binary n-cube, so the length of any $\preceq$-anti-chain is at most $\binom{n}{\lfloor n/2 \rfloor}$, by Sperner's theorem. This proves the claim.

The standard bound provided by Stirling's formula (or any of its elementary relaxations) establishes part **(1)**.

To prove **(2)**, deal more algebraically. Let P be a polynomial in $\mathcal{P}_n$ divisible by some Q^2, where $\deg Q = d > r$. Reduce modulo 2 to get the polynomials $\overline{P}$ and $\overline{Q}$, where $\deg \overline{Q} = d$, as the leading coefficient of Q is ± 1. Then $\overline{P}$ is divisible by $\overline{Q}^2 = \overline{Q}(X^2)$. Write $\overline{P} = \overline{P}_+(X^2) + X\overline{P}_-(X^2)$. Then $\overline{P}_+$ and $\overline{P}_-$ are both divisible by $\overline{Q}$. So, for a fixed $\overline{Q}$, the number of such polynomials does not exceed 2^{n-2d}. Hence for all degree d polynomials $\overline{Q}$, the number of such P's does not exceed $2^{d-1} \cdot 2^{n-2d} = 2^{n-d-1}$, so their fraction in $\mathcal{P}_n$ is at most 2^{-d-1}. Finally, sum over all $d \geq r$, to conclude that the fraction of P's in **(2)** does not exceed 2^{-r}.