Proof Round 2023-2024 Solutions

Problem 1. [5] Alice and Bob play a game on a $m \times n$ chessboard ($m \geq 1, n \geq 3$). They alternate turns, with Alice going first. On each turn, a player may place either a domino, covering exactly 2 squares on the chessboard, or a 3×1 tromino, covering exactly 3 squares on the chessboard, such that the newly placed piece does not overlap any previously placed pieces. Pieces may be placed either horizontally or vertically. Whoever cannot play a legal move at some point loses. For each (m,n), find who has the winning strategy.

Proposed by Eduardo Nascimento

Solution: Alice has the winning strategy if at least one of m,n are odd; otherwise, Bob has the winning strategy.

We make a symmetry argument. If mn is odd, the board has a central square. Alice can play a tromino centered at this square on the first turn, and then on subsequent turns, play the *reflection* of Bob's previous move through the center of the board. Thus, Alice wins the game.

If exactly one of m,n is odd, then the center of the board (as a rectangle) lies on the center of an edge incident to two adjacent squares. Alice can place a domino covering these two adjacent squares on the first turn, and then on subsequent turns, play the *reflection* of Bob's previous moves through the center of the board. Thus, Alice wins the game.

Otherwise, if m,n are both even, then the center of the board (as a rectangle) lies at a point where four squares of the chessboard meet, and so for every one of Bob's moves, he may play the reflection of Alice's previous move through the center of the board. So Bob wins the game.

Problem 2. **[10]** Let X be a finite set, and let $\mathscr{P}(X)$ be the *power set* of X; that is, $\mathscr{P}(X)$ is the set of all subsets of X. For instance, if $X = \{a,b,c\}$, then

$$\mathscr{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{b,c\}, \{a,c\}, \{a,b,c\}\}.$$

In particular, if $|X|$ is the cardinality of X, then the cardinality of $\mathscr{P}(X)$ is $2^{|X|}$.

A subset $\Sigma \subseteq \mathscr{P}(X)$ is called an *algebra* (on X) if it satisfies the following 3 properties:

(1) (Universal set) $X \in \Sigma$.
(2) (Closed under complement) If $A \in \Sigma$, then $X \setminus A \in \Sigma$.
(3) (Closed under union) If $A_1, A_2 \in \Sigma$, then $A_1 \cup A_2 \in \Sigma$.

For instance, let $X = \{a,b,c\}$. Then, $\mathscr{P}(X)$ itself is an algebra (this is the largest possible algebra on X). As a non-trivial example,

$$\{\emptyset, \{a,b\}, \{c\}, \{a,b,c\}\}$$

is also an algebra on X.

(a) **[1]** Give another two examples of algebras on the set $X = \{a,b,c\}$. (*No proof required*)

(b) **[2]** Let $X = \{1,2,\ldots,k\}$ for some integer $k \geq 3$. Suppose $\Sigma \subseteq \mathscr{P}(X)$ is an algebra such that the sets $\{1,2\}$ and $\{2,3\}$ are in Σ. Show that the one-element sets $\{1\}, \{2\}, \{3\}$ are in Σ.

(c) **[7]** Prove that for any finite set X, the cardinality of any algebra $\Sigma \subseteq \mathscr{P}(X)$ equals 2^n for some positive integer n. *Hint: Consider the following definition. A partition of X (with k parts) is a collection of non-empty subsets $C_1, C_2, \ldots, C_k$ of X such that $\bigcup_{i=1}^{k} C_i = X$, and $C_i \cap C_j = \emptyset$ for every $1 \leq i < j \leq k$. In particular, every element of X lies in exactly one part.*

Proposed by Brian Yang

*Solution **(a)**:* The subsets $\{\emptyset, \{a,b,c\}\}$, $\{\emptyset, \{a\}, \{b,c\}, \{a,b,c\}\}$ of $\mathscr{P}(X)$ are algebras on X (the first is called the *trivial algebra*).

*Solution **(b)**:* First observe for any algebra Σ on an arbitrary X that Σ being closed under complement and union implies Σ is also *closed under intersection*: that is, if $A_1, A_2 \in \Sigma$, then

$$A_1 \cap A_2 = X \setminus ((X \setminus A_1) \cup (X \setminus A_2)) \in \Sigma,$$

where the equality above is *DeMorgan's law*.

Now return to the problem statement. By closed under intersection $\{2\} = \{1,2\} \cap \{2,3\} \in \Sigma$. By closed under complement, $\{1,3,4,\ldots,k\} = X \setminus \{2\} \in \Sigma$. By closed under intersection, $\{1\} = \{1,2\} \cap \{1,3,4,\ldots,k\} \in \Sigma$. Similarly argue $\{3\} \in \Sigma$.

*Solution **(c)**:* Let Σ be an algebra on X. For any $x \in X$, let A_x be the intersection of all sets in Σ containing x. Then, $A_x \in \Sigma$, and by construction must be the smallest subset of X (with respect to inclusion) such that $x \in A_x$ and $A_x \in \Sigma$. Observe that no proper non-empty subset of A_x is in Σ. Indeed, assume on the contrary $B \subseteq A_x$ is proper and non-empty, with $B \in \Sigma$. If $x \in B$, then this contradicts minimality of A_x. Otherwise, $x \in A_x \setminus B$, where $A_x \setminus B \in \Sigma$ by closure under complement and intersection, again contradicting minimality of A_x.

Let $\mathscr{A}$ be the finite collection of sets $\{A_x \mid x \in X\}$ (for $x, y \in X$ distinct, we may have $A_x = A_y$). Note that distinct sets $A_1, A_2 \in \mathscr{A}$ are disjoint, otherwise $B = A_1 \cap A_2 \in \Sigma$ is non-empty and contained properly in either A_1 or A_2, a contradiction. Hence, $\mathscr{A}$ is a partition of X, say with $n \geq 1$ parts. Furthermore, for any set $A \in \Sigma$ and any $x \in X$, either $A_x \subseteq A$ or $A_x \cap A = \emptyset$ (in other words, A is a union of finitely many sets in $\mathscr{A}$); if not, then $B = A_x \cap A \in \Sigma$ is non-empty and contained properly in $A_x \in \mathscr{A}$, a contradiction. Thus, by closure under union, Σ consists of precisely all unions of subcollections of $\mathscr{A}$ (including the empty subcollection), and two different subcollections of $\mathscr{A}$ certainly give rise to two distinct subsets of X. Conclude $|\Sigma| = 2^n$, as requested.

Problem 3. [13] Let $m \geq 1$ be an integer. An *mth root of unity* is a complex number z such that $z^m = 1$. An mth root of unity z is called *primitive* if $z^m = 1$, and $z^d \neq 1$ for every integer $1 \leq d < m$. For instance, $w := \cos(\frac{8\pi}{6}) + i\sin(\frac{8\pi}{6})$ is a 6th root of unity, but not a primitive 6th root of unity. It is, however, a primitive 3rd root of unity.

(a) [2] Find, with proof, the product of all primitive mth roots of unity (your answer may depend on m).

(b) [4] Prove that the sum of all primitive mth roots of unity is non-zero if and only if m is *squarefree*, i.e. m is not divisible by the square of any prime number.

(c) [7] Suppose that m is *squarefree*. Prove that every mth root of unity z can be written as a finite sum or difference of primitive mth roots of unity. In other words, prove that there is some integer $k \geq 1$, primitive mth roots of unity $z_1, z_2, \ldots, z_k$ (not necessarily mutually distinct), and $a_i \in \{-1, +1\}$ for each $1 \leq i \leq k$, such that

$$z = a_1 z_1 + a_2 z_2 + \cdots + a_k z_k.$$

(It turns out that the converse is true as well. That is, if $m \geq 1$ is a not a square-free integer, then there is some mth root of unity z which cannot be written as a finite sum or difference of primitive mth roots of unity. This actually follows from **(b)** and a bit of linear algebra and field theory.)

Proposed by Brian Yang

*Solution **(a)**:* For $m = 1, 2$ the product of all primitive mth roots of unity is obviously $1, -1$, respectively.

For $m \geq 3$, observe any primitive mth root of unity z is non-real, so $z \neq \bar{z}$. Furthermore, for any integer d, we have $z^d = 1$ if and only if $\bar{z}^d = 1$. Hence, the primitive mth roots of unity come in complex conjugate pairs. The product of a complex number on the unit circle with its conjugate is 1, so the product of all primitive mth roots of unity is precisely 1.

*Solution **(b)**:* For any integer $n \geq 1$, denote by σ_n the sum of all primitive nth roots of unity, and $\Phi_n(x)$ the nth cyclotomic polynomial.

In general, prime factorize $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, and let $q = p_1 p_2 \ldots p_s$ be the product of the distinct prime divisors of m. Claim $\Phi_m(x) = \Phi_q(x^{\frac{m}{q}})$. Indeed, the degree of $\Phi_q(x^{\frac{m}{q}})$ is

$$\frac{m}{q} \cdot \varphi(q) = \prod_{j=1}^{s} p_j^{\alpha_j - 1} \varphi(p_j) = \prod_{j=1}^{s} \varphi(p_j^{\alpha_j}) = \varphi(m),$$

and any primitive mth root of unity z is a root of $\Phi_q(x^{\frac{m}{q}})$, as $z^{\frac{m}{q}}$ is a primitive qth root of unity. Thus, $\Phi_m(x), \Phi_q(x^{\frac{m}{q}})$ are both monic, have the same set of roots, and the same degree $\varphi(m)$. Since $\Phi_m(x)$ actually has no repeated roots, the claim follows. Consequently, if m is not squarefree, then $\frac{m}{q} > 1$, so by Vieta, the sum of the roots of $\Phi_m(x) = \Phi_q(x^{\frac{m}{q}})$, i.e. the sum of the primitive mth roots of unity, is 0.

On the other hand, suppose m is squarefree, so that $m = p_1 p_2 \ldots p_s$ (s distinct prime divisors). We claim $\sigma_m = (-1)^s$. Induct on s. For $s = 0$, the claim is obvious. The base case $s = 1$, i.e. $m = p_1$ is a prime, is also easy, as -1 is the sum of the p_1th roots of unity not equal to 1 (e.g. by Vieta), i.e. the sum of the primitive p_1th roots of unity.

For the inductive step, assume $s \geq 2$, and the requested claim has been proven for positive integers with up to $s-1$ distinct prime factors. Recall that the set of all mth roots of unity is the disjoint union of the sets of all primitive dth roots of unity, as d ranges over all divisors of m. For such d, if d has $0 \leq t < s$ distinct prime divisors, the induction assumption implies $\sigma_d = (-1)^t$. Furthermore, for any such $0 \leq t < s$, there are $\binom{s}{t}$ divisors d of m with exactly t distinct prime divisors. Since the sum of all mth roots of unity is 0, we deduce the equation

$$0 = \sum_{t=0}^{s-1} (-1)^t \binom{s}{t} + \sigma_m.$$

In lieu of the combinatorial identity $(1-1)^s = \sum_{t=0}^{s}(-1)^t\binom{s}{t}$, we conclude $\sigma_m = (-1)^s$, as requested.

Solution ***(c)****:* Again, write $m = p_1p_2\dots p_s$; induct on s. The base case $s = 1$, i.e. $m = p_1$ is a prime, is trivial (and has been verified in the proof of **(b)**).

For the inductive step, assume $s \geq 2$, and the requested claim has been proven for positive integers with up to $s-1$ distinct prime factors. Trivially, any primitive mth root of unity can be expressed as an integral linear combination of primitive mth roots of unity. Now, any other mth root of unity z is a primitive Dth root of unity for some D properly dividing m. Then, there exists d a proper divisor of m such that $D \mid d$ and m equals d times a prime number. By the inductive assumption, z is an integral linear combination of primitive dth roots of unity. Having fixed this notation, it suffices to prove that any primitive dth root of unity may be written as an integral linear combination of primitive mth roots of unity.

WLOG assume $p_1d = m$. Let $r_1 = p_2\dots p_s$. Notice that any arbitrary primitive dth root of unity is of the form $e^{\frac{2\pi i\cdot r_2}{m}}$, where r_2 is a residue $\pmod m$ where $p_1 \mid r_2$ and $p_k \nmid r_2$ for all $2 \leq k \leq s$. Compute

$$\sum_{j=0}^{p_1-1} e^{\frac{2\pi i\cdot(r_1j+r_2)}{m}} = e^{\frac{2\pi i\cdot r_2}{m}}\cdot\left(\sum_{j=1}^{p_1-1} e^{\frac{2\pi i\cdot r_1j}{m}}\right) + e^{\frac{2\pi i\cdot r_2}{m}} = e^{\frac{2\pi i\cdot r_2}{m}}\cdot\left(\sum_{j=0}^{p_1-1} e^{\frac{2\pi i\cdot j}{p_1}}\right) = 0$$

$$\implies e^{\frac{2\pi i\cdot r_2}{m}} = -\sum_{j=1}^{p_1-1} e^{\frac{2\pi i\cdot(r_1j+r_2)}{m}}.$$

Since $p_2,\dots,p_s \nmid r_1j+r_2$ for all integers j, and $p_1 \mid r_1j+r_2$ if and only if $p_1 \mid j$, we deduce $e^{\frac{2\pi i\cdot(r_1j+r_2)}{m}}$ is a primitive mth root of unity if and only if $p_1 \nmid j$. Therefore, the above equation writes $e^{\frac{2\pi i\cdot r_2}{m}}$, an arbitrary primitive dth root of unity, as a sum and difference of primitive mth roots of unity, implying the conclusion.

Problem 4. **[7]** Professor Tamuz is teaching a class containing some finite number of students (at least 1). Every pair of students in class are either friends or not. Prove that Professor Tamuz may partition the students in the class into some number of groups $N \geq 1$, labelled $1, 2, \ldots, N$, and pick N student representatives, one from each group, such that:

- No pair of students belonging to the same group are friends with each other.
- For any two different groups i and j, the representative of group i is friends with some student belonging to group j.

Proposed by Brian Yang

Solution: Let $G = (V, E)$ be the obvious graph-theoretic interpretation: V is the set of students in class and E the set of friendships between pairs of students. For $N \geq 1$, recall that an *N-coloring* of G is a map $c : V \to \{1, 2, \ldots, N\}$. An N-coloring c is called *proper* if for any edge $vw \in E$, we have $c(v) \neq c(w)$. We say that N is the *chromatic number* of G if N is the smallest positive integer such that there exists a proper N-coloring of G.

Now, suppose $N \geq 1$ is the chromatic number of G, and let $c : V \to \{1, 2, \ldots, N\}$ be any proper N-coloring of G. In fact, let $V := V_1 \sqcup \cdots \sqcup V_N$ be the partition induced by c, i.e. for $v \in V$ and $1 \leq i \leq n$, we have $v \in V_i$ if and only if $c(v) = i$. We claim that for every $1 \leq i \leq N$, there is a vertex $v_i \in V_i$ such that for every $1 \leq j \leq n,\ j \neq i$, v_i is adjacent to some $w \in V_j$. With the v_i's taking the role of the student representatives, this will verify that the partition $V_1 \sqcup \cdots \sqcup V_N$ witnesses that it is indeed possible for Professor Tamuz to split the students in class in groups and then pick student representatives in the way described in the problem statement.

Towards a contradiction, say that for every $v \in V_N$ (WLOG), we may pick $1 \leq j \leq N-1$ (depending on v) such that v is not adjacent to any vertices in V_j. Then, define an auxiliary coloring $c' : V \to \{1, 2, \ldots, N-1\}$ by $c'(v) = c(v)$ for every $v \in V_1 \sqcup \cdots \sqcup V_{N-1}$ and $c'(v) = j$ for every $v \in V_N$. Given $1 \leq j \leq N-1$, observe that every vertex $v \in V$ that is c'-colored by j is either in V_j or in V_N, and in the latter case, v is not adjacent to any vertices $w \in V_j$. Hence, any two vertices in V that are c'-colored by j are not adjacent, so c' is in fact a proper coloring. But this is a contradiction of N being the chromatic number.

Problem 5. [10] Say a positive integer x is *power-close* if there exist positive integers $k \geq 4, m \geq 2$ such that there is some $0 \leq i \leq m-1$ with k^m dividing $x-i$. Prove that there are infinitely many positive integers that are not power-close.

Proposed by Eduardo Nascimento

Solution: Say x is k,m power-close, if there is i as in the problem statement. Then, for each k,m, the density of k,m power-close positive integers is obviously $\frac{m}{k^m}$. By the union bound, this implies that the (upper) density of all power-close integers is at most

$$\sum_{k\geq 4}\sum_{m\geq 2}\frac{m}{k^m}.$$

Let $f(x) = \frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$ if $|x| < 1$. Then,

$$\frac{x}{(1-x)^2} = xf'(x) = \sum_{m=1}^{\infty} mx^m$$

on $x \in (-1,1)$, and so taking $x = \frac{1}{k}$, $k \geq 4$ yields

$$\sum_{m\geq 2}\frac{m}{k^m} = \frac{k}{(k-1)^2} - \frac{1}{k} = \frac{2k-1}{k(k-1)^2} < \frac{2}{(k-1)^2}.$$

Then,

$$\sum_{k\geq 4}\sum_{m\geq 2}\frac{m}{k^m} < \sum_{k\geq 4}\frac{2}{(k-1)^2} = \sum_{k\geq 3}\frac{2}{k^2} = 2\left(\frac{\pi^2}{6} - 1 - \frac{1}{4}\right) \lessapprox 0.79.$$

Conclude that the set of non power-close positive integers has positive lower density, and hence is infinite.

Problem 6. **[15]** Find all positive real numbers r, c with $r > 1$ satisfying the following: there exists a positive integer N such that $\lfloor cr^n \rfloor$ is a perfect cube for all positive integers $n \geq N$.

Proposed by Jeck Lim

Solution: The solutions are $r = a^3$ for some positive integer $a > 1$, and $c = \frac{b^3}{r^m}$ for some integers $b \geq 1, m \geq 0$. It is easy to see that these values work.

Now, on the other hand, fix r, c, N such that $\lfloor cr^n \rfloor$ is a perfect cube for all positive integers $n \geq N$. Fix an integer $N_1 \geq N$ sufficiently large such that for all $n \geq N_1$, we have $cr^n = a_n^3 + \varepsilon_n$ for some positive integer a_n and $0 \leq \varepsilon_n < 1$, and $a_{n+1} \geq a_n$. Then, $a_{n+1}^3 + \varepsilon_{n+1} = ra_n^3 + r\varepsilon_n$ for all $n \geq N_1$, so $a_n \to \infty$ and

$$\left(\frac{a_{n+1}}{a_n}\right)^3 - r = \frac{r\varepsilon_n - \varepsilon_{n+1}}{a_n^3} = O(a_n^{-3}) \quad \text{as } n \to \infty.$$

Now, observe for $x, y \geq 1$ that $x^2 + xy + y^2 \geq 1$ and $x^3 - y^3 = (x^2 + xy + y^2)(x - y)$, so that $|x - y| \leq |x^3 - y^3|$. In the current situation, this yields

$$\frac{a_{n+1}}{a_n} - \sqrt[3]{r} = O(a_n^{-3}), \quad \frac{a_{n+2}}{a_{n+1}} - \sqrt[3]{r} = O(a_{n+1}^{-3}) \quad \text{as } n \to \infty.$$

In fact, as $a_n \to \infty$ as $n \to \infty$, the expression $\frac{a_{n+1}}{a_n} - \sqrt[3]{r} = O(a_n^{-3})$ implies for any $\varepsilon > 0$ that $\left|\frac{a_{n+1}}{a_n} - \sqrt[3]{r}\right| < \varepsilon$ for all sufficiently large n. Thus, $a_n = \Theta(a_{n+1})$ and vice versa as $n \to \infty$. Consequently, taking the difference of the above two expressions yields

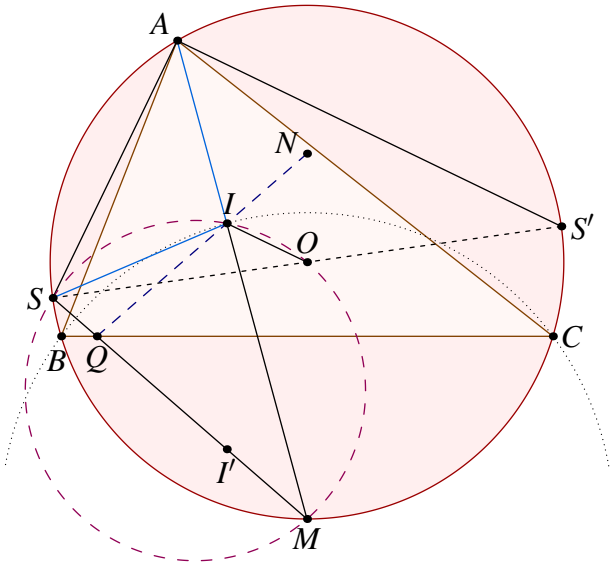
$$\frac{a_{n+1}^2 - a_n a_{n+2}}{a_n a_{n+1}} = O(a_{n+1}^{-3}) \quad \text{as } n \to \infty$$

Given n, if the LHS is nonzero, then it is at least $\frac{1}{a_n a_{n+1}}$ in absolute value. Since $\frac{1}{a_n a_{n+1}}$ is obviously not $O(a_{n+1}^{-3})$ as $n \to \infty$, it follows there is some integer $N_2 \geq N_1$ so large such that $\frac{a_{n+1}^2 - a_n a_{n+2}}{a_n a_{n+1}} = 0$, i.e. $\frac{a_{n+2}}{a_{n+1}} = \frac{a_{n+1}}{a_n}$ for all $n \geq N_2$. Since $\frac{1}{a_{n+1} a_n} \to \sqrt[3]{r}$ as $n \to \infty$, in fact we must have $\frac{a_{n+1}}{a_n} = \sqrt[3]{r}$ for $n \geq N_2$. Hence, $r\varepsilon_n = \varepsilon_{n+1}$ for $n \geq N_2$. If $\varepsilon_n > 0$ for $n \geq N_2$, then for sufficiently large integers m, we have $\varepsilon_{n+m} = r^m \varepsilon_n > 1$, a contradiction. Thus, $\varepsilon_n = 0$ for $n \geq N_2$, so $cr^n = a_n^3$ and $a_{n+m} = r^{\frac{m}{3}} a_n$ for all $n \geq N_2, m \geq 0$. Given $n \geq N_2$, for a_{n+m} to be an integer for all $m \geq 0$, we must have r be a perfect cube, and then $c = \frac{a_{N_2}^3}{r^{N_2}}$ is the of the desired form.

Problem 7. **[20]** Let ABC be a scalene triangle with incenter I and circumcircle Γ. Let M be the midpoint of arc $\widehat{BC}$ of Γ not containing A, and let X be a point on $\overline{BC}$ such that $IX = XM$. The incircle of ABC is tangent to $\overline{BC}$ at D, and denote by I' the reflection of I over D. Let T lie on Γ such that $\overline{AT} \perp \overline{TI'}$. Finally, $\overline{TD}$ meets Γ again at P. Prove that the circumcircle of triangle IXP is tangent to $\overline{AI}$.

Proposed by Brian Yang

Solution: Denote by Ψ the inversion about the circle (BIC) (recall by the incenter-excenter lemma that this circle has center M). It turns out this will be the main theme of the problem! Let $\overline{MI'}$ meet Γ at $S \neq M$.

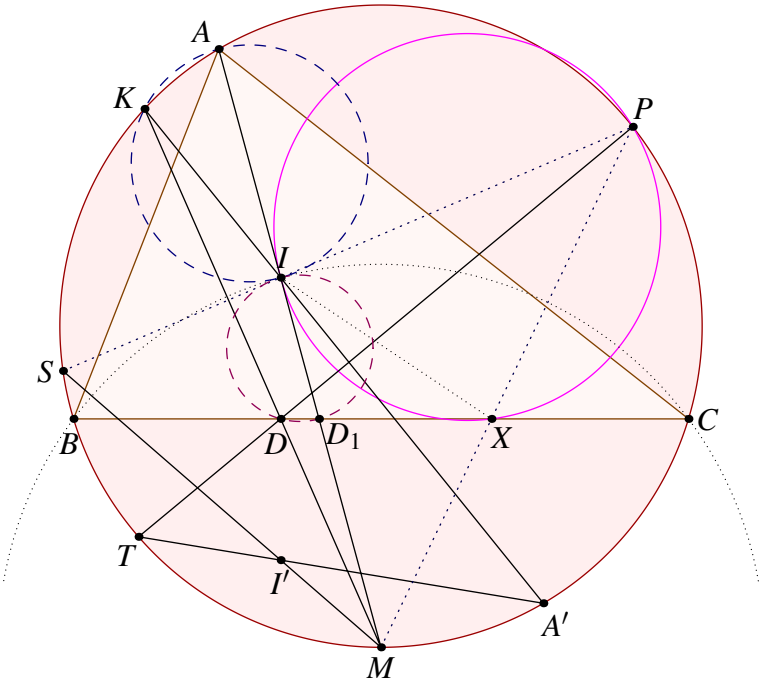


We begin with the following claim, independent of most of the problem setup:

Claim 1. $AI = SI$.

Proof 1. Let O be the center of Γ, and S' the antipode of S on Γ. Notice that the inversion Ψ fixes I, swaps S and $Q := \overline{SM} \cap \overline{BC}$, and swaps O and N, the symmetric of M over $\overline{BC}$. Since Q, I', M are collinear, so are Q, I, N by reflection, whence S, M, I, O are concyclic. Thus, $\angle MIO = \angle MSO = \angle MSS' = \angle MAS'$, so $\overline{IO} \parallel \overline{AS'}$. Then, $\overline{AS'} \perp \overline{AS}$ implies $\overline{IO} \perp \overline{AS}$, and this yields the claim. □

Now, let A' be the antipode of A on Γ (thus, T is the second point $\overline{A'I'}$ cuts Γ).



Claim 2 (Sharky-Devil). The lines $\overline{A'I}$ and $\overline{MD}$ meet on Γ.

Proof 2. Let K be the second point $\overline{A'I}$ meets Γ; we need to show K,D,M are collinear. In fact, we will show that K,D are swapped by the inversion Ψ. Since Ψ sends Γ to $\overline{BC}$, we have $\Psi(A) = \overline{AM} \cap \overline{BC} =: D_1$, so that Ψ swaps the circles (AI) and (ID_1). Now, notice D lies on (ID_1) by $\overline{ID} \perp \overline{BC}$. Since K lies on (AI) by $\overline{A'K} \perp \overline{KA}$, we deduce D is the image of K under Ψ. This verifies the requested collinearity. □

Having done all this work, we are ready to say things about P:

Claim 3. $PI = MI$.

Proof 3. By Claim 1 and power of a point at I, it suffices to prove P,I,S are collinear. But this holds by the converse of Pascal's theorem on $MSPTA'K$ (cf. Claim 2). □

Claim 4. M,X,P are collinear.

Proof 4. let $X' = \overline{BC} \cap \overline{MP}$. We have $MI^2 = MX' \cdot MP$ since Ψ swaps P and X' (or by the Shooting lemma). Thus, $\triangle MX'I \sim \triangle MIP$, so from $PI = MI$ (Claim 3) follows $IX' = X'M$. By uniqueness of X, conclude $X = X'$. □

In particular, $MI^2 = MX \cdot MP$, so (IXP) is indeed tangent to $\overline{AM}$.