HMMT February 2025

February 15, 2025

Team Round

1. **[20]** Let a, b, and c be pairwise distinct positive integers such that $\frac{1}{a}, \frac{1}{b}, \frac{1}{c}$ is an increasing arithmetic sequence in that order. Prove that $\gcd(a, b) > 1$.

   Proposed by: Srinivas Arun

   Solution 1: Observe that $\frac{1}{a} + \frac{1}{c} = \frac{2}{b}$, so $b(a + c) = 2ac$, and thus $a \mid b(a + c)$. If we assume that $\gcd(a, b) = 1$, then we must have $a \mid a + c$, so $a \mid c$. However, $\frac{1}{a} < \frac{1}{c}$, so $a > c$, contradiction. Thus, $\gcd(a, b) > 1$, as desired.

   Solution 2: Observe that $\frac{2}{b} - \frac{1}{a} = \frac{1}{c}$, so $(2a - b)c = ab$ and thus $2a - b \mid ab$. If we assume that $\gcd(a, b) = 1$, then $\gcd(2a - b, a) = 1$, so $2a - b \mid b$. Then $2a - b \mid (2a - b) + b = 2a$, so $2a - b \mid \gcd(2a, b) \leq 2$. Thus $2a - b \leq 2$. But $a > b$, contradiction. Thus, $\gcd(a, b) > 1$, as desired.

2. **[25]** A polyomino is a connected figure constructed by joining one or more unit squares edge-to-edge. Determine, with proof, the number of non-congruent polyominoes with no holes, perimeter 180, and area 2024.

   Proposed by: Albert Wang

   Answer: $\boxed{2}$

   Solution: Define the *bounding box* of a polyomino to be the smallest axis-aligned rectangle that contains the entire polyomino. Suppose a polyomino satisfying the given conditions has a bounding box with dimensions $w \times h$.

   Claim 1. $w + h \leq 90$.

   Proof. The polyomino has at least $2w$ horizontal edges and at least $2h$ vertical edges. Moreover, it has a perimeter of 180. Therefore, $2w + 2h \leq 180$, so $w + h \leq 90$. □

   Claim 2. The dimensions of the bounding box are either 44×46, 45×45, or 46×44.

   Proof. Note that $hw \geq 2024$ since it contains the polyomino with area 2024. Suppose for sake of contradiction that $h + w \leq 89$. Then,

   $$(h - w)^2 = (h + w)^2 - 4hw \leq 89^2 - 4 \cdot 2024 = -175,$$

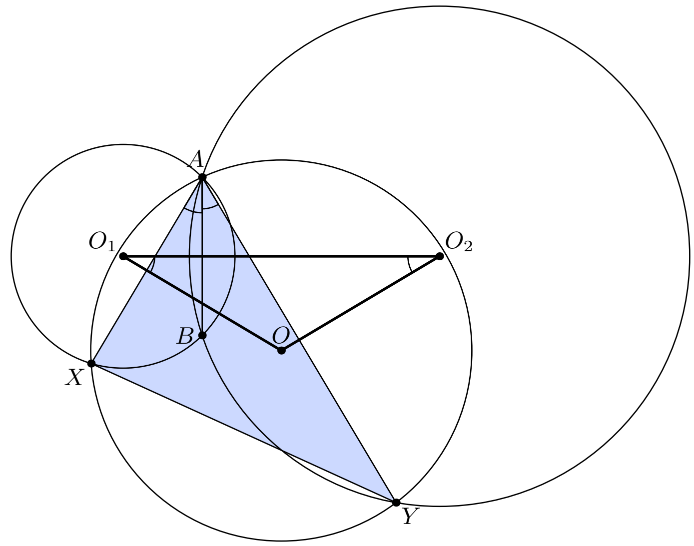
   contradiction. Therefore, $h + w = 90$, so we can let $(h, w) = (45 + x, 45 - x)$. Then, $2025 - x^2 = hw \geq 2024$ implies that $x \in \{-1, 0, 1\}$, as desired. □

   In the first and third cases, the bounding box has area 2024, so it must be the entire polyomino, giving us the 44×46 rectangle (and its rotation) as a possible answer. In the second case, the bounding box has area 2025, so one cell must be removed to form the polyomino. Removing the corner cell yields a polyomino with perimeter 180, and removing any other cells yields a polyomino with perimeter greater than 180. Therefore, the only other possibility is a 45×45 square missing a corner. Thus the answer is $\boxed{2}$.

3. **[30]** Let ω_1 and ω_2 be two circles intersecting at distinct points A and B. Point X varies along ω_1, and point Y on ω_2 is chosen such that AB bisects the angle $\angle XAY$. Prove that as X varies along ω_1, the circumcenter of $\triangle AXY$ (if it exists) varies along a fixed line.

   Proposed by: Pitchayut Saengrungkongka

   Solution 1:



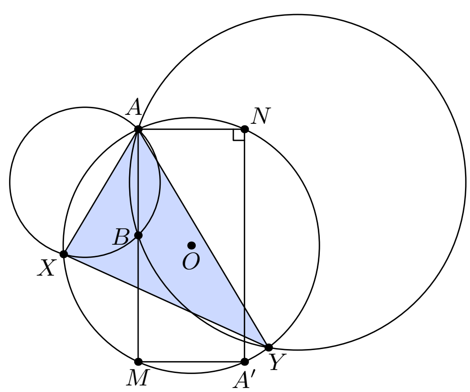
Let O_1, O_2, and O be the centers of ω_1, ω_2, and the circumcircle of $\triangle AXY$, respectively.

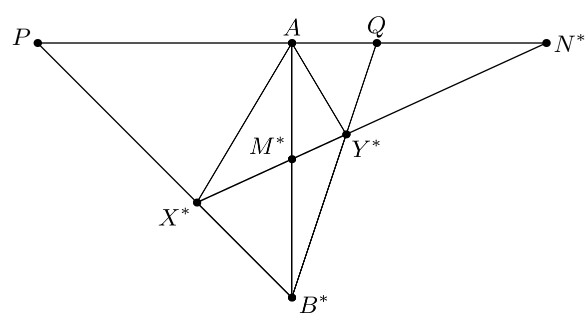
We claim that triangle OO_1O_2 is isosceles with $OO_1 = OO_2$, and thus in particular O always lies on the perpendicular bisector of O_1O_2.

To this end, observe that $OO_1 \perp AX$ and $O_1O_2 \perp AB$, so $\angle OO_1O_2 = \angle XAB$. Analogously, $\angle OO_2O_1 = \angle YAB$. So indeed OO_1O_2 is isosceles, and we are done.

Remark. One may also consider the antipodes of A on ω_1 and ω_2 for an equivalent but more natural angle-chase.

Solution 2:





Let A' be the A-antipode in circle (AXY). It suffices to show that A' lies on a fixed line. We will show that this line is one that is parallel to AB.

Let M be the second intersection of line AB with circle (AXY), and let N be the antipode of M on this circle. Since $AMA'N$ is a rectangle with N lying on the line through A perpendicular to AB, it suffices to show that N is fixed (independent of X and Y).

To this end, take an inversion at A with arbitrary radius, denoting images with $\bullet \mapsto \bullet^*$.

Observe that X^* and Y^* lie on the fixed lines $\ell_1 = \omega_1^*$ and $\ell_2 = \omega_2^*$. Let ℓ be the line through A perpendicular to AB^*, and suppose that ℓ_1 and ℓ_2 intersect ℓ at P and Q, respectively.

Since $\angle XAB = \angle BAY$, we have $\angle X^*AB^* = \angle B^*AY^*$. Circles ω_1, ω_2, and (AXY) are mapped to lines B^*X^*, B^*Y^*, and X^*Y^*. As $AN \perp AB$, it follows that N^* is the intersection of X^*Y^* and ℓ.

Finally, observe that $(N^*, A; P, Q) \overset{B^*}{=} (N^*, M^*; X, Y)$ is a harmonic bundle, as AM^* bisects $\angle X^*AY^*$ and $\angle M^*AN^* = 90°$. Since A, P, and Q are fixed, so is N^*. Thus N is fixed, and O lies on the perpendicular bisector of AN, which is also fixed.

Remark. An alternative approach to the last paragraph is to recall **Blanchet's theorem**, which states that PY^*, QX^*, and AB^* are concurrent. By Ceva and Menelaus, we get that $(N^*, A; P, Q) = -1$.

Remark. If one projects the kite/harmonic quadrilateral $NXMY$ from A' onto the line through the antipodes defined in the previous remark, we obtain that $A'N$ (a line parallel to AB) passes through the midpoint of the two antipodes, directly finishing.

4. **[35]** Jerry places at most one rook in each cell of a 2025×2025 grid of cells. A rook *attacks* another rook if the two rooks are in the same row or column and there are no other rooks between them.

Determine, with proof, the maximum number of rooks Jerry can place on the grid such that no rook attacks 4 other rooks.

Proposed by: Arul Kolla

Answer: $\boxed{8096}$

Solution 1: The answer is $2024 \times 4 = 8096$. More generally, for an $n \times n$ grid, the answer is $4n - 4$. Call a rook that attacks at most 3 other rooks *good*.

We use the following observation in both parts of the solution: a rook on the border of the grid must be good.

Lower Bound: Place rooks on all $4n - 4$ border cells of the grid. By the above observation, every rook is good.

Upper Bound: Consider any valid placement of rooks, and assume there exists a rook that is not on the border. We can move this rook to the border via a usual rook move, since this rook is good and thus the path to one of the four border cells in its row or column must be empty.

After this move, we claim the placement of rooks is still valid. Indeed:

- the moved rook is now on the border, so by the observation above, it must be good;
- any rook that used to attack this rook cannot attack more rooks after the move, so such rooks must still be good;
- any rook attacked in the final position must be either:
  - opposite the direction moved, in which case it attacked the moved rook both before and after the move (so is still good), or
  - perpendicular to the direction moved, in which case it is a border rook and must always be good.

By repeating the above process, we can always move from any good position to one where all rooks are on the border. This implies that the number of rooks in any good position is at most $4n - 4$. When $n = 2024$, the answer is $4n - 4 = \boxed{8096}$.

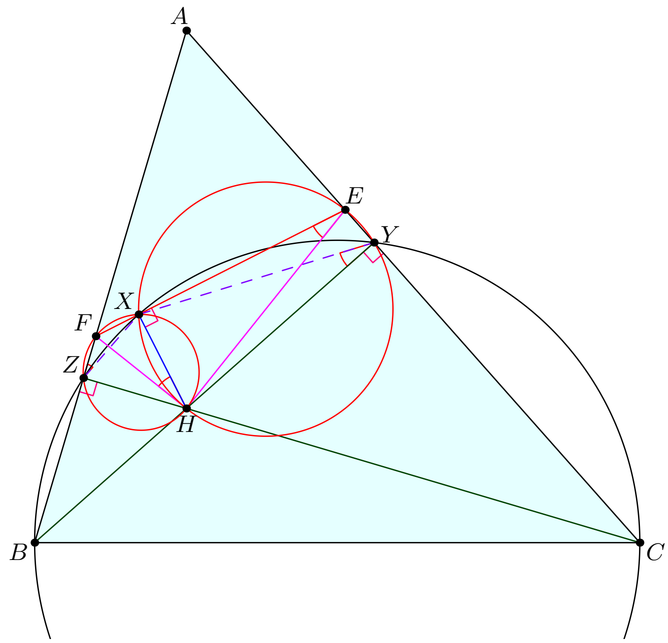
Solution 2: Consider the set of all rooks which are either the leftmost or rightmost in their row, or the topmost or bottommost in their column. Note that this set must include every rook, as any rook not in this set attacks a rook in all 4 directions.

Each column contributes at most 2 rooks to this set, and each row contributes at most 2 rooks. We can safely ignore the top and bottom rows in this count, as any rook in the top or bottom row is already the topmost or bottommost rook in its column. Thus the number of rooks in the set is at most $2 \cdot (2025 + 2025 - 2) = \boxed{8096}$, which can be constructed as seen before.

5. [35] Let $\triangle ABC$ be an acute triangle with orthocenter H. Points E and F are on segments $\overline{AC}$ and $\overline{AB}$, respectively, such that $\angle EHF = 90^\circ$. Let X be the foot of the altitude from H to $\overline{EF}$. Prove that $\angle BXC = 90^\circ$.

Proposed by: Pitchayut Saengrungkongka

Solution 1:



We use $\measuredangle$ to denote directed angles. Let Y and Z be the feet of the altitudes from B and C to AC and AB, respectively. Then $\measuredangle HZF = \measuredangle HXF = 90^\circ$, so $HZFX$ is cyclic. Similarly, $HYEX$ is cyclic. Therefore,

$$\measuredangle BYX = \measuredangle HYX = \measuredangle HEX = \measuredangle FHX = \measuredangle FZX = \measuredangle BZX.$$

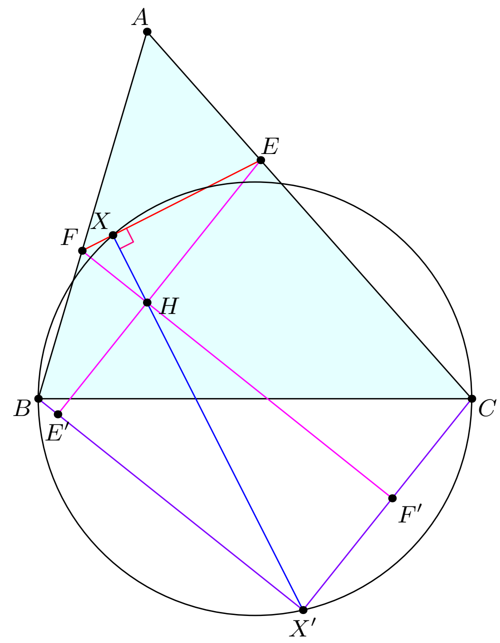
Hence, $BZXY$ is cyclic. A symmetric argument shows C lies on this circle as well. It follows that $\angle BXC = \angle BYC = 90^\circ$, as desired.

Solution 2: Let T be the foot of altitude from A to BC. For any point X, let X' denote the image of X under the negative inversion at H with radius $\sqrt{HA \cdot HT}$. Then B' and C' are the feet of the altitudes from B and C to sides AC and AB, respectively.

Claim 1. $\angle BX'C = 90^\circ$.

Proof. Because $HX \perp EF$ and $HE \perp HF$, the quadrilateral $HE'X'F'$ is a rectangle. Note that $\angle BE'H = \angle EB'H = 90^\circ$ and $\angle X'E'H = 90^\circ$. Consequently, X', B, and E' are collinear. Similarly, X', C, and F' are collinear. Then, $\angle BX'C = \angle E'X'F' = 90^\circ$, as desired. ☐

From the claim, X' lies on the circle with diameter BC (which B' and C' also lie on). Since this circle is invariant under the inversion, X lies on the circle with diameter BC as well, and $\angle BXC = 90^\circ$.



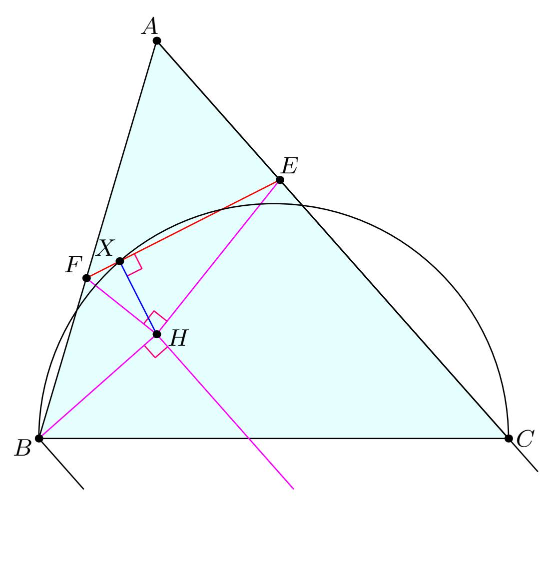
Solution 3: We begin by proving the following lemma.

Lemma 2. Let $ABCD$ be a quadrilateral and P be a point such that $\measuredangle APB + \measuredangle CPD = 180^\circ$. Then, the feet of the altitudes from P to each side of $ABCD$ are concyclic.

Proof. Let P_A, P_B, P_C, P_D the feet of the altitudes from P to AB, BC, CD, and DA respectively. Note that quadrilateral P_APP_BB is cyclic. By angle chasing,

$$\begin{aligned}\measuredangle P_DP_AP_B + \measuredangle P_BP_CP_D &= \measuredangle P_DP_AP + \measuredangle PP_AP_B + \measuredangle P_BP_CP + \measuredangle PP_CP_D \\ &= \measuredangle P_DAP + \measuredangle PBP_B + \measuredangle P_BCP + \measuredangle PDP_D \\ &= (180^\circ - \measuredangle APD) + (180^\circ - \measuredangle BPC) \\ &= \measuredangle BPA + \measuredangle DPC \\ &= 180^\circ.\end{aligned}$$

Therefore, $P_AP_BP_CP_D$ is cyclic as desired. □



Let P_∞ be the point at infinity on line AC. Let Y and Z be the feet of the altitudes from H to AB and AC, respectively. Note that $\angle EHF + \angle BHP_\infty = 90^\circ + 90^\circ = 180^\circ$. Thus, the feet of the altitudes from H to EF, EB, BP_∞, and CP_∞ are concyclic. In other words, $XYZB$ is cyclic. Since $BCYZ$ is a cyclic quadrilateral, we conclude X lies on this circle, giving us that $\angle BXC = 90^\circ$ as desired.

Remark. Here's another way to prove the lemma.

It is well known that, with the provided condition, there is a point P' that is the isogonal conjugate of P with respect to quadrilateral $ABCD$. Let P_A, P_B, P_C, and P_D be the feet of the altitudes from P to AB, BC, CD, and DA, respectively, and let Q be the foot of the altitude from P' to AB. Because P and P' are isogonal conjugates with respect to the triangle formed by lines AB, BC, and CD, we have $P_AP_BP_CQ$ is cyclic. Similarly, because P and P' are also isogonal conjugate with respect to the triangle formed by lines DA, AB, and BC, we have $P_DP_AP_BQ$ is cyclic. Consequently, $P_AP_BP_CP_C$ is cyclic as desired.

6. **[40]** Complex numbers $\omega_1, \ldots, \omega_n$ each have magnitude 1. Let z be a complex number distinct from $\omega_1, \ldots, \omega_n$ such that

$$\frac{z+\omega_1}{z-\omega_1} + \cdots + \frac{z+\omega_n}{z-\omega_n} = 0.$$

Prove that $|z| = 1$.

Proposed by: Karthik Venkata Vedula

Solution 1: We show that no solutions z not on the unit circle can exist. First, we eliminate $|z| > 1$.

Claim 1. For all j and $|z| > 1$, the real part of $\frac{z+\omega_j}{z-\omega_j}$ is positive.

Proof. We use geometry. Note that ω_j and $-\omega_j$ are antipodes on the unit circle. Since z lies outside the unit circle, it follows that $\angle \omega_j z(-\omega_j)$ is acute. But this means the complex number $\frac{z+\omega_j}{z-\omega_j}$ lies strictly in the first or fourth quadrant of the complex plane and thus has positive real part, as desired. □

It is then clear that whenever $|z| > 1$, the sum $\sum_{j=1}^{n} \frac{z+\omega_j}{z-\omega_j}$ has positive real part and thus cannot be 0. The case where $|z| < 1$ is analogous, except $\angle \omega_j z(-\omega_j)$ is obtuse instead, so $\frac{z+\omega_j}{z-\omega_j}$ has negative real part for all j. Therefore, all solutions z to the original equation must satisfy $|z| = 1$.

Solution 2: We show more generally that for any positive integers k, $a_1, \ldots, a_k$, and *distinct* ω_j on the unit circle, the equation

$$\sum_{j=1}^{k} a_j \left(\frac{z+\omega_i}{z-\omega_j} \right) = 0$$

has k distinct solutions on the unit circle. The original problem then follows upon consolidating duplicate ω_j's. Without loss of generality, assume that $\omega_1, \ldots, \omega_k$ are in this order going clockwise around the unit circle.

Claim 2. There is a solution on the (clockwise) arc from ω_j to ω_{j+1} for all j (where $\omega_{k+1} = \omega_1$).

Proof. First, ω_j and $-\omega_j$ are antipodes on the unit circle, so if z is on the unit circle, $\angle \omega_j z(-\omega_j) = 90^\circ$ This means $\frac{z+\omega_j}{z-\omega_j}$ is purely imaginary. Now consider the imaginary part of the left hand side of the equation, which is a real and continuous function on the arc strictly between ω_j and ω_{j+1} for each j. In particular, as z approaches ω_{j+1} from the clockwise direction, this function approaches ∞. On the other hand, as z approaches ω_j from the counterclockwise direction, this function approaches $-\infty$. By the Intermediate Value Theorem, there must be a solution on this arc, as desired. □

It follows that there are at least k solutions on the unit circle. But the equation is equivalent to a polynomial of degree k. Hence, there are exactly k solutions, all of which lie on the unit circle.

Remark. The coefficients a_j's are introduced to handle the case where some of $\omega_1, \dots, \omega_n$ are equal. Another way to get around this case is to utilize the fact that roots of polynomials are continuous, so we can take the limit where several ω_j's approach each other.

Remark. The Möbius transformation $z \mapsto i\frac{z-1}{z+1}$ sends the unit circle to a real line. One can rephrase both solutions as working on the real line instead of the unit circle.

7. **[45]** Determine, with proof, whether a square can be dissected into finitely many (not necessarily congruent) triangles, each of which has interior angles $30°$, $75°$, and $75°$.

Proposed by: Derek Liu

Answer: $\boxed{\text{No}}$

Solution 1: Assume for sake of contradiction that such a dissection exists. It has exactly half as many $30°$ angles as $75°$ angles.

Around any intersection point except the square's vertices, the only angles that can appear are $30°$, $75°$, and $180°$. The only combinations of these that sum to $180°$ or $360°$ are

$$\begin{aligned} 6 \cdot 30° &= 180°, \\ 30° + 2 \cdot 75° &= 180°, \\ 180° &= 180°, \\ 12 \cdot 30° &= 360°, \\ 7 \cdot 30° + 2 \cdot 75° &= 360°, \\ 2 \cdot 30° + 4 \cdot 75° &= 360°, \\ 6 \cdot 30° + 180° &= 360°, \\ 30° + 2 \cdot 75° + 180° &= 360°, \\ 180° + 180° &= 360°. \end{aligned}$$

In particular, around any such point, there are at least half as many $30°$ angles as $75°$ angles.

However, the square's vertices must each be surrounded by three $30°$ angles and zero $75°$ angles, as there is no other way to get a sum of $90°$. Thus the total number of $30°$ angles in the dissection must be at least 12 more than half the number of $75°$ angles, contradiction.

Thus no such dissection exists.

Solution 2: Again assume for sake of contradiction that a dissection exists. Interpret the dissection as a graph G, where the vertices of the graph are the vertices of all the triangles, and edges connect each pair of consecutive vertices along a line segment.

Call a vertex *flat* if it is on either the boundary of the square (including its corners) or the interior of an edge of any triangle. Let X be the number of flat vertices and Y be the number of non-flat vertices in G. Let E and F be the number of edges and faces (triangles) in the dissection, respectively. Then $(X+Y) - E + F = 1$.

Observing the angle combinations in the first solution, we see that any non-flat vertex must have at least 6 incident edges, and any flat vertex must have at least 4. Thus $2E \geq 6Y + 4X$, so $E \geq 3Y + 2X$.

The sum of the angles of all F triangles is πF. Around any non-flat vertex, such angles sum to 2π. Around any flat vertex, the angles sum to π, with the exception of the four corners of the square, where they sum to $\pi/2$ instead. Thus

$$F\pi = (X-4)\pi + 4(\pi/2) + Y(2\pi) = (X + 2Y - 2)\pi,$$

so $F = X + 2Y - 2$. This means

$$X + Y - E + F \leq (X + Y) - (3Y + 2X) + (X + 2Y - 2) = -2,$$

contradiction. Thus no dissection exists.

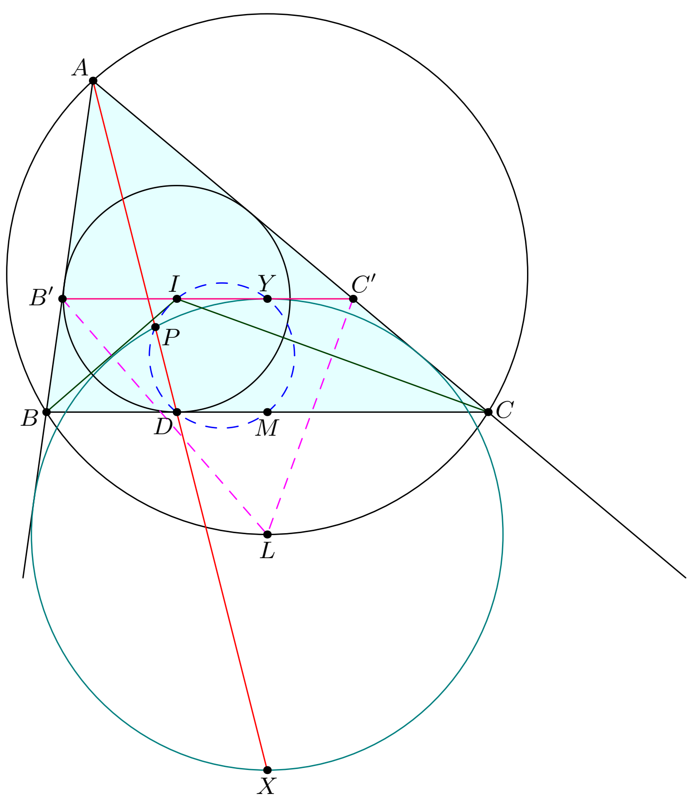
8. **[50]** Let $\triangle ABC$ be a triangle with incenter I. The incircle of triangle $\triangle ABC$ touches $\overline{BC}$ at D. Let M be the midpoint of $\overline{BC}$, and let line AI meet the circumcircle of triangle $\triangle ABC$ again at $L \neq A$. Let ω be the circle centered at L tangent to AB and AC. If ω intersects segment $\overline{AD}$ at point P, prove that $\angle IPM = 90^\circ$.

Proposed by: Pitchayut Saengrungkongka

Solution 1: Let X and Y be the bottom and top point on ω (i.e., the tangents of X and Y to ω are parallel to BC, and Y and A lie on the same side of BC). Note that A, P, D, and X are collinear by homothety between the incircle and ω. The key claim is the following.

Claim 1. Line IY is tangent to ω.

Proof. Let the line through I parallel to BC meet AB and AC at B' and C', respectively. Notice that $B'L$ is the perpendicular bisector of BI, so $B'L$ externally bisects $\angle AB'C'$. Similarly, $C'L$ externally bisects $\angle AC'B'$. Hence, L is the excenter of $\triangle AB'C'$, which means that $B'C'$ is tangent to ω. $\square$

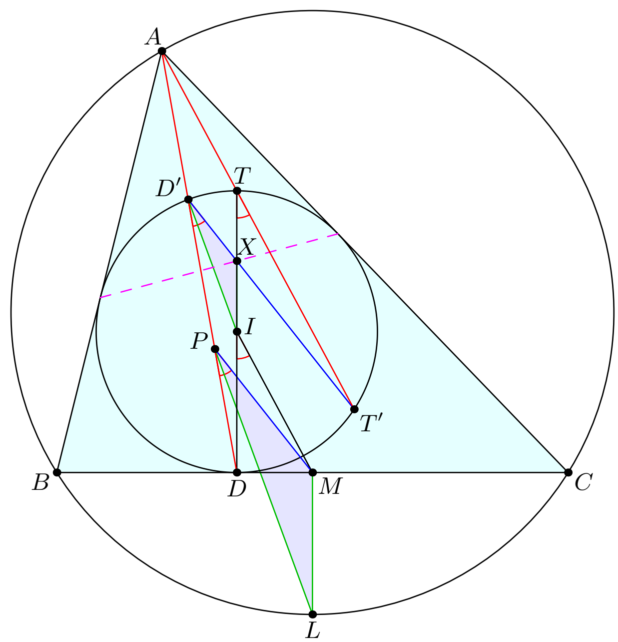


Now, we note that $LY \perp BC$, so L, Y, and M are collinear (on the perpendicular bisector of BC). Since $\angle YPX = 90^\circ$ and $\angle YMD = 90^\circ$, $PDMY$ is cyclic. However, $IYMD$ is a rectangle, so $IPDMY$ is a cyclic pentagon. Hence, $\angle IPM = \angle IDM = 90^\circ$.

Solution 2: Let the incircle touch AC and AB at E and F, respectively. Let DI intersect EF at X. Let D' be the other intersection of AD and the incircle.

Claim 2. $PM \parallel D'X$.

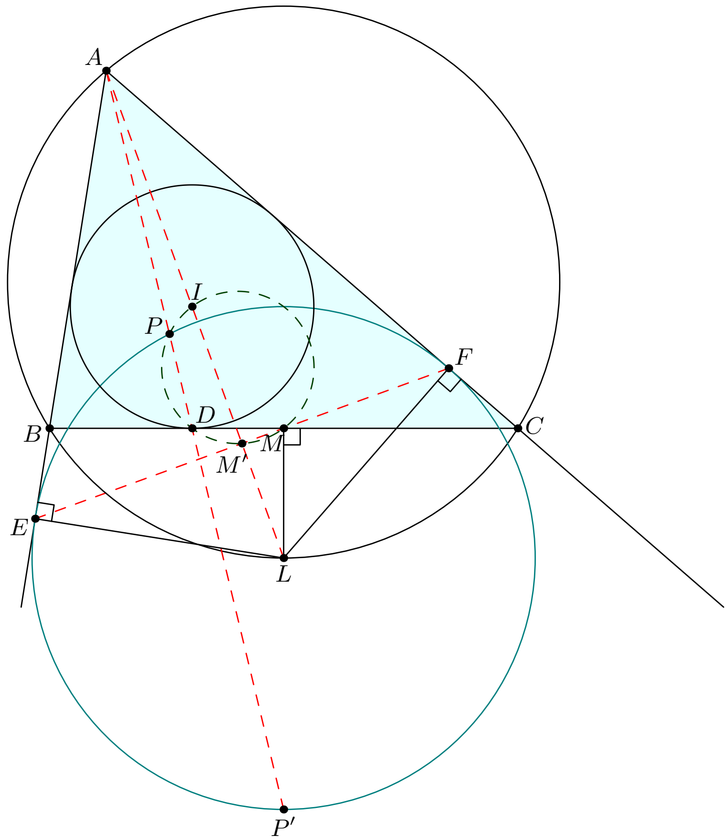
Proof. Consider the homothety at A that sends ω to the incircle. It sends L to I and P to D'. Furthermore, it's well-known that X lies on AM. Because $IX \parallel LM$, we also have that the homothety sends M to X. These facts imply that $D'X \parallel PM$. $\square$



Let T be the antipode of D on the incircle. Let AT intersect the incircle again at T'. Since X lies on the polar of A with respect to the incircle, by Brocard's theorem, we have D', X, and T' are collinear. It is well-known that $AT \parallel IM$. Therefore, $\angle DPM = \angle DD'X = \angle DD'T' = \angle DTT' = \angle DIM$. Consequently, $IMDP$ is cyclic, and $\angle IPM = \angle IDM = 90°$.

Solution 3: Let ω be tangent to AB and AC at E and F, respectively. Note that these are the feet of the altitudes from L to AB and AC, and L lies on the circumcircle of $\triangle ABC$ by Fact 5. As M is clearly the foot from L to BC, it follows that E, F, and M are collinear on the Simson Line of L with respect to $\triangle ABC$.

Lastly, we want P to be on the circle with diameter IM. This circle intersects EF again at the foot from M to AI, which is the midpoint of EF. Let this point be M'. Consider the homothety sending the incircle to ω. This clearly sends D to the second intersection of AD and ω, which is P', and it sends I to L. Note that $AP \cdot AP' = AE^2 = AM \cdot AL$, as the circle with diameter LE is tangent to AE. Thus, $PP'M'L$ is cyclic. Since $ID \parallel LP'$, I lies on $M'L$, and D lies on PP'. By Reim's, we also have $PDM'I$ is cyclic. As IM is a diameter of $(DM'I)$, we have $\angle IPM = 90°$.



9. **[60]** Let $\mathbb{Z}$ be the set of integers. Determine, with proof, all primes p for which there exists a function $f\colon \mathbb{Z} \to \mathbb{Z}$ such that for any integer x,

- $f(x+p) = f(x)$ and
- p divides $f(x + f(x)) - x$.

Proposed by: Marin Hristov Hristov

Answer: $\boxed{p = 5 \text{ and all primes } p \equiv \pm 1 \pmod 5}$

Solution: We work in $\mathbb{F}_p$, treating f as a map from $\mathbb{F}_p$ to itself. Clearly, $p = 2$ doesn't work. For $p > 2$ such that 5 is a quadratic residue mod p, as well as $p = 5$ itself, there exists some α such that $(2\alpha+1)^2 \equiv 5 \pmod p$. Taking $f(x) = \alpha x$ then works because

$$f(x + f(x)) - x = (\alpha^2 + \alpha - 1)x = \frac{1}{4}\left((2\alpha+1)^2 - 5\right)x \equiv 0 \pmod p.$$

To prove no other primes satisfy the conditions in the problem statement, note that f is surjective, as for any x, $f(x + f(x)) = x$. As $\mathbb{F}_p$ is finite, f is bijective. Plugging in $x = f(y)$ yields

$$f(f(y) + f(f(y))) = f(y) \implies f(y) + f(f(y)) = y.$$

Since f is bijective, there exists $z \in \mathbb{F}_p$ such that $f(z) = 0$, then $z = f(z+f(z)) = f(z) = 0$. Therefore, $f(0) = 0$. This is the only fixed point, as any fixed point d would satisfy $d = f(d) + f(f(d)) = 2d$, which is impossible if $d \neq 0$. Hence the remaining residues form nontrivial cycles y, $f(y)$, $f(f(y))$, etc. If the cycle containing y is of length n, then

$$\begin{aligned} f^{-1}(y) &= y + f(y), \\ f^{-2}(y) &= f^{-1}(y) + y = 2y + f(y), \\ &\vdots \\ f^{-(n-1)}(y) = f(y) &= F_n y + F_{n-1} f(y), && \text{(by induction)} \\ y &= F_{n+1} y + F_n f(y), \end{aligned}$$

where F_k is the k-th Fibonacci number. As $y \neq 0$ and $f(y) \neq 0$, the last two equations tell us

$$F_n^2 \equiv \left(\frac{(1 - F_{n-1}) f(y)}{y} \right) \left(\frac{(1 - F_{n+1}) y}{f(y)} \right) \equiv (F_{n+1} - 1)(F_{n-1} - 1) \pmod{p}.$$

Let $A = F_{n+1} - 1$ and $B = F_{n-1} - 1$ for brevity. The last equation becomes

$$(A - B)^2 \equiv AB \equiv \frac{1}{4}((A + B)^2 - (A - B)^2) \pmod{p} \Longrightarrow (A + B)^2 \equiv 5(A - B)^2 \pmod{p}.$$

As 5 is not a quadratic residue, this implies $F_{n+1} \equiv F_{n-1} \equiv 1 \pmod{p}$. Hence, if d is the smallest positive integer such that $F_d \equiv 0 \pmod{p}$ and $F_{d+1} \equiv 1 \pmod{p}$, then the Fibonacci sequence is periodic modulo p with period d, so $d \mid n$. The sum of all cycle lengths (excluding the fixed point 0) is $p - 1$, so $d \mid p - 1$. The following well-known lemma will give us a contradiction.

Lemma 1. If 5 is not a quadratic residue modulo a prime p, then $p \nmid F_{p-1}$.

Proof 1. Recall Binet's formula,

$$F_{p-1} = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^{p-1} - \left(\frac{1 - \sqrt{5}}{2} \right)^{p-1} \right).$$

Multiplying both sides by 2^{p-1} and expanding via the binomial theorem, we have

$$2^{p-1} F_{p-1} = 2 \sum_{k=0}^{\frac{p-3}{2}} 5^k \binom{p-1}{2k+1}.$$

However, $\binom{p-1}{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}$ for all k, so

$$p \mid F_{p-1} \quad \text{if and only if} \quad p \left| \sum_{k=0}^{\frac{p-3}{2}} 5^k = \frac{5^{\frac{p-1}{2}} - 1}{5 - 1}. \right.$$

Therefore $p \mid F_{p-1}$ if and only if $5^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, which doesn't hold if 5 is not a quadratic residue modulo p, as desired. □

Proof 2. Work in $\mathbb{F}_{p^2} = \mathbb{F}_p[\sqrt{5}]$. Since 5 is not a quadratic residue, we get that $(\sqrt{5})^p = -\sqrt{5}$. Using the fact that $(a + b)^p = a^p + b^p$ (because all other terms have coefficient divisible by p), we get that

$$\left(\frac{1 + \sqrt{5}}{2} \right)^p = \frac{1 - \sqrt{5}}{2} \Longrightarrow \left(\frac{1 + \sqrt{5}}{2} \right)^{p-1} = \left(\frac{1 - \sqrt{5}}{2} \right)^2 = \frac{3 - \sqrt{5}}{2}.$$

Similarly, $\left(\frac{1-\sqrt{5}}{2}\right)^{p-1} = \frac{3+\sqrt{5}}{2}$. Hence, by Binet's formula,

$$\begin{aligned} F_{p-1} &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{p-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{p-1}\right) \\ &= \frac{1}{\sqrt{5}}\left(\frac{3-\sqrt{5}}{2} - \frac{3+\sqrt{5}}{2}\right) = -1, \end{aligned}$$

so it is not divisible by p. $\square$

Hence, $F_{p-1} \not\equiv 0 \pmod{p}$ if 5 is not a quadratic residue modulo p, which contradicts $d \mid p-1$ above. This completes the solution.

10. **[60]** Determine, with proof, all possible values of $\gcd(a^2+b^2+c^2, abc)$ across all triples of positive integers (a, b, c).

Proposed by: Henrick Rabinovitz

Answer: $\boxed{\text{All positive integers } n \text{ such that } \nu_p(n) \neq 1 \text{ for all prime } p \equiv 3 \pmod{4}}$

Solution: First, we show that no other n work. If there does exist prime $p \equiv 3 \pmod 4$ such that $\nu_p(n) = 1$, then $p \mid abc$; without loss of generality, assume p divides a. Then, $p^2 \mid a^2$ and $p \mid a^2+b^2+c^2$, so $p \mid b^2+c^2$. Since p is 3 modulo 4, -1 is not a quadratic residue modulo p, so $b^2 \equiv -c^2 \pmod p$ only has the trivial solution $(b, c) = 0$. Therefore $p \mid b$ and $p \mid c$, so $p^2 \mid n$. This contradicts $\nu_p(n) = 1$, so no solutions outside of the claimed solution set exist.

Now, we give the construction. Let n be in the claimed solution set. We proceed in two steps.

Step 1 (Local step). For each prime p dividing n, we will construct a, b, and c modulo $p^{\nu_p(n)+1}$ such that $\nu_p(\gcd(a^2+b^2+c^2, abc)) = \nu_p(n)$.

We have a couple cases.

- **If $\nu_p(n) = 2k$** for some positive integer k, pick $a = p^k$, $b = p^k$, and $c = p^{k+1}$ for $p \neq 2$ and pick $a = b = c = p^k$ for $p = 2$.
- **If $p \not\equiv 3 \pmod 4$ and $\nu_p(n) = 2k+1$** for some nonnegative integer k, then by Fermat's Christmas theorem, there are positive integers x and y for which $x^2+y^2 = p$. Then pick $a = xp^k$, $b = yp^k$, and $c = p^{k+1}$.
- **If $p \equiv 3 \pmod 4$ and $\nu_p(n) = 2k+1$** for some nonnegative integer k, then $k \geq 1$ by assumption. We let x and y be positive integers for which $\nu_p(x^2+y^2+1) = 1$. (This is fairly standard. To briefly recall the proof, note that x and y satisfying $x^2+1 \equiv -y^2 \pmod p$ exist because some quadratic residue must be adjacent to a nonquadratic residue, and forcing $x^2+1 \not\equiv -y^2 \pmod{p^2}$ can be done by adding appropriate multiples of p to x or y.) Then, pick $a = xp^k$, $b = yp^k$, and $c = p^k$.

Step 2 (Global step). Given solutions (a_p, b_p, c_p) modulo $p^{\nu_p(n)+1}$ for each prime $p \mid n$, we construct a working solution (a, b, c) over positive integers.

By Chinese Remainder Theorem, we can pick positive integers a, b, and c such that for all prime $p \mid n$, $(a, b, c) \equiv (a_p, b_p, c_p) \pmod{p^{\nu_p(n)+1}}$. Now, we need to modify this construction to ensure that no other primes divide $\gcd(a^2+b^2+c^2, abc)$.

For every prime $p \mid c$ with $p \nmid n$, we modify a and b (by adding additional congruence relations) so that p does not divide a^2+b^2. Then, p does not divide $\gcd(a^2+b^2+c^2, abc)$ for any prime p such that $p \mid c$

and $p \nmid n$. Let

$$\begin{aligned} N &= \prod_{p \mid cn} p^{\nu_p(n)+1}, \\ S &= \{\text{primes } p \text{ such that } p \mid ab \text{ but } p \nmid cn\}, \\ P &= \prod_{p \in S} p^{\varphi(N)} \equiv 1 \pmod{N}. \end{aligned}$$

In particular, we have only fixed residues of a, b, c modulo N at this point. Now, let $a_1 = aP$ and $b_1 = bP$. This keeps all of our mod N conditions. We now claim that (a_1, b_1, c) works. To prove this, fix a prime p, and note that

- **if $\boldsymbol{p}$ divides $\boldsymbol{cn}$**, then since $a' \equiv a \pmod{N}$ and $b' \equiv b \pmod{N}$, we have $\nu_p(\gcd(a_1^2 + b_1^2 + c^2, a_1 b_1 c)) = \nu_p(n)$ from our construction of (a, b, c).
- **if $\boldsymbol{p \in S}$**, then we note that p divides $a_1^2 + b_1^2$, but not c^2, so p does not divide $a_1^2 + b_1^2 + c^2$.
- **if $\boldsymbol{p \notin S}$ and $\boldsymbol{p \nmid cn}$**, then p does not divide $a_1 b_1 c$.

This concludes the proof.