47^{th} United States of America Mathematical Olympiad
Day 1. 12:30 PM – 5:00 PM EDT
April 18, 2018

Note: For any geometry problem whose statement begins with an asterisk $(*)$, the first page of the solution must be a large, in-scale, clearly labeled diagram. Failure to meet this requirement will result in an automatic 1-point deduction.

USAMO 1. Let a, b, c be positive real numbers such that $a + b + c = 4\sqrt[3]{abc}$. Prove that

$$2(ab + bc + ca) + 4\min(a^2, b^2, c^2) \geq a^2 + b^2 + c^2.$$

USAMO 2. Find all functions $f : (0, \infty) \to (0, \infty)$ such that

$$f\left(x + \frac{1}{y}\right) + f\left(y + \frac{1}{z}\right) + f\left(z + \frac{1}{x}\right) = 1$$

for all $x, y, z > 0$ with $xyz = 1$.

USAMO 3. For a given integer $n \geq 2$, let $\{a_1, a_2, \ldots, a_m\}$ be the set of positive integers less than n that are relatively prime to n. Prove that if every prime that divides m also divides n, then $a_1^k + a_2^k + \cdots + a_m^k$ is divisible by m for every positive integer k.

47^{th} United States of America Mathematical Olympiad
Day 2. 12:30 PM – 5:00 PM EDT
April 19, 2018

Note: For any geometry problem whose statement begins with an asterisk ($*$), the first page of the solution must be a large, in-scale, clearly labeled diagram. Failure to meet this requirement will result in an automatic 1-point deduction.

USAMO 4. Let p be a prime, and let $a_1, a_2, \ldots, a_p$ be integers. Show that there exists an integer k such that the numbers

$$a_1 + k, a_2 + 2k, \ldots, a_p + pk$$

produce at least $\frac{1}{2}p$ distinct remainders upon division by p.

USAMO 5. ($*$) In convex cyclic quadrilateral $ABCD$, we know that lines AC and BD intersect at E, lines AB and CD intersect at F, and lines BC and DA intersect at G. Suppose that the circumcircle of $\triangle ABE$ intersects line CB at B and P, and that the circumcircle of $\triangle ADE$ intersects line CD at D and Q, where C, B, P, G and C, Q, D, F are collinear in this order. Prove that if lines FP and GQ intersect at M, then $\angle MAC = 90°$.

USAMO 6. Let a_n be the number of permutations $(x_1, x_2, \ldots, x_n)$ of the numbers $(1, 2, \ldots, n)$ such that the n ratios $\frac{x_k}{k}$ for $1 \le k \le n$ are all distinct. Prove that a_n is odd for all $n \ge 1$.

2018 U.S.A. Mathematical Olympiad Solutions

USAMO 1.

First solution. Assume without loss of generality that $c = \min(a, b, c)$. By the AM-GM inequality and the given condition, we have

$$\begin{aligned} 4c(a+b+c) + 4ab &\geq 2\sqrt{16 \cdot abc(a+b+c)} \\ &= 2\sqrt{16\left(\frac{a+b+c}{4}\right)^3 (a+b+c)} \\ &= (a+b+c)^2. \end{aligned}$$

Subtracting $2(ab + bc + ca)$ from both sides, this gives

$$2(ab + bc + ca) + 4c^2 \geq a^2 + b^2 + c^2,$$

as desired.

Remark. The equality in the AM-GM step occurs if and only if $c(a + b + c) = ab$. Solving for $a+b+c$ and substituting into the condition $a+b+c = 4\sqrt[3]{abc}$, this implies $8c^2 = ab$. Substituting this back into the equation $c(a + b + c) = ab$, we conclude that

$$c(a + b + c) = 8c^2 \implies a + b = 7c.$$

We then have

$$a - b = \pm\sqrt{(a + b)^2 - 4ab} = \pm\sqrt{49c^2 - 32c^2} = \pm\sqrt{17}c.$$

It follows that $\{2a, 2b\} = \{(7 - \sqrt{17})c, (7 + \sqrt{17})c\}$. Hence, equality holds if and only if (a, b, c) is a permutation of

$$\left((7 - \sqrt{17})r, (7 + \sqrt{17})r, 2r\right)$$

for some positive real number r.

Second solution. Suppose, as above, that $c = \min(a, b, c)$, and write $A = a/c$, $B = b/c$, and $D = A+B$. The given condition becomes $A+B+1 = 4\sqrt[3]{AB}$, or equivalently, $AB = (D+1)^3/64$. In terms of A and B, the problem asks us to prove that

$$2(AB + A + B) + 4 \geq A^2 + B^2 + 1,$$

which can be rearranged as

$$2(A + B) + 3 - (A + B)^2 + 4AB \geq 0.$$

After substituting in D, this inequality becomes

$$2D + 3 - D^2 + (D + 1)^3/16 \geq 0.$$

Since the left-hand side factors as $(D+1)(D-7)^2/16$, the inequality always holds.

Third solution: Assuming that $c = \min(a,b,c)$ and by adding $2(ab+bc+ca)$ to both sides, our inequality becomes

$$4c(a+b+c)+4ab \geq (a+b+c)^2.$$

Since both the given condition and the desired claim are homogeneous, we may assume without loss of generality that $a+b+c=8$, so our task is to prove that if $ab = 8/c$, then $32c + 4ab \geq 64$. This clearly holds, since for any positive real number c we have $32\left(c+\frac{1}{c}\right) \geq 64$.

USAMO 2.

For any $u, v, w \in (0,1)$ satisfying $u+v+w=1$, we may set $x = \frac{u}{v}$, $y = \frac{v}{w}$, and $z = \frac{w}{u}$ to obtain

$$f\left(\frac{u+v}{w}\right) + f\left(\frac{v+w}{u}\right) + f\left(\frac{w+u}{v}\right) = 1,$$

and thus

$$f\left(\frac{1}{w}-1\right) + f\left(\frac{1}{u}-1\right) + f\left(\frac{1}{v}-1\right) = 1.$$

First, let $g : (0,1) \to (0,\infty)$ be given by $g(x) = f\left(\frac{1}{x}-1\right)$, so that the above equation reads

$$g(u)+g(v)+g(w) = 1 \text{ for all } u,v,w \in (0,1) \text{ with } u+v+w=1.$$

Note that this condition implies actually $g(x) < 1$ for all x.

Next, consider the function $h : (-1/3, 2/3) \to (-1/3, 2/3)$ given by $h(x) = g(x+1/3) - 1/3$. Then, we have for all $x, y, z \in (-1/3, 2/3)$ with $x+y+z=0$ that

$$h(x)+h(y)+h(z) = 0. \tag{1}$$

We now establish the key properties of h in a series of claims.

Claim 1. *We have $h(0) = 0$ and for all $x \in (-1/3, 1/3)$, we have $h(-x) = -h(x)$.*

Proof. Setting $x = y = z = 0$ in (1) gives $h(0) = 0$. Then, setting $z = 0$ and $y = -x$ yields $h(-x) = -h(x)$, as long as $x \in (-1/3, 1/3)$. □

Claim 2. *For all $x, y \in (0, 2/3)$ with $x+y < 2/3$, we have $h(x+y) = h(x)+h(y)$.*

Proof. In the case where $x, y < 1/3$, we immediately have from Claim 1 and (1) that

$$h(x)+h(y) = -h(-x)-h(-y) = h(x+y).$$

This allows us to deduce the same property for all x and y satisfying the specified conditions. Indeed, we have

$$h(x+y) = h\left(\frac{x+y}{2}\right) + h\left(\frac{x+y}{2}\right) = 2h\left(\frac{x}{2}\right) + 2h\left(\frac{y}{2}\right) = h(x)+h(y),$$

where we have used the fact that $x+y < 2/3$ implies $x/2, y/2, (x+y)/2$ are all less than $1/3$. □

Claim 3. *For all $x \in (-1/3, 2/3)$, we have $h(x) = 3h(1/3)x$.*

Proof. Note that by repeated applications of Claim 2, we have $h(nx) = nh(x)$ for all real numbers x and positive integers n satisfying $nx \in (0, 2/3)$. Thus, for any positive integers p and q, we have

$$h\left(\frac{p}{q}\right) = 3ph\left(\frac{1}{3q}\right) = \frac{3p}{q}h(1/3),$$

which proves the claim when x is positive and rational.

Next, suppose for sake of contradiction that for some $x \in (0, 2/3)$, we have $|h(x) - 3h(1/3)x| = \delta > 0$. Consider any positive rational $r < x$. Then, we have by Claim 2 that

$$h(x-r) = h(x) - h(r) = h(x) - 3h(1/3)r = h(x) - 3h(1/3)x + 3h(1/3)(x-r).$$

Thus, by taking r sufficiently close to x, we can ensure that

$$x - r < \frac{1}{3 \cdot \lceil 1/\delta \rceil} \text{ and } |h(x-r)| > \frac{\delta}{2}.$$

However, this implies (again by repeated applications of Claim 2)

$$|h(2 \cdot \lceil 1/\delta \rceil \cdot (x-r))| = 2 \cdot \lceil 1/\delta \rceil \cdot |h(x-r)| > 1,$$

which is a contradiction, since h must take values in $(-1/3, 2/3)$.

Thus, we have proved the claim for all positive x in the domain of h. Applying Claim 1, the result extends also to negative x, completing the proof. □

By Claim 3, we conclude that h must take the form $h(x) = cx$, where c is a constant. Moreover, since h maps $(-1/3, 2/3)$ to itself, we must have $c \in [-1/2, 1]$. In terms of f, this means we must have

$$f(x) = g(1/(x+1)) = \frac{1}{3} + c \cdot \left(\frac{1}{x+1} - \frac{1}{3}\right)$$

for some constant $-1/2 \leq c \leq 1$. And we can readily check that all functions of this form do indeed work, by plugging this expression into the original equation, and choosing u, v, w such that $x = \frac{u}{v}, y = \frac{v}{w}, z = \frac{w}{u}$ as at the beginning of this solution (which can be done whenever $xyz = 1$).

USAMO 3.

The integer m in the statement of the problem is $\varphi(n)$, where φ is the Euler totient function. Throughout our proof we write $p^s \,||\, m$, if s is the greatest power of p that divides m.

We begin with the following lemma:

Lemma 1. If p is a prime and p^s divides n for some positive integer s, then $1^k + 2^k + \cdots + n^k$ is divisible by p^{s-1} for any integer $k \geq 1$.

Proof. Let $\{a_1, a_2, \dots, a_m\}$ be a complete reduced residue set modulo p^s and $m = p^{s-1}(p-1)$. First we prove by induction on s that for any positive integer k, $a_1^k + a_2^k + \cdots + a_m^k$ is divisible by p^{s-1}. The base case $s = 1$ is true. Suppose the statement holds for some value of s. Consider the statement for $s+1$. Note that

$$\{a_1, \dots, a_m, p^s + a_1, \dots, p^s + a_m, \dots, p^s(p-1) + a_1, \dots, p^s(p-1) + a_m\}$$

is a complete reduced residue set modulo p^{s+1}. Therefore, the desired sum of k-th powers is equal to

$$a_1^k + \cdots + a_m^k + \cdots + (p^s(p-1) + a_1)^k + \cdots + (p^s(p-1) + a_m)^k \equiv p(a_1^k + \cdots + a_m^k) \equiv 0 \pmod{p^s},$$

where we have used the induction hypothesis for the second congruence. This gives the induction step.

Now we are ready to prove the lemma. Because numbers from 1 to n can be split into blocks of consecutive numbers of length p^s, it is enough to show that $1^k + 2^k + \cdots + (p^s)^k$ is divisible by p^{s-1} for any positive integer k. We use induction on s. The statement is true for $s = 1$. Assume the statement is true for $s - 1$. The sum

$$1^k + 2^k + \cdots + (p^s)^k = a_1^k + a_2^k + \cdots + a_m^k + p^k \left(1^k + 2^k + \cdots + (p^{s-1})^k\right)$$

is divisible by p^{s-1}, because $p^{s-1} \mid a_1^k + \cdots + a_m^k$ and by the induction hypothesis $p^{s-2} \mid 1^k + \cdots + (p^{s-1})^k$. □

Now we proceed to prove a second lemma, from which the statement of the problem will immediately follow:

Lemma 2. Suppose p is a prime dividing n. Let $\{a_1, \dots, a_m\}$ be a complete reduced residue set mod n, and define s by $p^s \mid\mid m$. Then p^s divides $a_1^k + \cdots + a_m^k$ for any integer $k \geq 1$.

Proof. We fix p, and use induction on the number of prime factors of n (counted by multiplicity) that are different from p. If there are no prime factors other than p, then $n = p^{s+1}$, $m = p^s(p-1)$, and we proved in Lemma 1 that $a_1^k + \cdots + a_m^k$ is divisible by p^s. Now suppose the statement is true for n. We show that it is true for nq, where q is a prime not equal to p.

Case 1. q divides n. We have $p^s \mid\mid \varphi(n)$ and $p^s \mid\mid \varphi(nq)$, because $\varphi(nq) = q\varphi(n)$. If $\{a_1, a_2, \dots, a_m\}$ is a complete reduced residue set modulo n, then

$$\{a_1, \dots, a_m, n + a_1, \dots, n + a_m, \dots, n(q-1) + a_1, \dots, n(q-1) + a_m\}$$

is a complete reduced residue set modulo nq. The new sum of k-th powers is equal to

$$a_1^k + \cdots + a_m^k + \cdots + (n(q-1) + a_1)^k + \cdots + (n(q-1) + a_m)^k = mn^k \left(1^k + \cdots + (q-1)^k\right) +$$

$$\binom{k}{1}n^{k-1}\left(1^{k-1}+\cdots+(q-1)^{k-1}\right)(a_1+\cdots+a_m)+\cdots+q(a_1^k+\cdots+a_m^k).$$

This sum is divisible by p^s because $p^s \mid\mid m$ and $p^s \mid a_1^j + a_2^j + \cdots + a_m^j$ for any positive integer j.

Case 2. q doesn't divide n. Suppose $p^b \mid\mid q-1$, where $b \geq 0$. Note that $\varphi(nq) = \varphi(n)(q-1)$, so $p^s \mid\mid \varphi(n)$ and $p^{s+b} \mid\mid \varphi(nq)$. Let $\{a_1, \dots, a_m\}$ be a complete reduced residue set modulo n. The complete reduced residue set modulo nq consists of the mq numbers

$$\{a_1, \dots, a_m, n+a_1, \dots, n+a_m, \dots, n(q-1)+a_1, \dots, n(q-1)+a_m\}$$

with the m elements $\{qa_1, qa_2, \dots, qa_m\}$ removed.

The new sum of k-th powers is equal to

$$a_1^k+\cdots+a_m^k+\cdots+(n(q-1)+a_1)^k+\cdots+(n(q-1)+a_m)^k-q^k(a_1^k+\cdots+a_m^k)=$$

$$mn^k\left(1^k+\cdots+(q-1)^k\right)+\binom{k}{1}n^{k-1}\left(1^{k-1}+\cdots+(q-1)^{k-1}\right)(a_1+\cdots+a_m)+\cdots$$

$$\cdots+\binom{k}{k-1}n\left(1+\cdots+(q-1)\right)(a_1^{k-1}+\cdots+a_m^{k-1})+q(a_1^k+\cdots+a_m^k)-q^k(a_1^k+\cdots+a_m^k).$$

Each term

$$\binom{k}{j}n^{k-j}\left(1^{k-j}+\cdots+(q-1)^{k-j}\right)(a_1^j+\cdots+a_m^j),$$

for $0 \leq j \leq k-1$, is divisible by p^{s+b} because $p \mid n^{k-j}$, $p^s \mid a_1^j + \cdots + a_m^j$, and $p^{b-1} \mid 1^{k-j} + \cdots + (q-1)^{k-j}$ by Lemma 1.

Also $(q^k - q)(a_1^k + \cdots + a_m^k)$ is divisible by p^{s+b} because $p^b \mid q-1 \mid q^k - q$ and $p^s \mid a_1^k + \cdots + a_m^k$. Thus p^{s+b} divides our sum and our proof is complete. □

Remark. In fact, one can also show the converse statement: if $\{a_1, a_2, \dots, a_m\}$ is as defined in the problem and $a_1^k + a_2^k + \cdots + a_m^k$ is divisible by m for every positive integer k, then every prime that divides m also divides n.

USAMO 4.

The statement is trivial for $p = 2$, so assume $p = 2q+1$ is odd. Create a $p \times p$ table of numbers, as follows:

$$\begin{array}{cccc}
a_1+1\cdot 0 & a_2+2\cdot 0 & \cdots & a_p+p\cdot 0\\
a_1+1\cdot 1 & a_2+2\cdot 1 & \cdots & a_p+p\cdot 1\\
\vdots & \vdots & \ddots & \vdots\\
a_1+1\cdot(p-1) & a_2+2\cdot(p-1) & \cdots & a_p+p\cdot(p-1)
\end{array}$$

Interpret all the numbers above modulo p. Examine two different columns, say columns i and j. We claim they agree (modulo p) in exactly one row. Indeed, $a_i + ik \equiv a_j + jk \pmod{p}$ holds if and only if $(i-j)k \equiv a_j - a_i \pmod{p}$. Since p is prime and $i \not\equiv j \pmod{p}$, this condition holds for a unique value of k (namely, $k \equiv (a_j - a_i)(i-j)^{-1} \pmod{p}$).

Thus, there are $\binom{p}{2} = \frac{p(p-1)}{2} = pq$ pairs of integers that are congruent modulo p and lie in the same row of the table. Since there are only p rows, some row, say $\{a_n + nk\}_n$, must contain at most q such pairs.

We claim that this k satisfies our requirement. Indeed, if we read the p entries in this row one by one, each entry either is distinct from all the previous ones, or is congruent to at least one previous entry and thereby completes a pair. Since the latter case happens at most q times, there must be at least $p - q = (p+1)/2$ distinct entries (modulo p), completing the proof.

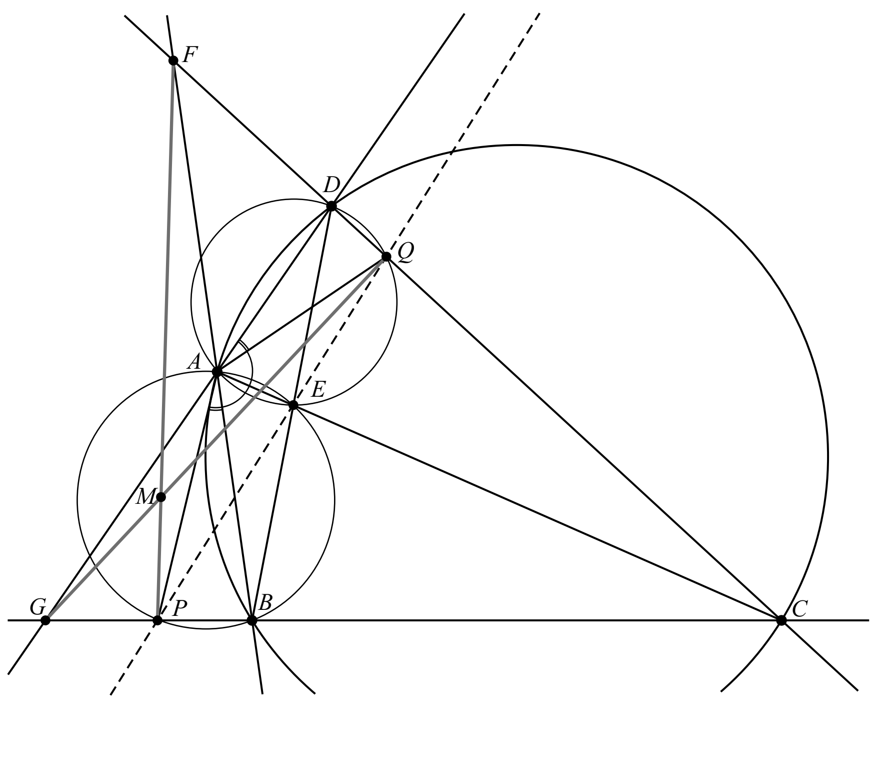
USAMO 5.

First solution. In this particular configuration, we have

$$\angle BAE = \angle BAC = \angle BDC = \angle EDQ = \angle EAQ,$$

$$\angle PAE = 180^\circ - \angle PBE = \angle CBD = \angle CAD = \angle EAD,$$

hence line AC is the internal angle bisector of angles BAQ and PAD. If we could prove that $\angle GAM = \angle MAP$, then line AM would prove to be the external angle bisector of $\angle BAQ$ and hence perpendicular to AC.



Since $\triangle PAF$ and $\triangle QAG$ are related by $\angle PAF = \angle QAG$, it now suffices to prove that

$$\frac{\sin \angle GAM}{\sin \angle MAQ} = \frac{\sin \angle PAM}{\sin \angle MAF}, \tag{1}$$

which is but a repeated application of the Law of Sines. Using the Ratio Lemma in $\triangle PAF$ and $\triangle QAG$, (1) is equivalent to

$$\frac{GM}{MQ}\Big/\frac{AG}{AQ} = \frac{PM}{MF}\Big/\frac{AP}{AF}, \qquad \text{i.e.} \qquad \frac{GM}{MP}\cdot\frac{FM}{MQ} = \frac{AF\cdot AG}{AP\cdot AQ}. \tag{2}$$

We now calculate

$$\frac{GM}{MP}\cdot\frac{FM}{MQ} = \frac{\sin\angle GPF}{\sin\angle CGQ}\cdot\frac{\sin\angle GQF}{\sin\angle PFC}$$

$$= \frac{GF\cdot\frac{\sin\angle CGF}{FP}}{CQ\cdot\frac{\sin\angle GCF}{GQ}}\cdot\frac{GF\cdot\frac{\sin\angle GFC}{GQ}}{PC\cdot\frac{\sin\angle GCF}{FP}} = \frac{GF^2}{\sin^2\angle GCF}\cdot\frac{\sin\angle CGF\cdot\sin\angle GFC}{CQ\cdot CP} = \frac{CF\cdot CG}{CP\cdot CQ}. \tag{3}$$

However, from $\triangle CAP \sim \triangle CBE$ and $\triangle CAQ \sim \triangle CDE$, we have $\frac{CP}{AP} = \frac{CE}{BE}$ and $\frac{CQ}{AQ} = \frac{CE}{DE}$. Hence

$$\frac{CP\cdot CQ}{AP\cdot AQ} = \frac{EC^2}{EB\cdot ED} = \frac{EC^2}{EA\cdot EC}. \tag{4}$$

Further computations give

$$\frac{CF}{AF}\cdot\frac{CG}{AG} = \frac{\sin\angle BAC}{\sin\angle ACD}\cdot\frac{\sin\angle CAD}{\sin\angle ACB} = \frac{\sin\angle BAC}{\sin\angle ACB}\cdot\frac{\sin\angle CAD}{\sin\angle ACD} = \frac{\sin\angle CDB}{\sin\angle BDA}\cdot\frac{CD}{DA} = \frac{EC}{EA}.$$

Combining this with (3) and (4), we finally have

$$\frac{GM}{MP}\cdot\frac{FM}{MQ} = \frac{CF\cdot CG}{CP\cdot CQ} = \frac{CF\cdot CG}{AP\cdot AQ}\cdot\frac{EA}{EC} = \frac{AF\cdot AG}{AP\cdot AQ},$$

which gives us (2) and therefore (1). This completes the proof.

Second solution. Using directed angles, $\angle PEA + \angle AEQ = \angle PBA + \angle ADQ = 0$, so P, E, Q are collinear. Also, $CP\cdot CB = CA\cdot CE = CQ\cdot CD$ implies that $PQDB$ is a cyclic quadrilateral.

Look at $PQDB$. Its opposite sides meet at C and E, and its Miquel point is A, the intersection of the circumcircles of $\triangle EBP$ and $\triangle EDQ$. It is well-known that the Miquel point of a cyclic quadrilateral is the projection of the intersection of its diagonals onto the line formed by the intersections of its opposite sides. Therefore, A is the projection of $H = BQ\cap PD$ onto line CE.

Applying Pappus's theorem to collinear triples (B, P, G) and (D, Q, F), we find that $BQ\cap PD = H$, $BF\cap GD = A$, and $PF\cap GQ = M$ are collinear. Note that H, A, M are all distinct because B, P, G and D, Q, F are distinct. Therefore, A is the projection of M onto CE as well, i.e. $\angle MAC = 90°$.

Third solution. Similarly to the first solution, we begin by noting that

$$\angle GAC = 180° - \angle DAC = 180° - \angle DBC = \angle PBE = 180° - \angle PAE.$$

Thus, AC is the external bisector of $\angle GAP$. By symmetry, AC is also the external bisector of $\angle FAQ$.

Now, for a small $\epsilon > 0$, consider a homothety of factor $1 - \epsilon$ centered at C taking A, G, and Q to A', G', and Q', respectively. Let

$$X = AP \cap A'G', \quad Y = AF \cap A'Q', \quad M' = PF \cap G'Q'.$$

Note that $A'G'Q'$ and APF are perspective from the point C. Thus, by Desargues' theorem, we know that X, Y, and M' are collinear.

Moreover, since AC externally bisects $\angle GAP$ and $G'A'||GA$, it follows that $\triangle AXA'$ is isosceles, and X lies on the perpendicular bisector of $\overline{AA'}$. Similarly, Y also lies on this perpendicular bisector, so the line through M', X, and Y is perpendicular to AC.

Now, taking $\epsilon \to 0$, we see that $M' \to M$ while $X \to A$ and $Y \to A$. It follows that MA is perpendicular to AC, as desired.

USAMO 6.

For any permutation $x = (x_1, x_2, \ldots, x_n)$ there is an inverse permutation $y = (y_1, y_2, \ldots, y_n)$ where we define $y_j = k$ if and only if $x_k = j$. Then the ratios for the permutation y are $\frac{y_j}{j} = \frac{k}{x_k}$, hence the reciprocals of those for the permutation x. Thus we see that y has distinct ratios if and only if x does. In particular, modulo 2, a_n is the same as the number of permutations x which are equal to their own inverse and have distinct ratios.

A permutation x is its own inverse if and only if it can be formed by breaking the numbers $1, 2, \ldots, n$ into singletons and pairs and defining $x_k = k$ if k is a singleton and $x_j = k$, $x_k = j$ if $\{j, k\}$ is a pair. Any singleton gives a ratio of 1, so the distinct ratio condition forces there to be at most one singleton (and hence, there is one singleton if n is odd and none if n is even). Thus we see that $a_n \equiv b_n \pmod 2$, where b_n is the number of ways to form $\lfloor n/2 \rfloor$ disjoint pairs of elements of $\{1, 2, \ldots, n\}$ such that no pair forms the same ratio as any other pair. (To avoid ambiguity, interpret "the ratio of a pair" to mean the ratio of its larger to its smaller element.)

Note that for any set of $\lfloor n/2 \rfloor$ disjoint pairs of elements of $\{1, 2, \ldots, n\}$, if we have two pairs with the same ratio, say $\{a, b\}$ and $\{c, d\}$ with $a/b = c/d$ (or equivalently $ad = bc$), then replacing $\{a, b\}$ and $\{c, d\}$ with $\{a, c\}$ and $\{b, d\}$ gives another such pairing. Accordingly, refer to a pair of pairs $\{\{a, b\}, \{c, d\}\}$ satisfying $a/b = c/d$ as a *potential swap*. Notice that this move is reversible: we can apply it to potential swap $\{\{a, b\}, \{c, d\}\}$ to get to potential swap $\{\{a, c\}, \{b, d\}\}$, and vice versa.

Now build a graph whose vertices are sets of $\lfloor n/2 \rfloor$ disjoint pairs of elements from $\{1, 2, \ldots, n\}$, and where two such pairings are connected by an edge if they differ by simultaneously applying the move above to some non-empty collection of (disjoint) potential swaps. This graph G has $(2\lfloor (n-1)/2 \rfloor + 1)!!$ vertices, hence an odd number of vertices. (The notation $k!!$ means $1 \cdot 3 \cdot 5 \cdots k$, where k is odd. To see why this formula holds, note that for even n, we have $n-1$ possible partners for the element 1 and then $(n-3)!!$ ways to pair up the remaining elements by induction. Then, for odd n, we have n choices for the singleton and $(n-2)!!$ ways to pair up the remaining elements.)

Moreover, b_n is the number of isolated vertices of G, since all pairs in a given pairing have different ratios if and only if there are no potential swaps.

Whenever we are given a set of $m \geq 2$ pairs all with the same ratio, then we can form k disjoint potential swaps from among these m pairs in $\binom{m}{2k}(2k-1)!!$ ways. (For $k = 0$, we define $(-1)!! = 1$.) Hence, the total number of ways to choose disjoint potential swaps from these m is

$$d_m = \sum_k \binom{m}{2k}(2k-1)!! \equiv \sum_k \binom{m}{2k} = 2^{m-1} \pmod 2.$$

Thus the number of choices (including the empty choice of no potential swaps) is even. More generally, if we are given a set of pairs, for which at least two of them (but not necessarily all) have the same ratio, then the number of ways to form disjoint potential swaps from them is again even: we can arrange the pairs into groups of pairs having the same ratio, and the desired number is just the product of d_m, as m ranges over the sizes of the various groups. Thus, for any collection of $\lfloor n/2 \rfloor$ disjoint pairs from $\{1, 2, \ldots, n\}$, if the pairs do not all have distinct ratios, then the number of ways of constructing zero or more disjoint potential swaps among these pairs is even. Excluding the empty choice, we see that every non-isolated vertex of G has odd degree. Thus, b_n can also be described as the number of vertices of G of even degree.

However, by the handshake lemma, any finite graph G has an even number of vertices of odd degree. Thus, G, having an odd number of vertices, also has an odd number of vertices of even degree. That is, b_n is odd and hence so is a_n.