Solutions to USA TST for IMO 2014

Evan Chen

March 15, 2022

Problem 1. Let ABC be an acute triangle, and let X be a variable interior point on the minor arc BC of its circumcircle. Let P and Q be the feet of the perpendiculars from X to lines CA and CB, respectively. Let R be the intersection of line PQ and the perpendicular from B to AC. Let ℓ be the line through P parallel to XR. Prove that as X varies along minor arc BC, the line ℓ always passes through a fixed point.

The fixed point is the orthocenter, since ℓ is a Simson line. See Lemma 4.4 of *Euclidean Geometry in Math Olympiads*.

Problem 2. Let a_1, a_2, a_3, ... be a sequence of integers, with the property that every consecutive group of a_i's averages to a perfect square. More precisely, for all positive integers n and k, the quantity

$$\frac{a_n + a_{n+1} + \cdots + a_{n+k-1}}{k}$$

is always the square of an integer. Prove that the sequence must be constant (all a_i are equal to the same perfect square).

Let $\nu_p(n)$ denote the largest exponent of p dividing n. The problem follows from the following proposition.

Proposition

Let (a_n) be a sequence of integers and let p be a prime. Suppose that every consecutive group of a_i's with length at most p averages to a perfect square. Then $\nu_p(a_i)$ is independent of i.

We proceed by induction on the smallest value of $\nu_p(a_i)$ as i ranges (which must be even, as each of the a_i are themselves a square). First we prove two claims.

Claim — If $j \equiv k \pmod p$ then $a_j \equiv a_k \pmod p$.

Proof. Taking groups of length p in our given, we find that $p \mid a_j + \cdots + a_{j+p-1}$ and $p \mid a_{j+1} + \cdots + a_{j+p}$ for any j. So $a_j \equiv a_{j+p} \pmod p$ and the conclusion follows. □

Claim — If some a_i is divisible by p then all of them are.

Proof. The case $p = 2$ is trivial so assume $p \geq 3$. Without loss of generality (via shifting indices) assume that $a_1 \equiv 0 \pmod p$, and define

$$S_n = a_1 + a_2 + \cdots + a_n \equiv a_2 + \cdots + a_n \pmod p.$$

Call an integer k with $2 \leq k < p$ a **pivot** if $1 - k^{-1}$ is a quadratic nonresidue modulo p.

We claim that for any pivot k, $S_k \equiv 0 \pmod p$. If not, then

$$\frac{a_1 + a_2 + \cdots + a_k}{k} \text{ and } \frac{a_2 + \cdots + a_k}{k-1}$$

are both qudaratic residues. Division implies that $\frac{k-1}{k} = 1 - k^{-1}$ is a quadratic residue, contradiction.

Next we claim that there is an integer m with $S_m \equiv S_{m+1} \equiv 0 \pmod p$, which implies $p \mid a_{m+1}$. If 2 is a pivot, then we simply take $m = 1$. Otherwise, there are $\frac{1}{2}(p-1)$ pivots, one for each nonresidue (which includes neither 0 nor 1), and all pivots lie in $[3, p-1]$, so we can find an m such that m and $m+1$ are both pivots.

Repeating this procedure starting with a_{m+1} shows that $a_{2m+1}, a_{3m+1}, \ldots$ must all be divisible by p. Combined with the first claim and the fact that $m < p$, we find that all the a_i are divisible by p. □

The second claim establishes the base case of our induction. Now assume all a_i are divisible by p and hence p^2. Then all the averages in our proposition (with length at most p) are divisible by p and hence p^2. Thus the map $a_i \mapsto \frac{1}{p^2} a_i$ gives a new sequence satisfying the proposition, and our inductive hypothesis completes the proof.

> **Remark.** There is a subtle bug that arises if one omits the condition that $k \le p$ in the proposition. When $k = p^2$ the average $\frac{a_1 + \cdots + a_{p^2}}{p^2}$ is not necessarily divisible by p even if all the a_i are. Hence it is not valid to divide through by p. This is why the condition $k \le p$ was added.

Problem 3. Let n be an even positive integer, and let G be an n-vertex (simple) graph with exactly $\frac{n^2}{4}$ edges. An unordered pair of distinct vertices $\{x, y\}$ is said to be *amicable* if they have a common neighbor (there is a vertex z such that xz and yz are both edges). Prove that G has at least $2\binom{n/2}{2}$ pairs of vertices which are amicable.

First, we prove the following lemma. (`https://en.wikipedia.org/wiki/Friendship_paradox`).

Lemma (On average, your friends are more popular than you)
For a vertex v, let $a(v)$ denote the average degree of the neighbors of v (setting $a(v) = 0$ if $\deg v = 0$). Then

$$\sum_v a(v) \ge \sum_v \deg v = 2\#E.$$

Proof. Ignoring isolated vertices, we can write

$$\begin{aligned}\sum_v a(v) &= \sum_v \frac{\sum_{w\sim v} \deg w}{\deg v} \\ &= \sum_v \sum_{w\sim v} \frac{\deg w}{\deg v} \\ &= \sum_{\text{edges } vw} \left(\frac{\deg w}{\deg v} + \frac{\deg v}{\deg w} \right) \\ &\overset{\text{AM-GM}}{\ge} \sum_{\text{edges } vw} 2 = 2\#E = \sum_v \deg v\end{aligned}$$

as desired. $\square$

Corollary (On average, your most popular friend is more popular than you)
For a vertex v, let $m(v)$ denote the maximum degree of the neighbors of v (setting $m(v) = 0$ if $\deg v = 0$). Then

$$\sum_v m(v) \ge \sum_v \deg v = 2\#E.$$

We can use this to count amicable pairs by noting that any particular vertex v is in at least $m(v) - 1$ amicable pairs. So, the number of amicable pairs is at least

$$\frac{1}{2}\sum_v (m(v) - 1) \ge \#E - \frac{1}{2}\#V.$$

Note that up until now we haven't used any information about G. But now if we plug in $\#E = n^2/4$, $\#V = n$, then we get exactly the desired answer. (Equality holds for $G = K_{n/2,n/2}$.)

Problem 4. Let n be a positive even integer, and let $c_1, c_2, \dots, c_{n-1}$ be real numbers satisfying

$$\sum_{i=1}^{n-1} |c_i - 1| < 1.$$

Prove that

$$2x^n - c_{n-1}x^{n-1} + c_{n-2}x^{n-2} - \cdots - c_1 x^1 + 2$$

has no real roots.

We will prove the polynomial is positive for all $x \in \mathbb{R}$. As $c_i > 0$, the result is vacuous for $x \le 0$, so we restrict attention to $x > 0$.

Then letting $c_i = 1 - d_i$ for each i, the inequality we want to prove becomes

$$x^n + 1 + \frac{x^{n+1} + 1}{x + 1} > \sum_1^{n-1} d_i x^i \qquad \text{given } \sum |d_i| < 1.$$

But obviously $x^n + 1 > x^i$ for any $1 \le i \le n-1$ and $x > 0$. So in fact $x^n + 1 > \sum_1^{n-1} |d_i| x^i$ holds for $x > 0$, as needed.

Problem 5. Let $ABCD$ be a cyclic quadrilateral, and let E, F, G, and H be the midpoints of AB, BC, CD, and DA respectively. Let W, X, Y and Z be the orthocenters of triangles AHE, BEF, CFG and DGH, respectively. Prove that the quadrilaterals $ABCD$ and $WXYZ$ have the same area.

The following solution is due to Grace Wang.

We begin with:

Claim — Point W has coordinates $\frac{1}{2}(2a+b+d)$.

Proof. The orthocenter of $\triangle DAB$ is $d+a+b$, and $\triangle AHE$ is homothetic to $\triangle DAB$ through A with ratio $1/2$. Hence $w = \frac{1}{2}(a+(d+a+b))$ as needed. □

By symmetry, we have

$$\begin{aligned} w &= \frac{1}{2}(2a+b+d) \\ x &= \frac{1}{2}(2b+c+a) \\ y &= \frac{1}{2}(2c+d+b) \\ z &= \frac{1}{2}(2d+a+c). \end{aligned}$$

We see that $w-y=a-c$, $x-z=b-d$. So the diagonals of $WXYZ$ have the same length as those of $ABCD$ as well as the same directed angle between them. This implies the areas are equal, too.

Problem 6. For a prime p, a subset S of residues modulo p is called a *sum-free multiplicative subgroup* of $\mathbb{F}_p$ if

- there is a nonzero residue α modulo p such that $S = \left\{1, \alpha^1, \alpha^2, \dots\right\}$ (all considered mod p), and
- there are no $a, b, c \in S$ (not necessarily distinct) such that $a + b \equiv c \pmod p$.

Prove that for every integer N, there is a prime p and a sum-free multiplicative subgroup S of $\mathbb{F}_p$ such that $|S| \geq N$.

We first prove the following general lemma.

Lemma

If $f, g \in \mathbb{Z}[X]$ are relatively prime nonconstant polynomials, then for sufficiently large primes p, they have no common root modulo p.

Proof. By Bézout Lemma, there exist polynomials $a(X)$ and $b(X)$ in $\mathbb{Z}[X]$ and a nonzero constant $c \in \mathbb{Z}$ satisfying the identity

$$a(X)f(X) + b(X)g(X) \equiv c.$$

So, plugging in $X = r$ we get $p \mid c$, so the set of permissible primes p is finite. □

With this we can give the construction.

Claim — Suppose that

- n is a positive integer with $n \not\equiv 0 \pmod 3$;
- p is a prime which is 1 mod n; and
- α is a primitive n'th root of unity modulo p.

Then $|S| = n$ and, if p is sufficiently large in n, is also sum-free.

Proof. The assertion $|S| = n$ is immediate from the choice of α. As for sum-free, assume for contradiction that

$$1 + \alpha^k \equiv \alpha^m \pmod p$$

for some integers $k, m \in \mathbb{Z}$. This means $(X+1)^n - 1$ and $X^n - 1$ have common root $X = \alpha^k$.

But

$$\gcd_{\mathbb{Z}[x]}\Big((X+1)^n - 1,\ X^n - 1\Big) = 1 \qquad \forall n \not\equiv 0 \pmod 3$$

because when $3 \nmid n$ the two polynomials have no common complex roots. (Indeed, if $|\omega| = |1+\omega| = 1$ then $\omega = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$.)

Thus p is bounded by the lemma, as desired. □