USA TSTST 2018 Solutions

United States of America — TST Selection Test

Evan Chen《陳誼廷》

60th IMO 2019 United Kingdom and 8th EGMO 2019 Ukraine

Contents

§0 Problems

1. As usual, let $\mathbb{Z}[x]$ denote the set of single-variable polynomials in x with integer coefficients. Find all functions $\theta\colon \mathbb{Z}[x] \to \mathbb{Z}$ such that for any polynomials $p, q \in \mathbb{Z}[x]$,

- $\theta(p+1) = \theta(p) + 1$, and
- if $\theta(p) \neq 0$ then $\theta(p)$ divides $\theta(p \cdot q)$.

2. In the nation of Onewaynia, certain pairs of cities are connected by one-way roads. Every road connects exactly two cities (roads are allowed to cross each other, e.g., via bridges), and each pair of cities has at most one road between them. Moreover, every city has exactly two roads leaving it and exactly two roads entering it.

We wish to close half the roads of Onewaynia in such a way that every city has exactly one road leaving it and exactly one road entering it. Show that the number of ways to do so is a power of 2 greater than 1 (i.e. of the form 2^n for some integer $n \geq 1$).

3. Let ABC be an acute triangle with incenter I, circumcenter O, and circumcircle Γ. Let M be the midpoint of $\overline{AB}$. Ray AI meets $\overline{BC}$ at D. Denote by ω and γ the circumcircles of $\triangle BIC$ and $\triangle BAD$, respectively. Line MO meets ω at X and Y, while line CO meets ω at C and Q. Assume that Q lies inside $\triangle ABC$ and $\angle AQM = \angle ACB$.

Consider the tangents to ω at X and Y and the tangents to γ at A and D. Given that $\angle BAC \neq 60^\circ$, prove that these four lines are concurrent on Γ.

4. For an integer $n > 0$, denote by $\mathcal{F}(n)$ the set of integers $m > 0$ for which the polynomial $p(x) = x^2 + mx + n$ has an integer root.

(a) Let S denote the set of integers $n > 0$ for which $\mathcal{F}(n)$ contains two consecutive integers. Show that S is infinite but

$$\sum_{n \in S} \frac{1}{n} \leq 1.$$

(b) Prove that there are infinitely many positive integers n such that $\mathcal{F}(n)$ contains three consecutive integers.

5. Let ABC be an acute triangle with circumcircle ω, and let H be the foot of the altitude from A to $\overline{BC}$. Let P and Q be the points on ω with $PA = PH$ and $QA = QH$. The tangent to ω at P intersects lines AC and AB at E_1 and F_1 respectively; the tangent to ω at Q intersects lines AC and AB at E_2 and F_2 respectively. Show that the circumcircles of $\triangle AE_1F_1$ and $\triangle AE_2F_2$ are congruent, and the line through their centers is parallel to the tangent to ω at A.

6. Let $S = \{1, \dots, 100\}$, and for every positive integer n define

$$T_n = \{(a_1, \dots, a_n) \in S^n \mid a_1 + \cdots + a_n \equiv 0 \pmod{100}\}.$$

Determine which n have the following property: if we color any 75 elements of S red, then at least half of the n-tuples in T_n have an even number of coordinates with red elements.

7. Let n be a positive integer. A frog starts on the number line at 0. Suppose it makes a finite sequence of hops, subject to two conditions:

- The frog visits only points in $\{1, 2, \ldots, 2^n - 1\}$, each at most once.
- The length of each hop is in $\{2^0, 2^1, 2^2, \ldots\}$. (The hops may be either direction, left or right.)

Let S be the sum of the (positive) lengths of all hops in the sequence. What is the maximum possible value of S?

8. For which positive integers $b > 2$ do there exist infinitely many positive integers n such that n^2 divides $b^n + 1$?

9. Show that there is an absolute constant $c < 1$ with the following property: whenever $\mathcal{P}$ is a polygon with area 1 in the plane, one can translate it by a distance of $\frac{1}{100}$ in some direction to obtain a polygon $\mathcal{Q}$, for which the intersection of the interiors of $\mathcal{P}$ and $\mathcal{Q}$ has total area at most c.

§1 Solutions to Day 1

§1.1 TSTST 2018/1, proposed by Evan Chen, Yang Liu

🔗 *Available online at* https://aops.com/community/p10570981.

Problem statement

As usual, let $\mathbb{Z}[x]$ denote the set of single-variable polynomials in x with integer coefficients. Find all functions $\theta\colon \mathbb{Z}[x] \to \mathbb{Z}$ such that for any polynomials $p, q \in \mathbb{Z}[x]$,

- $\theta(p+1) = \theta(p) + 1$, and
- if $\theta(p) \neq 0$ then $\theta(p)$ divides $\theta(p \cdot q)$.

The answer is $\theta : p \mapsto p(c)$, for each choice of $c \in \mathbb{Z}$. Obviously these work, so we prove these are the only ones. In what follows, $x \in \mathbb{Z}[x]$ is the identity polynomial, and $c = \theta(x)$.

¶ First solution (Merlijn Staps). Consider an integer $n \neq c$. Because $x - n \mid p(x) - p(n)$, we have

$$\theta(x-n) \mid \theta(p(x)) - p(n)) \implies c - n \mid \theta(p(x)) - p(n).$$

On the other hand, $c - n \mid p(c) - p(n)$. Combining the previous two gives $c - n \mid \theta(p(x)) - p(c)$, and by letting n large we conclude $\theta(p(x)) - p(c) = 0$, so $\theta(p(x)) = p(c)$.

¶ Second solution. First, we settle the case $\deg p = 0$. In that case, from the second property, $\theta(m) = m + \theta(0)$ for every integer $m \in \mathbb{Z}$ (viewed as a constant polynomial). Thus $m + \theta(0) \mid 2m + \theta(0)$, hence $m + \theta(0) \mid -\theta(0)$, so $\theta(0) = 0$ by taking m large. Thus $\theta(m) = m$ for $m \in \mathbb{Z}$.

Next, we address the case of $\deg p = 1$. We know $\theta(x + b) = c + b$ for $b \in \mathbb{Z}$. Now for each particular $a \in \mathbb{Z}$, we have

$$c + k \mid \theta(x + k) \mid \theta(ax + ak) = \theta(ax) + ak \implies c + k \mid \theta(ax) - ac.$$

for any $k \neq -c$. Since this is true for large enough k, we conclude $\theta(ax) = ac$. Thus $\theta(ax + b) = ac + b$.

We now proceed by induction on $\deg p$. Fix a polynomial p and assume it's true for all p of smaller degree. Choose a large integer n (to be determined later) for which $p(n) \neq p(c)$. We then have

$$\frac{p(c) - p(n)}{c - n} = \theta\left(\frac{p - p(n)}{x - n}\right) \mid \theta\left(p - p(n)\right) = \theta(p) - p(n).$$

Subtracting off $c - n$ times the left-hand side gives

$$\frac{p(c) - p(n)}{c - n} \mid \theta(p) - p(c).$$

The left-hand side can be made arbitrarily large by letting $n \to \infty$, since $\deg p \geq 2$. Thus $\theta(p) = p(c)$, concluding the proof.

¶ Authorship comments. I will tell you a story about the creation of this problem. Yang Liu and I were looking over the drafts of December and January TST in October 2017, and both of us had the impression that the test was too difficult. This sparked a non-serious suggestion that we should try to come up with a problem *now* that would be easy enough to use. While we ended up just joking about changing the TST, we did get this problem out of it.

Our idea was to come up with a functional equation that was different from the usual fare: at first we tried $\mathbb{Z}[x] \to \mathbb{Z}[x]$, but then I suggested the idea of using $\mathbb{Z}[x] \to \mathbb{Z}$, with the answer being the "evaluation" map. Well, what properties does that satisfy? One answer was $a - b \mid p(a) - p(b)$; this didn't immediately lead to anything, but eventually we hit on the form of the problem above off this idea. At first we didn't require $\theta(p) \neq 0$ in the bullet, but without the condition the problem was too easy, since 0 divides only itself; and so the condition was added and we got the functional equation.

I proposed the problem to USAMO 2018, but it was rejected (unsurprisingly; I think the problem may be too abstract for novice contestants). Instead it was used for TSTST, which I thought fit better.

§1.2 TSTST 2018/2, proposed by Victor Wang

🔗 *Available online at* https://aops.com/community/p10570985.

Problem statement

In the nation of Onewaynia, certain pairs of cities are connected by one-way roads. Every road connects exactly two cities (roads are allowed to cross each other, e.g., via bridges), and each pair of cities has at most one road between them. Moreover, every city has exactly two roads leaving it and exactly two roads entering it.
We wish to close half the roads of Onewaynia in such a way that every city has exactly one road leaving it and exactly one road entering it. Show that the number of ways to do so is a power of 2 greater than 1 (i.e. of the form 2^n for some integer $n \geq 1$).

In the language of graph theory, we have a simple digraph G which is 2-regular and we seek the number of sub-digraphs which are 1-regular. We now present two solution paths.

¶ First solution, combinatorial. We construct a simple undirected bipartite graph Γ as follows:

- the vertex set consists of two copies of $V(G)$, say V_{out} and V_{in}; and
- for $v \in V_{\text{out}}$ and $w \in V_{\text{in}}$ we have an undirected edge $vw \in E(\Gamma)$ if and only if the directed edge $v \to w$ is in G.

Moreover, the desired sub-digraphs of H correspond exactly to perfect matchings of Γ.

However the graph Γ is 2-regular and hence consists of several disjoint (simple) cycles of even length. If there are n such cycles, the number of perfect matchings is 2^n, as desired.

> **Remark.** The construction of Γ is not as magical as it may first seem.
> Suppose we pick a road $v_1 \to v_2$ to use. Then, the other road $v_3 \to v_2$ is certainly *not* used; hence some other road $v_3 \to v_4$ must be used, etc. We thus get a cycle of forced decisions until we eventually return to the vertex v_1.
> These cycles in the original graph G (where the arrows alternate directions) correspond to the cycles we found in Γ. It's merely that phrasing the solution in terms of Γ makes it cleaner in a linguistic sense, but not really in a mathematical sense.

¶ Second solution by linear algebra over $\mathbb{F}_2$ (Brian Lawrence). This is actually not that different from the first solution. For each edge e, we create an indicator variable x_e. We then require for each vertex v that:

- If e_1 and e_2 are the two edges leaving v, then we require $x_{e_1} + x_{e_2} \equiv 1 \pmod 2$.
- If e_3 and e_4 are the two edges entering v, then we require $x_{e_3} + x_{e_4} \equiv 1 \pmod 2$.

We thus get a large system of equations. Moreover, the solutions come in natural pairs $\vec{x}$ and $\vec{x} + \vec{1}$ and therefore the number of solutions is either zero, or a power of two. So we just have to prove there is at least one solution.

For linear algebra reasons, there can only be zero solutions if some nontrivial linear combination of the equations gives the sum $0 \equiv 1$. So suppose we added up some subset S of the equations for which every variable appeared on the left-hand side an even number of times. Then every variable that did appear appeared exactly twice; and accordingly

we see that the edges corresponding to these variables form one or more even cycles as in the previous solution. Of course, this means $|S|$ is even, so we really have $0 \equiv 0 \pmod 2$ as needed.

> **Remark.** The author's original proposal contained a second part asking to show that it was not always possible for the resulting H to be connected, even if G was strongly connected. This problem is related to IMO Shortlist 2002 C6, which gives an example of a strongly connected graph which does have a full directed Hamiltonian cycle.

§1.3 TSTST 2018/3, proposed by Yannick Yao, Evan Chen

🔗 *Available online at* https://aops.com/community/p10570988.

Problem statement

Let ABC be an acute triangle with incenter I, circumcenter O, and circumcircle Γ. Let M be the midpoint of $\overline{AB}$. Ray AI meets $\overline{BC}$ at D. Denote by ω and γ the circumcircles of $\triangle BIC$ and $\triangle BAD$, respectively. Line MO meets ω at X and Y, while line CO meets ω at C and Q. Assume that Q lies inside $\triangle ABC$ and $\angle AQM = \angle ACB$.
Consider the tangents to ω at X and Y and the tangents to γ at A and D. Given that $\angle BAC \neq 60^\circ$, prove that these four lines are concurrent on Γ.

Henceforth assume $\angle A \neq 60^\circ$; we prove the concurrence. Let L denote the center of ω, which is the midpoint of minor arc BC.

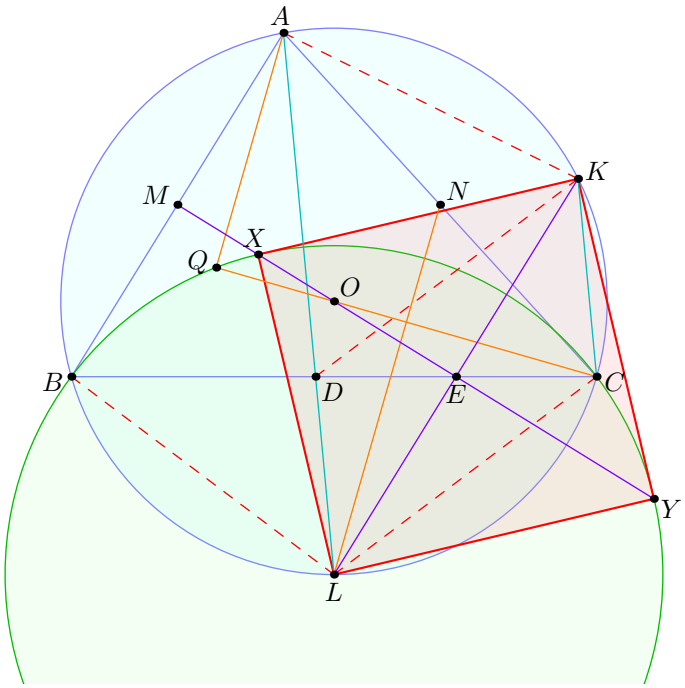
Claim — Let K be the point on ω such that $\overline{KL} \parallel \overline{AB}$ and $\overline{KC} \parallel \overline{AL}$. Then $\overline{KA}$ is tangent to γ, and we may put

$$x = KA = LB = LC = LX = LY = KX = KY.$$

Proof. By construction, $KA = LB = LC$. Also, $\overline{MO}$ is the perpendicular bisector of $\overline{KL}$ (since the chords $\overline{KL}$, $\overline{AB}$ of ω are parallel) and so $KXLY$ is a rhombus as well.

Moreover, $\overline{KA}$ is tangent to γ as well since

$$\measuredangle KAD = \measuredangle KAL = \measuredangle KAC + \measuredangle CAL = \measuredangle KBC + \measuredangle ABK = \measuredangle ABC. \qquad \square$$



Up to now we have not used the existence of Q; we henceforth do so.

Note that $Q \neq O$, since $\angle A \neq 60^\circ \implies O \notin \omega$. Moreover, we have $\angle AOM = \angle ACB$ too. Since O and Q both lie inside $\triangle ABC$, this implies that A, M, O, Q are concyclic. As $Q \neq O$ we conclude $\angle CQA = 90^\circ$.

The main claim is now:

> **Claim —** Assuming Q exists, the rhombus $LXKY$ is a square. In particular, $\overline{KX}$ and $\overline{KY}$ are tangent to ω.

First proof of Claim, communicated by Milan Haiman. Observe that $\triangle QLC \sim \triangle LOC$ since both triangles are isosceles and share a base angle. Hence, $CL^2 = CO \cdot CQ$.

Let N be the midpoint of $\overline{AC}$, which lies on $(AMOQ)$. Then,

$$x^2 = CL^2 = CO \cdot CQ = CN \cdot CA = \frac{1}{2}CA^2 = \frac{1}{2}LK^2$$

where we have also used the fact $AQON$ is cyclic. Thus $LK = \sqrt{2}x$ and so the rhombus $LXKY$ is actually a square. □

Second proof of Claim, Evan Chen. Observe that Q lies on the circle with diameter $\overline{AC}$, centered at N, say. This means that O lies on the radical axis of ω and (N), hence $\overline{NL} \perp \overline{CO}$ implying

$$\begin{aligned} NO^2 + CL^2 = NC^2 + LO^2 &= NC^2 + OC^2 = NC^2 + NO^2 + NC^2 \\ \implies x^2 &= 2NC^2 \\ \implies x &= \sqrt{2}NC = \frac{1}{\sqrt{2}}AC = \frac{1}{\sqrt{2}}LK. \end{aligned}$$

So $LXKY$ is a rhombus with $LK = \sqrt{2}x$. Hence it is a square. □

Third proof of Claim. A solution by trig is also possible. As in the previous claims, it suffices to show that $AC = \sqrt{2}x$.

First, we compute the length CQ in two ways; by angle chasing one can show $\angle CBQ = 180^\circ - (\angle BQC + \angle QCB) = \frac{1}{2}\angle A$, and so

$$\begin{aligned} AC \sin B = CQ &= \frac{BC}{\sin(90^\circ + \frac{1}{2}\angle A)} \cdot \sin \frac{1}{2}\angle A \\ \iff \sin^2 B &= \frac{\sin A \cdot \sin \frac{1}{2}\angle A}{\cos \frac{1}{2}\angle A} \\ \iff \sin^2 B &= 2\sin^2 \frac{1}{2}\angle A \\ \iff \sin B &= \sqrt{2}\sin \frac{1}{2}\angle A \\ \iff 2R\sin B &= \sqrt{2}\left(2R\sin \frac{1}{2}\angle A\right) \\ \iff AC &= \sqrt{2}x \end{aligned}$$

as desired (we have here used the fact $\triangle ABC$ is acute to take square roots).

It is interesting to note that $\sin^2 B = 2\sin^2 \frac{1}{2}\angle A$ can be rewritten as

$$\cos A = \cos^2 B$$

since $\cos^2 B = 1 - \sin^2 B = 1 - 2\sin^2 \frac{1}{2}\angle A = \cos A$; this is the condition for the existence of the point Q. □

We finish by proving that

$$KD = KA$$

and hence line $\overline{KD}$ is tangent to γ. Let $E = \overline{BC} \cap \overline{KL}$. Then

$$LE \cdot LK = LC^2 = LX^2 = \frac{1}{2}LK^2$$

and so E is the midpoint of $\overline{LK}$. Thus $\overline{MXOY}$, $\overline{BC}$, $\overline{KL}$ are concurrent at E. As $\overline{DL} \parallel \overline{KC}$, we find that $DLCK$ is a parallelogram, so $KD = CL = KA$ as well. Thus $\overline{KD}$ and $\overline{KA}$ are tangent to γ.

> **Remark.** The condition $\angle A \neq 60^\circ$ cannot be dropped, since if $Q = O$ the problem is not true.
> On the other hand, nearly all solutions begin by observing $Q \neq O$ and then obtaining $\angle AQO = 90^\circ$. This gives a way to construct the diagram by hand with ruler and compass. One draws an arbitrary chord $\overline{BC}$ of a circle ω centered at L, and constructs O as the circumcenter of $\triangle BLC$ (hence obtaining Γ). Then Q is defined as the intersection of ray CO with ω, and A is defined by taking the perpendicular line through Q on the circle Γ. In this way we can draw a triangle ABC satisfying the problem conditions.

¶ Authorship comments. In the notation of the present points, the question originally sent to me by Yannick Yao read:

> Circles (L) and (O) are drawn, meeting at B and C, with L on (O). Ray CO meets (L) at Q, and A is on (O) such that $\angle CQA = 90^\circ$. The angle bisector of $\angle AOB$ meets (L) at X and Y. Show that $\angle XLY = 90^\circ$.

Notice the points M and K are absent from the problem. I am told this was found as part of the computer game "Euclidea". Using this as the starting point, I constructed the TSTST problem by recognizing the significance of that special point K, which became the center of attention.

§2 Solutions to Day 2

§2.1 TSTST 2018/4, proposed by Ivan Borsenco

🔗 *Available online at* https://aops.com/community/p10570991.

Problem statement

For an integer $n > 0$, denote by $\mathcal{F}(n)$ the set of integers $m > 0$ for which the polynomial $p(x) = x^2 + mx + n$ has an integer root.

(a) Let S denote the set of integers $n > 0$ for which $\mathcal{F}(n)$ contains two consecutive integers. Show that S is infinite but

$$\sum_{n \in S} \frac{1}{n} \le 1.$$

(b) Prove that there are infinitely many positive integers n such that $\mathcal{F}(n)$ contains three consecutive integers.

We prove the following.

Claim — The set S is given explicitly by $S = \{x(x+1)y(y+1) \mid x, y > 0\}$.

Proof. Note that $m, m+1 \in \mathcal{F}(n)$ if and only if there exist integers $q > p \ge 0$ such that

$$m^2 - 4n = p^2$$
$$(m+1)^2 - 4n = q^2.$$

Subtraction gives $2m + 1 = q^2 - p^2$, so p and q are different parities. We can thus let $q - p = 2x + 1$, $q + p = 2y + 1$, where $y \ge x \ge 0$ are integers. It follows that

$$\begin{aligned} 4n &= m^2 - p^2 \\ &= \left(\frac{q^2 - p^2 - 1}{2}\right)^2 - p^2 = \left(\frac{q^2 - p^2 - 1}{2} - p\right)\left(\frac{q^2 - p^2 - 1}{2} + p\right) \\ &= \frac{q^2 - (p^2 + 2p + 1)}{2} \cdot \frac{q^2 - (p^2 - 2p + 1)}{2} \\ &= \frac{1}{4}(q - p - 1)(q - p + 1)(q + p - 1)(q + p + 1) = \frac{1}{4}(2x)(2x+2)(2y)(2y+2) \\ \implies n &= x(x+1)y(y+1). \end{aligned}$$

Since $n > 0$ we require $x, y > 0$. Conversely, if $n = x(x+1)y(y+1)$ for positive x and y then $m = \sqrt{p^2 + 4n} = \sqrt{(y-x)^2 + 4n} = 2xy + x + y = x(y+1) + (x+1)y$ and $m + 1 = 2xy + x + y + 1 = xy + (x+1)(y+1)$. Thus we conclude the main claim. □

From this, part (a) follows as

$$\sum_{n \in S} n^{-1} \le \left(\sum_{x \ge 1} \frac{1}{x(x+1)}\right)\left(\sum_{y \ge 1} \frac{1}{y(y+1)}\right) = 1 \cdot 1 = 1.$$

As for (b), retain the notation in the proof of the claim. Now $m + 2 \in S$ if and only if $(m+2)^2 - 4n$ is a square, say r^2. Writing in terms of p and q as parameters we find

$$r^2 = (m+2)^2 - 4n = m^2 - 4n + 4m + 4 = p^2 + 2 + 2(2m+1)$$

$$= p^2 + 2(q^2 - p^2) + 2 = 2q^2 - p^2 + 2$$
$$\iff 2q^2 + 2 = p^2 + r^2 \qquad (\dagger)$$

with $q > p$ of different parity and $n = \frac{1}{16}(q-p-1)(q-p+1)(q+p-1)(q+p+1)$.

Note that (by taking modulo 8) we have $q \not\equiv p \equiv r \pmod 2$, and so there are no parity issues and we will always assume $p < q < r$ in $(\dagger)$. Now, for every q, the equation $(\dagger)$ has a canonical solution $(p, r) = (q-1, q+1)$, but this leaves $n = 0$. Thus we want to show for infinitely many q there is a third way to write $2q^2 + 2$ as a sum of squares, which will give the desired p.

To do this, choose large integers q such that $q^2 + 1$ is divisible by at least three distinct 1 mod 4 primes. Since each such prime can be written as a sum of two squares, using Lagrange identity, we can deduce that $2q^2 + 2$ can be written as a sum of two squares in at least three different ways, as desired.

Remark. We can see that $n = 144$ is the smallest integer such that $\mathcal{F}(n)$ contains three consecutive integers and $n = 15120$ is the smallest integer such that $\mathcal{F}(n)$ contains four consecutive integers. It would be interesting to determine whether the number of consecutive elements in $\mathcal{F}(n)$ can be arbitrarily large or is bounded.

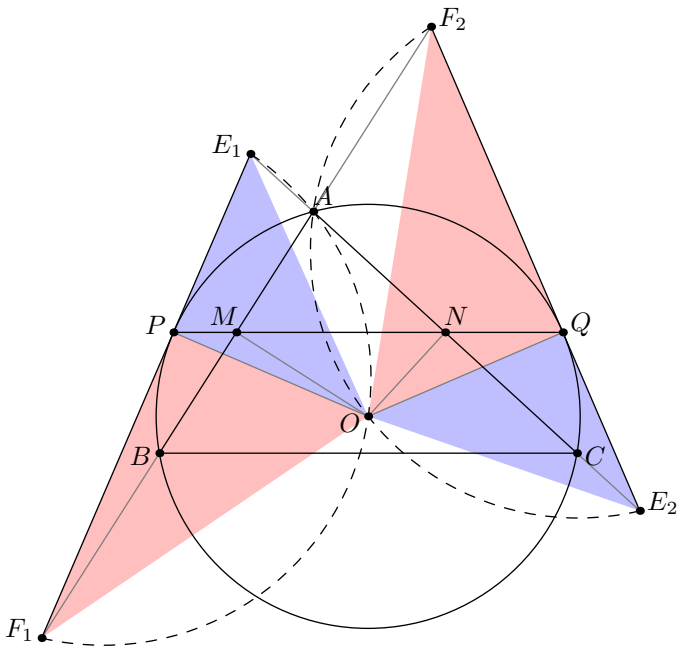
§2.2 TSTST 2018/5, proposed by Ankan Bhattacharya, Evan Chen

🔗 *Available online at* https://aops.com/community/p10571000.

Problem statement

Let ABC be an acute triangle with circumcircle ω, and let H be the foot of the altitude from A to $\overline{BC}$. Let P and Q be the points on ω with $PA = PH$ and $QA = QH$. The tangent to ω at P intersects lines AC and AB at E_1 and F_1 respectively; the tangent to ω at Q intersects lines AC and AB at E_2 and F_2 respectively. Show that the circumcircles of $\triangle AE_1F_1$ and $\triangle AE_2F_2$ are congruent, and the line through their centers is parallel to the tangent to ω at A.

Let O be the center of ω, and let $M = \overline{PQ} \cap \overline{AB}$ and $N = \overline{PQ} \cap \overline{AC}$ be the midpoints of $\overline{AB}$ and $\overline{AC}$ respectively. Refer to the diagram below.



The main idea is to prove two key claims involving O, which imply the result:

(i) quadrilaterals AOE_1F_1 and AOE_2F_2 are cyclic (giving the radical axis is $\overline{AO}$),

(ii) $\triangle OE_1F_1 \cong \triangle OE_2F_2$ (giving the congruence of the circles).

We first note that (i) and (ii) are equivalent. Indeed, because $OP = OQ$, (ii) is equivalent to just the similarity $\triangle OE_1F_1 \sim \triangle OE_2F_2$, and then by the spiral similarity lemma (or even just angle chasing) we have (i) $\iff$ (ii).

We now present five proofs, two of (i) and three of (ii). Thus, we are essentially presenting five different solutions.

¶ Proof of (i) by angle chasing. Note that

$$\measuredangle F_2E_2O = \measuredangle QE_2O = \measuredangle QNO = \measuredangle MNO = \measuredangle MAO = \measuredangle F_2AO$$

and hence E_2OAF_2 is cyclic. Similarly, E_1OAF_1 is cyclic.

¶ Proof of (i) by Simson lines. Since P, M, N are collinear, we see that $\overline{PMN}$ is the Simson line of O with respect to $\triangle AE_1F_1$.

¶ Proof of (ii) by butterfly theorem. By using the **Butterfly Theorem** on the three chords $\overline{AC}$, $\overline{PQ}$, $\overline{PQ}$ concurring at the midpoint N of $\overline{AC}$, it follows that $E_1N = NE_2$ (since $E_1 = \overline{PP} \cap \overline{AC}$, $E_2 = \overline{QQ} \cap \overline{AC}$). Thus

$$E_1P = \sqrt{E_1A \cdot E_1C} = \sqrt{E_2A \cdot E_2C} = E_2P.$$

But also $OP = OQ$ and hence $\triangle OPE_1 \cong \triangle OQE_2$. Similarly for the other pair.

¶ Proof of (ii) by projective geometry. Let $T = \overline{PP} \cap \overline{QQ}$. Let S be on $\overline{PQ}$ with $\overline{ST} \parallel \overline{AC}$; then $\overline{TS} \perp \overline{ON}$, and it follows $\overline{ST}$ is the polar of N (it passes through T by La Hire).

Now,

$$-1 = (PQ; NS) \overset{T}{=} (E_1E_2; N\infty)$$

with $\infty = \overline{AC} \cap \overline{ST}$ the point at infinity. Hence $E_1N = NE_2$ and we can proceed as in the previous solution.

Similarly $O \in \odot(E_2QN)$; by the spiral similarity lemma, $\triangle OPE_1 \overset{+}{\sim} \triangle OQE_2$. Since $OP = OQ$, $\triangle OPE_1 \overset{+}{\cong} \triangle OQE_2$. Similarly $\triangle OPF_1 \overset{+}{\cong} \triangle OQF_2$, so $\triangle OE_1F_1 \overset{+}{\cong} \triangle OE_2F_2$. Since $\triangle OE_1F_1 \cong \triangle OE_2F_2$, the circumcircles are congruent. The circumcircles share common chord $\overline{AO}$; thus the line joining their centers is parallel to the tangent to ω at A.

> **Remark.** The assumption that $\triangle ABC$ is acute is not necessary; it is only present to ensure that P lies on segment E_1F_1 and Q lies on segment E_2F_2, which may be helpful for contestants. The argument presented above is valid in all configurations. When one of $\angle B$ and $\angle C$ is a right angle, some of the points E_1, F_1, E_2, F_2 lie at infinity; when one of them is obtuse, both P and Q lie outside segments E_1F_1 and E_2F_2 respectively.

¶ Proof of (ii) by complex numbers. We will give using complex numbers on $\triangle ABC$ a proof that $|E_1P| = |E_2Q|$.

We place $APBCQ$ on the unit circle. Since $\overline{PQ} \parallel \overline{BC}$, we have $pq = bc$. Also, the midpoint of $\overline{AB}$ lies on $\overline{PQ}$, so

$$\begin{aligned} p + q &= \frac{a+b}{2} + \overline{\left(\frac{a+b}{2}\right)} \cdot pq \\ &= \frac{a+b}{2} + \frac{a+b}{2ab} \cdot bc \\ &= \frac{a(a+b)}{2a} + \frac{c(a+b)}{2a} \\ &= \frac{(a+b)(a+c)}{2a}. \end{aligned}$$

Now,

$$\begin{aligned} p - e_1 &= p - \frac{pp(a+c) - ac(p+p)}{pp - ac} \\ &= \frac{p(p^2 - p(a+c) + ac)}{pp - ac} = \frac{(p-a)(p-c)}{p^2 - ac}. \end{aligned}$$

$$|PE_1|^2 = (p-e_1)\cdot\overline{p-e_1} = \frac{(p-a)(p-c)}{p^2-ac}\cdot\frac{(\frac{1}{p}-\frac{1}{a})(\frac{1}{p}-\frac{1}{c})}{\frac{1}{p^2}-\frac{1}{ac}}$$
$$= -\frac{(p-a)^2(p-c)^2}{(p^2-ac)^2}.$$

Similarly,

$$|QE_2|^2 = -\frac{(q-a)^2(q-c)^2}{(q^2-ac)^2}.$$

But actually, we claim that

$$\frac{(p-a)(p-c)}{p^2-ac} = \frac{(q-a)(q-c)}{q^2-ac}.$$

One calculates

$$(p-a)(p-c)(q^2-ac) = p^2q^2 - pq^2a - pq^2c + q^2ac - p^2ac + pa^2c + pac^2 - (ac)^2$$

Thus $(p-a)(p-c)(q^2-ac) - (q-a)(q-c)(p^2-ac)$ is equal to

$$\begin{aligned}
&-(a+c)(pq)(q-p) + (q^2-p^2)ac - (p^2-q^2)ac + ac(a+c)(p-q) \\
&\qquad = (p-q)\left[(a+c)pq - 2(p+q)ac + ac(a+c)\right] \\
&\qquad = (p-q)\left[(a+c)bc - 2\cdot\frac{(a+b)(a+c)}{2a}\cdot ac + ac(a+c)\right] \\
&\qquad = (p-q)(a+c)\left[bc - c(a+b) + ac\right] = 0.
\end{aligned}$$

This proves $|E_1P| = |E_2Q|$. Together with the similar $|F_1P| = |F_2Q|$, we have proved (ii).

¶ Authorship comments. Ankan provides an extensive dialogue at https://aops.com/community/c6h1664170p10571644 of how he came up with this problem, which at first was intended just to be an AMC-level question about an equilateral triangle. Here, we provide just the change-log of the versions of this problem.

0. (*Original version*) Let ABC be an equilateral triangle with side 2 inscribed in circle ω, and let P be a point on small arc AB of its circumcircle. The tangent line to ω at P intersects lines AC and AB at E and F. If $PE = PF$, find EF. (Answer: 4.)

1. (*Generalize to isosceles triangle*) Let ABC be an isosceles triangle with $AB = AC$, and let M be the midpoint of $\overline{BC}$. Let P be a point on the circumcircle with $PA = PM$. The tangent to the circumcircle at P intersects lines AC and AB at E and F, respectively. Show that $PE = PF$.

2. (*Block coordinate bashes*) Let ABC be an isosceles triangle with $AB = AC$ and circumcircle ω, and let M be the midpoint of $\overline{BC}$. Let P be a point on ω with $PA = PM$. The tangent to ω at P intersects lines AC and AB at E and F, respectively. Show that the circumcircle of $\triangle AEF$ passes through the center of ω.

3. (*Delete isosceles condition*) Let ABC be a triangle with circumcircle ω, and let H be the foot of the altitude from A to $\overline{BC}$. Let P be a point on ω with $PA = PH$. The tangent to ω at P intersects lines AC and AB at E and F, respectively. Show that the circumcircle of $\triangle AEF$ passes through the center of ω.

4. (*Add in both tangents*) Let ABC be an acute triangle with circumcircle ω, and let H be the foot of the altitude from A to $\overline{BC}$. Let P and Q be the points on ω with $PA = PH$ and $QA = QH$. The tangent to ω at P intersects lines AC and AB at E_1 and F_1 respectively; the tangent to ω at Q intersects lines AC and AB at E_2 and F_2 respectively. Show that $E_1F_1 = E_2F_2$.

5. (*Merge v3 and v4*) Let ABC be an acute triangle with circumcircle ω, and let H be the foot of the altitude from A to $\overline{BC}$. Let P and Q be the points on ω with $PA = PH$ and $QA = QH$. The tangent to ω at P intersects lines AC and AB at E_1 and F_1 respectively; the tangent to ω at Q intersects lines AC and AB at E_2 and F_2 respectively. Show that the circumcircles of $\triangle AE_1F_1$ and $\triangle AE_2F_2$ are congruent, and the line through their centers is parallel to the tangent to ω at A.

The problem bears Evan's name only because he suggested the changes v2 and v5.

§2.3 TSTST 2018/6, proposed by Ray Li

🔗 *Available online at* https://aops.com/community/p10570994.

Problem statement

Let $S = \{1, \dots, 100\}$, and for every positive integer n define

$$T_n = \{(a_1, \dots, a_n) \in S^n \mid a_1 + \cdots + a_n \equiv 0 \pmod{100}\}.$$

Determine which n have the following property: if we color any 75 elements of S red, then at least half of the n-tuples in T_n have an even number of coordinates with red elements.

We claim this holds exactly for n even.

¶ First solution by generating functions. Define

$$R(x) = \sum_{s \text{ red}} x^s, \qquad B(x) = \sum_{s \text{ blue}} x^s.$$

(Here "blue" means "not-red", as always.) Then, the number of tuples in T_n with exactly k red coordinates is exactly equal to

$$\binom{n}{k} \cdot \frac{1}{100} \sum_{\omega} R(\omega)^k B(\omega)^{n-k}$$

where the sum is over all 100th roots of unity. So, we conclude the number of tuples in T_n with an even (resp odd) number of red elements is exactly

$$\begin{aligned}
X &= \frac{1}{100} \sum_{\omega} \sum_{k \text{ even}} \binom{n}{k} R(\omega)^k B(\omega)^{n-k} \\
Y &= \frac{1}{100} \sum_{\omega} \sum_{k \text{ odd}} \binom{n}{k} R(\omega)^k B(\omega)^{n-k} \\
\implies X - Y &= \frac{1}{100} \sum_{\omega} (B(\omega) - R(\omega))^n \\
&= \frac{1}{100} \left[(B(1) - R(1))^n + \sum_{\omega \neq 1} (2B(\omega))^n \right] \\
&= \frac{1}{100} \left[(B(1) - R(1))^n - (2B(1))^n + 2^n \sum_{\omega} B(\omega)^n \right] \\
&= \frac{1}{100} \left[(B(1) - R(1))^n - (2B(1))^n \right] + 2^n Z \\
&= \frac{1}{100} \left[(-50)^n - 50^n \right] + 2^n Z.
\end{aligned}$$

where

$$Z := \frac{1}{100} \sum_{\omega} B(\omega)^n \geq 0$$

counts the number of tuples in T_n which are all blue. Here we have used the fact that $B(\omega) + R(\omega) = 0$ for $\omega \neq 1$.

We wish to show $X - Y \geq 0$ holds for n even, but may fail when n is odd. This follows from two remarks:

- If n is even, then $X - Y = 2^n Z \geq 0$.
- If n is odd, then if we choose the coloring for which s is red if and only if $s \not\equiv 2 \pmod 4$; we thus get $Z = 0$. Then $X - Y = -\frac{2}{100} \cdot 50^n < 0$.

¶ Second solution by strengthened induction and random coloring. We again prove that n even work. Let us define

$$T_n(a) = \{(a_1, \dots, a_n) \in S^n \mid a_1 + \dots + a_n \equiv a \pmod{100}\}.$$

Also, call an n-tuple good if it has an even number of red elements. We claim that $T_n(a)$ also has at least 50% good tuples, by induction.

This follows by induction on $n \geq 2$. Indeed, the base case $n = 2$ can be checked by hand, since $T_2(a) = \{(x, a-x) \mid x \in S\}$. With the stronger claim, one can check the case $n = 2$ manually and proceed by induction to go from $n-2$ to n, noting that

$$T_n(a) = \bigsqcup_{b+c=a} T_{n-2}(b) \oplus T_2(c)$$

where $\oplus$ denotes concatenation of tuples, applied set-wise. The concatenation of an $(n-2)$-tuple and 2-tuple is good if and only if both or neither are good. Thus for each b and c, if the proportion of $T_{n-2}(b)$ which is good is $p \geq \frac{1}{2}$ and the proportion of $T_2(c)$ which is good is $q \geq \frac{1}{2}$, then the proportion of $T_{n-2}(b) \oplus T_2(c)$ which is good is $pq + (1-p)(1-q) \geq \frac{1}{2}$, as desired. Since each term in the union has at least half the tuples good, all of $T_n(a)$ has at least half the tuples good, as desired.

It remains to fail all odd n. We proceed by a suggestion of Yang Liu and Ankan Bhattacharya by showing that if we pick the 75 elements *randomly*, then any particular tuple in S^n has strictly less than 50% chance of being good. This will imply (by linearity of expectation) that T_n (or indeed any subset of S^n) will, for some coloring, have less than half good tuples.

Let $(a_1, \dots, a_n)$ be such an n-tuple. If any element appears in the tuple more than once, keep *discarding pairs* of that element until there are zero or one; this has no effect on the good-ness of the tuple. If we do this, we obtain an m-tuple $(b_1, \dots, b_m)$ with no duplicated elements where $m \equiv n \equiv 1 \pmod 2$. Now, the probability that any element is red is $\frac{3}{4}$, so the probability of being good is

$$\begin{aligned}\sum_{k \text{ even}}^{m} \binom{m}{k} \left(\frac{3}{4}\right)^k \left(-\frac{1}{4}\right)^{m-k} &= \frac{1}{2}\left[\left(\frac{3}{4}+\frac{1}{4}\right)^m - \left(\frac{3}{4}-\frac{1}{4}\right)^m\right] \\ &= \frac{1}{2}\left[1 - \left(\frac{1}{2}\right)^m\right] < \frac{1}{2}.\end{aligned}$$

> **Remark** (Adam Hesterberg)**.** Here is yet another proof that n even works. Group elements of T_n into equivalence classes according to the $n/2$ sums of pairs of consecutive elements (first and second, third and fourth, ...). For each such pair sum, there are at least as many monochrome pairs with that sum as nonmonochrome ones, since every nonmonochrome pair uses one of the 25 non-reds. The monochromaticity of the pairs is independent.
> If $p_i \leq \frac{1}{2}$ is the probability that the ith pair is nonmonochrome, then the probability that k pairs are nonmonochrome is the coefficient of x^k in $f(x) = \prod_i (xp_i + (1-p_i))$. Then the probability that evenly many pairs are nonmonochrome (and hence that evenly many coordinates are red) is the sum of the coefficients of even powers of x in f, which is $(f(1) + f(-1))/2 = (1 + \prod_i (1-2p_i))/2 \geq \frac{1}{2}$, as desired.

§3 Solutions to Day 3

§3.1 TSTST 2018/7, proposed by Ashwin Sah

🔗 *Available online at* https://aops.com/community/p10570996.

Problem statement

Let n be a positive integer. A frog starts on the number line at 0. Suppose it makes a finite sequence of hops, subject to two conditions:

- The frog visits only points in $\{1, 2, \dots, 2^n - 1\}$, each at most once.
- The length of each hop is in $\{2^0, 2^1, 2^2, \dots\}$. (The hops may be either direction, left or right.)

Let S be the sum of the (positive) lengths of all hops in the sequence. What is the maximum possible value of S?

We claim the answer is $\frac{4^n-1}{3}$.

We first prove the bound. First notice that the hop sizes are in $\{2^0, 2^1, \dots, 2^{n-1}\}$, since the frog must stay within bounds the whole time. Let a_i be the number of hops of size 2^i the frog makes, for $0 \le i \le n-1$.

Claim — For any $k = 1, \dots, n$ we have

$$a_{n-1} + \cdots + a_{n-k} \le 2^n - 2^{n-k}.$$

Proof. Let $m = n - k$ and look modulo 2^m. Call a jump *small* if its length is at most 2^{m-1}, and *large* if it is at least 2^m; the former changes the residue class of the frog modulo 2^m while the latter does not.

Within each fixed residue modulo 2^m, the frog can make at most $\frac{2^n}{2^m} - 1$ large jumps. So the total number of large jumps is at most $2^m \left(\frac{2^n}{2^m} - 1\right) = 2^n - 2^m$. □

(As an example, when $n = 3$ this means there are at most four hops of length 4, at most six hops of length 2 or 4, and at most seven hops total. Of course, if we want to max the length of the hops, we see that we want $a_2 = 4$, $a_1 = 2$, $a_0 = 1$, and in general equality is achieved when $a_m = 2^m$ for any m.)

Now, the total distance the frog travels is

$$S = a_0 + 2a_1 + 4a_2 + \cdots + 2^{n-1}a_{n-1}.$$

We rewrite using the so-called "summation by parts":

$$\begin{aligned}
S = a_0 + a_1 + \ &a_2 + \ a_3 + \ldots + \ a_{n-1} \\
+ \quad a_1 + \ &a_2 + \ a_3 + \ldots + \ a_{n-1} \\
+ \quad 2a_2 + &2a_3 + \ldots + 2a_{n-1} \\
+ \quad 4a_3 + &\ldots + 4a_{n-1} \\
\vdots \quad &\ddots \quad \vdots \\
+ \quad &2^{n-2}a_{n-1}.
\end{aligned}$$

Hence

$$\begin{aligned} S &\le (2^n - 2^0) + (2^n - 2^1) + 2(2^n - 2^2) + \cdots + 2^{n-2}(2^n - 2^{n-1}) \\ &= \frac{4^n - 1}{3}. \end{aligned}$$

It remains to show that equality can hold. There are many such constructions but most are inductive. Here is one approach. We will construct two family of paths such that there are 2^k hops of size 2^k, for every $0 \le k \le n-1$, and we visit each of $\{0, \dots, 2^n - 1\}$ once, starting on 0 and ending on x, for the two values $x \in \{1, 2^n - 1\}$.

The base case $n = 1$ is clear. To take a path from 0 to $2^{n+1} - 1$.

- Take a path on $\{0, 2, 4, \dots, 2^{n+1} - 2\}$ starting from 0 and ending on 2 (by inductive hypothesis).
- Take a path on $\{1, 3, 5, \dots, 2^{n+1} - 1\}$ starting from 1 and ending on $2^{n+1} - 1$ (by inductive hypothesis).
- Link them together by adding a single jump $2 \to 1$.

The other case is similar, but we route $0 \to (2^{n+1} - 2) \to (2^{n+1} - 1) \to 1$ instead. (This can also be visualized as hopping along a hypercube of binary strings; each inductive step takes two copies of the hypercube and links them together by a single edge.)

Remark (Ashwin Sah)**.** The problem can also be altered to ask for the minimum value of the sum of the reciprocals of the hop sizes, where further we stipulate that the frog must hit every point precisely once (to avoid triviality). With a nearly identical proof that also exploits the added condition $a_0 + \cdots + a_{n-1} = 2^n - 1$, the answer is n. This yields a nicer form for the generalization. The natural generalization changes the above problem by replacing 2^k with a_k where $a_k \mid a_{k+1}$, so that the interval covered by hops is of size a_n and the hop sizes are restricted to the a_i, where $a_0 = 1$. In this case, similar bounding yields

$$\sum_{i=1}^{2^n - 1} \frac{1}{b_k} \ge \sum_{i=0}^{n-1} \left(\frac{a_{k+1}}{a_k} - 1 \right).$$

Bounds for the total distance traveled happen in the same way as the solution above, and equality for both can be constructed in an analogous fashion.

§3.2 TSTST 2018/8, proposed by Ankan Bhattacharya, Evan Chen

🔗 *Available online at* https://aops.com/community/p10570998.

Problem statement

For which positive integers $b > 2$ do there exist infinitely many positive integers n such that n^2 divides $b^n + 1$?

This problem is sort of the union of IMO 1990/3 and IMO 2000/5.

The answer is any b such that $b+1$ is not a power of 2. In the forwards direction, we first prove more carefully the following claim.

Claim — If $b+1$ is a power of 2, then the only n which is valid is $n = 1$.

Proof. Assume $n > 1$ and let p be the smallest prime dividing n. We cannot have $p = 2$, since then $4 \mid b^n + 1 \equiv 2 \pmod 4$. Thus,

$$b^{2n} \equiv 1 \pmod p$$

so the order of $b \pmod p$ divides $\gcd(2n, p-1) = 2$. Hence $p \mid b^2 - 1 = (b-1)(b+1)$.

But since $b+1$ was a power of 2, this forces $p \mid b-1$. Then $0 \equiv b^n + 1 \equiv 2 \pmod p$, contradiction. □

On the other hand, suppose that $b+1$ is not a power of 2 (and that $b > 2$). We will inductively construct an infinite sequence of distinct primes p_0, p_1, ..., such that the following two properties hold for each $k \geq 0$:

- $p_0^2 \dots p_{k-1}^2 p_k \mid b^{p_0 \dots p_{k-1}} + 1$,
- and hence $p_0^2 \dots p_{k-1}^2 p_k^2 \mid b^{p_0 \dots p_{k-1} p_k} + 1$ by exponent lifting lemma.

This will solve the problem.

Initially, let p_0 be any odd prime dividing $b+1$. For the inductive step, we contend there exists an *odd* prime $q \notin \{p_0, \dots, p_k\}$ such that $q \mid b^{p_0 \dots p_k} + 1$. Indeed, this follows immediately by Zsigmondy theorem since $p_0 \dots p_k$ divides $b^{p_0 \dots p_{k-1}} + 1$. Since $(b^{p_0 \dots p_k})^q \equiv b^{p_0 \dots p_k} \pmod q$, it follows we can then take $p_{k+1} = q$. This finishes the induction.

To avoid the use of Zsigmondy, one can instead argue as follows: let $p = p_k$ for brevity, and let $c = b^{p_0 \dots p_{k-1}}$. Then $\frac{c^p+1}{c+1} = c^{p-1} - c^{p-2} + \dots + 1$ has GCD exactly p with $c+1$. Moreover, this quotient is always odd. Thus as long as $c^p + 1 > p \cdot (c+1)$, there will be some new prime dividing $c^p + 1$ but not $c+1$. This is true unless $p = 3$ and $c = 2$, but we assumed $b > 2$ so this case does not appear.

Remark (On new primes)**.** In going from $n^2 \mid b^n + 1$ to $(nq)^2 \mid b^{nq} + 1$, one does not necessarily need to pick a q such that $q \nmid n$, as long as $\nu_q(n^2) < \nu_q(b^n + 1)$. In other words it suffices to just check that $\frac{b^n+1}{n^2}$ is not a power of 2 in this process.
However, this calculation is a little more involved with this approach. One proceeds by noting that n is odd, hence $\nu_2(b^n + 1) = \nu_2(b+1)$, and thus $\frac{b^n+1}{n^2} = 2^{\nu_2(b+1)} \leq b+1$, which is a little harder to bound than the analogous $c^p + 1 > p \cdot (c+1)$ from the previous solution.

¶ Authorship comments. I came up with this problem by simply mixing together the main ideas of IMO 1990/3 and IMO 2000/5, late one night after a class. On the other hand, I do not consider it very original; it is an extremely "routine" number theory problem for experienced contestants, using highly standard methods. Thus it may not be that interesting, but is a good discriminator of understanding of fundamentals.

IMO 1990/3 shows that if $b = 2$, then the only n which work are $n = 1$ and $n = 3$. Thus $b = 2$ is a special case and for this reason the problem explicitly requires $b > 2$.

An alternate formulation of the problem is worth mentioning. Originally, the problem statement asked whether there existed n with at least 3 (or 2018, etc.) prime divisors, thus preventing the approach in which one takes a prime q dividing $\frac{b^n+1}{n^2}$. Ankan Bhattacharya suggested changing it to "infinitely many n", which is more natural.

These formulations are actually not so different though. Explicitly, suppose $k^2 \mid b^k + 1$ and $p \mid b^k + 1$. Consider any $k \mid n$ with $n^2 \mid b^n + 1$, and let p be an odd prime dividing $b^k + 1$. Then $2\nu_p(n) \le \nu_p(b^n + 1) = \nu_p(n/k) + \nu_p(b^k + 1)$ and thus

$$\nu_p(n/k) \le \nu_p\left(\frac{b^k + 1}{k^2}\right).$$

Effectively, this means we can only add each prime a certain number of times.

§3.3 TSTST 2018/9, proposed by Linus Hamilton

🔗 *Available online at* https://aops.com/community/p10571003.

Problem statement

Show that there is an absolute constant $c < 1$ with the following property: whenever $\mathcal{P}$ is a polygon with area 1 in the plane, one can translate it by a distance of $\frac{1}{100}$ in some direction to obtain a polygon $\mathcal{Q}$, for which the intersection of the interiors of $\mathcal{P}$ and $\mathcal{Q}$ has total area at most c.

The following solution is due to Brian Lawrence. We will prove the result with the generality of any measurable set $\mathcal{P}$ (rather than a polygon). For a vector v in the plane, write $\mathcal{P} + v$ for the translate of $\mathcal{P}$ by v.

Suppose $\mathcal{P}$ is a polygon of area 1, and $\varepsilon > 0$ is a constant, such that for any translate $\mathcal{Q} = \mathcal{P} + v$, where v has length exactly $\frac{1}{100}$, the intersection of $\mathcal{P}$ and $\mathcal{Q}$ has area at least $1 - \varepsilon$. The problem asks us to prove a lower bound on ε.

Lemma

Fix a sequence of n vectors $v_1, v_2, \ldots, v_n$, each of length $\frac{1}{100}$. A grasshopper starts at a random point x of $\mathcal{P}$, and makes n jumps to $x + v_1 + \cdots + v_n$. Then it remains in $\mathcal{P}$ with probability at least $1 - n\varepsilon$.

Proof. In order for the grasshopper to leave $\mathcal{P}$ at step i, the grasshopper's position before step i must be inside the difference set $\mathcal{P} \backslash (\mathcal{P} - v_i)$. Since this difference set has area at most ε, the probability the grasshopper leaves $\mathcal{P}$ at step i is at most ε. Summing over the n steps, the probability that the grasshopper ever manages to leave $\mathcal{P}$ is at most $n\varepsilon$. □

Corollary

Fix a vector w of length at most 8. A grasshopper starts at a random point x of $\mathcal{P}$, and jumps to $x + w$. Then it remains in $\mathcal{P}$ with probability at least $1 - 800\varepsilon$.

Proof. Apply the previous lemma with 800 jumps. Any vector w of length at most 8 can be written as $w = v_1 + v_2 + \cdots + v_{800}$, where each v_i has length exactly $\frac{1}{100}$. □

Now consider the process where we select a random starting point $x \in \mathcal{P}$ for our grasshopper, *and* a random vector w of length at most 8 (sampled uniformly from the closed disk of radius 8). Let q denote the probability of staying inside $\mathcal{P}$ we will bound q from above and below.

- On the one hand, suppose we pick w first. By the previous corollary, $q \geq 1 - 800\varepsilon$ (irrespective of the chosen w).
- On the other hand, suppose we pick x first. Then the possible landing points $x + w$ are uniformly distributed over a closed disk of radius 8, which has area 64π. The probability of landing in $\mathcal{P}$ is certainly at most $\frac{[\mathcal{P}]}{64\pi}$.

Consequently, we deduce

$$1 - 800\varepsilon \leq q \leq \frac{[\mathcal{P}]}{64\pi} \implies \varepsilon > \frac{1 - \frac{[\mathcal{P}]}{64\pi}}{800} > 0.001$$

as desired.

Remark. The choice of 800 jumps is only for concreteness; any constant n for which $\pi(n/100)^2 > 1$ works. I think $n = 98$ gives the best bound following this approach.