Solutions to the 80th William Lowell Putnam Mathematical Competition
Saturday, December 7, 2019

Kiran Kedlaya and Lenny Ng

A1 The answer is all nonnegative integers not congruent to 3 or 6 (mod 9). Let X denote the given expression; we first show that we can make X equal to each of the claimed values. Write $B=A+b$ and $C=A+c$, so that

$$X=(b^2-bc+c^2)(3A+b+c).$$

By taking $(b,c)=(0,1)$ or $(b,c)=(1,1)$, we obtain respectively $X=3A+1$ and $X=3A+2$; consequently, as A varies, we achieve every nonnegative integer not divisible by 3. By taking $(b,c)=(1,2)$, we obtain $X=9A+9$; consequently, as A varies, we achieve every positive integer divisible by 9. We may also achieve $X=0$ by taking $(b,c)=(0,0)$.

In the other direction, X is always nonnegative: either apply the arithmetic mean-geometric mean inequality, or write $b^2-bc+c^2=(b-c/2)^2+3c^2/4$ to see that it is nonnegative. It thus only remains to show that if X is a multiple of 3, then it is a multiple of 9. Note that $3A+b+c\equiv b+c \pmod 3$ and $b^2-bc+c^2\equiv(b+c)^2 \pmod 3$; consequently, if X is divisible by 3, then $b+c$ must be divisible by 3, so each factor in $X=(b^2-bc+c^2)(3A+b+c)$ is divisible by 3. This proves the claim.

Remark. The factorization of X used above can be written more symmetrically as

$$X=(A+B+C)(A^2+B^2+C^2-AB-BC-CA).$$

One interpretation of the factorization is that X is the determinant of the circulant matrix

$$\begin{pmatrix} A & B & C \\ C & A & B \\ B & C & A \end{pmatrix}$$

which has the vector $(1,1,1)$ as an eigenvector (on either side) with eigenvalue $A+B+C$. The other eigenvalues are $A+\zeta B+\zeta^2 C$ where ζ is a primitive cube root of unity; in fact, X is the norm form for the ring $\mathbb{Z}[T]/(T^3-1)$, from which it follows directly that the image of X is closed under multiplication. (This is similar to the fact that the image of A^2+B^2, which is the norm form for the ring $\mathbb{Z}[i]$ of Gaussian integers, is closed under multiplication.)

One can also the unique factorization property of the ring $\mathbb{Z}[\zeta]$ of Eisenstein integers as follows. The three factors of X over $\mathbb{Z}[\zeta_3]$ are pairwise congruent modulo $1-\zeta_3$; consequently, if X is divisible by 3, then it is divisible by $(1-\zeta_3)^3=-3\zeta_3(1-\zeta_3)$ and hence (because it is a rational integer) by 3^2.

A2 **Solution 1.** Let M and D denote the midpoint of AB and the foot of the altitude from C to AB, respectively, and let r be the inradius of $\triangle ABC$. Since C,G,M are collinear with $CM=3GM$, the distance from C to line AB is 3 times the distance from G to AB, and the latter is r since $IG\parallel AB$; hence the altitude CD has length $3r$. By the double angle formula for tangent, $\frac{CD}{DB}=\tan\beta=\frac{3}{4}$, and so $DB=4r$. Let E be the point where the incircle meets AB; then $EB=r/\tan(\frac{\beta}{2})=3r$. It follows that $ED=r$, whence the incircle is tangent to the altitude CD. This implies that $D=A$, ABC is a right triangle, and $\alpha=\frac{\pi}{2}$.

Remark. One can obtain a similar solution by fixing a coordinate system with B at the origin and A on the positive x-axis. Since $\tan\frac{\beta}{2}=\frac{1}{3}$, we may assume without loss of generality that $I=(3,1)$. Then C lies on the intersection of the line $y=3$ (because $CD=3r$ as above) with the line $y=\frac{3}{4}x$ (because $\tan\beta=\frac{3}{4}$ as above), forcing $C=(4,3)$ and so forth.

Solution 2. Let a,b,c be the lengths of BC,CA,AB, respectively. Let r, s, and K denote the inradius, semiperimeter, and area of $\triangle ABC$. By Heron's Formula,

$$r^2s^2=K^2=s(s-a)(s-b)(s-c).$$

If IG is parallel to AB, then

$$\frac{1}{2}rc=\text{area}(\triangle ABI)=\text{area}(\triangle ABG)=\frac{1}{3}K=\frac{1}{3}rs$$

and so $c=\frac{a+b}{2}$. Since $s=\frac{3(a+b)}{4}$ and $s-c=\frac{a+b}{4}$, we have $3r^2=(s-a)(s-b)$. Let E be the point at which the incircle meets AB; then $s-b=EB=r/\tan(\frac{\beta}{2})$ and $s-a=EA=r/\tan(\frac{\alpha}{2})$. It follows that $\tan(\frac{\alpha}{2})\tan(\frac{\beta}{2})=\frac{1}{3}$ and so $\tan(\frac{\alpha}{2})=1$. This implies that $\alpha=\frac{\pi}{2}$.

Remark. The equality $c=\frac{a+b}{2}$ can also be derived from the vector representations

$$G=\frac{A+B+C}{3},\qquad I=\frac{aA+bB+cC}{a+b+c}.$$

Solution 3. (by Catalin Zara) It is straightforward to check that a right triangle with $AC=3, AB=4, BC=5$ works. For example, in a coordinate system with $A=(0,0), B=(4,0), C=(0,3)$, we have

$$G=\left(\frac{4}{3},1\right),\qquad I=(1,1)$$

and for $D=(1,0)$,

$$\tan\frac{\beta}{2}=\frac{ID}{BD}=\frac{1}{3}.$$

It thus suffices to suggest that this example is unique up to similarity.

Let C' be the foot of the angle bisector at C. Then

$$\frac{CI}{IC'} = \frac{CA+CB}{AB}$$

and so IG is parallel to AB if and only if $CA+CB = 2AB$. We may assume without loss of generality that A and B are fixed, in which case this condition restricts C to an ellipse with foci at A and B. Since the angle β is also fixed, up to symmetry C is further restricted to a half-line starting at B; this intersects the ellipse in a unique point.

Remark. Given that $CA+CB = 2AB$, one can also recover the ratio of side lengths using the law of cosines.

A3 The answer is $M = 2019^{-1/2019}$. For any choices of $b_0,\dots,b_{2019}$ as specified, AM-GM gives

$$\mu \geq |z_1 \cdots z_{2019}|^{1/2019} = |b_0/b_{2019}|^{1/2019} \geq 2019^{-1/2019}.$$

To see that this is best possible, consider $b_0,\dots,b_{2019}$ given by $b_k = 2019^{k/2019}$ for all k. Then

$$P(z/2019^{1/2019}) = \sum_{k=0}^{2019} z^k = \frac{z^{2020}-1}{z-1}$$

has all of its roots on the unit circle. It follows that all of the roots of $P(z)$ have modulus $2019^{-1/2019}$, and so $\mu = 2019^{-1/2019}$ in this case.

A4 The answer is no. Let $g : \mathbb{R} \to \mathbb{R}$ be any continuous function with $g(t+2) = g(t)$ for all t and $\int_0^2 g(t)\,dt = 0$ (for instance, $g(t) = \sin(\pi t)$). Define $f(x,y,z) = g(z)$. We claim that for any sphere S of radius 1, $\iint_S f\,dS = 0$.

Indeed, let S be the unit sphere centered at (x_0,y_0,z_0). We can parametrize S by $S(\phi,\theta) = (x_0,y_0,z_0) + (\sin\phi\cos\theta, \sin\phi\sin\theta, \cos\phi)$ for $\phi \in [0,\pi]$ and $\theta \in [0,2\pi]$. Then we have

$$\begin{aligned}\iint_S f(x,y,z)\,dS &= \int_0^\pi \int_0^{2\pi} f(S(\phi,\theta)) \left\| \frac{\partial S}{\partial \phi} \times \frac{\partial S}{\partial \theta} \right\| d\theta\,d\phi \\ &= \int_0^\pi \int_0^{2\pi} g(z_0+\cos\phi)\sin\phi\,d\theta\,d\phi \\ &= 2\pi \int_{-1}^1 g(z_0+t)\,dt,\end{aligned}$$

where we have used the substitution $t = \cos\phi$; but this last integral is 0 for any z_0 by construction.

Remark. The solution recovers the famous observation of Archimedes that the surface area of a spherical cap is linear in the height of the cap. In place of spherical coordinates, one may also compute $\iint_S f(x,y,z)\,dS$ by computing the integral over a ball of radius r, then computing the derivative with respect to r and evaluating at $r = 1$.

Noam Elkies points out that a similar result holds in $\mathbb{R}^n$ for any n. Also, there exist nonzero continuous functions on $\mathbb{R}^n$ whose integral over any unit ball vanishes; this implies certain negative results about image reconstruction.

A5 The answer is $\frac{p-1}{2}$. Define the operator $D = x\frac{d}{dx}$, where $\frac{d}{dx}$ indicates formal differentiation of polynomials. For n as in the problem statement, we have $q(x) = (x-1)^n r(x)$ for some polynomial $r(x)$ in $\mathbb{F}_p$ not divisible by $x-1$. For $m = 0,\dots,n$, by the product rule we have

$$(D^m q)(x) \equiv n^m x^m (x-1)^{n-m} r(x) \pmod{(x-1)^{n-m+1}}.$$

Since $r(1) \neq 0$ and $n \not\equiv 0 \pmod{p}$ (because $n \leq \deg(q) = p-1$), we may identify n as the smallest nonnegative integer for which $(D^n q)(1) \neq 0$.

Now note that $q = D^{(p-1)/2} s$ for

$$s(x) = 1 + x + \cdots + x^{p-1} = \frac{x^p-1}{x-1} = (x-1)^{p-1}$$

since $(x-1)^p = x^p - 1$ in $\mathbb{F}_p[x]$. By the same logic as above, $(D^n s)(1) = 0$ for $n = 0,\dots,p-2$ but not for $n = p-1$. This implies the claimed result.

Remark. One may also finish by checking directly that for any positive integer m,

$$\sum_{k=1}^{p-1} k^m \equiv \begin{cases} -1 \pmod{p} & \text{if } (p-1)|m \\ 0 \pmod{p} & \text{otherwise.}\end{cases}$$

If $(p-1)|m$, then $k^m \equiv 1 \pmod{p}$ by the little Fermat theorem, and so the sum is congruent to $p-1 \equiv -1 \pmod{p}$. Otherwise, for any primitive root ℓ mod p, multiplying the sum by ℓ^m permutes the terms modulo p and hence does not change the sum modulo p; since $\ell^n \not\equiv 1 \pmod{p}$, this is only possible if the sum is zero modulo p.

A6 **Solution 1.** (by Harm Derksen) We assume that $\limsup_{x\to 0^+} x^r |g''(x)| < \infty$ and deduce that $\lim_{x\to 0^+} g'(x) = 0$. Note that

$$\limsup_{x\to 0^+} x^r \sup\{|g''(\xi)| : \xi \in [x/2,x]\} < \infty.$$

Suppose for the moment that there exists a function h on $(0,1)$ which is positive, nondecreasing, and satisfies

$$\lim_{x\to 0^+} \frac{g(x)}{h(x)} = \lim_{x\to 0^+} \frac{h(x)}{x^r} = 0.$$

For some $c > 0$, $h(x) < x^r < x$ for $x \in (0,c)$. By Taylor's theorem with remainder, we can find a function ξ on $(0,c)$ such that $\xi(x) \in [x-h(x),x]$ and

$$g(x-h(x)) = g(x) - g'(x)h(x) + \frac{1}{2}g''(\xi(x))h(x)^2.$$

We can thus express $g'(x)$ as

$$\frac{g(x)}{h(x)} + \frac{1}{2}x^r g''(\xi(x))\frac{h(x)}{x^r} - \frac{g(x-h(x))}{h(x-h(x))}\frac{h(x-h(x))}{h(x)}.$$

As $x \to 0^+$, $g(x)/h(x)$, $g(x-h(x))/h(x-h(x))$, and $h(x)/x^r$ tend to 0, while $x^r g''(\xi(x))$ remains bounded (because $\xi(x) \geq x - h(x) \geq x - x^r \geq x/2$ for x small) and $h(x-h(x))/h(x)$ is bounded in $(0,1]$. Hence $\lim_{x\to 0^+} g'(x) = 0$ as desired.

It thus only remains to produce a function h with the desired properties; this amounts to "inserting" a function between $g(x)$ and x^r while taking care to ensure the positive and nondecreasing properties. One of many options is $h(x) = x^r\sqrt{f(x)}$ where

$$f(x) = \sup\{|z^{-r}g(z)| : z \in (0,x)\},$$

so that

$$\frac{h(x)}{x^r} = \sqrt{f(x)}, \qquad \frac{g(x)}{h(x)} = \sqrt{f(x)}x^{-r}g(x).$$

Solution 2. We argue by contradiction. Assume that $\limsup_{x\to 0^+} x^r|g''(x)| < \infty$, so that there is an M such that $|g''(x)| < Mx^{-r}$ for all x; and that $\lim_{x\to 0^+} g'(x) \neq 0$, so that there is an $\varepsilon_0 > 0$ and a sequence $x_n \to 0$ with $|g'(x_n)| > \varepsilon_0$ for all n.

Now let $\varepsilon > 0$ be arbitrary. Since $\lim_{x\to 0^+} g(x)x^{-r} = 0$, there is a $\delta > 0$ for which $|g(x)| < \varepsilon x^r$ for all $x < \delta$. Choose n sufficiently large that $\frac{\varepsilon_0 x_n^r}{2M} < x_n$ and $x_n < \delta/2$; then $x_n + \frac{\varepsilon_0 x_n^r}{2M} < 2x_n < \delta$. In addition, we have $|g'(x)| > \varepsilon_0/2$ for all $x \in [x_n, x_n + \frac{\varepsilon_0 x_n^r}{2M}]$ since $|g'(x_n)| > \varepsilon_0$ and $|g''(x)| < Mx^{-r} \leq Mx_n^{-r}$ in this range. It follows that

$$\begin{aligned}
\frac{\varepsilon_0^2}{2}\frac{x_n^r}{2M} &< |g(x_n + \frac{\varepsilon_0 x_n^r}{2M}) - g(x_n)| \\
&\leq |g(x_n + \frac{\varepsilon_0 x_n^r}{2M})| + |g(x_n)| \\
&< \varepsilon\left((x_n + \frac{\varepsilon_0 x_n^r}{2M})^r + x_n^r\right) \\
&< \varepsilon(1+2^r)x_n^r,
\end{aligned}$$

whence $4M(1+2^r)\varepsilon > \varepsilon_0^2$. Since $\varepsilon > 0$ is arbitrary and M, r, ε_0 are fixed, this gives the desired contradiction.

Remark. Harm Derksen points out that the "or" in the problem need not be exclusive. For example, take

$$g(x) = \begin{cases} x^5\sin(x^{-3}) & x \in (0,1] \\ 0 & x = 0. \end{cases}$$

Then for $x \in (0,1)$,

$$\begin{aligned}
g'(x) &= 5x^4\sin(x^{-3}) - 3x\cos(x^{-3}) \\
g''(x) &= (20x^3 - 9x^{-3})\sin(x^{-3}) - 18\cos(x^{-3}).
\end{aligned}$$

For $r = 2$, $\lim_{x\to 0^+} x^{-r}g(x) = \lim_{x\to 0^+} x^3\sin(x^{-3}) = 0$, $\lim_{x\to 0^+} g'(x) = 0$ and $x^r g''(x) = (20x^5 - 9x^{-1})\sin(x^{-3}) - 18x^2\cos(x^{-3})$ is unbounded as $x \to 0^+$. (Note that $g'(x)$ is not differentiable at $x = 0$.)

B1 The answer is $5n+1$.

We first determine the set P_n. Let Q_n be the set of points in $\mathbb{Z}^2$ of the form $(0, \pm 2^k)$ or $(\pm 2^k, 0)$ for some $k \leq n$. Let R_n be the set of points in $\mathbb{Z}^2$ of the form $(\pm 2^k, \pm 2^k)$ for some $k \leq n$ (the two signs being chosen independently). We prove by induction on n that

$$P_n = \{(0,0)\} \cup Q_{\lfloor n/2 \rfloor} \cup R_{\lfloor (n-1)/2 \rfloor}.$$

We take as base cases the straightforward computations

$$\begin{aligned}
P_0 &= \{(0,0), (\pm 1, 0), (0, \pm 1)\} \\
P_1 &= P_0 \cup \{(\pm 1, \pm 1)\}.
\end{aligned}$$

For $n \geq 2$, it is clear that $\{(0,0)\} \cup Q_{\lfloor n/2 \rfloor} \cup R_{\lfloor (n-1)/2 \rfloor} \subseteq P_n$, so it remains to prove the reverse inclusion. For $(x,y) \in P_n$, note that $x^2 + y^2 \equiv 0 \pmod 4$; since every perfect square is congruent to either 0 or 1 modulo 4, x and y must both be even. Consequently, $(x/2, y/2) \in P_{n-2}$, so we may appeal to the induction hypothesis to conclude.

We next identify all of the squares with vertices in P_n. In the following discussion, let (a,b) and (c,d) be two opposite vertices of a square, so that the other two vertices are

$$\left(\frac{a-b+c+d}{2}, \frac{a+b-c+d}{2}\right)$$

and

$$\left(\frac{a+b+c-d}{2}, \frac{-a+b+c+d}{2}\right).$$

- Suppose that $(a,b) = (0,0)$. Then (c,d) may be any element of P_n not contained in P_0. The number of such squares is $4n$.
- Suppose that $(a,b), (c,d) \in Q_k$ for some k. There is one such square with vertices

  $$\{(0, 2^k), (0, 2^{-k}), (2^k, 0), (2^{-k}, 0)\}$$

  for $k = 0, \dots, \lfloor \frac{n}{2} \rfloor$, for a total of $\lfloor \frac{n}{2} \rfloor + 1$. To show that there are no others, by symmetry it suffices to rule out the existence of a square with opposite vertices $(a,0)$ and $(c,0)$ where $a > |c|$. The other two vertices of this square would be $((a+c)/2, (a-c)/2)$ and $((a+c)/2, (-a+c)/2)$. These cannot belong to any Q_k, or be equal to $(0,0)$, because $|a+c|, |a-c| \geq a - |c| > 0$ by the triangle inequality. These also cannot belong to any R_k because $(a+|c|)/2 > (a-|c|)/2$. (One can also phrase this argument in geometric terms.)
- Suppose that $(a,b), (c,d) \in R_k$ for some k. There is one such square with vertices

  $$\{(2^k, 2^k), (2^k, -2^k), (-2^k, 2^k), (-2^k, -2^k)\}$$

  for $k = 0, \dots, \lfloor \frac{n-1}{2} \rfloor$, for a total of $\lfloor \frac{n+1}{2} \rfloor$. To show that there are no others, we may reduce to the previous case: rotating by an angle of $\frac{\pi}{4}$ and then rescaling by a factor of $\sqrt{2}$ would yield a square with two opposite vertices in some Q_k not centered at $(0,0)$, which we have already ruled out.

– It remains to show that we cannot have $(a,b) \in Q_k$ and $(c,d) \in R_k$ for some k. By symmetry, we may reduce to the case where $(a,b) = (0,2^k)$ and $(c,d) = (2^\ell, \pm 2^\ell)$. If $d > 0$, then the third vertex $(2^{k-1}, 2^{k-1}+2^\ell)$ is impossible. If $d < 0$, then the third vertex $(-2^{k-1}, 2^{k-1}-2^\ell)$ is impossible.

Summing up, we obtain

$$4n + \left\lfloor \frac{n}{2} \right\rfloor + 1 + \left\lfloor \frac{n+1}{2} \right\rfloor = 5n+1$$

squares, proving the claim.

Remark. Given the computation of P_n, we can alternatively show that the number of squares with vertices in P_n is $5n+1$ as follows. Since this is clearly true for $n=1$, it suffices to show that for $n \geq 2$, there are exactly 5 squares with vertices in P_n, at least one of which is not in P_{n-1}. Note that the convex hull of P_n is a square S whose four vertices are the four points in $P_n \setminus P_{n-1}$. If v is one of these points, then a square with a vertex at v can only lie in S if its two sides containing v are in line with the two sides of S containing v. It follows that there are exactly two squares with a vertex at v and all vertices in P_n: the square corresponding to S itself, and a square whose vertex diagonally opposite to v is the origin. Taking the union over the four points in $P_n \setminus P_{n-1}$ gives a total of 5 squares, as desired.

B2 The answer is $\frac{8}{\pi^3}$.

Solution 1. By the double angle and sum-product identities for cosine, we have

$$\begin{aligned} 2\cos^2\left(\frac{(k-1)\pi}{2n}\right) - 2\cos^2\left(\frac{k\pi}{2n}\right) &= \cos\left(\frac{(k-1)\pi}{n}\right) - \cos\left(\frac{k\pi}{n}\right) \\ &= 2\sin\left(\frac{(2k-1)\pi}{2n}\right)\sin\left(\frac{\pi}{2n}\right), \end{aligned}$$

and it follows that the summand in a_n can be written as

$$\frac{1}{\sin\left(\frac{\pi}{2n}\right)}\left(-\frac{1}{\cos^2\left(\frac{(k-1)\pi}{2n}\right)} + \frac{1}{\cos^2\left(\frac{k\pi}{2n}\right)}\right).$$

Thus the sum telescopes and we find that

$$a_n = \frac{1}{\sin\left(\frac{\pi}{2n}\right)}\left(-1 + \frac{1}{\cos^2\left(\frac{(n-1)\pi}{2n}\right)}\right) = -\frac{1}{\sin\left(\frac{\pi}{2n}\right)} + \frac{1}{\sin^3\left(\frac{\pi}{2n}\right)}.$$

Finally, since $\lim_{x\to 0} \frac{\sin x}{x} = 1$, we have $\lim_{n\to\infty}\left(n \sin\frac{\pi}{2n}\right) = \frac{\pi}{2}$, and thus $\lim_{n\to\infty}\frac{a_n}{n^3} = \frac{8}{\pi^3}$.

Solution 2. We first substitute $n-k$ for k to obtain

$$a_n = \sum_{k=1}^{n-1} \frac{\sin\left(\frac{(2k+1)\pi}{2n}\right)}{\sin^2\left(\frac{(k+1)\pi}{2n}\right)\sin^2\left(\frac{k\pi}{2n}\right)}.$$

We then use the estimate

$$\frac{\sin x}{x} = 1 + O(x^2) \qquad (x \in [0,\pi])$$

to rewrite the summand as

$$\frac{\left(\frac{(2k-1)\pi}{2n}\right)}{\left(\frac{(k+1)\pi}{2n}\right)^2\left(\frac{k\pi}{2n}\right)^2}\left(1 + O\left(\frac{k^2}{n^2}\right)\right)$$

which simplifies to

$$\frac{8(2k-1)n^3}{k^2(k+1)^2\pi^3} + O\left(\frac{n}{k}\right).$$

Consequently,

$$\begin{aligned} \frac{a_n}{n^3} &= \sum_{k=1}^{n-1}\left(\frac{8(2k-1)}{k^2(k+1)^2\pi^3} + O\left(\frac{1}{kn^2}\right)\right) \\ &= \frac{8}{\pi^3}\sum_{k=1}^{n-1}\frac{(2k-1)}{k^2(k+1)^2} + O\left(\frac{\log n}{n^2}\right). \end{aligned}$$

Finally, note that

$$\sum_{k=1}^{n-1}\frac{(2k-1)}{k^2(k+1)^2} = \sum_{k=1}^{n-1}\left(\frac{1}{k^2} - \frac{1}{(k+1)^2}\right) = 1 - \frac{1}{n^2}$$

converges to 1, and so $\lim_{n\to\infty}\frac{a_n}{n^3} = \frac{8}{\pi^3}$.

B3 **Solution 1.** We first note that P corresponds to the linear transformation on $\mathbb{R}^n$ given by reflection in the hyperplane perpendicular to u: $P(u) = -u$, and for any v with $\langle u, v\rangle = 0$, $P(v) = v$. In particular, P is an orthogonal matrix of determinant -1.

We next claim that if Q is an $n \times n$ orthogonal matrix that does not have 1 as an eigenvalue, then $\det Q = (-1)^n$. To see this, recall that the roots of the characteristic polynomial $p(t) = \det(tI - Q)$ all lie on the unit circle in $\mathbb{C}$, and all non-real roots occur in conjugate pairs ($p(t)$ has real coefficients, and orthogonality implies that $p(t) = \pm t^n p(t^{-1})$). The product of each conjugate pair of roots is 1; thus $\det Q = (-1)^k$ where k is the multiplicity of -1 as a root of $p(t)$. Since 1 is not a root and all other roots appear in conjugate pairs, k and n have the same parity, and so $\det Q = (-1)^n$.

Finally, if neither of the orthogonal matrices Q nor PQ has 1 as an eigenvalue, then $\det Q = \det(PQ) = (-1)^n$, contradicting the fact that $\det P = -1$. The result follows.

Remark. It can be shown that any $n \times n$ orthogonal matrix Q can be written as a product of at most n hyperplane reflections (Householder matrices). If equality occurs, then $\det(Q) = (-1)^n$; if equality does not occur, then Q has 1 as an eigenvalue. Consequently, equality fails for one of Q and PQ, and that matrix has 1 as an eigenvalue.

Sucharit Sarkar suggests the following topological interpretation: an orthogonal matrix without 1 as an eigenvalue induces a fixed-point-free map from the $(n-1)$-sphere to itself, and the degree of such a map must be $(-1)^n$.

Solution 2. This solution uses the (reverse) *Cayley transform*: if Q is an orthogonal matrix not having 1 as an eigenvalue, then

$$A = (I-Q)(I+Q)^{-1}$$

is a skew-symmetric matrix (that is, $A^T = -A$).

Suppose then that Q does not have 1 as an eigenvalue. Let V be the orthogonal complement of u in $\mathbb{R}^n$. On one hand, for $v \in V$,

$$(I-Q)^{-1}(I-QP)v = (I-Q)^{-1}(I-Q)v = v.$$

On the other hand,

$$(I-Q)^{-1}(I-QP)u = (I-Q)^{-1}(I+Q)u = Au$$

and $\langle u, Au\rangle = \langle A^T u, u\rangle = \langle -Au, u\rangle$, so $Au \in V$. Put $w = (1-A)u$; then $(1-QP)w = 0$, so QP has 1 as an eigenvalue, and the same for PQ because PQ and QP have the same characteristic polynomial.

Remark. The *Cayley transform* is the following construction: if A is a skew-symmetric matrix, then $I+A$ is invertible and

$$Q = (I-A)(I+A)^{-1}$$

is an orthogonal matrix.

Remark. (by Steven Klee) A related argument is to compute $\det(PQ-I)$ using the *matrix determinant lemma*: if A is an invertible $n \times n$ matrix and v, w are $1 \times n$ column vectors, then

$$\det(A + vw^T) = \det(A)(1 + w^T A^{-1} v).$$

This reduces to the case $A = I$, in which case it again comes down to the fact that the product of two square matrices (in this case, obtained from v and w by padding with zeroes) retains the same characteristic polynomial when the factors are reversed.

B4 **Solution 1.** We compute that $m(f) = 2\ln 2 - \frac{1}{2}$. Label the given differential equations by (1) and (2). If we write, e.g., $x\frac{\partial}{\partial x}(1)$ for the result of differentiating (1) by x and multiplying the resulting equation by x, then the combination $x\frac{\partial}{\partial x}(1) + y\frac{\partial}{\partial y}(1) - (1) - (2)$ gives the equation $2xyf_{xy} = xy\ln(xy) + xy$, whence $f_{xy} = \frac{1}{2}(\ln(x) + \ln(y) + 1)$.

Now we observe that

$$\begin{aligned}
&f(s+1,s+1) - f(s+1,s) - f(s,s+1) + f(s,s) \\
&= \int_s^{s+1}\int_s^{s+1} f_{xy}\,dy\,dx \\
&= \frac{1}{2}\int_s^{s+1}\int_s^{s+1} (\ln(x)+\ln(y)+1)\,dy\,dx \\
&= \frac{1}{2} + \int_s^{s+1} \ln(x)\,dx.
\end{aligned}$$

Since $\ln(x)$ is increasing, $\int_s^{s+1}\ln(x)\,dx$ is an increasing function of s, and so it is minimized over $s \in [1,\infty)$ when $s = 1$. We conclude that

$$m(f) = \frac{1}{2} + \int_1^2 \ln(x)\,dx = 2\ln 2 - \frac{1}{2}$$

independent of f.

Remark. The phrasing of the question suggests that solvers were not expected to prove that $\mathscr{F}$ is nonempty, even though this is necessary to make the definition of $m(f)$ logically meaningful. Existence will be explicitly established in the next solution.

Solution 2. We first verify that

$$f(x,y) = \frac{1}{2}(xy\ln(xy) - xy)$$

is an element of $\mathscr{F}$, by computing that

$$\begin{aligned}
xf_x = yf_y &= \frac{1}{2}xy\ln(xy) \\
x^2 f_{xx} = y^2 f_{yy} &= xy.
\end{aligned}$$

(See the following remark for motivation for this guess.)

We next show that the only elements of $\mathscr{F}$ are $f + a\ln(x/y) + b$ where a, b are constants. Suppose that $f + g$ is a second element of $\mathscr{F}$. As in the first solution, we deduce that $g_{xy} = 0$; this implies that $g(x,y) = u(x) + v(y)$ for some twice continuously differentiable functions u and v. We also have $xg_x + yg_y = 0$, which now asserts that $xg_x = -yg_y$ is equal to some constant a. This yields that $g = a\ln(x/y) + b$ as desired.

We next observe that

$$g(s+1,s+1) - g(s+1,s) - g(s,s+1) + g(s,s) = 0,$$

so $m(f) = m(f+g)$. It thus remains to compute $m(f)$. To do this, we verify that

$$f(s+1,s+1) - f(s+1,s) - f(s,s+1) + f(s,s)$$

is nondecreasing in s by computing its derivative to be $\ln(s+1) - \ln(s)$ (either directly or using the integral representation from the first solution). We thus minimize by taking $s = 1$ as in the first solution.

Remark. One way to make a correct guess for f is to notice that the given equations are both symmetric in x and y and posit that f should also be symmetric. Any symmetric function of x and y can be written in terms of the variables $u = x + y$ and $v = xy$, so in principle we could translate the equations into those variables and solve. However, before trying this, we observe that xy appears explicitly in the equations, so it is reasonable to make a first guess of the form $f(x,y) = h(xy)$. For such a choice, we have

$$xf_x + yf_y = 2xyh' = xy\ln(xy)$$

which forces us to set $h(t) = \frac{1}{2}(t\ln(t) - t)$.

B5 **Solution 1.** We prove that $(j,k) = (2019,1010)$ is a valid solution. More generally, let $p(x)$ be the polynomial of degree N such that $p(2n+1) = F_{2n+1}$ for $0 \leq n \leq N$. We will show that $p(2N+3) = F_{2N+3} - F_{N+2}$.

Define a sequence of polynomials $p_0(x), \dots, p_N(x)$ by $p_0(x) = p(x)$ and $p_k(x) = p_{k-1}(x) - p_{k-1}(x+2)$ for $k \geq 1$. Then by induction on k, it is the case that $p_k(2n+1) = F_{2n+1+k}$ for $0 \leq n \leq N-k$, and also that p_k has degree (at most) $N-k$ for $k \geq 1$. Thus $p_N(x) = F_{N+1}$ since $p_N(1) = F_{N+1}$ and p_N is constant.

We now claim that for $0 \leq k \leq N$, $p_{N-k}(2k+3) = \sum_{j=0}^{k} F_{N+1+j}$. We prove this again by induction on k: for the induction step, we have

$$\begin{aligned} p_{N-k}(2k+3) &= p_{N-k}(2k+1) + p_{N-k+1}(2k+1) \\ &= F_{N+1+k} + \sum_{j=0}^{k-1} F_{N+1+j}. \end{aligned}$$

Thus we have $p(2N+3) = p_0(2N+3) = \sum_{j=0}^{N} F_{N+1+j}$.

Now one final induction shows that $\sum_{j=1}^{m} F_j = F_{m+2} - 1$, and so $p(2N+3) = F_{2N+3} - F_{N+2}$, as claimed. In the case $N = 1008$, we thus have $p(2019) = F_{2019} - F_{1010}$.

Solution 2. This solution uses the *Lagrange interpolation formula*: given $x_0, \dots, x_n$ and $y_0, \dots, y_n$, the unique polynomial P of degree at most n satisfying $P(x_i) = y_i$ for $i = 0, \dots, n$ is

$$\sum_{i=0}^{n} P(x_i) \prod_{j \neq i} \frac{x - x_j}{x_i - x_j} =$$

Write

$$F_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^{-n}), \qquad \alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}.$$

For $\gamma \in \mathbb{R}$, let $p_\gamma(x)$ be the unique polynomial of degree at most 1008 satisfying

$$p_1(2n+1) = \gamma^{2n+1}, p_2(2n+1) = \gamma^{2n+1} \, (n = 0, \dots, 1008);$$

then $p(x) = \frac{1}{\sqrt{5}}(p_\alpha(x) - p_\beta(x))$.

By Lagrange interpolation,

$$\begin{aligned} p_\gamma(2019) &= \sum_{n=0}^{1008} \gamma^{2n+1} \prod_{0 \leq j \leq 1008, j \neq n} \frac{2019 - (2j+1)}{(2n+1) - (2j+1)} \\ &= \sum_{n=0}^{1008} \gamma^{2n+1} \prod_{0 \leq j \leq 1008, j \neq n} \frac{1009 - j}{n - j} \\ &= \sum_{n=0}^{1008} \gamma^{2n+1} (-1)^{1008-n} \binom{1009}{n} \\ &= -\gamma((\gamma^2 - 1)^{1009} - (\gamma^2)^{1009}). \end{aligned}$$

For $\gamma \in \{\alpha, \beta\}$ we have $\gamma^2 = \gamma + 1$ and so

$$p_\gamma(2019) = \gamma^{2019} - \gamma^{1010}.$$

We thus deduce that $p(x) = F_{2019} - F_{1010}$ as claimed.

Remark. Karl Mahlburg suggests the following variant of this. As above, use Lagrange interpolation to write

$$p(2019) = \sum_{j=0}^{1008} \binom{1009}{j} F_j;$$

it will thus suffice to verify (by substiting $j \mapsto 1009 - j$) that

$$\sum_{j=0}^{1009} \binom{1009}{j} F_{j+1} = F_{2019}.$$

This identity has the following combinatorial interpretation. Recall that F_{n+1} counts the number of ways to tile a $1 \times n$ rectangle with 1×1 squares and 1×2 dominoes (see below). In any such tiling with $n = 2018$, let j be the number of squares among the first 1009 tiles. These can be ordered in $\binom{1009}{j}$ ways, and the remaining $2018 - j - 2(1009 - j) = j$ squares can be tiled in F_{j+1} ways.

As an aside, this interpretation of F_{n+1} is the oldest known interpretation of the Fibonacci sequence, long predating Fibonacci himself. In ancient Sanskrit, syllables were classified as long or short, and a long syllable was considered to be twice as long as a short syllable; consequently, the number of syllable patterns of total length n equals F_{n+1}.

Remark. It is not difficult to show that the solution $(j,k) = (2019,2010)$ is unique (in positive integers). First, note that to have $F_j - F_k > 0$, we must have $k < j$. If $j < 2019$, then

$$F_{2019} - F_{1010} = F_{2018} + F_{2017} - F_{1010} > F_j > F_j - F_k.$$

If $j > 2020$, then

$$F_j - F_k \geq F_j - F_{j-1} = F_{j-2} \geq F_{2019} > F_{2019} - F_{1010}.$$

Since $j = 2019$ obviously forces $k = 1010$, the only other possible solution would be with $j = 2020$. But then

$$(F_j - F_k) - (F_{2019} - F_{1010}) = (F_{2018} - F_k) + F_{1010}$$

which is negative for $k = 2019$ (it equals $F_{1010} - F_{2017}$) and positive for $k \leq 2018$.

B6 Such a set exists for every n. To construct an example, define the function $f : \mathbb{Z}^n \to \mathbb{Z}/(2n+1)\mathbb{Z}$ by

$$f(x_1, \dots, x_n) = x_1 + 2x_2 + \cdots + nx_n \pmod{2n+1},$$

then let S be the preimage of 0.

To check condition (1), note that if $p \in S$ and q is a neighbor of p differing only in coordinate i, then

$$f(q) = f(p) \pm i \equiv \pm i \pmod{2n+1}$$

and so $q \notin S$.

To check condition (2), note that if $p \in \mathbb{Z}^n$ is not in S, then there exists a unique choice of $i \in \{1, \ldots, n\}$ such that $f(p)$ is congruent to one of $+i$ or $-i$ modulo $2n+1$. The unique neighbor q of p in S is then obtained by either subtracting 1 from, or adding 1 to, the i-th coordinate of p.

Remark. According to Art of Problem Solving (thread c6h366290), this problem was a 1985 IMO submission from Czechoslovakia. For an application to steganography, see: J. Fridrich and P. Lisoněk, Grid colorings in steganography, *IEEE Transactions on Information Theory* **53** (2007), 1547–1549.