Solutions to the 70th William Lowell Putnam Mathematical Competition
Saturday, December 5, 2009

Kiran Kedlaya and Lenny Ng

A–1 Yes, it does follow. Let P be any point in the plane. Let $ABCD$ be any square with center P. Let E,F,G,H be the midpoints of the segments AB,BC,CD,DA, respectively. The function f must satisfy the equations

$$\begin{aligned}
0 &= f(A)+f(B)+f(C)+f(D)\\
0 &= f(E)+f(F)+f(G)+f(H)\\
0 &= f(A)+f(E)+f(P)+f(H)\\
0 &= f(B)+f(F)+f(P)+f(E)\\
0 &= f(C)+f(G)+f(P)+f(F)\\
0 &= f(D)+f(H)+f(P)+f(G).
\end{aligned}$$

If we add the last four equations, then subtract the first equation and twice the second equation, we obtain $0 = 4f(P)$, whence $f(P) = 0$.

Remark. Problem 1 of the 1996 Romanian IMO team selection exam asks the same question with squares replaced by regular polygons of any (fixed) number of vertices.

A–2 Multiplying the first differential equation by gh, the second by fh, and the third by fg, and summing gives

$$(fgh)' = 6(fgh)^2 + 6.$$

Write $k(x) = f(x)g(x)h(x)$; then $k' = 6k^2+6$ and $k(0) = 1$. One solution for this differential equation with this initial condition is $k(x) = \tan(6x+\pi/4)$; by standard uniqueness, this must necessarily hold for x in some open interval around 0. Now the first given equation becomes

$$\begin{aligned}
f'/f &= 2k(x) + 1/k(x)\\
&= 2\tan(6x+\pi/4) + \cot(6x+\pi/4);
\end{aligned}$$

integrating both sides gives

$$\ln(f(x)) = \frac{-2\ln\cos(6x+\pi/4) + \ln\sin(6x+\pi/4)}{6} + c,$$

whence $f(x) = e^c \left(\frac{\sin(6x+\pi/4)}{\cos^2(6x+\pi/4)}\right)^{1/6}$. Substituting $f(0) = 1$ gives $e^c = 2^{-1/12}$ and thus $f(x) = 2^{-1/12}\left(\frac{\sin(6x+\pi/4)}{\cos^2(6x+\pi/4)}\right)^{1/6}$.

Remark. The answer can be put in alternate forms using trigonometric identities. One particularly simple one is

$$f(x) = (\sec 12x)^{1/12}(\sec 12x + \tan 12x)^{1/4}.$$

A–3 The limit is 0; we will show this by checking that $d_n = 0$ for all $n \geq 3$. Starting from the given matrix, add the third column to the first column; this does not change the determinant. However, thanks to the identity $\cos x + \cos y = 2\cos\frac{x+y}{2}\cos\frac{x-y}{2}$, the resulting matrix has the form

$$\begin{pmatrix}
2\cos 2\cos 1 & \cos 2 & \cdots\\
2\cos(n+2)\cos 1 & \cos(n+2) & \cdots\\
2\cos(2n+2)\cos 1 & 2\cos(2n+2) & \cdots\\
\vdots & \vdots & \ddots
\end{pmatrix}$$

with the first column being a multiple of the second. Hence $d_n = 0$.

Remark. Another way to draw the same conclusion is to observe that the given matrix is the sum of the two rank 1 matrices $A_{jk} = \cos(j-1)n\cos k$ and $B_{jk} = -\sin(j-1)n\sin k$, and so has rank at most 2. One can also use the matrices $A_{jk} = e^{i((j-1)n+k)}$, $B_{jk} = e^{-i(j-1)n+k}$.

A–4 The answer is no; indeed, $S = \mathbb{Q}\setminus\{n+2/5 \mid n\in\mathbb{Z}\}$ satisfies the given conditions. Clearly S satisfies (a) and (b); we need only check that it satisfies (c). It suffices to show that if $x = p/q$ is a fraction with $(p,q) = 1$ and $p > 0$, then we cannot have $1/(x(x-1)) = n+2/5$ for an integer n. Suppose otherwise; then

$$(5n+2)p(p-q) = 5q^2.$$

Since p and q are relatively prime, and p divides $5q^2$, we must have $p \mid 5$, so $p = 1$ or $p = 5$. On the other hand, $p-q$ and q are also relatively prime, so $p-q$ divides 5 as well, and $p-q$ must be ± 1 or ± 5. This leads to eight possibilities for (p,q): $(1,0)$, $(5,0)$, $(5,10)$, $(1,-4)$, $(1,2)$, $(1,6)$, $(5,4)$, $(5,6)$. The first three are impossible, while the final five lead to $5n+2 = 16,-20,-36,16,-36$ respectively, none of which holds for integral n.

Remark. More generally, no rational number of the form m/n, where m,n are relatively prime and neither of $\pm m$ is a quadratic residue mod n, need be in S. If $x = p/q$ is in lowest terms and $1/(x(x-1)) = m/n+k$ for some integer k, then $p(p-q)$ is relatively prime to q^2; $q^2/(p(p-q)) = (m+kn)/n$ then implies that $m+kn = \pm q^2$ and so $\pm m$ must be a quadratic residue mod n.

A–5 No, there is no such group. By the structure theorem for finitely generated abelian groups, G can be written as a product of cyclic groups. If any of these factors has odd order, then G has an element of odd order, so the

product of the orders of all of its elements cannot be a power of 2.

We may thus consider only abelian 2-groups hereafter. For such a group G, the product of the orders of all of its elements has the form $2^{k(G)}$ for some nonnegative integer G, and we must show that it is impossible to achieve $k(G) = 2009$. Again by the structure theorem, we may write

$$G \cong \prod_{i=1}^{\infty} (\mathbb{Z}/2^i\mathbb{Z})^{e_i}$$

for some nonnegative integers $e_1, e_2, \ldots$, all but finitely many of which are 0.

For any nonnegative integer m, the elements of G of order at most 2^m form a subgroup isomorphic to

$$\prod_{i=1}^{\infty} (\mathbb{Z}/2^{\min\{i,m\}}\mathbb{Z})^{e_i},$$

which has 2^{s_m} elements for $s_m = \sum_{i=1}^{\infty} \min\{i,m\}e_i$. Hence

$$k(G) = \sum_{i=1}^{\infty} i(2^{s_i} - 2^{s_{i-1}}).$$

Since $s_1 \le s_2 \le \cdots$, $k(G)+1$ is always divisible by 2^{s_1}. In particular, $k(G) = 2009$ forces $s_1 \le 1$.

However, the only cases where $s_1 \le 1$ are where all of the e_i are 0, in which case $k(G) = 0$, or where $e_i = 1$ for some i and $e_j = 0$ for $j \ne i$, in which case $k(G) = (i-1)2^i + 1$. The right side is a strictly increasing function of i which equals 1793 for $i = 8$ and 4097 for $i = 9$, so it can never equal 2009. This proves the claim.

Remark. One can also arrive at the key congruence by dividing G into equivalence classes, by declaring two elements to be equivalent if they generate the same cyclic subgroup of G. For $h > 0$, an element of order 2^h belongs to an equivalence class of size 2^{h-1}, so the products of the orders of the elements of this equivalence class is 2^j for $j = h2^{h-1}$. This quantity is divisible by 4 as long as $h > 1$; thus to have $k(G) \equiv 1 \pmod 4$, the number of elements of G of order 2 must be congruent to 1 modulo 4. However, there are exactly $2^e - 1$ such elements, for e the number of cyclic factors of G. Hence $e = 1$, and one concludes as in the given solution.

A–6 We disprove the assertion using the example

$$f(x,y) = 3(1+y)(2x-1)^2 - y.$$

We have $b-a = d-c = 0$ because the identity $f(x,y) = f(1-x,y)$ forces $a = b$, and because

$$c = \int_0^1 3(2x-1)^2\,dx = 1,$$
$$d = \int_0^1 (6(2x-1)^2 - 1)\,dx = 1.$$

Moreover, the partial derivatives

$$\frac{\partial f}{\partial x}(x_0,y_0) = 3(1+y_0)(8x_0-4)$$
$$\frac{\partial f}{\partial y}(x_0,y_0) = 3(2x_0-1)^2 - 1.$$

have no common zero in $(0,1)^2$. Namely, for the first partial to vanish, we must have $x_0 = 1/2$ since $1+y_0$ is nowhere zero, but for $x_0 = 1/2$ the second partial cannot vanish.

Remark. This problem amounts to refuting a potential generalization of the Mean Value Theorem to bivariate functions. Many counterexamples are possible. Kent Merryfield suggests $y\sin(2\pi x)$, for which all four of the boundary integrals vanish; here the partial derivatives are $2\pi y\cos(2\pi x)$ and $\sin(2\pi x)$. Catalin Zara suggests $x^{1/3}y^{2/3}$. Qingchun Ren suggests $xy(1-y)$.

B–1 Every positive rational number can be uniquely written in lowest terms as a/b for a,b positive integers. We prove the statement in the problem by induction on the largest prime dividing either a or b (where this is considered to be 1 if $a = b = 1$). For the base case, we can write $1/1 = 2!/2!$. For a general a/b, let p be the largest prime dividing either a or b; then $a/b = p^k a'/b'$ for some $k \ne 0$ and positive integers a', b' whose largest prime factors are strictly less than p. We now have $a/b = (p!)^k \frac{a'}{(p-1)!^k b'}$, and all prime factors of a' and $(p-1)!^k b'$ are strictly less than p. By the induction assumption, $\frac{a'}{(p-1)!^k b'}$ can be written as a quotient of products of prime factorials, and so $a/b = (p!)^k \frac{a'}{(p-1)!^k b'}$ can as well. This completes the induction.

Remark. Noam Elkies points out that the representations are unique up to rearranging and canceling common factors.

B–2 The desired real numbers c are precisely those for which $1/3 < c \le 1$. For any positive integer m and any sequence $0 = x_0 < x_1 < \cdots < x_m = 1$, the cost of jumping along this sequence is $\sum_{i=1}^{m} (x_i - x_{i-1})x_i^2$. Since

$$\begin{aligned} 1 = \sum_{i=1}^{m} (x_i - x_{i-1}) &\ge \sum_{i=1}^{m} (x_i - x_{i-1})x_i^2 \\ &> \sum_{i=1}^{m} \int_{x_i}^{x_{i-1}} t^2\,dt \\ &= \int_0^1 t^2\,dt = \frac{1}{3}, \end{aligned}$$

we can only achieve costs c for which $1/3 < c \le 1$.

It remains to check that any such c can be achieved. Suppose $0 = x_0 < \cdots < x_m = 1$ is a sequence with $m \ge 1$. For $i = 1, \ldots, m$, let c_i be the cost of the sequence $0, x_i, x_{i+1}, \ldots, x_m$. For $i > 1$ and $0 < y \le x_{i-1}$, the cost of the sequence $0, y, x_i, \ldots, x_m$ is

$$c_i + y^3 + (x_i - y)x_i^2 - x_i^3 = c_i - y(x_i^2 - y^2),$$

which is less than c_i but approaches c_i as $y \to 0$. By continuity, for $i = 2, \dots, m$, every value in the interval $[c_{i-1}, c_i)$ can be achieved, as can $c_m = 1$ by the sequence $0, 1$.

To show that all costs c with $1/3 < c \leq 1$ can be achieved, it now suffices to check that for every $\varepsilon > 0$, there exists a sequence with cost at most $1/3 + \varepsilon$. For instance, if we take $x_i = i/m$ for $i = 0, \dots, m$, the cost becomes

$$\frac{1}{m^3}(1^2 + \cdots + m^2) = \frac{(m+1)(2m+1)}{6m^2},$$

which converges to $1/3$ as $m \to +\infty$.

Reinterpretation. The cost of jumping along a particular sequence is an upper Riemann sum of the function t^2. The fact that this function admits a Riemann integral implies that for any $\varepsilon > 0$, there exists δ_0 such that the cost of the sequence $x_0, \dots, x_m$ is at most $1/3 + \varepsilon$ as long as $\max_i\{x_i - x_{i-1}\} < \varepsilon$. (The computation of the integral using the sequence $x_i = i/m$ was already known to Archimedes.)

B–3 The answer is $n = 2^k - 1$ for some integer $k \geq 1$. There is a bijection between mediocre subsets of $\{1, \dots, n\}$ and mediocre subsets of $\{2, \dots, n+1\}$ given by adding 1 to each element of the subset; thus $A(n+1) - A(n)$ is the number of mediocre subsets of $\{1, \dots, n+1\}$ that contain 1. It follows that $A(n+2) - 2A(n+1) + A_n = (A(n+2) - A(n+1)) - (A(n+1) - A(n))$ is the difference between the number of mediocre subsets of $\{1, \dots, n+2\}$ containing 1 and the number of mediocre subsets of $\{1, \dots, n+1\}$ containing 1. This difference is precisely the number of mediocre subsets of $\{1, \dots, n+2\}$ containing both 1 and $n+2$, which we term "mediocre subsets containing the endpoints." Since $\{1, \dots, n+2\}$ itself is a mediocre subset of itself containing the endpoints, it suffices to prove that this is the only mediocre subset of $\{1, \dots, n+2\}$ containing the endpoints if and only if $n = 2^k - 1$ for some k.

If n is not of the form $2^k - 1$, then we can write $n + 1 = 2^a b$ for odd $b > 1$. In this case, the set $\{1 + mb \mid 0 \leq m \leq 2^a\}$ is a mediocre subset of $\{1, \dots, n+2\}$ containing the endpoints: the average of $1 + m_1 b$ and $1 + m_2 b$, namely $1 + \frac{m_1 + m_2}{2} b$, is an integer if and only if $m_1 + m_2$ is even, in which case this average lies in the set.

It remains to show that if $n = 2^k - 1$, then the only mediocre subset of $\{1, \dots, n+2\}$ containing the endpoints is itself. This is readily seen by induction on k. For $k = 1$, the statement is obvious. For general k, any mediocre subset S of $\{1, \dots, n+2 = 2^k + 1\}$ containing 1 and $2^k + 1$ must also contain their average, $2^{k-1} + 1$. By the induction assumption, the only mediocre subset of $\{1, \dots, 2^{k-1} + 1\}$ containing the endpoints is itself, and so S must contain all integers between 1 and $2^{k-1} + 1$. Similarly, a mediocre subset of $\{2^{k-1} + 1, \dots, 2^k + 1\}$ containing the endpoints gives a mediocre subset of $\{1, \dots, 2^{k-1} + 1\}$ containing the endpoints by subtracting 2^{k-1} from each element. By the induction assumption again, it follows that S must contain all integers between $2^{k-1} + 1$ and $2^k + 1$. Thus $S = \{1, \dots, 2^k + 1\}$ and the induction is complete.

Remark. One can also proceed by checking that a nonempty subset of $\{1, \dots, n\}$ is mediocre if and only if it is an arithmetic progression with odd common difference. Given this fact, the number of mediocre subsets of $\{1, \dots, n+2\}$ containing the endpoints is seen to be the number of odd factors of $n+1$, from which the desired result is evident. (The sequence $A(n)$ appears as sequence A124197 in the Encyclopedia of Integer Sequences.)

B–4 Any polynomial $P(x, y)$ of degree at most 2009 can be written uniquely as a sum $\sum_{i=0}^{2009} P_i(x, y)$ in which $P_i(x, y)$ is a homogeneous polynomial of degree i. For $r > 0$, let C_r be the path $(r\cos\theta, r\sin\theta)$ for $0 \leq \theta \leq 2\pi$. Put $\lambda(P_i) = \oint_{C_1} P$; then for $r > 0$,

$$\oint_{C_r} P = \sum_{i=0}^{2009} r^i \lambda(P_i).$$

For fixed P, the right side is a polynomial in r, which vanishes for all $r > 0$ if and only if its coefficients vanish. In other words, P is balanced if and only if $\lambda(P_i) = 0$ for $i = 0, \dots, 2009$.

For i odd, we have $P_i(-x, -y) = -P_i(x, y)$. Hence $\lambda(P_i) = 0$, e.g., because the contributions to the integral from θ and $\theta + \pi$ cancel.

For i even, $\lambda(P_i)$ is a linear function of the coefficients of P_i. This function is not identically zero, e.g., because for $P_i = (x^2 + y^2)^{i/2}$, the integrand is always positive and so $\lambda(P) > 0$. The kernel of λ on the space of homogeneous polynomials of degree i is thus a subspace of codimension 1.

It follows that the dimension of V is

$$(1 + \cdots + 2010) - 1005 = (2011 - 1) \times 1005 = 2020050.$$

B–5 **First solution.** If $f(x) \geq x$ for all $x > 1$, then the desired conclusion clearly holds. We may thus assume hereafter that there exists $x_0 > 1$ for which $f(x_0) < x_0$.

Rewrite the original differential equation as

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

Put $c_0 = \min\{0, f(x_0) - 1/x_0\}$. For all $x \geq x_0$, we have $f'(x) > -1/x^2$ and so

$$f(x) \geq f(x_0) - \int_{x_0}^{x} dt/t^2 > c_0.$$

In the other direction, we claim that $f(x) < x$ for all $x \geq x_0$. To see this, suppose the contrary; then by continuity, there is a least $x \geq x_0$ for which $f(x) \geq x$, and

this least value satisfies $f(x) = x$. However, this forces $f'(x) = 0 < 1$ and so $f(x-\varepsilon) > x - \varepsilon$ for $\varepsilon > 0$ small, contradicting the choice of x.

Put $x_1 = \max\{x_0, -c_0\}$. For $x \geq x_1$, we have $|f(x)| < x$ and so $f'(x) > 0$. In particular, the limit $\lim_{x\to+\infty} f(x) = L$ exists.

Suppose that $L < +\infty$; then $\lim_{x\to+\infty} f'(x) = 1/(1+L^2) > 0$. Hence for any sufficiently small $\varepsilon > 0$, we can choose $x_2 \geq x_1$ so that $f'(x) \geq \varepsilon$ for $x \geq x_2$. But then $f(x) \geq f(x_2) + \varepsilon(x - x_2)$, which contradicts $L < +\infty$. Hence $L = +\infty$, as desired.

Variant. (by Leonid Shteyman) One obtains a similar argument by writing

$$f'(x) = \frac{1}{1+f(x)^2} - \frac{f(x)^2}{x^2(1+f(x)^2)},$$

so that

$$-\frac{1}{x^2} \leq f'(x) - \frac{1}{1+f(x)^2} \leq 0.$$

Hence $f'(x) - 1/(1+f(x)^2)$ tends to 0 as $x \to +\infty$, so $f(x)$ is bounded below, and tends to $+\infty$ if and only if the improper integral $\int dx/(1+f(x)^2)$ diverges. However, if the integral were to converge, then as $x \to +\infty$ we would have $1/(1+f(x)^2) \to 0$; however, since f is bounded below, this again forces $f(x) \to +\infty$.

Second solution. (by Catalin Zara) The function $g(x) = f(x) + x$ satisfies the differential equation

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

This implies that $g'(x) > 0$ for all $x > 1$, so the limit $L_1 = \lim_{x\to+\infty} g(x)$ exists. In addition, we cannot have $L_1 < +\infty$, or else we would have $\lim_{x\to+\infty} g'(x) = 0$ whereas the differential equation forces this limit to be 1. Hence $g(x) \to +\infty$ as $x \to +\infty$.

Similarly, the function $h(x) = -f(x) + x$ satisfies the differential equation

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

This implies that $h'(x) \geq 0$ for all x, so the limit $L_2 = \lim_{x\to+\infty} h(x)$ exists. In addition, we cannot have $L_2 < +\infty$, or else we would have $\lim_{x\to+\infty} h'(x) = 0$ whereas the differential equation forces this limit to be 1. Hence $h(x) \to +\infty$ as $x \to +\infty$.

For some $x_1 > 1$, we must have $g(x), h(x) > 0$ for all $x \geq x_1$. For $x \geq x_1$, we have $|f(x)| < x$ and hence $f'(x) > 0$, so the limit $L = \lim_{x\to+\infty} f(x)$ exists. Once again, we cannot have $L < +\infty$, or else we would have $\lim_{x\to+\infty} f'(x) = 0$ whereas the original differential equation (e.g., in the form given in the first solution) forces this limit to be $1/(1+L^2) > 0$. Hence $f(x) \to +\infty$ as $x \to \infty$, as desired.

Third solution. (by Noam Elkies) Consider the function $g(x) = f(x) + \frac{1}{3}f(x)^3$, for which

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

for $x > 1$. Since evidently $g'(x) < 1$, $g(x) - x$ is bounded above for x large. As in the first solution, $f(x)$ is bounded below for x large, so $\frac{1}{3}f(x)^3 - x$ is bounded above by some $c > 0$. For $x \geq c$, we obtain $f(x) \leq (6x)^{1/3}$.

Since $f(x)/x \to 0$ as $x \to +\infty$, $g'(x) \to 1$ and so $g(x)/x \to 1$. Since $g(x)$ tends to $+\infty$, so does $f(x)$. (With a tiny bit of extra work, one shows that in fact $f(x)/(3x)^{1/3} \to 1$ as $x \to +\infty$.)

B–6 **First solution.** (based on work of Yufei Zhao) Since any sequence of the desired form remains of the desired form upon multiplying each term by 2, we may reduce to the case where n is odd. In this case, take $x = 2^h$ for some positive integer h for which $x \geq n$, and set

$$\begin{aligned}
a_0 &= 0 \\
a_1 &= 1 \\
a_2 &= 2x+1 = a_1 + 2x \\
a_3 &= (x+1)^2 = a_2 + x^2 \\
a_4 &= x^n + 1 = a_1 + x^n \\
a_5 &= n(x+1) = a_4 \mod a_3 \\
a_6 &= x \\
a_7 &= n = a_5 \mod a_6.
\end{aligned}$$

We may pad the sequence to the desired length by taking $a_8 = \cdots = a_{2009} = n$.

Second solution. (by James Merryfield) Suppose first that n is not divisible by 3. Recall that since 2 is a primitive root modulo 3^2, it is also a primitive root modulo 3^h for any positive integer h. In particular, if we choose h so that $3^{2h} > n$, then there exists a positive integer c for which $2^c \mod 3^{2h} = n$. We now take b to be a positive integer for which $2^b > 3^{2h}$, and then put

$$\begin{aligned}
a_0 &= 0 \\
a_1 &= 1 \\
a_2 &= 3 = a_1 + 2 \\
a_3 &= 3 + 2^b \\
a_4 &= 2^{2hb} \\
a_5 &= 3^{2h} = a_4 \mod a_3 \\
a_6 &= 2^c \\
a_7 &= n = a_6 \mod a_5.
\end{aligned}$$

If n is divisible by 3, we can force $a_7 = n - 1$ as in the above construction, then put $a_8 = a_7 + 1 = n$. In both cases, we then pad the sequence as in the first solution.

Remark. Hendrik Lenstra, Ronald van Luijk, and Gabriele Della Torre suggest the following variant of

the first solution requiring only 6 steps. For n odd and x as in the first solution, set

$$
\begin{aligned}
a_0 &= 0 \\
a_1 &= 1 \\
a_2 &= x+1 = a_1 + x \\
a_3 &= x^n + x + 1 = a_2 + x^n \\
a_4 &= x^{(n-1)(\phi(a_3)-1)} \\
a_5 &= \frac{x^n+1}{x+1} = a_4 \mod a_3 \\
a_6 &= n = a_5 \mod a_2.
\end{aligned}
$$

It seems unlikely that a shorter solution can be constructed without relying on any deep number-theoretic conjectures.