Solutions to the 72nd William Lowell Putnam Mathematical Competition
Saturday, December 3, 2011

Kiran Kedlaya and Lenny Ng

A1 We claim that the set of points with $0 \leq x \leq 2011$ and $0 \leq y \leq 2011$ that cannot be the last point of a growing spiral are as follows: $(0,y)$ for $0 \leq y \leq 2011$; $(x,0)$ and $(x,1)$ for $1 \leq x \leq 2011$; $(x,2)$ for $2 \leq x \leq 2011$; and $(x,3)$ for $3 \leq x \leq 2011$. This gives a total of

$$2012 + 2011 + 2011 + 2010 + 2009 = 10053$$

excluded points.

The complement of this set is the set of (x,y) with $0 < x < y$, along with (x,y) with $x \geq y \geq 4$. Clearly the former set is achievable as P_2 in a growing spiral, while a point (x,y) in the latter set is P_6 in a growing spiral with successive lengths 1, 2, 3, $x+1$, $x+2$, and $x+y-1$.

We now need to rule out the other cases. Write $x_1 < y_1 < x_2 < y_2 < \dots$ for the lengths of the line segments in the spiral in order, so that $P_1 = (x_1, 0)$, $P_2 = (x_1, y_1)$, $P_3 = (x_1 - x_2, y_1)$, and so forth. Any point beyond P_0 has x-coordinate of the form $x_1 - x_2 + \cdots + (-1)^{n-1} x_n$ for $n \geq 1$; if n is odd, we can write this as $x_1 + (-x_2 + x_3) + \cdots + (-x_{n-1} + x_n) > 0$, while if n is even, we can write this as $(x_1 - x_2) + \cdots + (x_{n-1} - x_n) < 0$. Thus no point beyond P_0 can have x-coordinate 0, and we have ruled out $(0,y)$ for $0 \leq y \leq 2011$.

Next we claim that any point beyond P_3 must have y-coordinate either negative or ≥ 4. Indeed, each such point has y-coordinate of the form $y_1 - y_2 + \cdots + (-1)^{n-1} y_n$ for $n \geq 2$, which we can write as $(y_1 - y_2) + \cdots + (y_{n-1} - y_n) < 0$ if n is even, and

$$y_1 + (-y_2 + y_3) + \cdots + (-y_{n-1} + y_n) \geq y_1 + 2 \geq 4$$

if $n \geq 3$ is odd. Thus to rule out the rest of the forbidden points, it suffices to check that they cannot be P_2 or P_3 for any growing spiral. But none of them can be $P_3 = (x_1 - x_2, y_1)$ since $x_1 - x_2 < 0$, and none of them can be $P_2 = (x_1, y_1)$ since they all have y-coordinate at most equal to their x-coordinate.

A2 For $m \geq 1$, write

$$S_m = \frac{3}{2}\left(1 - \frac{b_1 \cdots b_m}{(b_1+2)\cdots(b_m+2)}\right).$$

Then $S_1 = 1 = 1/a_1$ and a quick calculation yields

$$S_m - S_{m-1} = \frac{b_1 \cdots b_{m-1}}{(b_2+2)\cdots(b_m+2)} = \frac{1}{a_1 \cdots a_m}$$

for $m \geq 2$, since $a_j = (b_j+2)/b_{j-1}$ for $j \geq 2$. It follows that $S_m = \sum_{n=1}^m 1/(a_1 \cdots a_n)$.

Now if (b_j) is bounded above by B, then $\frac{b_j}{b_j+2} \leq \frac{B}{B+2}$ for all j, and so $3/2 > S_m \geq 3/2(1 - (\frac{B}{B+2})^m)$. Since $\frac{B}{B+2} < 1$, it follows that the sequence (S_m) converges to $S = 3/2$.

A3 We claim that $(c,L) = (-1, 2/\pi)$ works. Write $f(r) = \int_0^{\pi/2} x^r \sin x\,dx$. Then

$$f(r) < \int_0^{\pi/2} x^r\,dx = \frac{(\pi/2)^{r+1}}{r+1}$$

while since $\sin x \geq 2x/\pi$ for $x \leq \pi/2$,

$$f(r) > \int_0^{\pi/2} \frac{2x^{r+1}}{\pi}\,dx = \frac{(\pi/2)^{r+1}}{r+2}.$$

It follows that

$$\lim_{r\to\infty} r\left(\frac{2}{\pi}\right)^{r+1} f(r) = 1,$$

whence

$$\lim_{r\to\infty} \frac{f(r)}{f(r+1)} = \lim_{r\to\infty} \frac{r(2/\pi)^{r+1} f(r)}{(r+1)(2/\pi)^{r+2} f(r+1)} \cdot \frac{2(r+1)}{\pi r} = \frac{2}{\pi}.$$

Now by integration by parts, we have

$$\int_0^{\pi/2} x^r \cos x\,dx = \frac{1}{r+1}\int_0^{\pi/2} x^{r+1} \sin x\,dx = \frac{f(r+1)}{r+1}.$$

Thus setting $c = -1$ in the given limit yields

$$\lim_{r\to\infty} \frac{(r+1) f(r)}{r f(r+1)} = \frac{2}{\pi},$$

as desired.

A4 The answer is n odd. Let I denote the $n \times n$ identity matrix, and let A denote the $n \times n$ matrix all of whose entries are 1. If n is odd, then the matrix $A - I$ satisfies the conditions of the problem: the dot product of any row with itself is $n-1$, and the dot product of any two distinct rows is $n-2$.

Conversely, suppose n is even, and suppose that the matrix M satisfied the conditions of the problem. Consider all matrices and vectors mod 2. Since the dot product of a row with itself is equal mod 2 to the sum of the entries of the row, we have $Mv = 0$ where v is the vector $(1,1,\dots,1)$, and so M is singular. On the other hand, $MM^T = A - I$; since

$$(A-I)^2 = A^2 - 2A + I = (n-2)A + I = I,$$

we have $(\det M)^2 = \det(A-I) = 1$ and $\det M = 1$, contradicting the fact that M is singular.

A5 (by Abhinav Kumar) Define $G : \mathbb{R} \to \mathbb{R}$ by $G(x) = \int_0^x g(t)\,dt$. By assumption, G is a strictly increasing, thrice continuously differentiable function. It is also bounded: for $x > 1$, we have

$$0 < G(x) - G(1) = \int_1^x g(t)\,dt \leq \int_1^x dt/t^2 = 1,$$

and similarly, for $x < -1$, we have $0 > G(x) - G(-1) \geq -1$. It follows that the image of G is some open interval (A,B) and that $G^{-1} : (A,B) \to \mathbb{R}$ is also thrice continuously differentiable.

Define $H : (A,B) \times (A,B) \to \mathbb{R}$ by $H(x,y) = F(G^{-1}(x), G^{-1}(y))$; it is twice continuously differentiable since F and G^{-1} are. By our assumptions about F,

$$\begin{aligned}\frac{\partial H}{\partial x} + \frac{\partial H}{\partial y} = \frac{\partial F}{\partial x}(G^{-1}(x), G^{-1}(y)) \cdot \frac{1}{g(G^{-1}(x))} \\ + \frac{\partial F}{\partial y}(G^{-1}(x), G^{-1}(y)) \cdot \frac{1}{g(G^{-1}(y))} = 0.\end{aligned}$$

Therefore H is constant along any line parallel to the vector $(1,1)$, or equivalently, $H(x,y)$ depends only on $x-y$. We may thus write $H(x,y) = h(x-y)$ for some function h on $(-(B-A), B-A)$, and we then have $F(x,y) = h(G(x) - G(y))$. Since $F(u,u) = 0$, we have $h(0) = 0$. Also, h is twice continuously differentiable (since it can be written as $h(x) = H(x,0)$), so $|h'|$ is bounded on the closed interval $[-(B-A)/2, (B-A)/2]$, say by M.

Given $x_1, \dots, x_{n+1} \in \mathbb{R}$ for some $n \geq 2$, the numbers $G(x_1), \dots, G(x_{n+1})$ all belong to (A,B), so we can choose indices i and j so that $|G(x_i) - G(x_j)| \leq (B-A)/n \leq (B-A)/2$. By the mean value theorem,

$$|F(x_i, x_j)| = |h(G(x_i) - G(x_j))| \leq M \frac{B-A}{n},$$

so the claim holds with $C = M(B-A)$.

A6 Choose some ordering $h_1, \dots, h_n$ of the elements of G with $h_1 = e$. Define an $n \times n$ matrix M by settting $M_{ij} = 1/k$ if $h_j = h_i g$ for some $g \in \{g_1, \dots, g_k\}$ and $M_{ij} = 0$ otherwise. Let v denote the column vector $(1, 0, \dots, 0)$. The probability that the product of m random elements of $\{g_1, \dots, g_k\}$ equals h_i can then be interpreted as the i-th component of the vector $M^m v$.

Let $\hat{G}$ denote the dual group of G, i.e., the group of complex-valued characters of G. Let $\hat{e} \in \hat{G}$ denote the trivial character. For each $\chi \in \hat{G}$, the vector $v_\chi = (\chi(h_i))_{i=1}^n$ is an eigenvector of M with eigenvalue $\lambda_\chi = (\chi(g_1) + \cdots + \chi(g_k))/k$. In particular, $v_{\hat{e}}$ is the all-ones vector and $\lambda_{\hat{e}} = 1$. Put

$$b = \max\{|\lambda_\chi| : \chi \in \hat{G} - \{\hat{e}\}\};$$

we show that $b \in (0,1)$ as follows. First suppose $b = 0$; then

$$1 = \sum_{\chi \in \hat{G}} \lambda_\chi = \frac{1}{k} \sum_{i=1}^k \sum_{\chi \in \hat{G}} \chi(g_i) = \frac{n}{k}$$

because $\sum_{\chi \in \hat{(G)}} \chi(g_i)$ equals n for $i = 1$ and 0 otherwise. However, this contradicts the hypothesis that $\{g_1, \dots, g_k\}$ is not all of G. Hence $b > 0$. Next suppose $b = 1$, and choose $\chi \in \hat{G} - \{\hat{e}\}$ with $|\lambda_\chi| = 1$. Since each of $\chi(g_1), \dots, \chi(g_k)$ is a complex number of norm 1, the triangle inequality forces them all to be equal. Since $\chi(g_1) = \chi(e) = 1$, χ must map each of $g_1, \dots, g_k$ to 1, but this is impossible because χ is a nontrivial character and $g_1, \dots, g_k$ form a set of generators of G. This contradiction yields $b < 1$.

Since $v = \frac{1}{n} \sum_{\chi \in \hat{G}} v_\chi$ and $M v_\chi = \lambda_\chi v_\chi$, we have

$$M^m v - \frac{1}{n} v_{\hat{e}} = \frac{1}{n} \sum_{\chi \in \hat{G} - \{\hat{e}\}} \lambda_\chi^m v_\chi.$$

Since the vectors v_χ are pairwise orthogonal, the limit we are interested in can be written as

$$\lim_{m \to \infty} \frac{1}{b^{2m}} (M^m v - \frac{1}{n} v_{\hat{e}}) \cdot (M^m v - \frac{1}{n} v_{\hat{e}}).$$

and then rewritten as

$$\lim_{m \to \infty} \frac{1}{b^{2m}} \sum_{\chi \in \hat{G} - \{\hat{e}\}} |\lambda_\chi|^{2m} = \#\{\chi \in \hat{G} : |\lambda_\chi| = b\}.$$

By construction, this last quantity is nonzero and finite.

Remark. It is easy to see that the result fails if we do not assume $g_1 = e$: take $G = \mathbb{Z}/2\mathbb{Z}$, $n = 1$, and $g_1 = 1$.

Remark. Harm Derksen points out that a similar argument applies even if G is not assumed to be abelian, provided that the operator $g_1 + \cdots + g_k$ in the group algebra $\mathbb{Z}[G]$ is *normal*, i.e., it commutes with the operator $g_1^{-1} + \cdots + g_k^{-1}$. This includes the cases where the set $\{g_1, \dots, g_k\}$ is closed under taking inverses and where it is a union of conjugacy classes (which in turn includes the case of G abelian).

Remark. The matrix M used above has nonnegative entries with row sums equal to 1 (i.e., it corresponds to a Markov chain), and there exists a positive integer m such that M^m has positive entries. For any such matrix, the Perron-Frobenius theorem implies that the sequence of vectors $M^m v$ converges to a limit w, and there exists $b \in [0,1)$ such that

$$\limsup_{m \to \infty} \frac{1}{b^{2m}} \sum_{i=1}^n ((M^m v - w)_i)^2$$

is nonzero and finite. (The intended interpretation in case $b = 0$ is that $M^m v = w$ for all large m.) However, the limit need not exist in general.

B1 Since the rational numbers are dense in the reals, we can find positive integers a,b such that

$$\frac{3\varepsilon}{hk} < \frac{b}{a} < \frac{4\varepsilon}{hk}.$$

By multiplying a and b by a suitably large positive integer, we can also ensure that $3a^2 > b$. We then have

$$\frac{\varepsilon}{hk} < \frac{b}{3a} < \frac{b}{\sqrt{a^2+b}+a} = \sqrt{a^2+b}-a$$

and

$$\sqrt{a^2+b}-a = \frac{b}{\sqrt{a^2+b}+a} \leq \frac{b}{2a} < 2\frac{\varepsilon}{hk}.$$

We may then take $m = k^2(a^2+b), n = h^2a^2$.

B2 Only the primes 2 and 5 appear seven or more times. The fact that these primes appear is demonstrated by the examples

$$(2,5,2),(2,5,3),(2,7,5),(2,11,5)$$

and their reversals.

It remains to show that if either $\ell = 3$ or ℓ is a prime greater than 5, then ℓ occurs at most six times as an element of a triple in S. Note that $(p,q,r) \in S$ if and only if $q^2 - 4pr = a^2$ for some integer a; in particular, since $4pr \geq 16$, this forces $q \geq 5$. In particular, q is odd, as then is a, and so $q^2 \equiv a^2 \equiv 1 \pmod 8$; consequently, one of p,r must equal 2. If $r = 2$, then $8p = q^2 - a^2 = (q+a)(q-a)$; since both factors are of the same sign and their sum is the positive number $2q$, both factors are positive. Since they are also both even, we have $q+a \in \{2,4,2p,4p\}$ and so $q \in \{2p+1,p+2\}$. Similarly, if $p = 2$, then $q \in \{2r+1,r+2\}$. Consequently, ℓ occurs at most twice as many times as there are prime numbers in the list

$$2\ell+1, \ell+2, \frac{\ell-1}{2}, \ell-2.$$

For $\ell = 3, \ell-2 = 1$ is not prime. For $\ell \geq 7$, the numbers $\ell-2, \ell, \ell+2$ cannot all be prime, since one of them is always a nontrivial multiple of 3.

Remark. The above argument shows that the cases listed for 5 are the only ones that can occur. By contrast, there are infinitely many cases where 2 occurs if either the twin prime conjecture holds or there are infinitely many Sophie Germain primes (both of which are expected to be true).

B3 Yes, it follows that f is differentiable.

First solution. Note first that at 0, f/g and g are both continuous, as then is their product f. If $f(0) \neq 0$, then in some neighborhood of 0, f is either always positive or always negative. We can thus choose $\varepsilon \in \{\pm 1\}$ so that εf is the composition of the differentiable function $(fg)\cdot(f/g)$ with the square root function. By the chain rule, f is differentiable at 0.

If $f(0) = 0$, then $(f/g)(0) = 0$, so we have

$$(f/g)'(0) = \lim_{x\to 0} \frac{f(x)}{xg(x)}.$$

Since g is continuous at 0, we may multiply limits to deduce that $\lim_{x\to 0} f(x)/x$ exists.

Second solution. Choose a neighborhood N of 0 on which $g(x) \neq 0$. Define the following functions on $N \setminus \{0\}$: $h_1(x) = \frac{f(x)g(x)-f(0)g(0)}{x}$; $h_2(x) = \frac{f(x)g(0)-f(0)g(x)}{xg(0)g(x)}$; $h_3(x) = g(0)g(x)$; $h_4(x) = \frac{1}{g(x)+g(0)}$. Then by assumption, h_1,h_2,h_3,h_4 all have limits as $x \to 0$. On the other hand,

$$\frac{f(x)-f(0)}{x} = (h_1(x)+h_2(x)h_3(x))h_4(x),$$

and it follows that $\lim_{x\to 0} \frac{f(x)-f(0)}{x}$ exists, as desired.

B4 Number the games $1,\dots,2011$, and let $A = (a_{jk})$ be the 2011×2011 matrix whose jk entry is 1 if player k wins game j and $i = \sqrt{-1}$ if player k loses game j. Then $\overline{a_{hj}}a_{jk}$ is 1 if players h and k tie in game j; i if player h wins and player k loses in game j; and $-i$ if h loses and k wins. It follows that $T + iW = \overline{A}^T A$.

Now the determinant of A is unchanged if we subtract the first row of A from each of the other rows, producing a matrix whose rows, besides the first one, are $(1-i)$ times a row of integers. Thus we can write $\det A = (1-i)^{2010}(a+bi)$ for some integers a,b. But then $\det(T+iW) = \det(\overline{A}^T A) = 2^{2010}(a^2+b^2)$ is a nonnegative integer multiple of 2^{2010}, as desired.

B5 Define the function

$$f(y) = \int_{-\infty}^{\infty} \frac{dx}{(1+x^2)(1+(x+y)^2)}.$$

For $y \geq 0$, in the range $-1 \leq x \leq 0$, we have

$$\begin{aligned}(1+x^2)(1+(x+y)^2) &\leq (1+1)(1+(1+y)^2) = 2y^2+4y+4 \\ &\leq 2y^2+4+2(y^2+1) \leq 6+6y^2.\end{aligned}$$

We thus have the lower bound

$$f(y) \geq \frac{1}{6(1+y^2)};$$

the same bound is valid for $y \leq 0$ because $f(y) = f(-y)$.

The original hypothesis can be written as

$$\sum_{i,j=1}^{n} f(a_i - a_j) \leq An$$

and thus implies that

$$\sum_{i,j=1}^{n} \frac{1}{1+(a_i-a_j)^2} \leq 6An.$$

By the Cauchy-Schwarz inequality, this implies

$$\sum_{i,j=1}^{n}(1+(a_i-a_j)^2)\geq Bn^3$$

for $B=1/(6A)$.

Remark. One can also compute explicitly (using partial fractions, Fourier transforms, or contour integration) that $f(y)=\frac{2\pi}{4+y^2}$.

Remark. Praveen Venkataramana points out that the lower bound can be improved to Bn^4 as follows. For each $z\in\mathbb{Z}$, put $Q_{z,n}=\{i\in\{1,\dots,n\}: a_i\in[z,z+1)\}$ and $q_{z,n}=\#Q_{z,n}$. Then $\sum_z q_{z,n}=n$ and

$$6An\geq\sum_{i,j=1}^{n}\frac{1}{1+(a_i-a_j)^2}\geq\sum_{z\in\mathbb{Z}}\frac{1}{2}q_{z,n}^2.$$

If exactly k of the $q_{z,n}$ are nonzero, then $\sum_{z\in\mathbb{Z}}q_{z,n}^2\geq n^2/k$ by Jensen's inequality (or various other methods), so we must have $k\geq n/(6A)$. Then

$$\begin{aligned}\sum_{i,j=1}^{n}(1+(a_i-a_j)^2)&\geq n^2+\sum_{i,j=1}^{k}\max\{0,(|i-j|-1)^2\}\\&\geq n^2+\frac{k^4}{6}-\frac{2k^3}{3}+\frac{5k^2}{6}-\frac{k}{3}.\end{aligned}$$

This is bounded below by Bn^4 for some $B>0$.

In the opposite direction, one can weaken the initial upper bound to $An^{4/3}$ and still derive a lower bound of Bn^3. The argument is similar.

B6 In order to interpret the problem statement, one must choose a convention for the value of 0^0; we will take it to equal 1. (If one takes 0^0 to be 0, then the problem fails for $p=3$.)

First solution. By Wilson's theorem,

$$k!(p-1-k)!\equiv(-1)^k(p-1)!\equiv(-1)^{k+1}\pmod{p},$$

so we have a congruence of Laurent polynomials

$$\begin{aligned}\sum_{k=0}^{p-1}k!x^k&\equiv\sum_{k=0}^{p-1}\frac{(-1)^{k+1}x^k}{(p-1-k)!}\pmod{p}\\&\equiv -x^{p-1}\sum_{k=0}^{p-1}\frac{(-x)^{-k}}{k!}\pmod{p}.\end{aligned}$$

Replacing x with $-1/x$, we reduce the original problem to showing that the polynomial

$$g(x)=\sum_{k=0}^{p-1}\frac{x^k}{k!}$$

over $\mathbb{F}_p$ has at most $(p-1)/2$ nonzero roots in $\mathbb{F}_p$. To see this, write

$$h(x)=x^p-x+g(x)$$

and note that by Wilson's theorem again,

$$h'(x)=1+\sum_{k=1}^{p-1}\frac{x^{k-1}}{(k-1)!}=x^{p-1}-1+g(x).$$

If $z\in\mathbb{F}_p$ is such that $g(z)=0$, then $z\neq 0$ because $g(0)=1$. Therefore, $z^{p-1}=1$, so $h(z)=h'(z)=0$ and so z is at least a double root of h. Since h is a polynomial of degree p, there can be at most $(p-1)/2$ zeroes of g in $\mathbb{F}_p$, as desired.

Second solution. (By Noam Elkies) Define the polynomial f over $\mathbb{F}_p$ by

$$f(x)=\sum_{k=0}^{p-1}k!x^k.$$

Put $t=(p-1)/2$; the problem statement is that f has at most t roots modulo p. Suppose the contrary; since $f(0)=1$, this means that $f(x)$ is nonzero for at most $t-1$ values of $x\in\mathbb{F}_p^*$. Denote these values by $x_1,\dots,x_m$, where by assumption $m<t$, and define the polynomial Q over $\mathbb{F}_p$ by

$$Q(x)=\prod_{k=1}^{m}(x-x_m)=\sum_{k=0}^{t-1}Q_kx^k.$$

Then we can write

$$f(x)=\frac{P(x)}{Q(x)}(1-x^{p-1})$$

where $P(x)$ is some polynomial of degree at most m. This means that the power series expansions of $f(x)$ and $P(x)/Q(x)$ coincide modulo x^{p-1}, so the coefficients of $x^t,\dots,x^{2t-1}$ in $f(x)Q(x)$ vanish. In other words, the product of the square matrix

$$A=((i+j+1)!)_{i,j=0}^{t-1}$$

with the nonzero column vector $(Q_{t-1},\dots,Q_0)$ is zero. However, by the following lemma, $\det(A)$ is nonzero modulo p, a contradiction.

Lemma 1. *For any nonnegative integer m and any integer n,*

$$\det((i+j+n)!)_{i,j=0}^{m}=\prod_{k=0}^{m}k!(k+n)!.$$

Proof. Define the $(m+1)\times(m+1)$ matrix $A_{m,n}$ by $(A_{m,n})_{i,j}=\binom{i+j+n}{i}$; the desired result is then that $\det(A_{m,n})=1$. Note that

$$(A_{m,n-1})_{ij}=\begin{cases}(A_{m,n})_{ij} & i=0\\(A_{m,n})_{ij}-(A_{m,n})_{(i-1)j} & i>0;\end{cases}$$

that is, $A_{m,n-1}$ can be obtained from $A_{m,n}$ by elementary row operations. Therefore, $\det(A_{m,n})=\det(A_{m,n-1})$, so $\det(A_{m,n})$ depends only on m. The claim now follows by observing that $A_{0,0}$ is the 1×1 matrix with entry 1 and that $A_{m,-1}$ has the block representation $\begin{pmatrix}1&*\\0&A_{m-1,0}\end{pmatrix}$. $\square$

Remark. Elkies has given a more detailed discussion of the origins of this solution in the theory of orthogonal polynomials; see http://mathoverflow.net/questions/82648.