Solutions to the 62nd William Lowell Putnam Mathematical Competition
Saturday, December 1, 2001

Manjul Bhargava, Kiran Kedlaya, and Lenny Ng

A–1 The hypothesis implies $((b*a)*b)*(b*a) = b$ for all $a, b \in S$ (by replacing a by $b*a$), and hence $a*(b*a) = b$ for all $a, b \in S$ (using $(b*a)*b = a$).

A–2 Let P_n denote the desired probability. Then $P_1 = 1/3$, and, for $n > 1$,

$$\begin{aligned} P_n &= \left(\frac{2n}{2n+1}\right) P_{n-1} + \left(\frac{1}{2n+1}\right)(1 - P_{n-1}) \\ &= \left(\frac{2n-1}{2n+1}\right) P_{n-1} + \frac{1}{2n+1}. \end{aligned}$$

The recurrence yields $P_2 = 2/5$, $P_3 = 3/7$, and by a simple induction, one then checks that for general n one has $P_n = n/(2n+1)$.

Note: Richard Stanley points out the following noninductive argument. Put $f(x) = \prod_{k=1}^{n}(x+2k)/(2k+1)$; then the coefficient of x^i in $f(x)$ is the probability of getting exactly i heads. Thus the desired number is $(f(1) - f(-1))/2$, and both values of f can be computed directly: $f(1) = 1$, and

$$f(-1) = \frac{1}{3} \times \frac{3}{5} \times \cdots \times \frac{2n-1}{2n+1} = \frac{1}{2n+1}.$$

A–3 By the quadratic formula, if $P_m(x) = 0$, then $x^2 = m \pm 2\sqrt{2m} + 2$, and hence the four roots of P_m are given by $S = \{\pm\sqrt{m} \pm \sqrt{2}\}$. If P_m factors into two nonconstant polynomials over the integers, then some subset of S consisting of one or two elements form the roots of a polynomial with integer coefficients.

First suppose this subset has a single element, say $\sqrt{m} \pm \sqrt{2}$; this element must be a rational number. Then $(\sqrt{m} \pm \sqrt{2})^2 = 2 + m \pm 2\sqrt{2m}$ is an integer, so m is twice a perfect square, say $m = 2n^2$. But then $\sqrt{m} \pm \sqrt{2} = (n \pm 1)\sqrt{2}$ is only rational if $n = \pm 1$, i.e., if $m = 2$.

Next, suppose that the subset contains two elements; then we can take it to be one of $\{\sqrt{m} \pm \sqrt{2}\}$, $\{\sqrt{2} \pm \sqrt{m}\}$ or $\{\pm(\sqrt{m} + \sqrt{2})\}$. In all cases, the sum and the product of the elements of the subset must be a rational number. In the first case, this means $2\sqrt{m} \in \mathbb{Q}$, so m is a perfect square. In the second case, we have $2\sqrt{2} \in \mathbb{Q}$, contradiction. In the third case, we have $(\sqrt{m} + \sqrt{2})^2 \in \mathbb{Q}$, or $m + 2 + 2\sqrt{2m} \in \mathbb{Q}$, which means that m is twice a perfect square.

We conclude that $P_m(x)$ factors into two nonconstant polynomials over the integers if and only if m is either a square or twice a square.

Note: a more sophisticated interpretation of this argument can be given using Galois theory. Namely, if m is neither a square nor twice a square, then the number fields $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{2})$ are distinct quadratic fields, so their compositum is a number field of degree 4, whose Galois group acts transitively on $\{\pm\sqrt{m} \pm \sqrt{2}\}$. Thus P_m is irreducible.

A–4 Choose r, s, t so that $EC = rBC, FA = sCA, GB = tCB$, and let $[XYZ]$ denote the area of triangle XYZ. Then $[ABE] = [AFE]$ since the triangles have the same altitude and base. Also $[ABE] = (BE/BC)[ABC] = 1 - r$, and $[ECF] = (EC/BC)(CF/CA)[ABC] = r(1-s)$ (e.g., by the law of sines). Adding this all up yields

$$\begin{aligned} 1 &= [ABE] + [ABF] + [ECF] \\ &= 2(1-r) + r(1-s) = 2 - r - rs \end{aligned}$$

or $r(1+s) = 1$. Similarly $s(1+t) = t(1+r) = 1$.

Let $f : [0,\infty) \to [0,\infty)$ be the function given by $f(x) = 1/(1+x)$; then $f(f(f(r))) = r$. However, $f(x)$ is strictly decreasing in x, so $f(f(x))$ is increasing and $f(f(f(x)))$ is decreasing. Thus there is at most one x such that $f(f(f(x))) = x$; in fact, since the equation $f(z) = z$ has a positive root $z = (-1+\sqrt{5})/2$, we must have $r = s = t = z$.

We now compute $[ABF] = (AF/AC)[ABC] = z$, $[ABR] = (BR/BF)[ABF] = z/2$, analogously $[BCS] = [CAT] = z/2$, and $[RST] = |[ABC] - [ABR] - [BCS] - [CAT]| = |1 - 3z/2| = \frac{7-3\sqrt{5}}{4}$.

Note: the key relation $r(1+s) = 1$ can also be derived by computing using homogeneous coordinates or vectors.

A–5 Suppose $a^{n+1} - (a+1)^n = 2001$. Notice that $a^{n+1} + [(a+1)^n - 1]$ is a multiple of a; thus a divides $2002 = 2 \times 7 \times 11 \times 13$.

Since 2001 is divisible by 3, we must have $a \equiv 1 \pmod 3$, otherwise one of a^{n+1} and $(a+1)^n$ is a multiple of 3 and the other is not, so their difference cannot be divisible by 3. Now $a^{n+1} \equiv 1 \pmod 3$, so we must have $(a+1)^n \equiv 1 \pmod 3$, which forces n to be even, and in particular at least 2.

If a is even, then $a^{n+1} - (a+1)^n \equiv -(a+1)^n \pmod 4$. Since n is even, $-(a+1)^n \equiv -1 \pmod 4$. Since

$2001 \equiv 1 \pmod 4$, this is impossible. Thus a is odd, and so must divide $1001 = 7 \times 11 \times 13$. Moreover, $a^{n+1} - (a+1)^n \equiv a \pmod 4$, so $a \equiv 1 \pmod 4$.

Of the divisors of $7 \times 11 \times 13$, those congruent to 1 mod 3 are precisely those not divisible by 11 (since 7 and 13 are both congruent to 1 mod 3). Thus a divides 7×13. Now $a \equiv 1 \pmod 4$ is only possible if a divides 13.

We cannot have $a = 1$, since $1 - 2^n \neq 2001$ for any n. Thus the only possibility is $a = 13$. One easily checks that $a = 13, n = 2$ is a solution; all that remains is to check that no other n works. In fact, if $n > 2$, then $13^{n+1} \equiv 2001 \equiv 1 \pmod 8$. But $13^{n+1} \equiv 13 \pmod 8$ since n is even, contradiction. Thus $a = 13, n = 2$ is the unique solution.

Note: once one has that n is even, one can use that $2002 = a^{n+1} + 1 - (a+1)^n$ is divisible by $a+1$ to rule out cases.

A–6 The answer is yes. Consider the arc of the parabola $y = Ax^2$ inside the circle $x^2 + (y-1)^2 = 1$, where we initially assume that $A > 1/2$. This intersects the circle in three points, $(0,0)$ and $(\pm\sqrt{2A-1}/A, (2A-1)/A)$. We claim that for A sufficiently large, the length L of the parabolic arc between $(0,0)$ and $(\sqrt{2A-1}/A, (2A-1)/A)$ is greater than 2, which implies the desired result by symmetry. We express L using the usual formula for arclength:

$$\begin{aligned} L &= \int_0^{\sqrt{2A-1}/A} \sqrt{1+(2Ax)^2}\,dx \\ &= \frac{1}{2A}\int_0^{2\sqrt{2A-1}} \sqrt{1+x^2}\,dx \\ &= 2 + \frac{1}{2A}\left(\int_0^{2\sqrt{2A-1}} (\sqrt{1+x^2}-x)\,dx - 2\right), \end{aligned}$$

where we have artificially introduced $-x$ into the integrand in the last step. Now, for $x \geq 0$,

$$\sqrt{1+x^2}-x = \frac{1}{\sqrt{1+x^2}+x} > \frac{1}{2\sqrt{1+x^2}} \geq \frac{1}{2(x+1)};$$

since $\int_0^\infty dx/(2(x+1))$ diverges, so does $\int_0^\infty (\sqrt{1+x^2}-x)\,dx$. Hence, for sufficiently large A, we have $\int_0^{2\sqrt{2A-1}} (\sqrt{1+x^2}-x)\,dx > 2$, and hence $L > 2$.

Note: a numerical computation shows that one must take $A > 34.7$ to obtain $L > 2$, and that the maximum value of L is about 4.0027, achieved for $A \approx 94.1$.

B–1 Let R (resp. B) denote the set of red (resp. black) squares in such a coloring, and for $s \in R \cup B$, let $f(s)n + g(s) + 1$ denote the number written in square s, where $0 \leq f(s), g(s) \leq n-1$. Then it is clear that the value of $f(s)$ depends only on the row of s, while the value of $g(s)$ depends only on the column of s. Since every row contains exactly $n/2$ elements of R and $n/2$ elements of B,

$$\sum_{s\in R} f(s) = \sum_{s\in B} f(s).$$

Similarly, because every column contains exactly $n/2$ elements of R and $n/2$ elements of B,

$$\sum_{s\in R} g(s) = \sum_{s\in B} g(s).$$

It follows that

$$\sum_{s\in R} f(s)n + g(s) + 1 = \sum_{s\in B} f(s)n + g(s) + 1,$$

as desired.

Note: Richard Stanley points out a theorem of Ryser (see Ryser, *Combinatorial Mathematics*, Theorem 3.1) that can also be applied. Namely, if A and B are $0-1$ matrices with the same row and column sums, then there is a sequence of operations on 2×2 matrices of the form

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

or vice versa, which transforms A into B. If we identify 0 and 1 with red and black, then the given coloring and the checkerboard coloring both satisfy the sum condition. Since the desired result is clearly true for the checkerboard coloring, and performing the matrix operations does not affect this, the desired result follows in general.

B–2 By adding and subtracting the two given equations, we obtain the equivalent pair of equations

$$\begin{aligned} 2/x &= x^4 + 10x^2y^2 + 5y^4 \\ 1/y &= 5x^4 + 10x^2y^2 + y^4. \end{aligned}$$

Multiplying the former by x and the latter by y, then adding and subtracting the two resulting equations, we obtain another pair of equations equivalent to the given ones,

$$3 = (x+y)^5, \qquad 1 = (x-y)^5.$$

It follows that $x = (3^{1/5}+1)/2$ and $y = (3^{1/5}-1)/2$ is the unique solution satisfying the given equations.

B–3 Since $(k-1/2)^2 = k^2 - k + 1/4$ and $(k+1/2)^2 = k^2 + k + 1/4$, we have that $\langle n \rangle = k$ if and only if

$k^2 - k + 1 \le n \le k^2 + k$. Hence

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{2^{\langle n \rangle} + 2^{-\langle n \rangle}}{2^n} &= \sum_{k=1}^{\infty} \sum_{n, \langle n \rangle = k} \frac{2^{\langle n \rangle} + 2^{-\langle n \rangle}}{2^n} \\
&= \sum_{k=1}^{\infty} \sum_{n=k^2-k+1}^{k^2+k} \frac{2^k + 2^{-k}}{2^n} \\
&= \sum_{k=1}^{\infty} (2^k + 2^{-k})(2^{-k^2+k} - 2^{-k^2-k}) \\
&= \sum_{k=1}^{\infty} (2^{-k(k-2)} - 2^{-k(k+2)}) \\
&= \sum_{k=1}^{\infty} 2^{-k(k-2)} - \sum_{k=3}^{\infty} 2^{-k(k-2)} \\
&= 3.
\end{aligned}$$

Alternate solution: rewrite the sum as $\sum_{n=1}^{\infty} 2^{-(n+\langle n \rangle)} + \sum_{n=1}^{\infty} 2^{-(n-\langle n \rangle)}$. Note that $\langle n \rangle \neq \langle n+1 \rangle$ if and only if $n = m^2 + m$ for some m. Thus $n + \langle n \rangle$ and $n - \langle n \rangle$ each increase by 1 except at $n = m^2 + m$, where the former skips from $m^2 + 2m$ to $m^2 + 2m + 2$ and the latter repeats the value m^2. Thus the sums are

$$\sum_{n=1}^{\infty} 2^{-n} - \sum_{m=1}^{\infty} 2^{-m^2} + \sum_{n=0}^{\infty} 2^{-n} + \sum_{m=1}^{\infty} 2^{-m^2} = 2 + 1 = 3.$$

B–4 For a rational number p/q expressed in lowest terms, define its *height* $H(p/q)$ to be $|p| + |q|$. Then for any $p/q \in S$ expressed in lowest terms, we have $H(f(p/q)) = |q^2 - p^2| + |pq|$; since by assumption p and q are nonzero integers with $|p| \neq |q|$, we have

$$\begin{aligned}
H(f(p/q)) - H(p/q) &= |q^2 - p^2| + |pq| - |p| - |q| \\
&\ge 3 + |pq| - |p| - |q| \\
&= (|p| - 1)(|q| - 1) + 2 \ge 2.
\end{aligned}$$

It follows that $f^{(n)}(S)$ consists solely of numbers of height strictly larger than $2n + 2$, and hence

$$\cap_{n=1}^{\infty} f^{(n)}(S) = \emptyset.$$

Note: many choices for the height function are possible: one can take $H(p/q) = \max |p|, |q|$, or $H(p/q)$ equal to the total number of prime factors of p and q, and so on. The key properties of the height function are that on one hand, there are only finitely many rationals with height below any finite bound, and on the other hand, the height function is a sufficiently "algebraic" function of its argument that one can relate the heights of p/q and $f(p/q)$.

B–5 Note that $g(x) = g(y)$ implies that $g(g(x)) = g(g(y))$ and hence $x = y$ from the given equation. That is, g is injective. Since g is also continuous, g is either strictly increasing or strictly decreasing. Moreover, g cannot tend to a finite limit L as $x \to +\infty$, or else we'd have $g(g(x)) - ag(x) = bx$, with the left side bounded and the right side unbounded. Similarly, g cannot tend to a finite limit as $x \to -\infty$. Together with monotonicity, this yields that g is also surjective.

Pick x_0 arbitrary, and define x_n for all $n \in \mathbb{Z}$ recursively by $x_{n+1} = g(x_n)$ for $n > 0$, and $x_{n-1} = g^{-1}(x_n)$ for $n < 0$. Let $r_1 = (a + \sqrt{a^2 + 4b})/2$ and $r_2 = (a - \sqrt{a^2 + 4b})/2$ and r_2 be the roots of $x^2 - ax - b = 0$, so that $r_1 > 0 > r_2$ and $1 > |r_1| > |r_2|$. Then there exist $c_1, c_2 \in \mathbb{R}$ such that $x_n = c_1 r_1^n + c_2 r_2^n$ for all $n \in \mathbb{Z}$.

Suppose g is strictly increasing. If $c_2 \neq 0$ for some choice of x_0, then x_n is dominated by r_2^n for n sufficiently negative. But taking x_n and x_{n+2} for n sufficiently negative of the right parity, we get $0 < x_n < x_{n+2}$ but $g(x_n) > g(x_{n+2})$, contradiction. Thus $c_2 = 0$; since $x_0 = c_1$ and $x_1 = c_1 r_1$, we have $g(x) = r_1 x$ for all x. Analogously, if g is strictly decreasing, then $c_2 = 0$ or else x_n is dominated by r_1^n for n sufficiently positive. But taking x_n and x_{n+2} for n sufficiently positive of the right parity, we get $0 < x_{n+2} < x_n$ but $g(x_{n+2}) < g(x_n)$, contradiction. Thus in that case, $g(x) = r_2 x$ for all x.

B–6 Yes, there must exist infinitely many such n. Let S be the convex hull of the set of points (n, a_n) for $n \ge 0$. Geometrically, S is the intersection of all convex sets (or even all halfplanes) containing the points (n, a_n); algebraically, S is the set of points (x, y) which can be written as $c_1(n_1, a_{n_1}) + \cdots + c_k(n_k, a_{n_k})$ for some $c_1, \ldots, c_k$ which are nonnegative of sum 1.

We prove that for infinitely many n, (n, a_n) is a vertex on the upper boundary of S, and that these n satisfy the given condition. The condition that (n, a_n) is a vertex on the upper boundary of S is equivalent to the existence of a line passing through (n, a_n) with all other points of S below it. That is, there should exist $m > 0$ such that

$$a_k < a_n + m(k - n) \qquad \forall k \ge 1. \tag{1}$$

We first show that $n = 1$ satisfies (1). The condition $a_k/k \to 0$ as $k \to \infty$ implies that $(a_k - a_1)/(k-1) \to 0$ as well. Thus the set $\{(a_k - a_1)/(k-1)\}$ has an upper bound m, and now $a_k \le a_1 + m(k-1)$, as desired.

Next, we show that given one n satisfying (1), there exists a larger one also satisfying (1). Again, the condition $a_k/k \to 0$ as $k \to \infty$ implies that $(a_k - a_n)/(k-n) \to 0$ as $k \to \infty$. Thus the sequence $\{(a_k - a_n)/(k-n)\}_{k>n}$ has a maximum element; suppose $k = r$ is the largest value of k that achieves this maximum, and put $m = (a_r - a_n)/(r-n)$. Then the line through (r, a_r) of slope m lies strictly above (k, a_k) for $k > r$ and passes through or lies above (k, a_k) for

$k < r$. Thus (1) holds for $n = r$ with m replaced by $m - \epsilon$ for suitably small $\epsilon > 0$.

By induction, we have that (1) holds for infinitely many n. For any such n there exists $m > 0$ such that for $i = 1, \ldots, n-1$, the points $(n-i, a_{n-i})$ and $(n+i, a_{n+i})$ lie below the line through (n, a_n) of slope m. That means $a_{n+i} < a_n + mi$ and $a_{n-i} < a_n - mi$; adding these together gives $a_{n-i} + a_{n+i} < 2a_n$, as desired.