Solutions to the 71st William Lowell Putnam Mathematical Competition
Saturday, December 4, 2010

Kiran Kedlaya and Lenny Ng

A1 The largest such k is $\lfloor \frac{n+1}{2} \rfloor = \lceil \frac{n}{2} \rceil$. For n even, this value is achieved by the partition

$$\{1,n\}, \{2,n-1\}, \dots;$$

for n odd, it is achieved by the partition

$$\{n\}, \{1,n-1\}, \{2,n-2\}, \dots.$$

One way to see that this is optimal is to note that the common sum can never be less than n, since n itself belongs to one of the boxes. This implies that $k \leq (1 + \cdots + n)/n = (n+1)/2$. Another argument is that if $k > (n+1)/2$, then there would have to be two boxes with one number each (by the pigeonhole principle), but such boxes could not have the same sum.

Remark. A much subtler question would be to find the smallest k (as a function of n) for which no such arrangement exists.

A2 The only such functions are those of the form $f(x) = cx + d$ for some real numbers c, d (for which the property is obviously satisfied). To see this, suppose that f has the desired property. Then for any $x \in \mathbb{R}$,

$$\begin{aligned} 2f'(x) &= f(x+2) - f(x) \\ &= (f(x+2) - f(x+1)) + (f(x+1) - f(x)) \\ &= f'(x+1) + f'(x). \end{aligned}$$

Consequently, $f'(x+1) = f'(x)$.

Define the function $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = f(x+1) - f(x)$, and put $c = g(0)$, $d = f(0)$. For all $x \in \mathbb{R}$, $g'(x) = f'(x+1) - f'(x) = 0$, so $g(x) = c$ identically, and $f'(x) = f(x+1) - f(x) = g(x) = c$, so $f(x) = cx + d$ identically as desired.

A3 If $a = b = 0$, then the desired result holds trivially, so we assume that at least one of a, b is nonzero. Pick any point $(a_0, b_0) \in \mathbb{R}^2$, and let L be the line given by the parametric equation $L(t) = (a_0, b_0) + (a, b)t$ for $t \in \mathbb{R}$. By the chain rule and the given equation, we have $\frac{d}{dt}(h \circ L) = h \circ L$. If we write $f = h \circ L : \mathbb{R} \to \mathbb{R}$, then $f'(t) = f(t)$ for all t. It follows that $f(t) = Ce^t$ for some constant C. Since $|f(t)| \leq M$ for all t, we must have $C = 0$. It follows that $h(a_0, b_0) = 0$; since (a_0, b_0) was an arbitrary point, h is identically 0 over all of $\mathbb{R}^2$.

A4 Put

$$N = 10^{10^{10^n}} + 10^{10^n} + 10^n - 1.$$

Write $n = 2^m k$ with m a nonnegative integer and k a positive odd integer. For any nonnegative integer j,

$$10^{2^m j} \equiv (-1)^j \pmod{10^{2^m} + 1}.$$

Since $10^n \geq n \geq 2^m \geq m+1$, 10^n is divisible by 2^n and hence by 2^{m+1}, and similarly 10^{10^n} is divisible by 2^{10^n} and hence by 2^{m+1}. It follows that

$$N \equiv 1 + 1 + (-1) + (-1) \equiv 0 \pmod{10^{2^m} + 1}.$$

Since $N \geq 10^{10^n} > 10^n + 1 \geq 10^{2^m} + 1$, it follows that N is composite.

A5 We start with three lemmas.

Lemma 1. *If $\mathbf{x}, \mathbf{y} \in G$ are nonzero orthogonal vectors, then $\mathbf{x} * \mathbf{x}$ is parallel to $\mathbf{y}$.*

Proof. Put $\mathbf{z} = \mathbf{x} \times \mathbf{y} \neq 0$, so that $\mathbf{x}, \mathbf{y}$, and $\mathbf{z} = \mathbf{x} * \mathbf{y}$ are nonzero and mutually orthogonal. Then $\mathbf{w} = \mathbf{x} \times \mathbf{z} \neq 0$, so $\mathbf{w} = \mathbf{x} * \mathbf{z}$ is nonzero and orthogonal to $\mathbf{x}$ and $\mathbf{z}$. However, if $(\mathbf{x}*\mathbf{x}) \times \mathbf{y} \neq 0$, then $\mathbf{w} = \mathbf{x}*(\mathbf{x}*\mathbf{y}) = (\mathbf{x}*\mathbf{x})*\mathbf{y} = (\mathbf{x}*\mathbf{x}) \times \mathbf{y}$ is also orthogonal to $\mathbf{y}$, a contradiction. □

Lemma 2. *If $\mathbf{x} \in G$ is nonzero, and there exists $\mathbf{y} \in G$ nonzero and orthogonal to $\mathbf{x}$, then $\mathbf{x} * \mathbf{x} = 0$.*

Proof. Lemma 1 implies that $\mathbf{x} * \mathbf{x}$ is parallel to both $\mathbf{y}$ and $\mathbf{x} \times \mathbf{y}$, so it must be zero. □

Lemma 3. *If $\mathbf{x}, \mathbf{y} \in G$ commute, then $\mathbf{x} \times \mathbf{y} = 0$.*

Proof. If $\mathbf{x} \times \mathbf{y} \neq 0$, then $\mathbf{x} * \mathbf{y} = \mathbf{x} \times \mathbf{y} = -\mathbf{y} \times \mathbf{x} = -\mathbf{y} * \mathbf{x}$, so $\mathbf{x} * \mathbf{y} \neq \mathbf{y} * \mathbf{x}$. □

We proceed now to the proof. Assume by way of contradiction that there exist $\mathbf{a}, \mathbf{b} \in G$ with $\mathbf{a} \times \mathbf{b} \neq 0$. Put $\mathbf{c} = \mathbf{a} \times \mathbf{b} = \mathbf{a} * \mathbf{b}$, so that $\mathbf{a}, \mathbf{b}, \mathbf{c}$ are nonzero and linearly independent. Let $\mathbf{e}$ be the identity element of G. Since $\mathbf{e}$ commutes with $\mathbf{a}, \mathbf{b}, \mathbf{c}$, by Lemma 3 we have $\mathbf{e} \times \mathbf{a} = \mathbf{e} \times \mathbf{b} = \mathbf{e} \times \mathbf{c} = 0$. Since $\mathbf{a}, \mathbf{b}, \mathbf{c}$ span $\mathbb{R}^3$, $\mathbf{e} \times \mathbf{x} = 0$ for all $\mathbf{x} \in \mathbb{R}^3$, so $\mathbf{e} = 0$.

Since $\mathbf{b}, \mathbf{c}$, and $\mathbf{b} \times \mathbf{c} = \mathbf{b} * \mathbf{c}$ are nonzero and mutually orthogonal, Lemma 2 implies

$$\mathbf{b} * \mathbf{b} = \mathbf{c} * \mathbf{c} = (\mathbf{b} * \mathbf{c}) * (\mathbf{b} * \mathbf{c}) = 0 = \mathbf{e}.$$

Hence $\mathbf{b} * \mathbf{c} = \mathbf{c} * \mathbf{b}$, contradicting Lemma 3 because $\mathbf{b} \times \mathbf{c} \neq 0$. The desired result follows.

A6 **First solution.** Note that the hypotheses on f imply that $f(x) > 0$ for all $x \in [0, +\infty)$, so the integrand is a continuous function of f and the integral makes sense. Rewrite the integral as

$$\int_0^\infty \left(1 - \frac{f(x+1)}{f(x)}\right)\,dx,$$

and suppose by way of contradiction that it converges to a finite limit L. For $n \geq 0$, define the Lebesgue measurable set

$$I_n = \{x \in [0,1] : 1 - \frac{f(x+n+1)}{f(x+n)} \leq 1/2\}.$$

Then $L \geq \sum_{n=0}^\infty \frac{1}{2}(1 - \mu(I_n))$, so the latter sum converges. In particular, there exists a nonnegative integer N for which $\sum_{n=N}^\infty (1 - \mu(I_n)) < 1$; the intersection

$$I = \bigcup_{n=N}^\infty I_n = [0,1] - \bigcap_{n=N}^\infty ([0,1] - I_n)$$

then has positive Lebesgue measure.

By Taylor's theorem with remainder, for $t \in [0, 1/2]$,

$$\begin{aligned}
-\log(1-t) &\leq t + t^2 \sup_{t \in [0,1/2]} \left\{\frac{1}{(1-t)^2}\right\} \\
&= t + \frac{4}{3}t^2 \leq \frac{5}{3}t.
\end{aligned}$$

For each nonnegative integer $n \geq N$, we then have

$$\begin{aligned}
L &\geq \int_N^n \left(1 - \frac{f(x+1)}{f(x)}\right)\,dx \\
&= \sum_{i=N}^{n-1} \int_0^1 \left(1 - \frac{f(x+i+1)}{f(x+i)}\right)\,dx \\
&\geq \sum_{i=N}^{n-1} \int_I \left(1 - \frac{f(x+i+1)}{f(x+i)}\right)\,dx \\
&\geq \frac{3}{5} \sum_{i=N}^{n-1} \int_I \log \frac{f(x+i)}{f(x+i+1)}\,dx \\
&= \frac{3}{5} \int_I \left(\sum_{i=N}^{n-1} \log \frac{f(x+i)}{f(x+i+1)}\right)\,dx \\
&= \frac{3}{5} \int_I \log \frac{f(x+N)}{f(x+n)}\,dx.
\end{aligned}$$

For each $x \in I$, $\log f(x+N)/f(x+n)$ is a strictly increasing unbounded function of n. By the monotone convergence theorem, the integral $\int_I \log(f(x+N)/f(x+n))\,dx$ grows without bound as $n \to +\infty$, a contradiction. Thus the original integral diverges, as desired.

Remark. This solution is motivated by the commonly-used fact that an infinite product $(1+x_1)(1+x_2)\cdots$ converges absolutely if and only if the sum $x_1 + x_2 + \cdots$ converges absolutely. The additional measure-theoretic argument at the beginning is needed because one cannot bound $-\log(1-t)$ by a fixed multiple of t uniformly for all $t \in [0,1)$.

Second solution. (Communicated by Paul Allen.) Let $b > a$ be nonnegative integers. Then

$$\begin{aligned}
\int_a^b \frac{f(x) - f(x+1)}{f(x)}dx &= \sum_{k=a}^{b-1} \int_0^1 \frac{f(x+k) - f(x+k+1)}{f(x+k)}dx \\
&= \int_0^1 \sum_{k=a}^{b-1} \frac{f(x+k) - f(x+k+1)}{f(x+k)}dx \\
&\geq \int_0^1 \sum_{k=a}^{b-1} \frac{f(x+k) - f(x+k+1)}{f(x+a)}dx \\
&= \int_0^1 \frac{f(x+a) - f(x+b)}{f(x+a)}dx.
\end{aligned}$$

Now since $f(x) \to 0$, given a, we can choose an integer $l(a) > a$ for which $f(l(a)) < f(a+1)/2$; then $\frac{f(x+a) - f(x+l(a))}{f(x+a)} \geq 1 - \frac{f(l(a))}{f(a+1)} > 1/2$ for all $x \in [0,1]$. Thus if we define a sequence of integers a_n by $a_0 = 0$, $a_{n+1} = l(a_n)$, then

$$\begin{aligned}
\int_0^\infty \frac{f(x) - f(x+1)}{f(x)}dx &= \sum_{n=0}^\infty \int_{a_n}^{a_{n+1}} \frac{f(x) - f(x+1)}{f(x)}dx \\
&> \sum_{n=0}^\infty \int_0^1 (1/2)dx,
\end{aligned}$$

and the final sum clearly diverges.

Third solution. (By Joshua Rosenberg, communicated by Catalin Zara.) If the original integral converges, then on one hand the integrand $(f(x) - f(x+1))/f(x) = 1 - f(x+1)/f(x)$ cannot tend to 1 as $x \to \infty$. On the other hand, for any $a \geq 0$,

$$\begin{aligned}
0 &< \frac{f(a+1)}{f(a)} \\
&< \frac{1}{f(a)} \int_a^{a+1} f(x)\,dx \\
&= \frac{1}{f(a)} \int_a^\infty (f(x) - f(x+1))\,dx \\
&\leq \int_a^\infty \frac{f(x) - f(x+1)}{f(x)}\,dx,
\end{aligned}$$

and the last expression tends to 0 as $a \to \infty$. Hence by the squeeze theorem, $f(a+1)/f(a) \to 0$ as $a \to \infty$, a contradiction.

B1 **First solution.** No such sequence exists. If it did, then the Cauchy-Schwartz inequality would imply

$$\begin{aligned}
8 &= (a_1^2 + a_2^2 + \cdots)(a_1^4 + a_2^4 + \cdots) \\
&\geq (a_1^3 + a_2^3 + \cdots)^2 = 9,
\end{aligned}$$

contradiction.

Second solution. (Communicated by Catalin Zara.) Suppose that such a sequence exists. If $a_k^2 \in [0,1]$ for all k, then $a_k^4 \leq a_k^2$ for all k, and so

$$4 = a_1^4 + a_2^4 + \cdots \leq a_1^2 + a_2^2 + \cdots = 2,$$

contradiction. There thus exists a positive integer k for which $a_k^2 \geq 1$. However, in this case, for m large, $a_k^{2m} > 2m$ and so $a_1^{2m} + a_2^{2m} + \cdots \neq 2m$.

Third solution. We generalize the second solution to show that for any positive integer k, it is impossible for a sequence $a_1, a_2, \dots$ of complex numbers to satisfy the given conditions in case the series $a_1^k + a_2^k + \cdots$ converges absolutely. This includes the original problem by taking $k = 2$, in which case the series $a_1^2 + a_2^2 + \cdots$ consists of nonnegative real numbers and so converges absolutely if it converges at all.

Since the sum $\sum_{i=1}^\infty |a_i|^k$ converges by hypothesis, we can find a positive integer n such that $\sum_{i=n+1}^\infty |a_i|^k < 1$. For each positive integer d, we then have

$$\left| kd - \sum_{i=1}^n a_i^{kd} \right| \leq \sum_{i=n+1}^\infty |a_i|^{kd} < 1.$$

We thus cannot have $|a_1|, \dots, |a_n| \leq 1$, or else the sum $\sum_{i=1}^n a_i^{kd}$ would be bounded in absolute value by n independently of d. But if we put $r = \max\{|a_1|, \dots, |a_n|\} > 1$, we obtain another contradiction because for any $\epsilon > 0$,

$$\limsup_{d \to \infty} (r - \epsilon)^{-kd} \left| \sum_{i=1}^n a_i^{kd} \right| > 0.$$

For instance, this follows from applying the root test to the rational function

$$\sum_{i=1}^n \frac{1}{1 - a_i^k z} = \sum_{d=0}^\infty \left(\sum_{i=1}^n a_i^{kd} \right) z^d,$$

which has a pole within the circle $|z| \leq r^{-1/k}$. (An elementary proof is also possible.)

Fourth solution. (Communicated by Noam Elkies.) Since $\sum_k a_k^2 = 2$, for each positive integer k we have $a_k^2 \leq 2$ and so $a_k^4 \leq 2a_k^2$, with equality only for $a_k^2 \in \{0, 2\}$. Thus to have $\sum_k a_k^4 = 4$, there must be a single index k for which $a_k^2 = 2$, and the other a_k must all equal 0. But then $\sum_k a_k^{2m} = 2^m \neq 2m$ for any positive integer $m > 2$.

Remark. Manjul Bhargava points out it is easy to construct sequences of complex numbers with the desired property if we drop the condition of absolute convergence. Here is an inductive construction (of which several variants are possible). For $n = 1, 2, \dots$ and $z \in \mathbb{C}$, define the finite sequence

$$s_{n,z} = \left(\frac{1}{z} e^{2\pi i j/n} : j = 0, \dots, n-1 \right).$$

This sequence has the property that for any positive integer j, the sum of the j-th powers of the terms of $s_{n,z}$ equals $1/z^j$ if j is divisible by n and 0 otherwise. Moreover, any partial sum of j-th powers is bounded in absolute value by $n/|z|^j$.

The desired sequence will be constructed as follows. Suppose that we have a finite sequence which has the correct sum of j-th powers for $j = 1, \dots, m$. (For instance, for $m = 1$, we may start with the singleton sequence 1.) We may then extend it to a new sequence which has the correct sum of j-th powers for $j = 1, \dots, m+1$, by appending k copies of $s_{m+1,z}$ for suitable choices of a positive integer k and a complex number z with $|z| < m^{-2}$. This last restriction ensures that the resulting infinite sequence $a_1, a_2, \dots$ is such that for each positive integer m, the series $a_1^m + a_2^m + \cdots$ is convergent (though not absolutely convergent). Its partial sums include a subsequence equal to the constant value m, so the sum of the series must equal m as desired.

B2 The smallest distance is 3, achieved by $A = (0,0)$, $B = (3,0)$, $C = (0,4)$. To check this, it suffices to check that AB cannot equal 1 or 2. (It cannot equal 0 because if two of the points were to coincide, the three points would be collinear.)

The triangle inequality implies that $|AC - BC| \leq AB$, with equality if and only if A, B, C are collinear. If $AB = 1$, we may assume without loss of generality that $A = (0,0)$, $B = (1,0)$. To avoid collinearity, we must have $AC = BC$, but this forces $C = (1/2, y)$ for some $y \in \mathbb{R}$, a contradiction. (One can also treat this case by scaling by a factor of 2 to reduce to the case $AB = 2$, treated in the next paragraph.)

If $AB = 2$, then we may assume without loss of generality that $A = (0,0), B = (2,0)$. The triangle inequality implies $|AC - BC| \in \{0, 1\}$. Also, for $C = (x, y)$, $AC^2 = x^2 + y^2$ and $BC^2 = (2-x)^2 + y^2$ have the same parity; it follows that $AC = BC$. Hence $c = (1, y)$ for some $y \in \mathbb{R}$, so y^2 and $y^2 + 1 = BC^2$ are consecutive perfect squares. This can only happen for $y = 0$, but then A, B, C are collinear, a contradiction again.

Remark. Manjul Bhargava points out that more generally, a *Heronian triangle* (a triangle with integer sides and rational area) cannot have a side of length 1 or 2 (and again it is enough to treat the case of length 2). The original problem follows from this because a triangle whose vertices have integer coordinates has area equal to half an integer (by Pick's formula or the explicit formula for the area as a determinant).

B3 It is possible if and only if $n \geq 1005$. Since

$$1 + \cdots + 2009 = \frac{2009 \times 2010}{2} = 2010 \times 1004.5,$$

for $n \leq 1004$, we can start with an initial distribution in which each box B_i starts with at most $i - 1$ balls (so in particular B_1 is empty). From such a distribution, no moves are possible, so we cannot reach the desired final distribution.

Suppose now that $n \geq 1005$. By the pigeonhole principle, at any time, there exists at least one index i for which the box B_i contains at least i balls. We will describe any such index as being *eligible*. The following sequence of operations then has the desired effect.

(a) Find the largest eligible index i. If $i = 1$, proceed to (b). Otherwise, move i balls from B_i to B_1, then repeat (a).

(b) At this point, only the index $i = 1$ can be eligible (so it must be). Find the largest index j for which B_j is nonempty. If $j = 1$, proceed to (c). Otherwise, move 1 ball from B_1 to B_j; in case this makes j eligible, move j balls from B_j to B_1. Then repeat (b).

(c) At this point, all of the balls are in B_1. For $i = 2, \dots, 2010$, move one ball from B_1 to B_i n times.

After these operations, we have the desired distribution.

B4 **First solution.** The pairs (p, q) satisfying the given equation are those of the form $p(x) = ax + b, q(x) = cx + d$ for $a, b, c, d \in \mathbb{R}$ such that $bc - ad = 1$. We will see later that these indeed give solutions.

Suppose p and q satisfy the given equation; note that neither p nor q can be identically zero. By subtracting the equations

$$p(x)q(x+1) - p(x+1)q(x) = 1$$
$$p(x-1)q(x) - p(x)q(x-1) = 1,$$

we obtain the equation

$$p(x)(q(x+1) + q(x-1)) = q(x)(p(x+1) + p(x-1)).$$

The original equation implies that $p(x)$ and $q(x)$ have no common nonconstant factor, so $p(x)$ divides $p(x+1) + p(x-1)$. Since each of $p(x+1)$ and $p(x-1)$ has the same degree and leading coefficient as p, we must have

$$p(x+1) + p(x-1) = 2p(x).$$

If we define the polynomials $r(x) = p(x+1) - p(x)$, $s(x) = q(x+1) - q(x)$, we have $r(x+1) = r(x)$, and similarly $s(x+1) = s(x)$. Put

$$a = r(0), b = p(0), c = s(0), d = q(0).$$

Then $r(x) = a, s(x) = c$ for all $x \in \mathbb{Z}$, and hence identically; consequently, $p(x) = ax+b, q(x) = cx+d$ for all $x \in \mathbb{Z}$, and hence identically. For p and q of this form,

$$p(x)q(x+1) - p(x+1)q(x) = bc - ad,$$

so we get a solution if and only if $bc - ad = 1$, as claimed.

Second solution. (Communicated by Catalin Zara.) Again, note that p and q must be nonzero. Write

$$p(x) = p_0 + p_1 x + \cdots + p_m x^m$$
$$q(x) = q_0 + q_1 x + \cdots + q_n x^n$$

with $p_m, q_n \neq 0$, so that $m = \deg(p), n = \deg(q)$. It is enough to derive a contradiction assuming that $\max\{m, n\} > 1$, the remaining cases being treated as in the first solution.

Put $R(x) = p(x)q(x+1) - p(x+1)q(x)$. Since $m+n \geq 2$ by assumption, the coefficient of x^{m+n-1} in $R(x)$ must vanish. By easy algebra, this coefficient equals $(m-n)p_m q_n$, so we must have $m = n > 1$.

For $k = 1, \dots, 2m-2$, the coefficient of x^k in $R(x)$ is

$$\sum_{i+j>k, j>i} \left(\binom{j}{k-i} - \binom{i}{k-j} \right) (p_i q_j - p_j q_i)$$

and must vanish. For $k = 2m-2$, the only summand is for $(i, j) = (m-1, m)$, so $p_{m-1} q_m = p_m q_{m-1}$.

Suppose now that $h \geq 1$ and that $p_i q_j = p_j q_i$ is known to vanish whenever $j > i \geq h$. (By the previous paragraph, we initially have this for $h = m-1$.) Take $k = m + h - 2$ and note that the conditions $i + j > h, j \leq m$ force $i \geq h-1$. Using the hypothesis, we see that the only possible nonzero contribution to the coefficient of x^k in $R(x)$ is from $(i, j) = (h-1, m)$. Hence $p_{h-1} q_m = p_m q_{h-1}$; since $p_m, q_m \neq 0$, this implies $p_{h-1} q_j = p_j q_{h-1}$ whenever $j > h-1$.

By descending induction, we deduce that $p_i q_j = p_j q_i$ whenever $j > i \geq 0$. Consequently, $p(x)$ and $q(x)$ are scalar multiples of each other, forcing $R(x) = 0$, a contradiction.

Third solution. (Communicated by David Feldman.) As in the second solution, we note that there are no solutions where $m = \deg(p), n = \deg(q)$ are distinct and $m + n \geq 2$. Suppose p, q form a solution with $m = n \geq 2$. The desired identity asserts that the matrix

$$\begin{pmatrix} p(x) & p(x+1) \\ q(x) & q(x+1) \end{pmatrix}$$

has determinant 1. This condition is preserved by replacing $q(x)$ with $q(x) - tp(x)$ for any real number t. In particular, we can choose t so that $\deg(q(x) - tp(x)) < m$; we then obtain a contradiction.

B5 **First solution.** The answer is no. Suppose otherwise. For the condition to make sense, f must be differentiable. Since f is strictly increasing, we must have $f'(x) \geq 0$ for all x. Also, the function $f'(x)$ is strictly increasing: if $y > x$ then $f'(y) = f(f(y)) > f(f(x)) = f'(x)$. In particular, $f'(y) > 0$ for all $y \in \mathbb{R}$.

For any x_0, if $f(x_0) = b$ and $f'(x_0) = a > 0$, then $f'(x) > a$ for $x > x_0$ and thus $f(x) \geq a(x - x_0) + b$ for $x \geq x_0$. Then either $b < x_0$ or $a = f'(x_0) = f(f(x_0)) = f(b) \geq a(b - x_0) + b$. In the latter case, $b \leq a(x_0 + 1)/(a + 1) \leq x_0 + 1$. We conclude in either case that $f(x_0) \leq x_0 + 1$ for all $x_0 \geq -1$.

It must then be the case that $f(f(x)) = f'(x) \leq 1$ for all x, since otherwise $f(x) > x + 1$ for large x. Now by the above reasoning, if $f(0) = b_0$ and $f'(0) = a_0 > 0$, then $f(x) > a_0 x + b_0$ for $x > 0$. Thus for $x > \max\{0, -b_0/a_0\}$, we have $f(x) > 0$ and $f(f(x)) > a_0 x + b_0$. But then $f(f(x)) > 1$ for sufficiently large x, a contradiction.

Second solution. (Communicated by Catalin Zara.) Suppose such a function exists. Since f is strictly increasing and differentiable, so is $f \circ f = f'$. In particular, f is twice differentiable; also, $f''(x) = f'(f(x))f'(x)$ is the product of two strictly increasing nonnegative functions, so it is also strictly increasing and nonnegative. In particular, we can choose $\alpha > 0$ and $M \in \mathbb{R}$ such that $f''(x) > 4\alpha$ for all $x \geq M$. Then for all $x \geq M$,

$$f(x) \geq f(M) + f'(M)(x - M) + 2\alpha(x - M)^2.$$

In particular, for some $M' > M$, we have $f(x) \geq \alpha x^2$ for all $x \geq M'$.

Pick $T > 0$ so that $\alpha T^2 > M'$. Then for $x \geq T$, $f(x) > M'$ and so $f'(x) = f(f(x)) \geq \alpha f(x)^2$. Now

$$\frac{1}{f(T)} - \frac{1}{f(2T)} = \int_T^{2T} \frac{f'(t)}{f(t)^2}\,dt \geq \int_T^{2T} \alpha\,dt;$$

however, as $T \to \infty$, the left side of this inequality tends to 0 while the right side tends to $+\infty$, a contradiction.

Third solution. (Communicated by Noam Elkies.) Since f is strictly increasing, for some y_0, we can define the inverse function $g(y)$ of f for $y \geq y_0$. Then $x = g(f(x))$, and we may differentiate to find that $1 = g'(f(x))f'(x) = g'(f(x))f(f(x))$. It follows that $g'(y) = 1/f(y)$ for $y \geq y_0$; since g takes arbitrarily large values, the integral $\int_{y_0}^{\infty} dy/f(y)$ must diverge. One then gets a contradiction from any reasonable lower bound on $f(y)$ for y large, e.g., the bound $f(x) \geq \alpha x^2$ from the second solution. (One can also start with a linear lower bound $f(x) \geq \beta x$, then use the integral expression for g to deduce that $g(x) \leq \gamma \log x$, which in turn forces $f(x)$ to grow exponentially.)

B6 For any polynomial $p(x)$, let $[p(x)]A$ denote the $n \times n$ matrix obtained by replacing each entry A_{ij} of A by $p(A_{ij})$; thus $A^{[k]} = [x^k]A$. Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ denote the characteristic polynomial of A. By the Cayley-Hamilton theorem,

$$\begin{aligned} 0 &= A \cdot P(A) \\ &= A^{n+1} + a_{n-1}A^n + \cdots + a_0 A \\ &= A^{[n+1]} + a_{n-1}A^{[n]} + \cdots + a_0 A^{[1]} \\ &= [xp(x)]A. \end{aligned}$$

Thus each entry of A is a root of the polynomial $xp(x)$.

Now suppose $m \geq n + 1$. Then

$$\begin{aligned} 0 &= [x^{m+1-n}p(x)]A \\ &= A^{[m+1]} + a_{n-1}A^{[m]} + \cdots + a_0 A^{[m+1-n]} \end{aligned}$$

since each entry of A is a root of $x^{m+1-n}p(x)$. On the other hand,

$$\begin{aligned} 0 &= A^{m+1-n} \cdot P(A) \\ &= A^{m+1} + a_{n-1}A^m + \cdots + a_0 A^{m+1-n}. \end{aligned}$$

Therefore if $A^k = A^{[k]}$ for $m + 1 - n \leq k \leq m$, then $A^{m+1} = A^{[m+1]}$. The desired result follows by induction on m.

Remark. David Feldman points out that the result is best possible in the following sense: there exist examples of $n \times n$ matrices A for which $A^k = A^{[k]}$ for $k = 1, \ldots, n$ but $A^{n+1} \neq A^{[n+1]}$.