# Solutions to the 75th William Lowell Putnam Mathematical Competition
# Saturday, December 6, 2014

Kiran Kedlaya and Lenny Ng

A1 The coefficient of $x^n$ in the Taylor series of $(1-x+x^2)e^x$ for $n=0,1,2$ is $1,0,\frac{1}{2}$, respectively. For $n \geq 3$, the coefficient of $x^n$ is

$$\begin{aligned} \frac{1}{n!} - \frac{1}{(n-1)!} + \frac{1}{(n-2)!} &= \frac{1-n+n(n-1)}{n!} \\ &= \frac{n-1}{n(n-2)!}. \end{aligned}$$

If $n-1$ is prime, then the lowest-terms numerator is clearly either 1 or the prime $n-1$ (and in fact the latter, since $n-1$ is relatively prime to $n$ and to $(n-2)!$). If $n-1$ is composite, either it can be written as $ab$ for some $a \neq b$, in which case both $a$ and $b$ appear separately in $(n-2)!$ and so the numerator is 1, or $n-1=p^2$ for some prime $p$, in which case $p$ appears in $(n-2)!$ and so the numerator is either 1 or $p$. (In the latter case, the numerator is actually 1 unless $p=2$, as in all other cases both $p$ and $2p$ appear in $(n-2)!$.)

A2 Let $v_1,\dots,v_n$ denote the rows of $A$. The determinant is unchanged if we replace $v_n$ by $v_n - v_{n-1}$, and then $v_{n-1}$ by $v_{n-1}-v_{n-2}$, and so forth, eventually replacing $v_k$ by $v_k - v_{k-1}$ for $k \geq 2$. Since $v_{k-1}$ and $v_k$ agree in their first $k-1$ entries, and the $k$-th entry of $v_k - v_{k-1}$ is $\frac{1}{k} - \frac{1}{k-1}$, the result of these row operations is an upper triangular matrix with diagonal entries $1, \frac{1}{2}-1, \frac{1}{3}-\frac{1}{2}, \dots, \frac{1}{n}-\frac{1}{n-1}$. The determinant is then

$$\begin{aligned} \prod_{k=2}^n \left( \frac{1}{k} - \frac{1}{k-1} \right) &= \prod_{k=2}^n \left( \frac{-1}{k(k-1)} \right) \\ &= \frac{(-1)^{n-1}}{(n-1)!n!}. \end{aligned}$$

Note that a similar calculation can be made whenever $A$ has the form $A_{ij} = \min\{a_i, a_j\}$ for any monotone sequence $a_1,\dots,a_n$. Note also that the standard Gaussian elimination algorithm leads to the same upper triangular matrix, but the nonstandard order of operations used here makes the computations somewhat easier.

**Remark:** The inverse of $A$ can be identified explicitly: for $n \geq 2$, it is the matrix $B$ given by

$$B_{ij} = \begin{cases} -1 & i=j=1 \\ -2i^2 & 1 < i = j < n \\ -(n-1)n & i=j=n \\ ij & |i-j| = 1 \\ 0 & \text{otherwise.} \end{cases}$$

For example, for $n=5$,

$$B = \begin{pmatrix} -1 & 2 & 0 & 0 & 0 \\ 2 & -8 & 6 & 0 & 0 \\ 0 & 6 & -18 & 12 & 0 \\ 0 & 0 & 12 & -32 & 20 \\ 0 & 0 & 0 & 20 & -20 \end{pmatrix}.$$

Let $C$ denote the matrix obtained from $B$ by replacing the bottom-right entry with $-2n^2$ (for consistency with the rest of the diagonal). Expanding in minors along the bottom row produces a second-order recursion for $\det(C)$ solving to $\det(C) = (-1)^n (n!)^2$; a similar expansion then yields $\det(B) = (-1)^{n-1} n!(n-1)!$.

**Remark:** This problem and solution are due to one of us (Kedlaya). The statement appears in the comments on sequence A010790 (i.e., the sequence $(n-1)!n!$) in the On-Line Encyclopedia of Integer Sequences (`http://oeis.org`), attributed to Benoit Cloitre in 2002.

A3 **First solution:** Using the identity

$$(x+x^{-1})^2 - 2 = x^2 + x^{-2},$$

we may check by induction on $k$ that $a_k = 2^{2^k} + 2^{-2^k}$; in particular, the product is absolutely convergent. Using the identities

$$\begin{aligned} \frac{x^2+1+x^{-2}}{x+1+x^{-1}} &= x-1+x^{-1}, \\ \frac{x^2-x^{-2}}{x-x^{-1}} &= x+x^{-1}, \end{aligned}$$

we may telescope the product to obtain

$$\begin{aligned} \prod_{k=0}^\infty \left( 1 - \frac{1}{a_k} \right) &= \prod_{k=0}^\infty \frac{2^{2^k} - 1 + 2^{-2^k}}{2^{2^k} + 2^{-2^k}} \\ &= \prod_{k=0}^\infty \frac{2^{2^{k+1}} + 1 + 2^{-2^{k+1}}}{2^{2^k} + 1 + 2^{-2^k}} \cdot \frac{2^{2^k} - 2^{-2^k}}{2^{2^{k+1}} - 2^{2^{-k-1}}} \\ &= \frac{2^{2^0} - 2^{-2^0}}{2^{2^0} + 1 + 2^{-2^0}} = \frac{3}{7}. \end{aligned}$$

**Second solution:** (by Catalin Zara) In this solution, we do not use the explicit formula for $a_k$. We instead note first that the $a_k$ form an increasing sequence which cannot approach a finite limit (since the equation $L = L^2-2$ has no real solution $L > 2$), and is thus unbounded. Using the identity

$$a_{k+1} + 1 = (a_k - 1)(a_k + 1),$$

one checks by induction on $n$ that

$$\prod_{k=0}^{n}\left(1-\frac{1}{a_k}\right)=\frac{2}{7}\,\frac{a_{n+1}+1}{a_0a_1\cdots a_n}.$$

Using the identity

$$a_{n+2}^2-4=a_{n+1}^4-4a_{n+1}^2,$$

one also checks by induction on $n$ that

$$a_0a_1\cdots a_n=\frac{2}{3}\sqrt{a_{n+1}^2-4}.$$

Hence

$$\prod_{k=0}^{n}\left(1-\frac{1}{a_k}\right)=\frac{3}{7}\,\frac{a_{n+1}+1}{\sqrt{a_{n+1}^2-4}}$$

tends to $\frac{3}{7}$ as $a_{n+1}$ tends to infinity, hence as $n$ tends to infinity.

A4 **First solution:** Let $a_n=P(X=n)$; we want the minimum value for $a_0$. If we write $S_k=\sum_{n=1}^{\infty}n^k a_n$, then the given expectation values imply that $S_1=1$, $S_2=2$, $S_3=5$. Now define $f(n)=11n-6n^2+n^3$, and note that $f(1)=f(2)=f(3)=6$ and $f(n)>0$ for $n\geq 4$; thus $4=11S_1-6S_2+S_3=\sum_{n=1}^{\infty}f(n)a_n\geq 6(a_1+a_2+a_3)$. It follows that $a_0\geq 1-a_1-a_2-a_3\geq\frac{1}{3}$. Equality is achieved when $a_0=\frac{1}{3}$, $a_1=\frac{1}{2}$, $a_3=\frac{1}{6}$, and $a_n=0$ for all other $n$, and so the answer is $\frac{1}{3}$.

**Second solution:** (by Tony Qiao) Define the *probability generating function* of $P$ as the power series

$$G(z)=\sum_{n=0}^{\infty}P(x=n)z^n.$$

We compute that $G(1)=G'(1)=G''(1)=G'''(1)=1$. By Taylor's theorem with remainder, for any $x\in[0,1]$, there exists $c\in[x,1]$ such that

$$G(x)=1+(x-1)+\frac{(x-1)^2}{2!}+\frac{(x-1)^3}{3!}+\frac{G''''(c)}{4!}(x-1)^4.$$

In particular, $G(0)=\frac{1}{3}+\frac{1}{24}G''''(c)$ for some $c\in[0,1]$. However, since $G$ has nonnegative coefficients and $c\geq 0$, we must have $G''''(c)\geq 0$, and so $G(0)\geq\frac{1}{3}$. As in the first solution, we see that this bound is best possible.

A5 **First solution:** Suppose to the contrary that there exist positive integers $i\neq j$ and a complex number $z$ such that $P_i(z)=P_j(z)=0$. Note that $z$ cannot be a nonnegative real number or else $P_i(z),P_j(z)>0$; we may put $w=z^{-1}\neq 0,1$. For $n\in\{i+1,j+1\}$ we compute that

$$w^n=nw-n+1,\qquad \overline{w}^n=n\overline{w}-n+1;$$

note crucially that these equations also hold for $n\in\{0,1\}$. Therefore, the function $f:[0,+\infty)\to\mathbb{R}$ given by

$$f(t)=|w|^{2t}-t^2\,|w|^2+2t(t-1)\mathrm{Re}(w)-(t-1)^2$$

satisfies $f(t)=0$ for $t\in\{0,1,i+1,j+1\}$. On the other hand, for all $t\geq 0$ we have

$$f'''(t)=(2\log|w|)^3\,|w|^{2t}>0,$$

so by Rolle's theorem, the equation $f^{(3-k)}(t)=0$ has at most $k$ distinct solutions for $k=0,1,2,3$. This yields the desired contradiction.

**Remark:** By similar reasoning, an equation of the form $e^x=P(x)$ in which $P$ is a real polynomial of degree $d$ has at most $d+1$ real solutions. This turns out to be closely related to a concept in mathematical logic known as *o-minimality*, which in turn has deep consequences for the solution of Diophantine equations.

**Second solution:** (by Noam Elkies) We recall a result commonly known as the *Eneström-Kakeya theorem.*

**Lemma 1.** *Let*

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

*be a polynomial with real coefficients such that* $0<a_0\leq a_1\leq\cdots\leq a_n$. *Then every root* $z\in\mathbb{C}$ *of* $f$ *satisfies* $|z|\leq 1$.

*Proof.* If $f(z)=0$, then we may rearrange the equality $0=f(z)(z-1)$ to obtain

$$a_nz^{n+1}=(a_n-a_{n-1})z^n+\cdots+(a_1-a_0)z+a_0.$$

But if $|z|>1$, then

$$|a_nz^{n+1}|\leq(|a_n-a_{n-1}|+\cdots+|a_1-a_0|)|z|^n\leq|a_nz^n|,$$

contradiction. □

**Corollary 2.** *Let*

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

*be a polynomial with positive real coefficients. Then every root* $z\in\mathbb{C}$ *of* $f$ *satisfies* $r\leq|z|\leq R$ *for*

$$\begin{aligned} r&=\min\{a_0/a_1,\dots,a_{n-1}/a_n\}\\ R&=\max\{a_0/a_1,\dots,a_{n-1}/a_n\}.\end{aligned}$$

*Proof.* The bound $|z|\leq R$ follows by applying the lemma to the polynomial $f(x/R)$. The bound $|z|\geq r$ follows by applying the lemma to the reverse of the polynomial $f(x/r)$. □

Suppose now that $P_i(z)=P_j(z)=0$ for some $z\in\mathbb{C}$ and some integers $i<j$. We clearly cannot have $j=i+1$, as then $P_i(0)\neq 0$ and so $P_j(z)-P_i(z)=(i+1)z^i\neq 0$; we thus have $j-i\geq 2$. By applying Corollary 2 to $P_i(x)$, we see that $|z|\leq 1-\frac{1}{i}$. On the other hand, by applying Corollary 2 to $(P_j(x)-P_i(x))/x^{i-1}$, we see that $|z|\geq 1-\frac{1}{i+2}$, contradiction.

**Remark:** Elkies also reports that this problem is his submission, dating back to 2005 and arising from work of Joe Harris. It dates back further to Example 3.7 in:

Hajime Kaji, On the tangentially degenerate curves, *J. London Math. Soc. (2)* **33** (1986), 430–440, in which the second solution is given.

**Remark:** Elkies points out a mild generalization which may be treated using the first solution but not the second: for integers $a < b < c < d$ and $z \in \mathbb{C}$ which is neither zero nor a root of unity, the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ z^a & z^b & z^c & z^d \end{pmatrix}$$

has rank 3 (the problem at hand being the case $a = 0, b = 1, c = i+1, d = j+1$).

**Remark:** It seems likely that the individual polynomials $P_k(x)$ are all irreducible, but this appears difficult to prove.

**Third solution:** (by David Feldman) Note that

$$P_n(x)(1-x) = 1 + x + \cdots + x^{n-1} - nx^n.$$

If $|z| \geq 1$, then

$$n|z|^n \geq |z|^{n-1} + \cdots + 1 \geq |z^{n-1} + \cdots + 1|,$$

with the first equality occurring only if $|z| = 1$ and the second equality occurring only if $z$ is a positive real number. Hence the equation $P_n(z)(1-z) = 0$ has no solutions with $|z| \geq 1$ other than the trivial solution $z = 1$. Since

$$P_n(x)(1-x)^2 = 1 - (n+1)x^n + nx^{n+1},$$

it now suffices to check that the curves

$$C_n = \{z \in \mathbb{C} : 0 < |z| < 1, |z|^n \, |n+1-zn| = 1\}$$

are pairwise disjoint as $n$ varies over positive integers.

Write $z = u + iv$; we may assume without loss of generality that $v \geq 0$. Define the function

$$E_z(n) = n \log|z| + \log|n+1-zn|.$$

One computes that for $n \in \mathbb{R}$, $E_z''(n) < 0$ if and only if

$$\frac{u-v-1}{(1-u)^2+v^2} < n < \frac{u+v-1}{(1-u)^2+v^2}.$$

In addition, $E_z(0) = 0$ and

$$E_z'(0) = \frac{1}{2}\log(u^2+v^2) + (1-u) \geq \log(u) + 1 - u \geq 0$$

since $\log(u)$ is concave. From this, it follows that the equation $E_z(n) = 0$ can have at most one solution with $n > 0$.

**Remark:** The reader may notice a strong similarity between this solution and the first solution. The primary difference is we compute that $E_z'(0) \geq 0$ instead of discovering that $E_z(-1) = 0$.

**Remark:** It is also possible to solve this problem using a $p$-adic valuation on the field of algebraic numbers in place of the complex absolute value; however, this leads to a substantially more complicated solution. In lieu of including such a solution here, we refer to the approach described by Victor Wang here: `http://www.artofproblemsolving.com/Forum/viewtopic.php?f=80&t=616731`.

A6 The largest such $k$ is $n^n$. We first show that this value can be achieved by an explicit construction. Let $e_1, \dots, e_n$ be the standard basis of $\mathbb{R}^n$. For $i_1, \dots, i_n \in \{1, \dots, n\}$, let $M_{i_1,\dots,i_n}$ be the matrix with row vectors $e_{i_1}, \dots, e_{i_n}$, and let $N_{i_1,\dots,i_n}$ be the transpose of $M_{i_1,\dots,i_n}$. Then $M_{i_1,\dots,i_n} N_{j_1,\dots,j_n}$ has $k$-th diagonal entry $e_{i_k} \cdot e_{j_k}$, proving the claim.

We next show that for any families of matrices $M_i, N_j$ as described, we must have $k \leq n^n$. Let $V$ be the *$n$-fold tensor product* of $\mathbb{R}^n$, i.e., the vector space with orthonormal basis $e_{i_1} \otimes \cdots \otimes e_{i_n}$ for $i_1, \dots, i_n \in \{1, \dots, n\}$. Let $m_i$ be the tensor product of the rows of $M_i$; that is,

$$m_i = \sum_{i_1,\dots,i_n=1}^{n} (M_i)_{1,i_1} \cdots (M_i)_{n,i_n} e_{i_1} \otimes \cdots \otimes e_{i_n}.$$

Similarly, let $n_j$ be the tensor product of the columns of $N_j$. One computes easily that $m_i \cdot n_j$ equals the product of the diagonal entries of $M_i N_j$, and so vanishes if and only if $i \neq j$. For any $c_i \in \mathbb{R}$ such that $\sum_i c_i m_i = 0$, for each $j$ we have

$$0 = \left(\sum_i c_i m_i\right) \cdot n_j = \sum_i c_i (m_i \cdot n_j) = c_j.$$

Therefore the vectors $m_1, \dots, m_k$ in $V$ are linearly independent, implying $k \leq n^n$ as desired.

**Remark:** Noam Elkies points out that similar argument may be made in the case that the $M_i$ are $m \times n$ matrices and the $N_j$ are $n \times m$ matrices.

B1 These are the integers with no 0's in their usual base 10 expansion. If the usual base 10 expansion of $N$ is $d_k 10^k + \cdots + d_0 10^0$ and one of the digits is 0, then there exists an $i \leq k-1$ such that $d_i = 0$ and $d_{i+1} > 0$; then we can replace $d_{i+1}10^{i+1} + (0)10^i$ by $(d_{i+1} - 1)10^{i+1} + (10)10^i$ to obtain a second base 10 over-expansion.

We claim conversely that if $N$ has no 0's in its usual base 10 expansion, then this standard form is the unique base 10 over-expansion for $N$. This holds by induction on the number of digits of $N$: if $1 \leq N \leq 9$, then the result is clear. Otherwise, any base 10 over-expansion $N = d_k 10^k + \cdots + d_1 10 + d_0 10^0$ must have $d_0 \equiv N \pmod{10}$, which uniquely determines $d_0$ since $N$ is not a multiple of 10; then $(N - d_0)/10$ inherits the base 10 over-expansion $d_k 10^{k-1} + \cdots + d_1 10^0$, which must be unique by the induction hypothesis.

**Remark:** Karl Mahlburg suggests an alternate proof of uniqueness (due to Shawn Williams): write the usual expansion $N = d_k 10^k + \cdots + d_0 10^0$ and suppose $d_i \neq 0$ for all $i$. Let $M = c_l 10^l + \cdots + c_0 10^0$ be an over-expansion with at least one 10. To have $M = N$, we must have $l \leq k$; we may pad the expansion of $M$ with zeroes to force $l = k$. Now define $e_i = c_i - d_i$; since $1 \leq d_i \leq 9$ and $0 \leq c_i \leq 10$, we have $0 \leq |e_i| \leq 9$. Moreover, there exists at least one index $i$ with $e_i \neq 0$, since any index for which $c_i = 10$ has this property. But if $i$ is the largest such index, we have

$$\begin{aligned} 10^i \leq |e_i 10^i| &= \left| -\sum_{j=0}^{i-1} e_i 10^i \right| \\ &\leq \sum_{j=0}^{i-1} |e_i| 10^i| \leq 9 \cdot 10^{i-1} + \cdots + 9 \cdot 10^0, \end{aligned}$$

a contradiction.

B2 In all solutions, we assume that the function $f$ is integrable.

**First solution:** Let $g(x)$ be 1 for $1 \leq x \leq 2$ and $-1$ for $2 < x \leq 3$, and define $h(x) = g(x) - f(x)$. Then $\int_1^3 h(x)\,dx = 0$ and $h(x) \geq 0$ for $1 \leq x \leq 2$, $h(x) \leq 0$ for $2 < x \leq 3$. Now

$$\begin{aligned} \int_1^3 \frac{h(x)}{x}\,dx &= \int_1^2 \frac{|h(x)|}{x}\,dx - \int_2^3 \frac{|h(x)|}{x}\,dx \\ &\geq \int_1^2 \frac{|h(x)|}{2}\,dx - \int_2^3 \frac{|h(x)|}{2}\,dx = 0, \end{aligned}$$

and thus $\int_1^3 \frac{f(x)}{x}\,dx \leq \int_1^3 \frac{g(x)}{x}\,dx = 2\log 2 - \log 3 = \log \frac{4}{3}$. Since $g(x)$ achieves the upper bound, the answer is $\log \frac{4}{3}$.

**Reformulation:** (by Karl Mahlburg and Karthik Adimurthi) Since $f$ is integrable, it can be expressed in terms of the Hadamard basis

$$H_0(x) = \begin{cases} 1 & x \in [1,2) \\ -1 & x \in [2,3] \\ 0 & x \notin [1,3] \end{cases}$$
$$H_{n+1}(x) = H_n(2(x-1)+1) + H_n(2(x-2)+1).$$

More precisely, we have $f(x) = \sum_n c_n H_n(x)$ for some $c_n$ with $|c_0| + |c_1| + |\cdots| \leq 1$. Let $g_n = \int_1^3 (H_n(x)/x)\,dx$; it is easy to show that the $g_n$ are strictly decreasing in $n$. Thus

$$\int_1^3 (f(x)/x)dx = c_0 g_0 + c_1 g_1 + \cdots \leq 1 \cdot g_0 = \log \frac{4}{3}.$$

**Second solution:** (Art of Problem Solving, user `libra_gold`) Define the function $F(x) = \int_1^x f(t)\,dt$ for $1 \leq x \leq 3$; then $F(1) = F(3) = 0$ and $F(x) \leq \min\{x-1, 3-x\}$. Using integration by parts, we obtain

$$\begin{aligned} \int_1^3 \frac{f(x)}{x}\,dx &= \int_1^3 \frac{F(x)}{x^2}\,dx \\ &\leq \int_1^2 \frac{x-1}{x^2}\,dx + \int_2^3 \frac{3-x}{x^2}\,dx \\ &= \log \frac{4}{3}. \end{aligned}$$

(Some minor adjustment is needed to make this completely rigorous, e.g., approximating $f$ uniformly by continuous functions.)

B3 **First solution:** Assume by way of contradiction that $A$ has rank at most 1; in this case, we can find rational numbers $a_1, \dots, a_m$, $b_1, \dots, b_n$ such that $A_{ij} = a_i b_j$ for all $i, j$. By deleting rows or columns, we may reduce to the case where the $a_i$'s and $b_j$'s are all nonzero.

Recall that any nonzero rational number $q$ has a unique prime factorization

$$q = \pm 2^{c_1} 3^{c_2} 5^{c_3} \cdots$$

with exponents in $\mathbb{Z}$. Set

$$c(q) = (c_1, c_2, c_3, \dots).$$

Note that $|a_i b_j|$ is prime if and only if $c(a_i) + c(b_j)$ has one entry equal to 1 and all others equal to 0. The condition that $m+n$ distinct primes appear in the matrix implies that the vector space

$$\left\{ \sum_i x_i c(a_i) + \sum_j y_i c(b_j) : x_i, y_j \in \mathbb{R}, \sum_i x_i = \sum_j y_j \right\}$$

contains a linearly independent set of size $m+n$. But that space evidently has dimension at most $m+n-1$, contradiction.

**Second solution:** In this solution, we use standard terminology of graph theory, considering only simple undirected graphs (with no self-loops or multiple edges). We first recall the quick induction proof that that a graph on $k$ vertices with no cycles contains at most $k-1$ edges: for $k = 1$, the claim is trivially true because there can be no edges. For $k > 1$, choose any vertex $v$ and let $d$ be its degree. Removing the vertex $v$ and the edges incident to it leaves a disjoint union of $d$ different graphs, each having no cycles. If the numbers of vertices in these graphs are $k_1, \dots, k_d$, by induction the total number of edges in the original graph is at most $(k_1 - 1) + \cdots + (k_d - 1) + d = k - 1$.

Returning to the original problem, suppose that $A$ has rank at most 1. Draw a bipartite graph whose vertices correspond to the rows and columns of $A$, with an edge joining a particular row and column if the entry where they intersect has prime absolute value. By the previous paragraph, this graph must contain a cycle. Since the graph is bipartite, this cycle must be of length $2k$ for some integer $k \geq 2$ (we cannot have $k = 1$ because the graph has no repeated edges). Without loss of generality, we may assume that the cycle consists of row 1, column 1, row 2, column 2, and so on. There must then exist distinct prime numbers $p_1, \dots, p_{2k}$ such that

$$|A_{11}| = p_1, |A_{21}| = p_2, \dots, |A_{kk}| = p_{2k-1}, |A_{1k}| = p_{2k}.$$

However, since $A$ has rank 1, the $2 \times 2$ minor $A_{11}A_{ij} - A_{i1}A_{1j}$ must vanish for all $i, j$. If we put $r_i = |A_{i1}|$ and $c_j = |A_{ij}/A_{11}|$, we have

$$\begin{aligned} p_1 \cdots p_{2k} &= (r_1c_1)(r_2c_1)\cdots(r_kc_k)(r_1c_k) \\ &= (r_1c_1\cdots r_kc_k)^2, \end{aligned}$$

which contradicts the existence of unique prime factorizations for positive rational numbers: the prime $p_1$ occurs with exponent 1 on the left, but with some even exponent on the right. This contradiction completes the proof.

B4 Define the polynomial $f_n(x) = \sum_{k=0}^n 2^{k(n-k)}x^k$. Since

$$f_1(x) = 1 + x, f_2(x) = 1 + 2x + x^2 = (1+x)^2,$$

the claim holds for for $n = 1, 2$. For $n \geq 3$, we show that the quantities

$$f_n(-2^{-n}), f_n(-2^{-n+2}), \dots, f_n(-2^n)$$

alternate in sign; by the intermediate value theorem, this will imply that $f_n$ has a root in each of the $n$ intervals $(-2^{-n}, -2^{-n+2}), \dots, (-2^{n-2}, -2^n)$, forcing $f_n$ to have as many distinct real roots as its degree.

For $j \in \{0, \dots, n\}$, group the terms of $f_n(x)$ as

$$\begin{aligned} &\cdots \\ &+ 2^{(j-5)(n-j+5)}x^{j-5} + 2^{(j-4)(n-j+4)}x^{j-4} \\ &+ 2^{(j-3)(n-j+3)}x^{j-3} + 2^{(j-2)(n-j+2)}x^{j-2} \\ &+ 2^{(j-1)(n-j+1)}x^{j-1} + 2^{j(n-j)}x^j + 2^{(j+1)(n-j-1)}x^{j+1} \\ &+ 2^{(j+2)(n-j-2)}x^{j+2} + 2^{(j+3)(n-j-3)}x^{j+3} \\ &+ 2^{(j+4)(n-j-4)}x^{j+4} + 2^{(j+5)(n-j-5)}x^{j+5} \\ &\cdots. \end{aligned}$$

Depending on the parity of $j$ and of $n - j$, there may be a single monomial left on each end. When evaluating at $x = -2^{-n+2j}$, the trinomial evaluates to 0. In the binomials preceding the trinomial, the right-hand term dominates, so each of these binomials contributes with the sign of $x^{j-2k}$, which is $(-1)^j$. In the binomials following the trinomial, the left-hand term dominates, so again the contribution has sign $(-1)^j$.

Any monomials which are left over on the ends also contribute with sign $(-1)^j$. Since $n \geq 3$, there exists at least one contribution other than the trinomial, so $f_n(-2^{-n+2j})$ has overall sign $(-1)^j$, proving the claimed alternation.

**Remark:** Karl Mahlburg suggests an alternate interpretation of the preceding algebra: write $2^{-j^2}f_n(2^{-n+2j})$ as

$$\begin{aligned} &2^{-j^2} - 2^{-(j-1)^2} + \cdots + (-1)^{j-1}2^{-1} + (-1)^j2^{-1} \\ &+ (-1)^j2^{-1} + (-1)^{j+1}2^{-1} + (-1)^{j+2}2^{-2} + \cdots, \end{aligned}$$

where the two central terms $(-1)^j2^{-1}$ arise from splitting the term arising from $x^j$. Then each row is an alternating series whose sum carries the sign of $(-1)^j$ unless it has only two terms. Since $n \geq 3$, one of the two sums is forced to be nonzero.

**Remark:** One of us (Kedlaya) received this problem and solution from David Speyer in 2009 and submitted it to the problem committee.

B5 We show that Patniss wins if $p = 2$ and Keeta wins if $p > 2$ (for all $n$). We first analyze the analogous game played using an arbitrary finite group $G$. Recall that for any subset $S$ of $G$, the set of elements $g \in G$ which commute with all elements of $S$ forms a subgroup $Z(S)$ of $G$, called the *centralizer* (or *commutant*) of $S$. At any given point in the game, the set $S$ of previously chosen elements is contained in $Z(S)$. Initially $S = \emptyset$ and $Z(S) = G$; after each turn, $S$ is increased by one element and $Z(S)$ is replaced by a subgroup. In particular, if the order of $Z(S)$ is odd at some point, it remains odd thereafter; conversely, if $S$ contains an element of even order, then the order of $Z(S)$ remains even thereafter. Therefore, any element $g \in G$ for which $Z(\{g\})$ has odd order is a winning first move for Patniss, while any other first move by Patniss loses if Keeta responds with some $h \in Z(\{g\})$ of even order (e.g., an element of a 2-Sylow subgroup of $Z(\{g\})$). In both cases, the win is guaranteed no matter what moves follow.

Now let $G$ be the group of invertible $n \times n$ matrices with entries in $\mathbb{Z}/p\mathbb{Z}$. If $p > 2$, then $Z(S)$ will always contain the scalar matrix $-1$ of order 2, so the win for Keeta is guaranteed. (An explicit winning strategy is to answer any move $g$ with the move $-g$.)

If $p = 2$, we establish the existence of $g \in G$ such that $Z(\{g\})$ has odd order using the existence of an irreducible polynomial $P(x)$ of degree $n$ over $\mathbb{Z}/p\mathbb{Z}$ (see remark). We construct an $n \times n$ matrix over $\mathbb{Z}/p\mathbb{Z}$ with characteristic polynomial $P(x)$ by taking the *companion matrix* of $P(x)$: write $P(x) = x^n + P_{n-1}x^{n-1} + \cdots + P_0$ and set

$$g = \begin{pmatrix} 0 & 0 & \cdots & 0 & -P_0 \\ 1 & 0 & \cdots & 0 & -P_1 \\ 0 & 1 & \cdots & 0 & -P_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -P_{n-1} \end{pmatrix}.$$

In particular, $\det(g) = (-1)^nP_0 \neq 0$, so $g \in G$. Over an algebraic closure of $\mathbb{Z}/p\mathbb{Z}$, $g$ becomes diagonalizable with distinct eigenvalues, so any matrix commuting with $g$ must also be diagonalizable, and hence of odd order. In particular, $Z(\{g\})$ is of odd order, so Patniss has a winning strategy.

**Remark:** It can be shown that in the case $p = 2$, the only elements $g \in G$ for which $Z(\{g\})$ has odd order are those for which $g$ has distinct eigenvalues: in any other case, $Z(\{g\})$ contains a subgroup isomorphic to the group of $k \times k$ invertible matrices over $\mathbb{Z}/2\mathbb{Z}$ for some $k > 1$, and this group has order $(2^k - 1)(2^k - 2) \cdots (2^k - 2^{k-1})$.

**Remark:** We sketch two ways to verify the existence of an irreducible polynomial of degree $n$ over $\mathbb{Z}/p\mathbb{Z}$ for any positive integer $n$ and any prime number $p$. One is to use Möbius inversion to count the number of irreducible polynomials of degree $n$ over $\mathbb{Z}/p\mathbb{Z}$ and then give a positive lower bound for this count. The other is to first establish the existence of a finite field $\mathbb{F}$ of cardinality $p^n$, e.g., as the set of roots of the polynomial $x^{p^n} - 1$ inside a splitting field, and then take the minimal polynomial of a nonzero element of $\mathbb{F}$ over $\mathbb{Z}/p\mathbb{Z}$ which is a primitive $(p^n - 1)$-st root of unity in $\mathbb{F}$ (which exist because the multiplicative group of $\mathbb{F}$ contains at most one cyclic subgroup of any given order). One might be tempted to apply the primitive element theorem for $\mathbb{F}$ over $\mathbb{Z}/p\mathbb{Z}$, but in fact one of the preceding techniques is needed in order to verify this result for finite fields, as the standard argument that "most" elements of the upper field are primitive breaks down for finite fields.

One may also describe the preceding analysis in terms of an identification of $\mathbb{F}$ as a $\mathbb{Z}/p\mathbb{Z}$-vector space with the space of column vectors of length $n$. Under such an identification, if we take $g$ to be an element of $\mathbb{F} - \{0\}$ generating this group, then any element of $Z(\{g\})$ commutes with all of $\mathbb{F} - \{0\}$ and hence must define an $\mathbb{F}$-linear endomorphism of $\mathbb{F}$. Any such endomorphism is itself multiplication by an element of $\mathbb{F}$, so $Z(\{g\})$ is identified with the multiplicative group of $\mathbb{F}$, whose order is the odd number $2^n - 1$.

B6 Let us say that a linear function $g$ on an interval is *integral* if it has the form $g(x) = a + bx$ for some $a, b \in \mathbb{Z}$, and that a piecewise linear function is *integral* if on every interval where it is linear, it is also integral.

For each positive integer $n$, define the $n$-th *Farey sequence* $F_n$ as the sequence of rational numbers in $[0,1]$ with denominators at most $n$. It is easily shown by induction on $n$ that any two consecutive elements $\frac{r}{s}, \frac{r'}{s'}$ of $F_n$, written in lowest terms, satisfy $\gcd(s,s') = 1$, $s + s' > n$, and $r's - rs' = 1$. Namely, this is obvious for $n = 1$ because $F_1 = \frac{0}{1}, \frac{1}{1}$. To deduce the claim for $F_n$ from the claim for $F_{n-1}$, let $\frac{r}{s}, \frac{r'}{s'}$ be consecutive elements of $F_{n-1}$. If $s + s' = n$, then for $m = r + r'$ we have $\frac{r}{s} < \frac{m}{n} < \frac{r'}{s'}$ and the pairs $\frac{r}{s}, \frac{m}{n}$ and $\frac{m}{n}, \frac{r'}{s'}$ satisfy the desired conditions. Conversely, if $s + s' > n$, then we cannot have $\frac{r}{s} < \frac{m}{n} < \frac{r'}{s'}$ for $a \in \mathbb{Z}$, as this yields the contradiction

$$n = (ms - nr)s' + (r'n - ms') \geq s + s' > n;$$

hence $\frac{r}{s}, \frac{r'}{s'}$ remain consecutive in $F_n$.

Let $f_n : [0,1] \to \mathbb{R}$ be the piecewise linear function which agrees with $f$ at each element of $F_n$ and is linear between any two consecutive elements of $F_n$. Between any two consecutive elements $\frac{r}{s}, \frac{r'}{s'}$ of $F_n$, $f_n$ coincides with some linear function $a + bx$. Since $sf(\frac{r}{s}), s'f(\frac{r'}{s'}) \in \mathbb{Z}$, we deduce first that

$$b = ss'(f(\frac{r'}{s'}) - f(\frac{r}{s}))$$

is an integer of absolute value at most $K$, and second that both $as = sf(\frac{r}{s}) - br$ and $as' = s'f(\frac{r'}{s'}) - br'$ are integral. It follows that $f_n$ is integral.

We now check that if $n > 2K$, then $f_n = f_{n-1}$. For this, it suffices to check that for any consecutive elements $\frac{r}{s}, \frac{m}{n}, \frac{r'}{s'}$ in $F_n$, the linear function $a_0 + b_0 x$ matching $f_{n-1}$ from $\frac{r}{s}$ to $\frac{r'}{s'}$ has the property that $f(\frac{m}{n}) = a_0 + b_0 \frac{m}{n}$. Define the integer $t = nf(\frac{m}{n}) - a_0 n - b_0 m$. We then compute that the slope of $f_n$ from $\frac{r}{s}$ to $\frac{m}{n}$ is $b_0 + st$, while the slope of $f_n$ from $\frac{m}{n}$ to $\frac{r'}{s'}$ is at most $b_0 - s't$. In order to have $|b_0 + st|, |b_0 - s't| \leq K$, we must have $(s + s')\,|t| \leq 2K$; since $s + s' = n > 2K$, this is only possible if $t = 0$. Hence $f_n = f_{n-1}$, as claimed.

It follows that for any $n > 2K$, we must have $f_n = f_{n+1} = \cdots$. Since the condition on $f$ and $K$ implies that $f$ is continuous, we must also have $f_n = f$, completing the proof.

**Remark:** The condition on $f$ and $K$ is called *Lipschitz continuity*.

**Remark:** An alternate approach is to prove that for each $x \in [0,1)$, there exists $\varepsilon \in (0, 1 - x)$ such that the restriction of $f$ to $[x, x + \varepsilon)$ is linear; one may then deduce the claim using the compactness of $[0,1]$. In this approach, the role of the Farey sequence may also be played by the convergents of the continued fraction of $x$ (at least in the case where $x$ is irrational).

**Remark:** This problem and solution are due to one of us (Kedlaya). Some related results can be proved with the Lipschitz continuity condition replaced by suitable convexity conditions. See for example: Kiran S. Kedlaya and Philip Tynan, Detecting integral polyhedral functions, *Confluentes Mathematici* **1** (2009), 87–109. Such results arise in the theory of $p$-adic differential equations; see for example: Kiran S. Kedlaya and Liang Xiao, Differential modules on $p$-adic polyannuli, *J. Inst. Math. Jusssieu* **9** (2010), 155–201 (errata, *ibid.*, 669–671).