SIMON MARAIS mathematics competition

2025 SOLUTIONS

Problem A1 (proposed by Anand Deopurkar)

A function $f\colon [0,\infty) \to [0,\infty)$ is *max-poly* if there exist finitely many polynomials with real coefficients $p_1(x), p_2(x), \ldots, p_n(x)$ such that

- $p_i(x) \geq 0$ for all $x \geq 0$ and $1 \leq i \leq n$, and
- $f(x) = \max(p_1(x), p_2(x), \ldots, p_n(x))$ for all $x \geq 0$.

Determine whether the function $f(x) = \min(x, x^2)$ is max-poly.

Solution 1 No, it is not.

Since $f(0) = 0$, it suffices to consider p_i with $p_i(0) = 0$. Consider a max-poly function

$$g(x) = \max(p_1, \ldots, p_n)$$

with polynomials p_i that send $[0,\infty)$ to $[0,\infty)$ and 0 to 0. Suppose x^m (respectively x^M) is the lowest (respectively highest) power of x that appears in any of the p_i. By the non-negativity, these powers appear with positive coefficients and $m \leq M$. Close to 0 (respectively ∞), the function $g(x)$ behaves like x^m (respectively x^M) up to scaling. The given f, however, behaves like x^2 near 0 and like x near ∞, and $2 \not\leq 1$.

Solution 2

Suppose $f(x)$ is max-poly, with $f(x) = \max(p_1(x), \ldots, p_n(x))$. Let k be a positive integer. Then $f(k) = k$. Therefore $p_i(k) = k$ for some i. Hence there exists i such that $p_i(k) = k$ for infinitely many k. As p_i is a polynomial, $p_i(x) = x$. Hence $f(x) \geq p_i(x)$, a contradiction.

Problem A2 (proposed by Anand Deopurkar)

Let p be a prime number. Given a square matrix M with entries in $\mathbb{Z}/p\mathbb{Z}$, an *eigenvector* of M is a non-zero vector $\mathbf{v}$ with entries in $\mathbb{Z}/p\mathbb{Z}$ such that $M\mathbf{v} = \lambda\mathbf{v}$ for some $\lambda \in \mathbb{Z}/p\mathbb{Z}$.

For each positive integer n, determine the average number of eigenvectors of an $n \times n$ matrix with entries in $\mathbb{Z}/p\mathbb{Z}$.

(Here $\mathbb{Z}/p\mathbb{Z}$ refers to the integers modulo p.)

Solution

Set $F = \mathbf{Z}/p\mathbf{Z}$. We will prove the following Lemma

Lemma. *Let $\mathbf{v} \in F^n$ be nonzero and suppose $\lambda \in F$. Then the number of $n \times n$ matrices M with entries in F satisfying $M\mathbf{v} = \lambda\mathbf{v}$ is equal to p^{n^2-n}.*

Let us for now assume the Lemma is true. Then the number of pairs $(M, \mathbf{v})$ with $\mathbf{v}$ an eigenvector of M is equal to

$$p^{n^2-n}(p^{n^2} - 1)p,$$

the first factor coming from the above lemma, the second from the number of choices of nonzero $\mathbf{v}$ and the third from the number of choices of the eigenvalue λ. The total number of matrices M is equal to p^{n^2}. Hence the average number of eigenvectors is

$$\frac{p^{n^2-n}(p^{n^2} - 1)p}{p^{n^2}} = \frac{p^n - 1}{p^{n-1}}.$$

We now give four proofs of the Lemma

Proof 1. As $\mathbf{v}$ is nonzero, there exists $v_2, v_3, \ldots, v_n$ such that $\mathbf{v}, v_2, v_3, \ldots, v_n$ is a basis of F^n. Recall that a matrix is completely determined by its action on a basis. To have $M\mathbf{v} = \lambda\mathbf{v}$ then this determines the action of M on the first basis element, and then Mv_i can be any element of F^n for $i = 2, 3, \ldots, n$. These choices are independent and there are p^n elements of F^n, so in total there are $(p^n)^{n-1}$ choices of M satisfying $M\mathbf{v} = \lambda\mathbf{v}$. □

Proof 2. The matrix M satisfies $M\mathbf{v} = \lambda\mathbf{v}$ if and only if M has the form $M = A + \lambda I$ with A satisfying $A\mathbf{v} = 0$. The map $T : \mathrm{Mat}_{n\times n}(F) \to F^n$ given by $A \mapsto A\mathbf{v}$ is linear, and since $\mathbf{v} \neq 0$ it has full rank. (For example, if the ith entry $v^{(i)}$ of v is nonzero then the n matrices with all entries 0 apart from a single 1 in the ith column have nonzero images; or we can write the matrix of T as an $n \times n^2$ block diagonal matrix with all diagonal blocks equal to $\mathbf{v}^T$.) Hence the kernel of T has dimension $n^2 - n$, and so the number of matrices M satisfying $M\mathbf{v} = \lambda\mathbf{v}$ is p^{n^2-n+1}. as required. □

Proof 3. We take the same approach as Proof 2, but we calculate the size of the kernel by solving the linear system $A\mathbf{v} = 0$ more explicitly. Without loss of generality suppose that $\mathbf{v}^{(n)} \neq 0$. Then if $A\mathbf{v} = 0$ the entries in the nth column of A are given by

$$a_{in} = -(\mathbf{v}^{(n)})^{-1} \sum_{j=1}^{n-1} a_{ij}\mathbf{v}^{(j)}. \tag{1}$$

This shows that we can choose the first $n-1$ columns of A freely, and then the nth column is completely determined. So the kernel has cardinality p^{n^2-n}, as found above. □

Proof 4. Let P be an invertible matrix with first column $\mathbf{v}$; such a matrix exists by extending $\mathbf{v}$ to a basis for V with first element $\mathbf{v}$, and using the basis vectors as the columns of P. Then P satisfies $P\mathbf{e}_1 = \mathbf{v}$, where $\mathbf{e}_1$ is the first standard basis vector, and it is known or easily proved that $\mathbf{v}$ is an eigenvector of M if and only if $\mathbf{e}_1$ is an eigenvector of $P^{-1}MP$. The map on $n \times n$ matrices given by $M \mapsto P^{-1}MP$ is a bijection. We may therefore assume without loss of generality that $\mathbf{v} = \mathbf{e}_1$.

Now $\mathbf{e}_1$ is an eigenvector of M if and only if the first column of M is a scalar multiple of $\mathbf{e}_1$. So the entries in the first column of M in rows 2 to n must all be 0, and the remaining $n^2 - n + 1$ entries of M may be chosen freely. This proves the claim. □

Problem A3 (proposed by Norman Do)

Consider the matrix

$$M = \begin{bmatrix} t+1 & t \\ 1 & 1 \end{bmatrix},$$

whose entries are polynomials in the variable t. Let $a(t)$ denote the polynomial in the first row and first column of M^{2025} and let $b(t)$ denote the polynomial in the first row and second column of M^{2025}.

Prove that $a(t)$ has 2025 distinct real roots $\alpha_1, \alpha_2, \ldots, \alpha_{2025}$ and that $b(t)$ has 2025 distinct real roots $\beta_1, \beta_2, \ldots, \beta_{2025}$ satisfying

$$\alpha_1 < \beta_1 < \alpha_2 < \beta_2 < \cdots < \alpha_{2025} < \beta_{2025}.$$

Solution 1

Make the substitution $t = \lambda + \lambda^{-1} - 2$ (throughout our computations we will assume $\lambda \neq \pm 1$ and note separately that $b(t)$ has zero as a root). Then we have

$$M = \begin{bmatrix} \lambda + \lambda^{-1} - 1 & \lambda + \lambda^{-1} - 2 \\ 1 & 1 \end{bmatrix}$$

Its eigenvectors are $\begin{bmatrix} \lambda - 1 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 - \lambda \\ \lambda \end{bmatrix}$ with eigenvalues λ and λ^{-1} respectively. We may therefore diagonalise M thusly:

$$M = \begin{bmatrix} \lambda - 1 & 1 - \lambda \\ 1 & \lambda \end{bmatrix} \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} \begin{bmatrix} \lambda - 1 & 1 - \lambda \\ 1 & \lambda \end{bmatrix}^{-1}$$

Therefore we have

$$M^n = \begin{bmatrix} \lambda - 1 & 1 - \lambda \\ 1 & \lambda \end{bmatrix} \begin{bmatrix} \lambda^n & 0 \\ 0 & \lambda^{-n} \end{bmatrix} \begin{bmatrix} \lambda - 1 & 1 - \lambda \\ 1 & \lambda \end{bmatrix}^{-1}.$$

From this we get the equations

$$a_n(t) = \frac{\lambda^{2n+1} + 1}{\lambda^n(\lambda + 1)}$$
$$b_n(t) = \frac{(\lambda - 1)(\lambda^{2n} - 1)}{\lambda^n(\lambda + 1)}$$

The n roots of $a_n(t)$ correspond to $\lambda = \exp(\frac{\pi i k}{2n+1})$ for $k = 1, 3, 5, \ldots, 2n-1$ and hence are

$$t = 2\cos\left(\frac{\pi k}{2n+1}\right) - 2$$

The n roots of $b_n(t)$ correspond to $\lambda = \exp(\frac{\pi i l}{n})$ for $l = 0, 1, \ldots, n-1$ (the $l = 0$ case is $\lambda = 1$ which should be studied separately, in this case it is easy to see that 0 is a root of $b_n(t)$), and hence are

$$t = 2\cos\left(\frac{\pi l}{n}\right) - 2$$

The cosine function is monotone on $[0, \pi]$ and we have the inequalities

$$0 < \frac{1}{2n+1} < \frac{1}{n} < \frac{3}{2n+1} < \frac{2}{n} < \cdots < \frac{2n-3}{2n+1} < \frac{n-1}{n} < \frac{2n-1}{2n+1}$$

which proves the desired interlacing property of the roots of $a_n(t)$ and $b_n(t)$.

Solution 2

For each non-negative integer n, let

$$M^n = \begin{bmatrix} a_n(t) & b_n(t) \\ c_n(t) & d_n(t) \end{bmatrix},$$

where M^0 denotes the 2×2 identity matrix. We have the identity

$$\begin{bmatrix} a_{n+1}(t) & b_{n+1}(t) \end{bmatrix} = \begin{bmatrix} a_n(t) & b_n(t) \end{bmatrix} \begin{bmatrix} t+1 & t \\ 1 & 1 \end{bmatrix}$$

from which we obtain

$$a_{n+1}(t) = (t+1)a_n(t) + b_n(t) \tag{2}$$
$$b_{n+1}(t) = ta_n(t) + b_n(t) \tag{3}$$

Subtracting (3) from (2) yields

$$a_{n+1}(t) = b_{n+1}(t) + a_n(t). \tag{4}$$

It follows from (4) and (3) and the base cases $a_1(t) = t+1$ and $b_1(t) = t$ that for positive integers n, $a_n(t)$ and $b_n(t)$ are monic polynomials of degree n with non-negative integer coefficients. Furthermore, $a_n(t)$ has constant term 1 while $b_n(t)$ has constant term 0. Note that the real roots of $a_n(t)$ must be negative, while the real roots of $b_n(t)$ must be non-positive.

We now state and prove the following lemma, which will be crucial for the remainder of the proof.

Lemma: Let $q(t)$ and $r(t)$ be polynomials with positive leading coefficient, of degrees $d+1$ and d respectively. Suppose that $q(t)$ has $d+1$ real roots $\rho_0, \rho_1, \ldots, \rho_{d+1}$ and that $r(t)$ has d real roots $\sigma_1, \sigma_2, \ldots, \sigma_d$ such that

$$\rho_1 > \sigma_1 > \rho_2 > \sigma_2 > \cdots > \rho_d > \sigma_d > \rho_{d+1}.$$

Then the polynomial $p(t) = q(t) + r(t)$ has $d+1$ real roots $\tau_1, \tau_2, \ldots, \tau_{d+1}$ such that

$$\rho_i > \tau_i > \sigma_i \quad \text{for } 1 \leq i \leq d+1.$$

Proof: For convenience set $\rho_{d+1} = -\infty$ and $\rho_0 = \infty$. The polynomial $q(t)$ has the same number of real roots as its degree, so changes sign when crossing each root. As its leading coefficient is positive, $q(t) > 0$ on (ρ_1, ∞), hence $q(t) < 0$ on (ρ_2, ρ_1), hence $q(t) > 0$ on (ρ_3, ρ_2), et cetera. A similar story holds for $r(t)$.

If i is odd, $\rho_i \in (\sigma_i, \sigma_{i-1})$ on which $r(t)$ is positive. So $p(\rho_i) > 0$. Furthermore $\sigma_i \in (\rho_{i+1}, \rho_i)$ on which $q(t)$ is negative, so $p(\sigma_i) < 0$. If i is even, all signs are swapped, so in all cases we get $p(\rho_i)$ and $p(\sigma_i)$ have different signs.

By the intermediate value theorem, $p(t)$ must have a root $\tau_i \in (\sigma_i, \rho_i)$ as required. □

Lemma. Let $q(t)$ be a degree $d+1$ polynomial with non-negative coefficients and let $r(t)$ be a degree d polynomial with non-negative coefficients, for some positive integer d. Suppose that $q(t)$ has $d+1$ real roots $\rho_1, \rho_2, \ldots, \rho_{d+1}$ and that $r(t)$ has d real roots $\sigma_1, \sigma_2, \ldots, \sigma_d$ such that

$$\rho_1 < \sigma_1 < \rho_2 < \sigma_2 < \cdots < \rho_d < \sigma_d < \rho_{d+1}.$$

Then $p(t) = q(t) + r(t)$ is a polynomial with $d+1$ real roots $\tau_1, \tau_2, \ldots, \tau_{d+1}$ such that

$$\tau_1 < \rho_1 < \tau_2 < \rho_2 < \cdots < \tau_{d+1} < \rho_{d+1}.$$

Proof. The polynomial $r(t)$ has positive leading coefficient and changes sign at $\sigma_1, \sigma_2, \ldots, \sigma_d$. It follows that the signs of $r(\rho_1), r(\rho_2), \ldots, r(\rho_{d+1})$ alternate, where $r(\rho_{d+1})$ is positive.

The relation $p(t) = q(t) + r(t)$ implies that $p(\rho_1) = r(\rho_1), p(\rho_2) = r(\rho_2), \ldots, p(\rho_{d+1}) = r(\rho_{d+1})$. In particular, the signs of $p(\rho_1), p(\rho_2), \ldots, p(\rho_{d+1})$ alternate, where $p(\rho_{d+1})$ is positive. As $p(t)$ has positive leading coefficient, it follows from the intermediate value theorem that $p(t)$ has at least one root on each of the intervals $(-\infty, \rho_1), (\rho_1, \rho_2), \ldots, (\rho_{d-1}, \rho_d), (\rho_d, \rho_{d+1})$. As $p(t)$ has degree $d+1$, it must be the case that $p(t)$ has exactly $d+1$ real roots $\tau_1 < \tau_2 < \cdots < \tau_{d+1}$ and these satisfy the desired inequalities. □

We now prove the following statements for all integers $n \geq 2$, simultaneously by induction.

- The polynomial $a_n(t)$ has n real roots $\alpha_1^{(n)} < \alpha_2^{(n)} < \cdots < \alpha_n^{(n)} < 0$.
- The polynomial $b_n(t)$ has n real roots $\beta_1^{(n)} < \beta_2^{(n)} < \cdots < \beta_n^{(n)} = 0$.
- The roots of $a_{n-1}(t)$ and $b_n(t)$ satisfy

$$\beta_1^{(n)} < \alpha_1^{(n-1)} < \beta_2^{(n)} < \alpha_2^{(n-1)} < \cdots < \alpha_{n-1}^{(n-1)} < \beta_n^{(n)}.$$

- The roots of $a_n(t)$ and $b_n(t)$ satisfy

$$\alpha_1^{(n)} < \beta_1^{(n)} < \alpha_2^{(n)} < \beta_2^{(n)} < \cdots < \alpha_n^{(n)} < \beta_n^{(n)}.$$

It is straightforward to verify the base case $n = 2$, where we have

- $a_2(t) = t^2 + 3t + 1$ has roots $\alpha_1^{(2)} = \frac{-3-\sqrt{5}}{2} = -2.61803398\cdots$ and $\alpha_2^{(2)} = \frac{-3+\sqrt{5}}{2} = -0.38196601\cdots$, and
- $b_2(t) = t^2 + 2t$ has roots $\beta_1^{(2)} = -2$ and $\beta_2^{(2)} = 0$.

Now suppose that the statement holds true for some integer $n \geq 2$. By the lemma above applied to the relation $b_{n+1}(t)/t = a_n(t) + b_n(t)/t$, we have

$$\beta_1^{(n+1)} < \alpha_1^{(n)} < \beta_2^{(n+1)} < \alpha_2^{(n)} < \cdots < \beta^{(n+1)}{}_n < \alpha_n^{(n)} < \beta_{n+1}^{(n+1)} = 0.$$

This allows us to apply the lemma above to the relation $a_{n+1}(t) = b_{n+1}(t) + a_n(t)$ to obtain

$$\alpha_1^{(n+1)} < \beta_1^{(n+1)} < \alpha_2^{(n+1)} < \beta_2^{(n+1)} < \cdots < \alpha_{n+1}^{(n+1)} < \beta_{n+1}^{(n+1)}.$$

This completes the induction and the statement of the problem is recovered by setting $n = 2025$.

Problem A4 (proposed by Anand Deopurkar and Peter McNamara)

Let V be a finite-dimensional subspace of the real vector space of C^∞ functions from $\mathbb{R}$ to $\mathbb{R}$. Suppose that for all functions $g(x) \in V$, we have $g(2x) \in V$.

Prove that every function in V is a polynomial.

(A function from $\mathbb{R}$ to $\mathbb{R}$ is C^∞ if its k-th derivative exists at every point, for all positive integers k.)

Solution 1

We work instead with C^∞ functions from $\mathbb{R}$ to $\mathbb{C}$ (this step can be avoided by alternatively proving that the operator T below only has real eigenvalues). Note V is now a $\mathbb{C}$-vector space.

Let T be the linear transformation $T : V \to V$ given by $(Tf)(x) = f(2x)$.

As V is a finite-dimensional $\mathbb{C}$-vector space, there exists a basis $f_1, f_2, \dots f_n$ of V such that T is upper-triangular with respect to this basis (by putting T into Jordan normal form).

Lemma. If f is a C^∞-function and $\lambda \in \mathbb{C}$ is such that

$$f(2x) - \lambda f(x)$$

is a polynomial, then $f(x)$ is a polynomial.

Proof: Since $f(2x) - \lambda f(x)$ is a polynomial, there exists an integer k such that

$$\frac{d^k}{dx^k}\left(f(2x) - \lambda f(x)\right) = 0.$$

We also choose k to be large enough such that $2^k > |\lambda|$.

Our equation rearranges to

$$f^{(k)}(x) = \frac{2^k}{\lambda} f^{(k)}(x).$$

If $x_0 \in \mathbb{R}$ is such that $f^{(k)}(x_0) \neq 0$, then this implies that the sequence $f^{(k)}(x_0)$, $f^{(k)}(\frac{x_0}{2})$, $f^{(k)}(\frac{x_0}{4})$, $f^{(k)}(\frac{x_0}{8})$, ... is unbounded.

However, as f is C^∞,

$$\lim_{m\to\infty} f^{(k)}\left(\frac{x_0}{2^m}\right) = f^{(k)}\left(\lim_{m\to\infty} \frac{x_0}{2^m}\right) = f^{(k)}(0),$$

a contradiction.

Therefore $f^{(k)}$ is identically zero, which implies that f is a polynomial, completing the proof of the lemma. □

We now prove by strong induction on m that f_m is a polynomial for $m = 1, 2, \dots, n$.

As T is upper-triangular, there exists $\lambda \in \mathbb{C}$ such that

$$f_m(2x) - \lambda f_m(x) \in \operatorname{span}\{f_1, f_2, \ldots, f_{m-1}\}.$$

By the inductive hypothesis, this is a polynomial. By the lemma, we obtain that f_m is a polynomial, completing the inductive step.

As every element of a basis of V is a polynomial, every element of V is a polynomial, as required.

Solution 2

We will first prove a technical lemma that we need later in the proof.

Lemma: Let $\theta_1, \theta_2, \ldots, \theta_m$ be m distinct elements of $[0, 2\pi)$. Let $h_1(x), h_2(x), \ldots, h_m(x)$ be m polynomials with coefficients in $\mathbb{C}$. Suppose that

$$\lim_{k\to\infty} \sum_{j=1}^{m} h_j(k) e^{ik\theta_j} = 0,$$

where the limit is taken over integers k. Then $h_1(x) = h_2(x) = \cdots = h_m(x) = 0$.

Proof. Let d be the maximum of the degrees of $h_1, h_2, \ldots, h_m$ and let c_j be the coefficient of x^d in $h_j(x)$. Note that $\lim_{k\to\infty} \frac{h_j(k)}{k^d} = c_d$. Now divide through by k^d and use this limit to deduce that

$$\lim_{k\to\infty} \sum_{j=1}^{m} c_j e^{ik\theta_j} = 0. \tag{5}$$

Consider the sequence $(N\theta_1, N\theta_2, \ldots, N\theta_m)$ where $N \in \mathbb{N}$. This is a sequence inside the compact space $(\mathbb{R}/2\pi\mathbb{Z})^m$, hence there is a convergent subsequence $(N_l\theta_1, N_l\theta_2, \ldots, N_l\theta_m)$. Let $k_l = N_{l+1} - N_l$. From convergence we get that $\lim_{l\to\infty} e^{ik_l\theta_j} = 1$ for all j. Now take the limit in (5) along the subsequences $k_l + p$ for $p = 0, 1, \ldots, m-1$ to get

$$\sum_{j=1}^{p} c_j e^{ip\theta_j} = 0.$$

This is a system of m linear equations in the m variables $c_1, \ldots, c_m$. The matrix of coefficients is the Vandermonde matrix in $e^{i\theta_1}, e^{i\theta_2}, \ldots, e^{i\theta_m}$, which is invertible as $\theta_1, \theta_2, \ldots, \theta_m$ are distinct elements of $[0, 2\pi)$. Hence $c_1 = c_2 = \cdots = c_m = 0$. This implies that all h_j are equal to zero as one of these is a leading coefficient, completing the proof of the lemma. □

Now suppose $f(x) \in V$. Since V is finite dimensional, the functions $f(x), f(2x), f(4x), \ldots$ are linearly dependent. Choose a non-trivial linear dependency

$$\sum_{i=0}^{n} a_i f(2^i z) = 0. \tag{6}$$

Without loss of generality assume $a_n \neq 0$. Suppose k is such that $|2^k a_n| > |a_{n-1}| + |a_{n-2}| + \cdots + |a_1| + |a_0|$. Differentiate our linear dependency k times and set $z = 0$ to get

$$f^{(k)}(0) \sum_{i=0}^{n} 2^{ki} a_i = 0.$$

By our inequality, the term involving a_n dominates the others, so the sum cannot be zero. Hence $f^{(k)}(0) = 0$. This is true for all sufficiently large k.

Now think of equation (6) as a linear recurrence for the values $f(x), f(2x), f(4x), \ldots$. We solve it to get a solution of the form

$$f(2^k z_0) = \sum_{j=1}^{m} g_j(z_0, k)\lambda_j^k \tag{7}$$

where the λ_j are distinct complex numbers and g_j is a polynomial in k. Note by the algorithmic method to compute the g_j, we must have that g_j is C^∞.

There is

$$f^{(l)}(2^k z_0) = \sum_{j=1}^{m} \frac{\partial^l g_j}{\partial z^l}(z_0, k) \left(\frac{\lambda_j}{2^l}\right)^k. \tag{8}$$

We have already shown that every sufficiently large derivative of f vanishes at 0. Assume l is large enough such that the l-th derivative of f vanishes at 0, and that $|\lambda_j/2^l| < 1$ for all j.

Assume without loss of generality that $|\lambda_1| = |\lambda_2| = \cdots = |\lambda_m|$ and $|\lambda_1| < |\lambda_i|$ for $i > m$. Let $\theta_i = \arg(\lambda_i)$.

Rewrite our equation as

$$f^{(l)}(2^n x) = \left(\frac{|\lambda_1|}{2^l}\right)^n \left(\sum_{j=1}^{m} g_j^{(l)}(x, n)e^{in\theta_j} + G(x)\right)$$

From our inequalities on the magnitudes of the λ_i, we have $\lim_{n\to-\infty} G(x) = 0$. Now take the limit as n tends to negative infinity. As f is C^∞, the limit of the left hand side is $f^{(l)}(0)$ which we know is zero. As $|\lambda_1| < 2^l$, we can use the lemma to deduce that $g_j^{(l)}(n, x) = 0$ for $j = 1, 2, \ldots, m$.

We can repeat the same argument to deduce that $g_j^{(l)}(n, x) = 0$ for all j. Substituting this into (7) we deduce that $f^{(l)}(x) = 0$ for all x. Hence f is a polynomial.

Problem B1 (proposed by Liam Baker)

A function $f\colon \{1, 2, \ldots, n\} \to \{m+1, m+2, \ldots, m+n\}$, where m and n are positive integers, is said to be *beaut* if

- a divides $f(a)$ for all $a \in \{1, 2, \ldots, n\}$, and
- $f(a) \neq f(b)$ for all distinct elements a and b of $\{1, 2, \ldots, n\}$ with $\gcd(a, b) \neq 1$.

Determine all positive integers n such that, for every positive integer m, there exists a beaut function $f : \{1, 2, \ldots, n\} \to \{m+1, m+2, \ldots, m+n\}$.

Solution

We show the answer is $n \leq 5$.

First we show how to construct a beaut function f when $n \leq 5$ and m is arbitrary. In checking these functions are beaut, note that the only time the second condition is ever invoked for $n \leq 5$ is when a and b are 2 and 4.

$n = 1$**:** The function $f(1) = m + 1$ is beaut.

$n = 2$**:** One of $m + 1$ and $m + 2$ is even, setting $f(2)$ to be this value and arbitrarily assigning $f(1)$ gives a beaut function.

$n = 3$**:** At least one of $m + 1$ and $m + 2$ is even, set $f(2)$ to be this value. At least one of $m + 1$, $m + 2$ and $m + 3$ is divisible by 3, set $f(3)$ to be this value. Set $f(1)$ arbitrarily.

$n = 4$**:** Exactly one of $m + 1, \ldots, m + 4$ is divisible by 4 (let's call it a) and another is divisible by 2 but not by 4 (let's call it $b = a \pm 2$); let $f(4) = a$ and $f(2) = b \neq f(4)$. Define $f(3)$ and $f(2)$ as in the $n = 3$ case

$n = 5$**:** Proceed as in the $n = 4$ case, and ensure that $f(5)$ is the element of $\{m + 1, m + 2, \ldots, m + 5\}$ that is divisible by 5.

We now show that if $n \geq 6$ then there exists m for which no beaut function exists.

If n is even, then note that n and $n - 2$ have a common divisor of 2 and are both greater than $n/2$. Set $m = n(n-2) - \frac{n}{2}$, the range from $m + 1$ to $m + n$ is

$$n(n-2) - \frac{n}{2} + 1, \ldots, n(n-2), \ldots, n(n-2) + \frac{n}{2},$$

which has only one number divisible by n or by $n-2$, namely $n(n-2)k$, since $n > n-2 > \frac{n}{2}$. Thus if such an f were to exist, then $f(n-2)$ and $f(n)$ would both have to be equal to $n(n-2)$, which violates the second condition on f.

If n is odd, then note that $n - 1$ and $n - 3$ have a common divisor of 2 and are both greater than $n/2$. Set $m = (n-1)(n-3) - \frac{n+1}{2}$, the range from $m + 1$ to $m + n$ is

$$(n-1)(n-3) - \frac{n-1}{2}, \ldots, (n-1)(n-3), \ldots, (n-1)(n-3) + \frac{n-1}{2},$$

which has only one number divisible by $n-1$ or by $n-3$, namely $(n-1)(n-3)$, since $n-1 > n-3 > \frac{n-1}{2}$. Thus if such an f were to exist, then $f(n-3)$ and $f(n-1)$ would both have to be equal to $(n-1)(n-3)$, which violates the second condition on f.

Problem B2 (proposed by Peter McNamara)

Let W be the interior of a convex quadrilateral in $\mathbb{R}^2$ which has no two sides parallel.

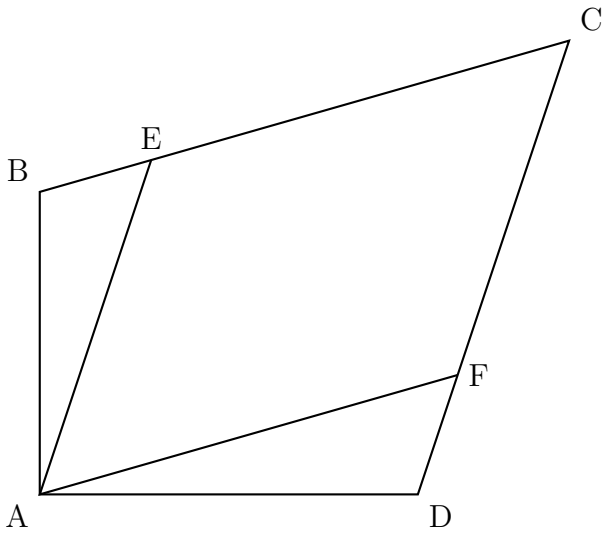
Prove that there exist two triangles in $\mathbb{R}^2$ whose interiors S and T satisfy

$$W = \{\mathbf{s} + \mathbf{t} \mid \mathbf{s} \in S,\ \mathbf{t} \in T\}.$$

Solution

Let $ABCD$ be the quadrilateral. Let P be the intersection of AB and CD and let Q be the intersection of AD and BC. Suppose without loss of generality that P is closer to A than B and that Q is closer to A than D. Let E be the point on BC such that AE is parallel to CD. Let F be the point on CD such that AF is parallel to BC.

Without loss of generality we can assume A is the origin. Then take our triangles to be $S = ABE$ and $T = ADF$.



The set W is then the convex hull of the 9 points

Problem B3 (proposed by Peter McNamara)

Let n be a positive integer and let $\omega = e^{\frac{2\pi i}{n}}$. Suppose $z_1, z_2, \ldots, z_n$ are distinct complex numbers. Define A to be the $n \times n$ matrix whose (j,k)-th entry is $(z_j - \omega^k)^n$, for $1 \leq j, k \leq n$.

Given that $\det A = 0$, prove that $z_1 z_2 \cdots z_n = 1$.

Solution 1

We consider $\det A$ as a polynomial in the n variables $z_1, z_2, \ldots, z_n$. The (j,k)-th entry can be expanded out using the binomial theorem as

$$(z_j - \omega^k)^n = \sum_{a=0}^{n} \binom{n}{a} z_j^a (-\omega^k)^{n-a}.$$

Note that all occurrences of a single variable appear in the same row. From this observation we can deduce that the coefficient of $z_1^{a_1} z_2^{a_2} \cdots z_n^{a_n}$ is

$$\prod_{j=1}^{n} \binom{n}{a_j} \det\left(\left[(-\omega^k)^{n-a_j} \right]_{j,k=1}^{n} \right). \tag{9}$$

If $i \neq j$ and $a_i \equiv a_j \pmod{n}$, then, as ω is an n-th root of 1, the matrix in (9) has two rows that are a scalar multiple of each other, which forces its determinant to be zero. This shows that unless $(a_1, a_2, \ldots, a_n)$ is a permutation of $(0, 1, 2, \ldots, n-1)$ or of $(1, 2, 3, \ldots, n)$, then the coefficient of $z_1^{a_1} z_2^{a_2} \cdots z_n^{a_n}$ in $\det A$ is zero.

Now suppose $(a_1, a_2, \ldots, a_n)$ is a permutation of $(0, 1, \ldots, n-1)$. We now compare the coefficients of $z_1^{a_1} z_2^{a_2} \cdots z_n^{a_n}$ and $z_1^{a_1+1} z_2^{a_2+1} \cdots z_n^{a_n+1}$ using (9).

The product of binomial coefficients is the same in each case. The determinants differ by a factor of

$$(-\omega)(-\omega^2) \cdots (-\omega^n) = (-1)^n \omega^{\frac{n(n+1)}{2}}.$$

If n is odd, then $\frac{n+1}{2} \in \mathbb{Z}$ and $\omega^n = 1$, so this factor is -1. If n is even then $\omega^{n/2} = -1$ and $n+1$ is odd, so again this factor is -1. In all cases we get these coefficients differ by a factor of -1, which implies that $\det A$ is divisible by $z_1 z_2 \cdots z_n - 1$.

Since A has two rows equal whenever two of the variables $z_1, z_2, \ldots, z_n$ are equal, it is divisible by $z_i - z_j$ for all $i \neq j$. As $\mathbb{C}[z_1, z_2, \ldots, z_n]$ is a unique factorisation domain, we deduce that $\det A$ is divisible by their product, multiplied by $z_1 z_2 \cdots z_n - 1$. Our analysis of which monomials can appear shows that the degree of A is at most $1 + 2 + \cdots + n$, and hence

$$\det A = \lambda(z_1 z_2 \cdots z_n - 1) \prod_{1 \leq i < j \leq n} (z_i - z_j)$$

for some scalar λ.

It suffices to show that $\lambda \neq 0$. We do this by looking at the coefficient of $z_1 z_2^2 \cdots z_n^n$. From (9), this is a Vandermonde matrix in the distinct variables $-\omega, -\omega^2, \ldots, -\omega^n$, hence is nonzero as required.

Solution 2

Let $f_k(z) = (z - \omega^k)^n$. First we prove that the polynomials $f_1(z), f_2(z), \ldots, f_n(z)$ are linearly independent. To do this, suppose we have a linear dependency $a_1 f_1 + a_2 f_2 + \cdots + a_n f_n = 0$. Comparing the coefficients of $z^0, z^1, \ldots, z^{n-1}$, we get a system of linear equations whose matrix is (up to trivial rescaling of rows) equal to the Vandermonde matrix with parameters $-\omega, -\omega^2, \ldots, -\omega^n$. These parameters are distinct, so the matrix is invertible, forcing all scalars $a_1, a_2, \ldots, a_n$ to be zero, as required.

Since $\det A = 0$, there exist complex numbers $a_1, a_2, \ldots a_n$, not all zero, such that

$$\sum_{k=1}^{n} a_k f_k(z_j) = 0$$

for $j = 1, 2, \ldots, n$.

Let $f(z) = \sum_{k=1}^{n} a_k f_k(z)$. Then $f(z_j) = 0$ for $j = 1, 2, \ldots, n$. As the degree of $f(z)$ is at most n, we have

$$f(z) = \lambda \prod_{j=1}^{n} (z - z_j)$$

for some $\lambda \in \mathbb{C}$. Since $f_1(z), f_2(z), \ldots, f_n(z)$ are linearly independent, $\lambda \neq 0$.

Note that each polynomial f_k has constant term equal to $(-1)^n$ times its leading term. Hence $f(z)$ has constant term equal to $(-1)^n$ times its leading term. Its constant term is $(-1)^n z_1 z_2 \cdots z_n \lambda$ while its leading term is λ. As $\lambda \neq 0$, we conclude that $z_1 z_2 \cdots z_n = 1$.

Solution 3

Consider the determinant $\det A$ as a one-variable polynomial in the variable z_1, call it $P(z_1)$. This has degree at most n. If $z_1 = z_i$ for some $i \neq 1$, then A has two rows equal, so the polynomial is zero. We have thus found $n-1$ roots of $P(z_1)$. The constant term of $P(z_1)$ can be found by substituting $z_1 = 0$, which leaves all rows the same except the first becomes all $(-1)^n$. The leading term can be found by replacing the first row with all 1's. Hence the leading term is $(-1)^n$ times the constant term. This implies that the product of the roots is 1, which implies that $z_1 z_2 \cdots z_n - 1$ divides $P(z_1)$. We therefore have

$$\det(A) = (z_1 - z_2)(z_1 - z_3) \cdots (z_1 - z_n)(z_1 z_2 \cdots z_n - 1) Q(z_2, z_3, \ldots, z_n),$$

for some polynomial $Q(z_2, z_3, \ldots, z_n)$. (we use the fact that $\mathbb{C}[z_1, z_2, \ldots, z_n]$ is a unique factorisation domain). Note that $\det(A)$ is antisymmetric. This implies that

$$Q(z_2, z_3, \ldots, z_n) = \lambda \prod_{2 \leq i < j \leq n} (z_i - z_j)$$

for some complex number λ. It remains to show that $\lambda \neq 0$, which we can do as in either of the previous solutions.

Problem B4 (proposed by Peter McNamara)

1. Determine all triples of integers (x, y, q) that satisfy the equation

$$x^3 + x^2 + x + 1 = y^q,$$

where $q \geq 3$ is odd.

2. Determine all quadruples of integers (x, y, n, q) that satisfy the equation

$$x^n + x^{n-1} + \cdots + x + 1 = y^q,$$

where $n, q \geq 2$.

Solution 1 to part (a)

We show the only solutions are $(x, y) = (-1, 0)$ and $(x, y) = (0, 1)$ (both of which are a solution for all q). When $y = 0$ we have $(x + 1)(x^2 + 1) = 0$ so this is the only solution. We now assume $y \neq 0$. Without loss of generality we assume q is prime.

Let $d = \gcd(x + 1, x^2 + 1)$. Then $x \equiv -1 \pmod{d}$ so $x^2 + 1 \equiv 2 \pmod{d}$. Hence $d = 1$ or $d = 2$.

Case I: $d = 1$.

From $(x + 1)(x^2 + 1) = y^q$ we get $x + 1 = s^q$ and $x^2 + 1 = t^q$ for some integers s and t (as q is odd, -1 is a q-th power so we do not have to worry about signs). Eliminating x from these equations results in

$$t^q = (s^q - 1)^2 + 1.$$

The case $s = 0$ corresponds to the trivial solution already found. The case $s = 1$ is disallowed as $y \neq 0$.

If $s > 1$ then t^q is less than $(s^2)^q$. Now let $z = s^2 - 1$. We have $(1 + z)^{q/2} \geq 1 + z^{q/2}$ (from the convexity of $f(x) = x^t + (1 - x)^{1-t}$ on $(0, 1)$ for $t > 1$). This rearranges to $t^q \geq (s^2 - 1)^q + 1 > (s^2 - 1)^q$ and we have sandwiched t^q between two consecutive q-th powers.

Now suppose $s < 0$. In this case, as q is odd we have $t^q > (s^2)^q$. We now show $t^q < (s^2+1)^q$. Substitute $r = -s$ for convenience, we have to show that $(r^q + 1)^2 + 1 < (r^2 + 1)^q$. Define $f(r) = (r^2 + 1)^q - (r^q + 1)^2 - 1$. Now

$$f'(r) = 2rq\left((r^2 + 1)^{q-1} - (r^q + 1)r^{q-2}\right) = 2qr\left(\sum_{i=0}^{q-2} \binom{q-1}{i} r^{2i} - r^{q-1}\right).$$

The term $(q-1)r^{2(q-2)}$ is larger than r^{q-1} as $q \geq 3$ and $r \geq 1$, which implies that $f'(r) > 0$ for $r > 1$. This together with $f(1) = 2^q - 5 > 0$ implies that $f(r) > 0$ for all $r \geq 1$ as required. Again we have sandwiched t^q between two consecutive q-th powers, which is impossible so there are no further solutions in this case.

Case II: $d = 2$.

In this case x is odd. Hence $x^2 + 1 \equiv 2 \pmod 4$. So from $(x+1)(x^2+1) = y^q$ we get $x + 1 = 2^{q-1}s^q$ and $x^2 + 1 = 2t^q$ for some integers s and t, again remembering q is odd so we don't have to worry about signs. We now move to the Gaussian integers and factor the latter as $(x + i)(x - i) = 2t^q$.

As x is odd, $1 + i \mid x + i$. Write $x + i = (1 + i)z$, which implies $x - i = (1 - i)\overline{z}$. Suppose e divides z and $\overline{z}$. Then $e \mid x \pm i$, so subtracting gives $e \mid 2i$. However note that $1 + i \nmid z$ as otherwise $2 \mid x + i$ but x is odd. Hence we have $\gcd(z, \overline{z}) = 1$.

Note that $(z\overline{z})^q = t^q$. Therefore (as all units of $\mathbb{Z}[i]$ are q-th powers), we can write $z = w^q$ for some $w \in \mathbb{Z}[i]$.

Write $w = a + bi$. Consider the imaginary part of the equation

$$x + i = (1 + i)(a + bi)^q. \tag{10}$$

We first consider the case where $q \equiv 3 \pmod 4$. First work modulo q, remembering that q is prime. Taking the imaginary part of the above gives $1 \equiv a^q - b^q \pmod q$ so $a - b \equiv 1 \pmod q$ by Fermat's little theorem. The imaginary part of (10) is an equation of the form

$$1 = P(a, b)$$

where $P(a, b)$ is a polynomial in a and b divisible by $a - b$. Hence it must be that $a - b = 1$.

Now substitute $a = b + 1$ into (10) so we have $x + i = (1 + i)(1 + (1 + i)b)^q$ and again take the imaginary part. We are left with a polynomial equation of the form $Q(b) = 0$. This polynomial Q has zero constant term, linear coefficient equal to $2q$ and all other coefficients divisible by $2q$. Hence $b \in \{-1, 0, 1\}$.

Substitute $b = a - 1$ into (10) so we have $x + i = (1 + i)((1 + i)a - i)^q$ and again take the imaginary part. We are left with a polynomial equation of the form $R(a) = 0$. This polynomial R has zero constant term, linear coefficient equal to $2q$ and all other coefficients divisible by $2q$. Hence $a \in \{-1, 0, 1\}$.

This leaves us with two solutions $a = 0$ and $b = 0$, which translate to $x = 1$ and $x = -1$. The former is not a solution as 4 is not a perfect q-th power and the latter gives the known solution where $y = 0$.

We now consider the case where $q \equiv 1 \pmod 4$. By the same argument as in the previous case we see that $a + b \equiv 1 \pmod q$ and that taking the imaginary part of (10) gives an equation of the form

$$1 = (a + b)P(a, b)$$

where $P(a, b)$ is a symmetric polynomial with integer coefficients. Hence $a + b = 1$.

Substitute $b = 1 - a$ into the equation $P(a, b) = 1$. We get a polynomial equation $Q(a) = 0$.

This equation has 0 as a double root. Because of the symmetry between a and b, we see that 1 is a double root. The two terms with the smallest 2-adic coefficient are the quadratic and quartic terms. (up to sign, the coefficient of a^{2r} is $2^r \binom{q}{2r}$ and the coefficient

of a^{4r-3} is $2^{2r}\binom{q}{4r-3}$, other coefficients being zero, to understand their 2-adic behaviour, write

$$\binom{q}{s} = \frac{q(q-1)}{s(s-1)}\binom{q-2}{s-2}$$

which gives a lower bound of $v_2(q-1) - \log_2(s)$ for its 2-adic valuation). Hence all other roots are not 2-adically integral. The two solutions $a = 1$ and $a = 0$ lead to $x = \pm 1$ and we conclude as before.

Solution 2 to part (a)

Proceed as the first solution until we get to $x + i = (1 + i)w^q$. Here is an alternative way to finish.

Subtract $x + i = (1 + i)w^q$ from its complex conjugate to get $2i = (i + 1)w^q - (1 - i)\overline{w}^q$. The right hand side has a factor of $w + i\overline{w}$ if $q \equiv 1 \pmod 4$ while it has a factor of $w - i\overline{w}$ if $q \equiv 3 \pmod 4$. This factor both divides and is divisible by $1 + i$ so is an associate of $1 + i$. This forces w to live on one of four lines in the plane.

Let us now assume $q \equiv 1 \pmod 4$ (the other case is similar): We have $w + i\overline{w} = \pm(1 + i)$ and

$$\prod_{j=1}^{q-1} |w + i\overline{w}\zeta^j| = 1$$

where ζ is a primitive q-th root of 1.

If we consider the factors $|w + i\overline{w}\zeta^j|$, they all have modulus larger than that of $|w + i\overline{w}| = \sqrt{2}$ unless

$$4 \arcsin\left(\frac{1}{\sqrt{2}|w|}\right) > \frac{2\pi}{q}.$$

Using the inequality $\sin(\theta) \geq \frac{3\theta}{\pi}$ which is valid for $0 \leq \theta \leq \pi/6$, we rearrange to get

$$|w| < \frac{\sqrt{2}}{3}q$$

On the other hand, we have

$$(1 + i)w^q \equiv i - 1 \pmod{2^{q-1}}.$$

Note that as $\gcd(z, \overline{z}) = 1$, we have $1 + i \nmid w$. So we can write $w = \alpha + u$ where u is a unit and $(1 + i)^3 \mid \alpha$. Write the above equation as

$$(1 + i)\sum_{j=0}^{q} \binom{q}{j} \alpha^j u^{q-j} \equiv 1 - i \pmod{2^{q-1}}.$$

Modulo 4, as $(1 + i)^3 \mid \alpha$, this becomes

$$(1 + i)^q \equiv i - 1 \pmod 4.$$

This forces $(1 + i)^q = i - 1$. Hence our congruence becomes

$$(1 + i)^{2q-3} \mid \sum_{j=1}^{q} \binom{q}{j} \alpha^j u^{q-j}$$

The term with $j = 1$ has strictly lower $(1+i)$-adic valuation than every other term. Hence it is divisible by $(1+i)^{2q-3}$. As q is odd, we get $(1+i)^{2q-3} \mid \alpha$. So either $\alpha = 0$ or

$$|w| \geq \sqrt{2}^{2q-3} - 1.$$

The $\alpha = 0$ case implies w is a unit, hence z is a unit and $x = \pm 1$, and we conclude as in the first proof.

If $\alpha \neq 0$, then by Bernoulli's inequality, we get

$$|w| > (2q-3)(\sqrt{2}-1).$$

This is a contradiction to $|w| < \frac{\sqrt{2}}{3}q$ provided $q > \frac{9}{4-\sqrt{2}}$, which is true as $q \equiv 1 \pmod 4$.

The $q \equiv 3 \pmod 4$ case proceeds similarly, except the Bernoulli inequality step when $q = 3$ gets skipped and replaced by a direct comparison of the two inequalities.

Remarks about the unsolved part The unsolved problem is the Nagell-Ljunggren equation. It has four known solutions with $|x| > 1$, where (x, y, n, q) is equal to $(3, 11, 5, 2)$, $(7, 20, 4, 2)$, $(18, 7, 3, 3)$ and $(-19, 7, 3, 3)$.

Problem C1 (proposed by Jon Smit and Chris Tuffley)

A frog makes a sequence of jumps in the plane. On its i-th jump, it jumps a distance of $2i-1$, either directly to the north or directly to the east.

For each positive integer n, determine the closest distance the frog can be to its starting point after completing such a sequence of n jumps.

Solution 1

We show that the answer is

- $\sqrt{10}$ if $n = 2$,
- $\sqrt{\frac{n^4+1}{2}}$ if n is odd,
- $\sqrt{\frac{n^4}{2}}$ if n is even and $n > 2$.

Let a and b be the total northward and eastward distance travelled respectively. We have

$$a + b = 1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

We must minimise

$$a^2 + b^2 = \frac{(a+b)^2 + (a-b)^2}{2} = \frac{n^4}{2} + \frac{(a-b)^2}{2}.$$

This is minimised if and only if a and b are as close to each other as possible.

Since $a - b$ has the same parity as n, a lower bound on $|a-b|$ is either 0 or 1 depending on whether n is even or odd. We will show this bound is realisable except for $n = 2$, in which case the lower bound is clearly 2.

If $n = 0$ or 1 it is trivial. If $n = 3$ we move east on the first two steps and north on the last step. if $n = 6$ we move east on the first, second, third and fifth steps and north on the fourth and sixth steps. In each case $|a-b|$ is 0 or 1 according to the parity of n.

For $n \geq 4$ and $n \neq 6$ we move as for the case $n-4$, then move east on the $(n-3)$-rd and n-th steps, while moving north on the $(n-1)$-st and $(n-2)$-nd steps. By doing this, the difference between the distance we moved east and north is the same for n steps as it is for $n-4$ steps. So by induction the quantity $|a-b|$ is either 0 or 1 depending on whether n is even or odd. This completes our proof.

Solution 2

Suppose $n \geq 2$ (the small cases being easy to work out separately). As in the first solution we need to split the odd numbers from 1 to $2n-1$ inclusive into two so that the two sums are either $n^2/2$, $n^2/2$ or $(n^2-1)/2$, $(n^2+1)/2$.

Choose m such that $m^2 \leq n^2/2 < (m+1)^2$. Starting with the set $1, 3, 5, ..., 2m+1$ and deleting one element we can get every number as its sum between m^2 and $(m+1)^2 - 1$

inclusive that has the same parity as m. If we delete 1 and one other element we can get every number as its sum from $m^2 - 1$ to $(m+1)^2 - 4$ inclusive that has the opposite parity to m. This construction yields every number in the range from m^2 to $(m+1)^2 - 1$ inclusive except for $(m+1)^2 - 2$. This all works provided $m + 1$ is at least 3, which is true as long as n is at least 3 (m^2 is a square strictly less than n^2, so we must have $(m+1)^2 \leq n^2$ too).

So we have hit one of our targets unless n is even and $n^2/2 = (m+1)^2 - 2 = m^2 + 2m - 1$. If n is at least 5 then we can take $5, 7, 9, ..., 2m - 1$ together with $2m + 3$, which gives us the sum $m^2 + 2m - 1$.

Problem C2 (proposed by Ka Ho Law)

For integers a and b, let $N(a, b)$ denote the number of rational numbers x that satisfy the equation

$$2x^4 + 2ax^2 + x + b = 0.$$

Determine the maximum possible value of $N(a, b)$.

Solution 1

We will show the answer is 1.

When $a = 0$ and $b = -3$, the equation becomes $2x^4 + x - 3 = 0$, which has a rational root $x = 1$. We prove below that the equation cannot have two or more rational roots, so that the answer is 1.

Suppose the equation $2x^4+2ax^2+x+b = 0$ has two rational roots. This quartic therefore has two linear factors. By grouping them together we can write $2x^4 + 2ax^2 + x + b$ as a product of two quadratics with rational coefficients.

By Gauss' lemma, these quadratic factors can be taken to have coefficients in $\mathbb{Z}$. Without loss of generality, the leading coefficient of our factors can be taken to be positive. Since 2 is prime, our factorisation must take the form

$$2x^4 + 2ax^2 + x + b = (x^2 + mx + n)(2x^2 + sx + t)$$

for some integers m, n, s, and t.

Comparing the coefficients of x^3 gives

$$0 = 2m + s.$$

Therefore s is even.

Comparing the coefficients of x^2 gives

$$2a = 2n + ms + t.$$

Therefore t is even.

As s and t are even, our quartic has all coefficients even, but one of its coefficients is 1, a contradiction, completing the proof.

Remark

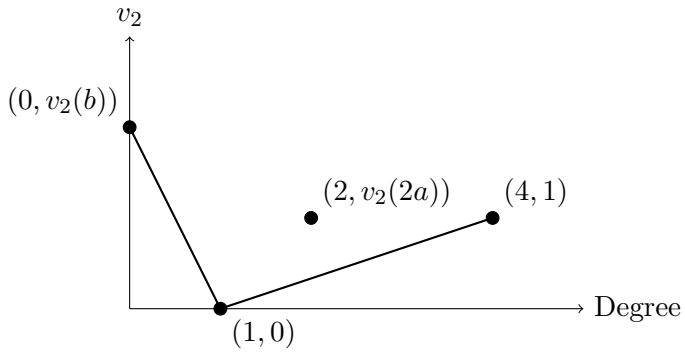
Here is a way to avoid the use of Gauss' Lemma. By the rational root theorem every rational root is either an integer or a half-integer. The half-integer case is not possible, as when you substitute in $x = \frac{n}{2}$ with n odd, the term $2x^4$ has a denominator of 8, while the denominators of the other terms are at most 4, so cannot cancel. Hence if $2x^4+2ax^2+x+b$ has two rational roots, they're both integer roots and we can get our factorisation over $\mathbb{Z}$ (using the division algorithm) without appealing to Gauss' Lemma.

Solution 2

As in the previous proof we notice that one rational root is possible, and proceed to prove that more than one rational root is not possible. We will analyse the number of rational roots of the quartic polynomial

$$f(x) = 2x^4 + 2ax^2 + x + b$$

using its 2-adic Newton polygon.



We have $v_2(b) \geq 0$, $v_2(1) = 0$, $v_2(2a) \geq 1$, $v_2(0) = \infty$ and $v_2(2) = 1$. Thus we know the points $(1, 0)$ and $(4, 1)$ are vertices of the Newton polygon.

The segment from $(1, 0)$ to $(4, 1)$ has slope $\frac{1}{3}$, implying that three of the roots in $\overline{\mathbb{Q}}_2$ have valuation $-\frac{1}{3}$. Since rational numbers have integer 2-adic valuations, these roots cannot be rational.

As a quartic can have at most four roots, the polynomial can have at most one rational root, as required.

Problem C3 (proposed by Angelo Di Pasquale)

A function $f(x, y)$ of two real variables is *angelic* if there exists a finite formula for it using only x, y, addition, subtraction, parentheses, and the absolute value function. For example, $x - (|y + y - x| + y)$ and $x + x + x - x$ are angelic functions.

Determine whether the function $\max(x, y)$ is angelic.

Solution 1

We show the answer is no. Let $f(x, y)$ be angelic. It is easy to see by induction on the length of the expression for $f(x, y)$ that $f(x, 1)$ is a piecewise linear function, whose set of gradients are all integers of the same parity. This is enough to deduce the contradiction as $\max(x, 1)$ has gradients of opposite parity.

Solution 2

It suffices to show that there is no angelic function $f(x, y)$ that agrees with $\max(x, y)$ when x and y are integers.

Note that $-x \equiv x \pmod 2$ and also $|x| \equiv x \pmod 2$ for any integer x. Thus, modulo 2, any angelic function is equivalent to the one given by taking a formula for it and by changing all $-$ signs to $+$ signs and erasing all the absolute value signs.

Hence, modulo 2, any angelic function is equivalent to 0 or x or y or $x + y$. We now check that none of these agree with $\max(x, y)$ modulo 2:

$$\begin{aligned}
\max(x, y) &\equiv 0 \pmod 2 && \text{falsified by } (x, y) = (1, 1) \\
\max(x, y) &\equiv x \pmod 2 && \text{falsified by } (x, y) = (0, 1) \\
\max(x, y) &\equiv y \pmod 2 && \text{falsified by } (x, y) = (1, 0) \\
\max(x, y) &\equiv x + y \pmod 2 && \text{falsified by } (x, y) = (1, 1)
\end{aligned}$$

Solution 3

As in the previous solution, when restricted to integers, we see that any angelic function $f(x, y)$ is equivalent to one that only uses $+$ signs in modulo 2. So if $f(x, y) = \max(x, y)$, then

$$0 = \max(-1, 0) = f(-1, 0) \equiv f(1, 0) = \max(1, 0) = 1 \pmod 2$$

which is a contradiction.

Problem C4 (proposed by Ivan Guo)

Let $f, g, h\colon \mathbb{R} \to \mathbb{R}$ be three convex functions such that $f(x) + g(x) \leq h(x)$ for all $x \in \mathbb{R}$. Prove that there exist convex functions $u, v : \mathbb{R} \to \mathbb{R}$ such that

- $f(x) \leq u(x)$ and $g(x) \leq v(x)$ for all $x \in \mathbb{R}$, and
- $h(x) = u(x) + v(x)$ for all $x \in \mathbb{R}$.

(A function $f\colon \mathbb{R} \to \mathbb{R}$ is *convex* if $f(\lambda x + (1-\lambda)y) \leq \lambda f(x) + (1-\lambda)f(y)$ for all $x, y \in \mathbb{R}$ and $0 \leq \lambda \leq 1$.)

Solution

Let u be the convex envelope of $h - g$, i.e., the largest convex function no greater than $h - g$ (or construct u by taking the convex hull of the epigraph of $h - g$). Let $v = h - u$. By definition, $u \geq f$ and $v \geq g$. So it suffices to prove that v is convex.

Given $a \leq b$, let $u_{ab}(x)$ be the function linearly interpolated between $(a, u(a))$ and $(b, u(b))$. We want to show that, for any $a \leq x \leq b$, $v_{ab}(x) \geq v(x)$.

By the property of the convex hull, for any x, there exist y, z (possibly equal, also possibly infinite) with $y \leq x \leq z$, such that $(x, u(x))$ lies on the line segment joining $(y, h(y) - g(y)) = (y, u(y))$ and $(z, h(z) - g(z)) = (z, u(z))$ (if one of y or z is infinite then $h - g$ is asymptotically linear in that direction and we take the point at infinity). In other words, u is linear on $[y, z]$, and $v = h - u$ is convex on $[y, z]$.

There are three cases:

1) If $[a, b] \subseteq [y, z]$, since v is convex on $[y, z]$, it is convex on $[a, b]$.

2) If $[y, z] \subseteq [a, b]$, then, since $h(y) - u(y) = g(y)$ and g is convex,

$$v(y) = h(y) - u(y) = g(y) \leq g_{ab}(y) \leq v_{ab}(y).$$

Similarly, $v(z) \leq v_{ab}(z)$. Since v is convex on $[y, z]$, we must have $v(x) \leq v_{yz}(x) \leq v_{ab}(x)$.

3) If exactly one of y, z is in $[a, b]$, without loss of generality assume $a \leq y \leq b \leq z$. Similar to case 2, $v(y) \leq v_{ab}(y)$. Since v is convex on $[y, z]$ and hence on $[y, b]$, we must have $v(x) \leq v_{yb}(x) \leq v_{ab}(x)$.

Therefore in all cases, $v_{ab}(x) \geq v(x)$ and we are done.