IMC 2024

Second Day, August 8, 2024

Solutions

Problem 6. Prove that for any function $f\colon \mathbb{Q} \to \mathbb{Z}$, there exist $a, b, c \in \mathbb{Q}$ such that $a < b < c$, $f(b) \geq f(a)$, and $f(b) \geq f(c)$.

(proposed by Mehdi Golafshan & Markus A. Whiteland, University of Liège, Liège)

Solution 1. We can replace $f(x)$ by the function $g(x) = f(1-x)$, so without loss of generality we can assume $f(0) \leq f(1)$.

If $f(1) \geq f(2)$ then we can choose $(a, b, c) = (0, 1, 2)$. Otherwise we have $f(0) \leq f(1) < f(2)$.

If there is some $x \in (1, 2)$ such that $f(x) \geq f(2)$ then we can chose $(a, b, c) = (1, x, 2)$; similarly, if there is some $x \in (1, 2)$ with $f(x) \leq f(1)$ then choose $(a, b, c) = (0, 1, x)$. Hence, in the remaining cases we have $f(1) \leq f(x) \leq f(2)$ for all $x \in (1, 2)$.

Now f is bonded on the interval $[1, 2]$, so it has only finitely many values on this interval. Since there are infintely many rational numbers in $[0, 1]$, there is a value y that is attained infinitely many times. The we can choose $1 \leq a < b < c \leq 2$ such that $f(a) = f(b) = f(c) = y$.

Solution 2. Assume towards a contradiction that there is a function f which does not satisfy the claim: for all rationals a, b, c with $a < b < c$ we have $f(b) < f(a)$ or $f(b) < f(c)$.

Let x and y be arbitrary rationals with $x < y$. Let $I(x, y) = [x, y] \cap \mathbb{Q}$. We first observe that $\inf f(I(x, y)) = -\infty$. Indeed, if the infimum was finite, then, as the set $f(I(x, y))$ is bounded ($\sup f(I(x, y)) = \max\{f(x), f(y)\}$) and thus finite, there are three points having the same value under f, which leads to a contradiction regarding our assumption on f.

So, going back to the question at hand, let x, b, y be arbitrary rationals with $x < b < y$. Applying the above observation to the set $I(x, b)$, there exists a point $a \in I(x, b)$ such that $f(a) < f(b)$. Similarly, there exists a point $c \in I(b, y)$ such that $f(c) < f(b)$. Hence we have the points a, b, c with $a < b < c$ and $f(b) > \max\{f(a), f(c)\}$, which contradicts our assumption on f.

Problem 7. Let n be a positive integer. Suppose that A and B are invertible $n \times n$ matrices with complex entries such that $A + B = I$ (where I is the identity matrix) and

$$(A^2 + B^2)(A^4 + B^4) = A^5 + B^5.$$

Find all possible values of $\det(AB)$ for the given n.

(proposed by Sergey Bondarev, Sergey Chernov, Belarusian State University, Minsk)

Hint: Find a polynomial $p(x)$ such that $p(AB) = 0$.

Solution 1. Notice first that $AB = A(I - A) = A - A^2 = (I - A)A = BA$, so A and B commute.
Let $C = AB = BA$; then

$$\begin{aligned}
A^2 + B^2 &= (A + B)^2 - 2AB = I - 2C,\\
A^4 + B^4 &= (A + B)^4 - 4AB(A + B)^2 + 2A^2B^2 = I - 4C + 2C^2,\\
A^5 + B^5 &= (A + B)^5 - 5AB(A + B)^3 + 5A^2B^2(A + B) = I - 5C + 5C^2,
\end{aligned}$$

so

$$\begin{aligned}
0 &= (A^5 + B^5) - (A^2 + B^2)(A^4 + B^4) = (I - 5C + 5C^2) - (I - 2C)(I - 4C + 2C^2)\\
&= 4C^3 - 5C^2 + C = 4C(C - I)(C - \tfrac{1}{4}I);
\end{aligned}$$

since C is invertible, we have

$$(C - I)(C - \tfrac{1}{4}I) = 0.$$

Hence, the polynomial $p(x) = (x - 1)(x - \frac{1}{4})$ annihilates the matrix $C = AB$ and therefore all eigenvalues of C are roots of $p(x)$, so the possible eigenvalues are 1 and $\frac{1}{4}$. The determinant is the product of the n eigenvalues, so

$$\det(AB) = \det C \in \left\{1, \tfrac{1}{4}, \tfrac{1}{4^2}, \dots, \tfrac{1}{4^n}\right\}.$$

Now show that these values are indeed possible.
If

$$A = \operatorname{diag}\Big(\underbrace{\tfrac{1}{2}, \dots, \tfrac{1}{2}}_{k}, \underbrace{e^{i\pi/3}, \dots, e^{i\pi/3}}_{n-k}\Big) \quad \text{and} \quad B = \operatorname{diag}\Big(\underbrace{\tfrac{1}{2}, \dots, \tfrac{1}{2}}_{k}, \underbrace{e^{-i\pi/3}, \dots, e^{-i\pi/3}}_{n-k}\Big),$$

then $A + B = I$, $AB = \operatorname{diag}\Big(\underbrace{\tfrac{1}{4}, \dots, \tfrac{1}{4}}_{k}, \underbrace{1, \dots, 1}_{n-k}\Big)$ and $\det(AB) = \frac{1}{4^k}$.

Problem 8. Define the sequence $x_1, x_2, \ldots$ by the initial terms $x_1 = 2$, $x_2 = 4$, and the recurrence relation

$$x_{n+2} = 3x_{n+1} - 2x_n + \frac{2^n}{x_n} \quad \text{for } n \geq 1.$$

Prove that $\lim\limits_{n\to\infty} \frac{x_n}{2^n}$ exists and satisfies

$$\frac{1+\sqrt{3}}{2} \leq \lim_{n\to\infty} \frac{x_n}{2^n} \leq \frac{3}{2}.$$

(proposed by Karen Keryan, Yerevan State University & American University of Armenia, Armenia)

Hint: Prove that $2x_n \leq x_{n+1} \leq 2x_n + n$.

Solution. Let's prove by induction that $x_{n+1} \geq 2x_n$. It holds for $n = 1$. Assume it holds for n. Then by the induction hypothesis we have that $x_n \geq 2x_{n-1} \geq \ldots \geq 2^{n-1}x_1 > 0$ and

$$x_{n+2} = 2x_{n+1} + (x_{n+1} - 2x_n) + \frac{2^n}{x_n} > 2x_{n+1}.$$

Similarly we prove that $x_{n+1} \leq 2x_n + n$. Again it holds for $n = 1$. Assume that the inequality holds for n. Then using that $x_n \geq 2^n$ and the induction hypothesis we obtain

$$x_{n+2} \leq 3x_{n+1} - 2x_n + 1 \leq 2x_{n+1} + (2x_n + n) - 2x_n + 1 = 2x_{n+1} + n + 1.$$

Using the previous inequalities we obtain that the sequence $y_n = \frac{x_n}{2^n}$ is increasing and $y_{n+1} \leq y_n + \frac{n}{2^n} \leq \ldots \leq y_1 + \sum_{k=1}^{n} \frac{k}{2^k} < \infty$, thus $\lim\limits_{n\to\infty} y_n = \frac{x_n}{2^n} = c$ exists.

The recurrence relation has the following form for y_n:

$$4y_{n+2} - 2y_{n+1} = 4y_{n+1} - 2y_n + \frac{1}{2^n \cdot y_n}.$$

By summing up the above equality for $n = 1, \ldots, m$ we obtain

$$4y_{m+2} - 2y_{m+1} = 4y_2 - 2y_1 + \sum_{n=1}^{m} \frac{1}{2^n \cdot y_n} = 2 + \sum_{n=1}^{m} \frac{1}{2^n \cdot y_n}. \tag{1}$$

Now using the facts that $y_1 = 1$, y_n increases and $\lim_{n\to\infty} y_n = c$ we obtain $1 \leq y_n \leq c$. Hence

$$\frac{1}{c} \leq \sum_{n=1}^{\infty} \frac{1}{2^n \cdot y_n} \leq 1.$$

Thus we get from (1)

$$2c = \lim_{m\to\infty} (4y_{m+2} - 2y_{m+1}) = 2 + \sum_{n=1}^{\infty} \frac{1}{2^n \cdot y_n} \in \left[2 + \frac{1}{c}, 3\right].$$

So we have $2c^2 \geq 2c + 1$ and $2c \leq 3$. Recall that $c \geq 1$. Therefore $1 + \sqrt{3} \leq 2c \leq 3$, which finishes the proof.

Problem 9. A matrix $A = (a_{ij})$ is called *nice*, if it has the following properties:

(i) the set of all entries of A is $\{1, 2, \ldots, 2t\}$ for some integer t;

(ii) the entries are non-decreasing in every row and in every column: $a_{i,j} \le a_{i,j+1}$ and $a_{i,j} \le a_{i+1,j}$;

(iii) equal entries can appear only in the same row or the same column: if $a_{i,j} = a_{k,\ell}$, then either $i = k$ or $j = \ell$;

(iv) for each $s = 1, 2, \ldots, 2t-1$, there exist $i \ne k$ and $j \ne \ell$ such that $a_{i,j} = s$ and $a_{k,\ell} = s+1$.

Prove that for any positive integers m and n, the number of nice $m \times n$ matrices is even.

For example, the only two nice 2×3 matrices are $\begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 & 3 \\ 2 & 4 & 4 \end{pmatrix}$.

(proposed by Fedor Petrov, St Petersburg State University)

Solution. Define a *standard Young tableaux* of shape $m \times n$ as an $m \times n$ matrix with the set of entries $\{1, 2, \ldots, mn\}$, increasing in every row and in every column as in (ii).

Call two standard Young tableaux Y_1, Y_2 *friends*, if they differ by a switch of two consecutive numbers $x, x+1$ (the places of x and $x+1$ must be not neighbouring, for such a switch preserving the monotonicity in rows and columns).

For a nice $m \times n$ matrix A we construct a standard Young tableaux Y_A of shape $m \times n$ as follows: if A has n_i entries equal to i ($i = 1, 2, \ldots, 2t$), we replace them by the numbers from $n_1 + \ldots + n_{i-1} + 1$ to $n_1 + \ldots + n_i$ preserving monotonicity.

Note that our Y_A has exactly $2t - 1$ friends, where $2t$ is the number of distinct entries in A, and moreover, every standard Young tableaux with odd number of friends corresponds to a unique nice matrix. It remains to apply the handshaking lemma (i.e., the sum of the degrees equals twice the number of edges in this graph).

Problem 10. We say that a square-free positive integer n is *almost prime* if

$$n \mid x^{d_1} + x^{d_2} + ... + x^{d_k} - kx$$

for all integers x, where $1 = d_1 < d_2 < ... < d_k = n$ are all the positive divisors of n. Suppose that r is a Fermat prime (i.e. it is a prime of the form $2^{2^m} + 1$ for an integer $m \geq 0$), p is a prime divisor of an almost prime integer n, and $p \equiv 1 \pmod{r}$. Show that, with the above notation, $d_i \equiv 1 \pmod{r}$ for all $1 \leq i \leq k$.

(An integer n is called *square-free* if it is not divisible by d^2 for any integer $d > 1$.)

(proposed by Tigran Hakobyan, Yerevan State University, Vanadzor, Armenia)

Solution. We first prove the following claims.

Lemma 1. If n is almost prime then $\gcd(n, \varphi(n)) = 1$.

Proof. Assume to the contrary that $\gcd(n, \varphi(n)) > 1$ so that there are primes p and q dividing n such that $p \equiv 1 (\text{mod } q)$. For $0 \leq i \leq p-2$ let h_i be the number of positive divisors of n congruent to i modulo $p-1$ and similarly for $0 \leq j \leq q-1$ let ν_j denote the number of positive divisors of n congruent to j modulo q. Observe that the polynomial $F_n(x) = x^{d_1} + x^{d_2} + ... + x^{d_k} - kx$ defines the zero function on $\mathbb{F}_p$ due to the condition of the problem. On the other hand, $F_n(x) = (h_1 - k)x + \sum_{i \neq 1} h_i x^i$ in $\mathbb{F}_p[x]$, so that $p | h_i$ for all $0 \leq i \leq p-2, i \neq 1$. It follows that $2^{\omega(n)-1} = \nu_0 = h_0 + h_q + h_{2q} + ... \equiv 0 (\text{mod } p)$ which is a contradiction (here $\omega(n)$ means the number of distinct prime divisors of n). Therefore our assumption was wrong and the lemma is proved. □

Lemma 2. Let q be a prime number and let h be a positive integer coprime to $q-1$. If l is the order of h modulo $q-1$, then there exists $a \in \mathbb{F}_q$ such that $a^{h^l} = a$ and

$$a - a^h + a^{h^2} - ... + (-1)^{l-1} a^{h^{l-1}} \neq 0$$

Proof. Observe that $a^{h^l} = a$ for any $a \in \mathbb{F}_q$ since $q - 1 | h^l - 1$. On the other hand, the numbers $h^0, h^1, ..., h^{l-1}$ leave different remainders upon division by $q-1$ and therefore the polynomial

$$f(x) = x - x^h + x^{h^2} - ... + (-1)^{l-1} x^{h^{l-1}}$$

defines a function on $\mathbb{F}_q$, which is not identically zero. Hence the existence of an element with the required properties is proved. □

Lemma 3. If n is almost prime then for any primes p and q dividing n, the order of p modulo $q-1$ is an odd number.

Proof. Observe that due to Lemma 1 the order l of p modulo $q-1$ is well defined and assume to the contrary that l is an even number. According to Lemma 2 there exists $a \in \mathbb{F}_q$ such that $a^{p^l} = a$ and $f(a) \neq 0$, where $f(x) = x - x^p + x^{p^2} - ... + (-1)^{l-1} x^{p^{l-1}}$. Let us consider the sequence $(a_i)_{i=0}^{l} \subset \mathbb{F}_q$ defined by $a_0 = a$ and $a_{i+1} = -a_i^p$ for $0 \leq i \leq l-1$. Notice that since l is even by the assumption, we have $a_l = a_0^{p^l} = a_0$. It follows that

$$\sum_{i=0}^{l-1} \sum_{d|n} a_i^d = \sum_{i=0}^{l-1} \left(\sum_{d|\frac{n}{p}} a_i^d + \sum_{d|\frac{n}{p}} a_i^{pd} \right) = \sum_{i=0}^{l-1} \sum_{d|\frac{n}{p}} \left(a_{i+1}^d + a_i^{pd} \right) = 0,$$

since d is always odd being a divisor of n (Recall that $\gcd(n, \varphi(n)) = 1$ due to Lemma 1, so that n is odd, except the trivial case $n = 2$), and $a_{i+1} = -a_i^p$ for all $0 \leq i \leq l-1$. On the other hand, according to the condition of the problem, $\sum_{d|n} a_i^d = k a_i$ in $\mathbb{F}_q$ for all i, which shows that

$$kf(a) = k \sum_{i=0}^{l-1} a_i = \sum_{i=0}^{l-1} k a_i = \sum_{i=0}^{l-1} \sum_{d|n} a_i^d = 0$$

in $\mathbb{F}_q$ which is impossible, since $f(a) \neq 0$ by construction and $k = 2^{\omega(n)-1}$ is coprime to q. The attained contradiction shows that our assumption was wrong and concludes the proof of the lemma. □

Let us get back to the problem. Suppose that $p|n$ is prime and $r = 2^{2^m}+1$ is a Fermat's prime such that $p \equiv 1 (\text{mod } r)$. If q is any prime divisor of n, then by Lemma 3 we have that $q^l \equiv 1 (\text{mod } p-1)$ for some odd l, so that $q^l \equiv 1 (\text{mod } r)$ and therefore $q = q^{\text{gcd}(l,r-1)} \equiv 1 (\text{mod } r)$. Hence $d \equiv 1 (\text{mod } r)$ for any divisor d of n. □