IMC 2023

First Day, August 2, 2023

Solutions

Problem 1. Find all functions $f : \mathbb{R} \to \mathbb{R}$ that have a continuous second derivative and for which the equality $f(7x+1) = 49f(x)$ holds for all $x \in \mathbb{R}$.

(proposed by Alex Avdiushenko, Neapolis University Paphos, Cyprus)

Hint:

- The fixed point of $7x+1$ is $-1/6$.
- Differentiating twice cancels out the coefficient 49.

Solution. Differentiating the equation twice, we get

$$f''(7x+1) = f''(x) \quad \text{or} \quad f''(x) = f''\left(\frac{x-1}{7}\right). \tag{1}$$

Take an arbitrary $x \in \mathbb{R}$, and construct a sequence by the recurrence

$$x_0 = x, \quad x_{k+1} = \frac{x_k - 1}{7}.$$

By (1), the values of f'' at all points of this sequence are equal. The limit of this sequence is $-\frac{1}{6}$, since $\left|x_{k+1} + \frac{1}{6}\right| = \frac{1}{7}\left|x_k + \frac{1}{6}\right|$.

Due to the continuity of f'', the values of f'' at all points of this sequence are equal to $f''\left(-\frac{1}{6}\right)$, which means that $f''(x)$ is a constant.

Then f is an at most quadratic polynomial, $f(x) = ax^2 + bx + c$. Substituting this expression into the original equation, we get a system of equations, from which we find $a = 36c$, $b = 12c$, and hence

$$f(x) = c(6x+1)^2.$$

Problem 2. Let A, B and C be $n \times n$ matrices with complex entries satisfying

$$A^2 = B^2 = C^2 \quad \text{and} \quad B^3 = ABC + 2I.$$

Prove that $A^6 = I$.

(proposed by Mike Daas, Universiteit Leiden)

Hint: Factorize $B^3 - ABC$.

Solution. Note that $B^3 = A^2B$, from which it follows that

$$A^2B - ABC = 2I \implies A(AB - BC) = 2I.$$

Similarly, using that $B^3 = BC^2$, we find that

$$BC^2 - ABC = 2I \implies (BC - AB)C = 2I.$$

It follows that A is a left-inverse of $(AB - BC)/2$, whereas $-C$ is a right inverse. Hence $A = -C$ and as such, it must hold that $ABA = 2I - B^3$. It follows that ABA must commute with B, and so it follows that $(AB)^2 = (BA)^2$. Now we compute that

$$(AB - BA)(AB + BA) = (AB)^2 + AB^2A - BA^2B - (BA)^2 = (AB)^2 + A^4 - B^4 - (AB)^2 = 0.$$

However, we noted before that the matrix $AB - BC = AB + BA$ must be invertible. As such, it must follow that $AB = BA$. We conclude that $ABA = A^2B = B^3$ and so it readily follows that $B^3 = I$. Finally, $A^6 = B^6 = (B^3)^2 = I^2 = I$, completing the proof.

Problem 3. Find all polynomials P in two variables with real coefficients satisfying the identity

$$P(x,y)P(z,t) = P(xz - yt, xt + yz).$$

(proposed by Giorgi Arabidze, Free University of Tbilisi, Georgia)

Hint: The polynomials $(x+iy)^n$ and $(x-iy)^m$ are trivial complex solutions. Suppose that $P(x,y) = (x+iy)^n(x-iy)^m Q(x,y)$, where $Q(x,y)$ is divisible neither by $x+iy$ nor $x = iy$ and consider $Q(x,y)$.

Solution. First we find all polynomials $P(x,y)$ with complex coefficients which satisfies the condition of the problem statement. The identically zero polynomial clearly satisfies the condition. Let consider other polynomials.

Let $i^2 = -1$ and $P(x,y) = (x+iy)^n(x-iy)^m Q(x,y)$, where n and m are non-negative integers and $Q(x,y)$ is a polynomial with complex coefficients such that it is not divisible neither by $x+iy$ nor by $x - iy$. By the problem statement we have $Q(x,y)Q(z,t) = Q(xz - yt, xt + yz)$. Note that $z = t = 0$ gives $Q(x,y)Q(0,0) = Q(0,0)$. If $Q(0,0) \neq 0$, then $Q(x,y) = 1$ for all x and y. Thus $P(x,y) = (x+iy)^n(x-iy)^m$. Now consider the case when $Q(0,0) = 0$.

Let $x = iy$ and $z = -it$. We have $Q(iy,y)Q(-it,t) = Q(0,0) = 0$ for all y and t. Since $Q(x,y)$ is not divisible by $x - iy$, $Q(iy,y)$ is not identically zero and since $Q(x,y)$ is not divisible by $x+iy$, $Q(-it,t)$ is not identically zero. Thus there exist y and t such that $Q(iy,y) \neq 0$ and $Q(-it,t) \neq 0$ which is impossible because $Q(iy,y)Q(-it,t) = 0$ for all y and t.

Finally, $P(x,y)$ polynomials with complex coefficients which satisfies the condition of the problem statement are $P(x,y) = 0$ and $P(x,y) = (x+iy)^n(x-iy)^m$. It is clear that if $n \neq m$, then $P(x,y) = (x+iy)^n(x-iy)^m$ cannot be polynomial with real coefficients. So we need to require $n = m$, and for this case $P(x,y) = (x+iy)^n(x-iy)^n = (x^2+y^2)^n$.

So, the answer of the problem is $P(x,y) = 0$ and $P(x,y) = (x^2+y^2)^n$ where n is any non-negative integer.

Problem 4. Let p be a prime number and let k be a positive integer. Suppose that the numbers $a_i = i^k + i$ for $i = 0, 1, \ldots, p-1$ form a complete residue system modulo p. What is the set of possible remainders of a_2 upon division by p?

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

Hint: Consider $\prod_{i=0}^{p-1}(i^k + i)$.

Solution. First observe that $p = 2$ does not satisfy the condtion, so p must be an odd prime.

Lemma. If $p > 2$ is a prime and $\mathbb{F}_p$ is the field containing p elements, then for any integer $1 \leq n < p$ one has the following equality in the field $\mathbb{F}_p$

$$\prod_{\alpha \in \mathbb{F}_p^*} (1 + \alpha^n) = \begin{cases} 0, & \text{if } \dfrac{p-1}{\gcd(p-1, n)} \text{ is even} \\ 2^n, & \text{otherwise} \end{cases}$$

Proof. We may safely assume that $n | p-1$ since it can be easily proved that the set of n-th powers of the elements of $\mathbb{F}_p^*$ coincides with the set of $\gcd(p-1, n)$-th powers of the same elements. Assume that $t_1, t_2, ..., t_n$ are the roots of the polynomial $t^n + 1 \in \mathbb{F}_p[x]$ in some extension of the field $\mathbb{F}_p$. It follows that

$$\prod_{\alpha \in \mathbb{F}_p^*} (1 + \alpha^n) = \prod_{\alpha \in \mathbb{F}_p^*} \prod_{i=1}^{n} (\alpha - t_i) = \prod_{i=1}^{n} \prod_{\alpha \in \mathbb{F}_p^*} (\alpha - t_i) = \prod_{i=1}^{n} \prod_{\alpha \in \mathbb{F}_p^*} (t_i - \alpha) = \prod_{i=1}^{n} \Phi(t_i),$$

where we define $\Phi(t) = \prod_{\alpha \in \mathbb{F}_p^*} (t - \alpha) = t^{p-1} - 1$. Therefore

$$\prod_{\alpha \in \mathbb{F}_p^*} (1 + \alpha^n) = \prod_{i=1}^{n} (t_i^{p-1} - 1) = \prod_{i=1}^{n} ((t_i^n)^{\frac{p-1}{n}} - 1) = \prod_{i=1}^{n} ((-1)^{\frac{p-1}{n}} - 1) = \begin{cases} 0, & \text{if } \frac{p-1}{n} \text{ is even} \\ 2^n, & \text{otherwise} \end{cases}$$

Let us now get back to our problem. Suppose the numbers $i^k + i, 0 \leq i \leq p-1$ form a complete residue system modulo p. It follows that

$$\prod_{\alpha \in \mathbb{F}_p^*} (\alpha^k + \alpha) = \prod_{\alpha \in \mathbb{F}_p^*} \alpha$$

so that $\prod_{\alpha \in \mathbb{F}_p^*} (\alpha^{k-1} + 1) = 1$ in $\mathbb{F}_p$. According to the Lemma, this means that $2^{k-1} = 1$ in $\mathbb{F}_p$, or equivalently, that $2^{k-1} \equiv 1 (\text{mod } p)$. Therefore $a_2 = 2^k + 2 \equiv 4 (\text{mod } p)$ so that the remainder of a_2 upon division by p is either 4 when $p > 3$ or is 1, when $p = 3$.

Problem 5. Fix positive integers n and k such that $2 \leq k \leq n$ and a set M consisting of n fruits. A *permutation* is a sequence $x = (x_1, x_2, \ldots, x_n)$ such that $\{x_1, \ldots, x_n\} = M$. Ivan *prefers* some (at least one) of these permutations. He realized that for every preferred permutation x, there exist k indices $i_1 < i_2 < \ldots < i_k$ with the following property: for every $1 \leq j < k$, if he swaps x_{i_j} and $x_{i_{j+1}}$, he obtains another preferred permutation.

Prove that he prefers at least $k!$ permutations.

(proposed by Ivan Mitrofanov, École Normale Superieur Paris)

Hint: For every permutation z of M, choose a preferred permutation x such that $\sum_{m \in M} x^{-1}(m) z^{-1}(m)$ is maximal.

Solution. Let S be the set of all $n!$ permutations of M, and let P be the set of preferred permutations. For every permutation $x \in S$ and $m \in M$, let $x^{-1}(m)$ denote the unique number $i \in \{1, 2, \ldots, n\}$ with $x_i = m$.

For every $x \in P$, define

$$A(x) = \left\{ z \in S \ : \ \forall y \in P \quad \sum_{m \in M} x^{-1}(m) z^{-1}(m) \geq \sum_{m \in M} y^{-1}(m) z^{-1}(m) \right\}.$$

For every permutation $z \in S$, we can choose a permutation $x \in P$ for which $\sum_{m \in M} x^{-1}(m) z^{-1}(m)$ is maximal, and then we have $z \in A(x)$; hence, all $z \in S$ is contained in at least one set $A(x)$.

So, it suffices to prove that $|A(x)| \leq \frac{n!}{k!}$ for every preferred permutation x. Fix $x \in P$, and consider an arbitrary $z \in A(x)$. Let the indices $i_1 < \ldots < i_k$ be as in the statement of the problem, and let $m_j = x_{i_j}$ for $j = 1, 2, \ldots, k$.

For $s = 1, 2, \ldots, k-1$ consider the permutation y obtained from x by swapping m_s and m_{s+1}. Since $y \in P$, the definition of $A(x)$ provides

$$i_s z^{-1}(m_s) + i_{s+1} z^{-1}(m_{s+1}) \geq i_{s+1} z^{-1}(m_s) + i_s z^{-1}(m_{s+1}),$$

$$z^{-1}(m_{s+1}) \geq z^{-1}(m_s).$$

Therefore, the elements $m_1, m_2, \ldots, m_k$ appear in z in this order. There are exactly $n!/k!$ permutations with this property, so $|A(x)| \leq \frac{n!}{k!}$.