Integer divisibility

MOPSS

20 March 2025

Mathematics Olympiad

Problem Solving Sessions

MOPSS

Department of Mathematics
IISER Bhopal

https://jpsaha.github.io/MOTP/MOPSS/

Suggested readings

- Evan Chen's
  - advice *On reading solutions*, available at https://blog.evanchen.cc/2017/03/06/on-reading-solutions/.
  - *Advice for writing proofs/Remarks on English*, available at https://web.evanchen.cc/handouts/english/english.pdf.
- Evan Chen discusses why *math olympiads are a valuable experience for high schoolers* in the post on *Lessons from math olympiads*, available at https://blog.evanchen.cc/2018/01/05/lessons-from-math-olympiads/.

List of problems and examples

§1 Integer divisibility

Lemma 1

If P is a polynomial with integer coefficients and a, b are integers, then $P(a) - P(b)$ is a multiple of $a - b$.

Example 1.1. Let $P(x)$ be a polynomial with integer coefficients such that $P(0), P(1)$ are odd. Show that $P(x)$ does not have any integer root.

Solution 1. If $P(x)$ admits an integer root α, then $\alpha, \alpha - 1$ are odd, which is impossible. ■

Example 1.2 (India RMO 2016g P8)**.** At some integer points a polynomial with integer coefficients take values $1, 2$ and 3. Prove that there exist not more than one integer at which the polynomial is equal to 5.

Solution 2. Denote the polynomial by $P(x)$. On the contrary, let us assume that there are at least two distinct integers where $P(x)$ takes the value 5.

Let a, b, c be integers such that

$$P(a) = 1, P(b) = 2, P(c) = 3.$$

Note that $a - b$ divides $P(a) - P(b)$, $b - c$ divides $P(b) - P(c)$. It follows that $a - b = \pm 1, b - c = \pm 1$. Since a, b are of opposite parity, and so are the integers b, c, we obtain that a, c are of the same parity. Noting that $c - a$ divides $P(c) - P(a) = 2$, it follows that $c - a = \pm 2$. Combining this with $a - b = \pm 1, b - c = \pm 1$, we get $a - b = b - c = 1$ or $a - b = b - c = -1$.

This shows that $P(b-1) = 1, P(b) = 2, P(b+1) = 3$ holds or $P(b+1) = 1, P(b) = 2, P(b-1) = 3$ holds. Note that in the first case, the polynomial $R(x) := P(x - b)$ takes the values $1, 2, 3$ at the integers $-1, 0, 1$ respectively. In the second case, the polynomial $S(x) = P(-x + b)$ takes the values $1, 2, 3$ at the integers $-1, 0, 1$ respectively. This proves that there is a polynomial $Q(x)$ with integer coefficients which takes the values $1, 2, 3$ at $-1, 0, 1$ respectively.

From the hypothesis, it follows that there are distinct integers i, j such that $Q(i) = Q(j) = 5$. Note that $i - 1$ divides $Q(i) - Q(1) = 2$, i divides $Q(i) - Q(0) = 3$, $i + 1$ divides $Q(i) - Q(-1) = 4$. Since i divdes 3, we obtain $i = \pm 1, \pm 3$. Using $Q(-1) = 1, Q(1) = 3$, we get $i \neq -1, i \neq 1$. This gives $i = \pm 3$. Noting that $i - 1$ divides 2, we obtain $i \neq -3$, and hence $i = 3$. Similarly, it follows that $j = 3$. ■

Example 1.3. Let $P(x)$ be a polynomial with integer coefficients such that $P(20), P(25)$ are of absolute value equal to 1. Show that $P(x)$ does not vanish at any integer.

Solution 3. On the contrary, let us assume that $P(x)$ vanishes at an integer α. Note that $\alpha - 20$ divides 1, and so does $\alpha - 25$. This shows that $\alpha - 20, \alpha - 25$ are absolute value equal to 1. Applying triangle inequality, we obtain

$$5 \leq |\alpha - 20| + |\alpha - 5| \leq 2,$$

which is impossible. ■

Example 1.4 (USAMO 1974 P1)**.** Let a, b, and c denote three distinct integers, and let P denote a polynomial having all integral coefficients. Show that it is impossible that $P(a) = b$, $P(b) = c$, and $P(c) = a$.

Solution 4. Note that

$$a - b \mid P(a) - P(b) = b - c \mid P(b) - P(c) \mid c - a \mid P(c) - P(a) = a - b.$$

Consequently, the integers $a - b, b - c, c - a$ are of the same absolute value. Denote their absolute value by k. Note that their sum is zero. However, the sum is equal to mk, for some $m \in \{\pm 1, \pm 3\}$. Hence, k is equal to zero.

This yields that $a = b = c$. ■

Here is a more general result.

Example 1.5. Let $P(x)$ be a polynomial with integer coefficients, and let n be an odd positive integer. Suppose that $x_1, x_2, \ldots, x_n$ is a sequence of integers such that $x_2 = P(x_1), x_3 = P(x_2), \ldots, x_n = P(x_{n-1})$, and $x_1 = P(x_n)$. Prove that all the x_i's are equal.

Walkthrough — Show that

$$a_1 - a_2 \mid a_2 - a_3 \mid a_3 - a_4 \mid \cdots \mid a_n - a_1 \mid a_1 - a_2.$$

Note that sum of these differences is an odd multiple of their absolute value.

Lemma 2

Let P be a polynomial with integer coefficients. Suppose a is an integer and k is a positive integer such that $P^k(a) = a$, where P^k denotes the k-fold composite map from $\mathbb{Z} \to \mathbb{Z}$. Show that $P^2(a) = a$.

Proof. Let ℓ denote the smallest positive integer such that $P^\ell(a) = a$. If $\ell = 1$ or $\ell = 2$, then we are done. Henceforth, we assume that $\ell \geq 3$.

Note that

$$P(a) - a \mid P^2(a) - P(a) \mid \cdots \mid P^\ell(a) - P^{\ell-1}(a) = a - P^{\ell-1}(a) \mid P(a) - a.$$

Since $a - P^{\ell-1}(a)$ is nonzero, it follows that the above differences are nonzero. Consequently, for any $1 \leq i \leq \ell$,

$$P^{i+1}(a) - P^i(a) = \pm(P^i(a) - P^{i-1}(a)).$$

If $P^{i+1}(a) = P^{i-1}(a)$ holds for some $1 \leq i \leq \ell$, then applying $P^{\ell-i+1}$ to both sides, we obtain $P^2(a) = a$, which contradicts the assumption that $\ell \geq 3$. It follows that for any $1 \leq i \leq \ell$,

$$P^{i+1}(a) - P^i(a) = P(a) - a$$

holds, which implies that

$$\sum_{i=0}^{\ell-1} (P^{i+1}(a) - P^i(a)) = \ell(P(a) - a).$$

This gives $P(a) = a$, which contradicts the assumption that $\ell \geq 3$. This completes the proof. ☐

Example 1.6 (IMO 2006 P5)**.** (Dan Schwarz, Romania) Let $P(x)$ be a polynomial of degree $n > 1$ with integer coefficients, and let k be a positive integer. Consider the polynomial $Q(x) = P(P(\ldots P(P(x))\ldots))$, where P occurs k times. Prove that there are at most n integers t such that $Q(t) = t$.

Solution 5. By the above lemma, it reduces to considering the case $Q(x) = P^2(x)$.

Suppose Q has more than n fixed points. Since P is not linear, it follows that P cannot have n fixed points, and hence not all the fixed points of Q are fixed points of P. Let b be a non-fixed point of P, and $Q(b) = b$. Suppose a be a fixed point of Q, other than b.

Let us first consider the case that $P(a) \neq a$. Note that

$$P(b) - a \mid P(a) - b \mid P(b) - a$$

holds, and

$$a - b \mid P(a) - P(b) \mid a - b$$

holds too. This yields that

$$|P(a) - b| = |P(b) - a|, \quad |P(a) - P(b)| = |a - b|.$$

If

$$P(a) - b = a - P(b), \text{ and } P(a) - P(b) = a - b$$

hold, then b would be a fixed point of P. It follows that at least one of

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

holds. Consequently, we obtain

$$P(a) + a = P(b) + b.$$

Next, let us consider the case that $P(a) = a$. Note that

$$P(b) - a \mid b - a \mid P(b) - a.$$

Since b is not a fixed point for P, it follows that

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

which yields

$$P(a) + a = P(b) + b.$$

This proves that all the roots of $Q(x) = x$ are the roots of $P(x)+x = P(b)+b$. Since $P(x)$ has degree $n > 1$, it follows that the polynomial $P(x)+x-P(b)-b$ is of degree n, and it has more than n roots, which is impossible.

Hence, there are at most n integers t such that $Q(t) = t$ holds. ■

Example 1.7 (Tournament of Towns, Spring 2014, Senior, A Level, P4 by G.K. Zhukov)**.** In the plane, the points with integer coordinates (x, y) satisfying $0 \leq y \leq 10$ are marked. Consider a polynomial of degree 20 with integer coefficients. Determine the maximum possible number of marked points which can lie on its graph.