Unexpected Applications of Mean Value Theorem(s) in Number Theory

Navid Safaei
Sharif University of Technology, Tehran, Iran

In this article we provide a useful strategy for tackling some rather difficult number theory problems concerning polynomials with specific number theoretic conditions. We use the mean value theorem, Taylor's formula and some basic properties of limits.

1 Main theorems

The key results used in the sequel are:

Theorem 1.1. *(Cauchy's mean value theorem) Let $f, g : [a, b] \to \mathbf{R}$ be continuous functions which are differentiable on (a, b), with $f(a) \neq f(b)$ and such that f' does not vanish on (a, b). Then*

$$\frac{g(b) - g(a)}{f(b) - f(a)} = \frac{g'(c)}{f'(c)}$$

for some $c \in (a, b)$.

Theorem 1.2. *(Taylor's formula) If $f : [a, b] \to \mathbf{R}$ is at least of class C^2 on (a, b), then for any $x, y \in (a, b)$ we can find c between x and y such that*

$$f(x) = f(y) + (x - y)f'(y) + \frac{(x - y)^2}{2} f''(c).$$

2 Introductory problems

Problem 1 Two real quadratic polynomials f, g have the property that $g(x)$ is an integer whenever $f(x)$ is an integer (for some real number x). Prove that there are integers m, n such that $g(x) = mf(x) + n$ for all x.

Bulgarian Olympiad 1996

Solution Replacing f (resp. g) by $-f$ (resp. $-g$) we may assume that the leading coefficients of f, g are positive, so that f, g are increasing on (M, ∞) for some $M > 0$. For any integer $n > f(M)$ we can find $x_n > M$ such that $f(x_n) = n$, and the corresponding sequence (x_n) is increasing. Moreover, by assumption $g(x_n) = g_n$ are integers. Clearly $\lim_{n\to\infty} x_n = \infty$. By Cauchy's mean value theorem

$$\frac{g(x_{n+1}) - g(x_n)}{f(x_{n+1}) - f(x_n)} = \frac{g'(c_n)}{f'(c_n)}, \quad \text{i.e.} \quad g(x_{n+1}) - g(x_n) = \frac{g'(c_n)}{f'(c_n)}$$

for some $c_n \in (x_n, x_{n+1})$. Note that $\lim_{n\to\infty} c_n = \infty$ and since f, g have the same degree we have $\lim_{n\to\infty} \frac{g'(c_n)}{f'(c_n)} = \frac{b}{a}$, where a, b are the leading coefficients of f, g. It follows that $\lim_{n\to\infty} g_{n+1} - g_n = \frac{b}{a}$ and since the g_n's are integers we must have $g_{n+1} - g_n = \frac{b}{a}$ for all n large enough. But then

$$g(x_{n+1}) - g(x_n) = \frac{b}{a}(f(x_{n+1}) - f(x_n))$$

for n large enough and so the polynomial $g - \frac{b}{a}f$ takes the same value at x_n and x_{n+1} for n large enough. This polynomial must be constant and the result follows (note that $\frac{b}{a}$ is indeed an integer, by the above discussion). Note that we did not use the fact that f, g are quadratic polynomials, the only hypothesis needed in the proof was that $\deg(f) = \deg(g)$.

3 Main Results

Problem 3 Find all polynomials P with real coefficients for which there is $a \in (1, \infty)$ such that for any integer x there is an integer z with $aP(x) = P(z)$.

Saint Petersburg 2016

Solution Clearly the zero polynomial is the only constant solution of the problem, so assume that P is a solution with P nonconstant. Dividing P by its leading coefficient, we may assume that P is monic, say of degree d. By assumption there is a sequence of integers z_n such that $aP(n) = P(z_n)$ for all $n \geq 1$. Let $A = \sqrt[d]{a}$ and write $P(X) = X^d + bX^{d-1} + Q(X)$ with $\deg(Q) \leq d-2$. Clearly $|z_n| \to \infty$ as $n \to \infty$. Passing to the limit in the equality

$$a\frac{P(n)}{n^d} = \frac{P(z_n)}{z_n^d}\left(\frac{z_n}{n}\right)^d,$$

we deduce that $|z_n|/n \to A$ as $n \to \infty$, in particular $x_n := \frac{z_n}{An}$ is bounded.

Next, the equality $A^d P(n) = P(z_n)$ can be rewritten

$$An(x_n^d - 1) + b(x_n^{d-1} - A) = \frac{A^d Q(n) - Q(z_n)}{(An)^{d-1}}$$

and the right-hand side converges to 0 since $\deg(Q) < d-1$ and since x_n is bounded. It follows that

$$\lim_{n\to\infty} An(x_n^d - 1) + b(x_n^{d-1} - A) = 0. \qquad (1),$$

in particular $x_n^d - 1 = O(1/n)$.

Suppose first that d is odd, then x_n tends to 1 and relation (1) implies that $An(x_n - 1)$ converges to $B := -b(1-A)/d$, thus $z_n - An$ converges to B. Since z_n is an integer, we have $z_n = An + B$ for n large enough (note that $z_{n+1} - z_n$ converges to A, thus it equals A for n large enough). Thus $A^d P(n) = P(An + B)$ for n large enough and $A^d P(X) = P(AX + B)$. We finish then this case using the useful

Lemma 3.1. *Let A, B be real numbers, with $A \neq \pm 1$. The only polynomials P of degree d such that*

$$A^d P(X) = P(AX + B)$$

are the polynomials $P(X) = c(X - x_0)^d$ with $c \in \mathbf{R}^*$, where $x_0 = \frac{B}{1-A}$.

Proof. Letting $Q(X) = P(X + x_0)$ we obtain

$$Q(AX) = P(AX + x_0) = P(A(X + x_0) + B) = A^d P(X + x_0) = A^d Q(X).$$

Writing $Q(X) = c_0 + c_1 X + ... + c_d X^d$ we deduce that $c_i(A^i - A^d) = 0$, so that $c_i = 0$ for $i < d$ and the result follows.

□

We conclude that if d is odd, any solution is of the form $c(X - x_0)^d$, and these are indeed solutions.

Suppose now that d is even. We can no longer deduce that x_n tends to 1 and the analysis becomes more delicate. Write $d = 2k$. Since $|x_n^d - 1| \geq |x_n^2 - 1|$ and $x_n^d - 1 = O(1/n)$, we have $x_n^2 - 1 = O(1/n)$. But then $An(x_n^d - 1) - Ank(x_n^2 - 1)$ and $b(x_n^{d-1} - x_n)$ converge to 0, so that relation (1) yields $\lim_{n\to\infty} Ank(x_n^2 - 1) + b(x_n - A) = 0$. We conclude that $An(x_n^2 - 1) + \frac{b}{k}x_n$ converges. Recalling that $x_n = \frac{z_n}{An}$ and setting

$$v_n = z_n + \frac{b}{2k},$$

it follows easily that $\lim_{n\to\infty} \frac{v_n^2}{An} - An = \frac{bA}{k}$ converges. In particular $\frac{|v_n|}{An} \to 1$ and then $\lim_{n\to\infty}(|v_n| - An) = \frac{bA}{2k}$.

Choose $i_n \neq j_n \in \{n, n+1, n+2\}$ such that z_{i_n} and z_{j_n} have the same sign (this is clearly possible for each n). Then $|v_{i_n}|-|v_{j_n}| = \pm(z_{i_n}-z_{j_n})$ is an integer. However $|v_{i_n}|-Ai_n-|v_{j_n}|+Aj_n$ tends to 0. Since $j_n - i_n$ takes infinitely many times the same value, which is a number in $\{-2,-1,1,2\}$, we deduce that $2A$ is an integer.

Finally, choose an increasing sequence k_n and a number $\varepsilon \in \{-1,1\}$ such that $\varepsilon z_{k_n} > 0$ for all n large enough. Then $\varepsilon v_{k_n} = |v_{k_n}|$ for large enough and $\varepsilon z_{k_n} - Ak_n$ converges to $\frac{b(A-\varepsilon)}{2k}$. Since $2A$ is an integer, this forces

$$\varepsilon z_{k_n} - Ak_n = C := \frac{b(A-\varepsilon)}{2k}$$

for n large enough. But then

$$A^d P(k_n) = P(\varepsilon A k_n + \varepsilon C)$$

and finally $(\varepsilon A)^d P(X) = P(\varepsilon A X + \varepsilon C)$. Applying the previous lemma, we deduce again that $P(X) = c(X-x_0)^d$ for some c, x_0, and these are indeed solutions.

Problem 4 Find all monic polynomials with integer coefficients f such that $f(\mathbf{Z})$ is closed under multiplication.

Iranian TST 2007

Solution We may assume that f has positive leading coefficient. Looking for non-constant solutions and replacing f with $f(X+a)$ for a suitable integer a, we may assume that $f(1) > 1$. By assumption there is a sequence z_n of integers such that $P(1)P(n) = P(z_n)$, and the solution of the previous problem shows that $P(X) = (X-x_0)^d$ for some x_0, which must be an integer for P to have integer coefficients.

We are ready to deal with the most challenging problems of the article, which has remained unsolved for many years.

Problem 5 Find all monic polynomials P with integer coefficients such that for any positive integer m there is a positive integer n such that $P(m)P(m+1) = P(n)$.

Gabriel Dospinescu

Solution We will assume that P is non-constant (clearly the constant polynomial 1 is a solution of the problem) and let $d = \deg(P) > 0$. Choose M such that P is increasing on (M, ∞) and for each $n > M$ choose a positive integer x_n such that

$$P(n)P(n+1) = P(x_n).$$

For n large enough $x_n > M$ and $x_{n+1} > x_n$, and clearly $\lim_{n\to\infty} x_n = \infty$. We will now split the proof in a series of steps.

Lemma 3.2. *We have* $\lim_{n\to\infty} \frac{x_n}{n^2} = 1$.

Proof. It suffices to let $n \to \infty$ in the relation

$$\frac{P(n)P(n+1)}{n^{2d}} = \frac{P(x_n)}{x_n^d} \cdot \left(\frac{x_n}{n^2}\right)^d.$$

and observe that $\frac{P(x_n)}{x_n^d}$ converges to 1, and so does the left-hand side. □

Lemma 3.3. *We have* $\lim_{n\to\infty} \frac{x_{n+1}-x_n}{n} = 2$.

Proof. We start by observing that

$$P(x_{n+1}) - P(x_n) = P(n+1)(P(n+2) - P(n)).$$

By the mean value theorem

$$P(x_{n+1}) - P(x_n) = (x_{n+1} - x_n)P'(y_n)$$

for some y_n between x_n and x_{n+1}. Note that thanks to the previous lemma $\lim_{n\to\infty} \frac{P'(y_n)}{n^{2d-2}} = d$. Moreover

$$\lim_{n\to\infty} \frac{P(n+1)(P(n+2) - P(n))}{n^{2d-1}} = \lim_{n\to\infty} \frac{P(n+2) - P(n)}{n^{d-1}} = 2d.$$

The result follows by letting $n \to \infty$ in the relation

$$\frac{P(n+1)(P(n+2) - P(n))}{n^{2d-1}} = \frac{P(x_{n+1}) - P(x_n)}{n^{2d-1}} = \frac{x_{n+1} - x_n}{n} \cdot \frac{P'(y_n)}{n^{2d-2}}$$

and by using the previous discussion. □

The crucial step and the most beautiful result of this article is the following:

Lemma 3.4. *For all large enough n we have*

$$x_{n+1} - 2x_n + x_{n-1} = 2.$$

Proof. Taylor's formula yields the existence of $c_n \in (x_n, x_{n+1})$ and $d_n \in (x_{n-1}, x_n)$ such that

$$P(x_{n+1}) = P(x_n) + (x_{n+1} - x_n)P'(x_n) + \frac{(x_{n+1} - x_n)^2}{2}P''(c_n)$$

and

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

Consider the polynomial

$$Q(X) = P(X)P(X+1) = X^{2d} + ...$$

and observe that

$$P(x_{n+1}) + P(x_{n-1}) - 2P(x_n) = Q(n+1) - 2Q(n) + Q(n-1).$$

The mean value theorem applied twice shows that

$$Q(n+1) - 2Q(n) + Q(n-1) = Q''(r_n)$$

for some $r_n \in (n-1, n+1)$, so that

$$\lim_{n\to\infty} \frac{Q(n+1) - 2Q(n) + Q(n-1)}{n^{2d-2}} = \lim_{n\to\infty} \frac{Q''(r_n)}{n^{2d-2}} = 2d(2d-1).$$

Combining the previous relations yields

$$\lim_{n\to\infty} (x_{n+1} - 2x_n + x_{n-1})\frac{P'(x_n)}{n^{2d-2}} + \frac{(x_{n+1} - x_n)^2 P''(c_n)}{2n^{2d-2}} + \frac{(x_{n-1} - x_n)^2 P''(d_n)}{2n^{2d-2}} = 2d(2d-1).$$

Using the previous lemma we obtain

$$\lim_{n\to\infty} \frac{(x_{n+1} - x_n)^2 P''(c_n)}{2n^{2d-2}} = \lim_{n\to\infty} \frac{(x_{n-1} - x_n)^2 P''(d_n)}{2n^{2d-2}} = 2d(d-1),$$

and since $\lim_{n\to\infty} \frac{P'(x_n)}{n^{2d-2}} = d$, we obtain

$$d \cdot \lim_{n\to\infty} (x_{n+1} - 2x_n + x_{n-1}) + 4d(d-1) = 2d(2d-1),$$

yielding $\lim_{n\to\infty}(x_{n+1} - 2x_n + x_{n-1}) = 2$. The result follows, since $x_{n+1} - 2x_n + x_{n-1}$ are integers. □

Considering $y_n = x_n - x_{n-1}$, we have $y_{n+1} - y_n = 2$ for n large enough by the previous lemma, so that $y_n = 2n + c$ for n large enough and some integer c, and then $x_n = n^2 + an + b$ for some integers a, b and all large enough n.

Remark 3.5. More generally, for each map $g : \mathbf{Z}_{\geq n_0} \to \mathbf{R}$ set $\Delta g(n) = g(n+1) - g(n)$. If k is a positive integer and if $\Delta^k g = 0$, then $g(n) = P(n)$ for $n \geq n_0$, where P is a polynomial of degree at most $k-1$. Indeed, by Lagrange's interpolation formula we can find a polynomial P of degree at most $k-1$ such that $g(n) = P(n)$ for $n = n_0, n_0+1, \ldots, n_0+k-1$. Setting $Q(n) = P(n) - g(n)$ for $n \geq n_0$, we have $\Delta^k Q = 0$ for all $n \geq n_0$. Thus it suffices to prove that if Q satisfies $\Delta^k Q = 0$ and $Q(n_0) = ... = Q(n_0+k-1) = 0$, then $Q(n) = 0$ for all $n \geq n_0$. This follows immediately by induction on k.

Summarizing the previous work, we have two integers a, b such that

$$P(X)P(X+1) = P(X^2 + aX + b).$$

One easily checks that for any positive integer k the polynomial $R_k(X) = (X^2 + (a-1)X + b)^k$ satisfies

$$R_k(X)R_k(X+1) = R_k(X^2 + aX + b).$$

Suppose first that P has even degree, say $2d$, and write $P = R_d + Q$ for some polynomial Q of degree smaller than $2d$. Since $R_d(X)R_d(X+1) = R_d(X^2 + aX + b)$, we deduce that

$$R_d(X)Q(X+1) + Q(X)P(X+1) = Q(X^2 + aX + b).$$

Writing $Q = a_k X^k + ...$ with $a_k \neq 0$, we see that X^{2d+k} has coefficient $2a_k$ in the left-hand side and coefficient 0 in the right-hand side, which has degree $2\deg(Q) = 2k < 2d + k$. Thus necessarily $Q = 0$ and $P = R_d$. By the previous step

$$P(X)^2 = (X^2 + (a-1)X + b)^d.$$

Since d is odd, this forces $X^2 + (a-1)X + b$ being a square of a polynomial, thus we must have $(a-1)^2 = 4b$ and then $P(X) = (X+k)^d$ for some integer k.

So we have found all such polynomials.

Navid Safaei, Sharif University of Technology, Tehran, Iran