USEMO 2019/2

Evan Chen

Twitch Solves ISL

Episode 10

Problem

Let $\mathbb{Z}[x]$ denote the set of single-variable polynomials in x with integer coefficients. Find all functions $\theta\colon \mathbb{Z}[x] \to \mathbb{Z}[x]$ (i.e. functions taking polynomials to polynomials) such that

- for any polynomials $p, q \in \mathbb{Z}[x]$, $\theta(p + q) = \theta(p) + \theta(q)$;
- for any polynomial $p \in \mathbb{Z}[x]$, p has at least one integer root if and only if $\theta(p)$ has at least one integer root.

Video

https://youtu.be/V2TNgUwbs6A

External Link

https://aops.com/community/p15412166

Solution

The answer is that

$$\theta(x) = r(x) \cdot p(\pm x + c)$$

for any choice of $c \in \mathbb{Z}$, $r(x)$ without an integer root, with the choice of sign fixed. For the converse direction we present two approaches.

First solution. It's clear that this works, so we prove it is the only one. Let $r(x) = \theta(1)$, which has no integer root since the constant 1 has no roots at all.

Part 1. We fix a positive integer n and start by determining $\theta(x^n)$ which is the bulk of the problem. Let $f(x) = \theta(x^n)$. We look at

$$\theta(ax^n + b) = a \cdot f(x) + b \cdot r(x).$$

Let $g(x) = f(x)/r(x)$, a quotient of two polynomials whose denominator never vanishes. By using the problem condition in both directions, varying $x \in \mathbb{Z}$ and $-b/a \in \mathbb{Q}$, we find that

$$\frac{f(x)}{r(x)} \text{ takes on exactly the values } \dots, (-2)^n, (-1)^n, 0^n, 1^n, 2^n, 3^n, \dots \text{ for } x \in \mathbb{Z}$$

So let $g(x) = f(x)/r(x)$ now.

Claim (Rational functions can't be integer-valued forever)**.** Since g maps integers to integers, it must actually be a polynomial with rational coefficients.

Proof. We will only need the condition that g maps integers to integers.

If not, then by the division algorithm, we have $g(x) = d(x) + \frac{f_1(x)}{f_2(x)}$ for some polynomials $d(x), f_1(x), f_2(x)$ in $\mathbb{Q}[x]$ with $\deg f_2 > \deg f_1 \ge 0$. There exists an integer D such that $D \cdot d(x) \in \mathbb{Z}[x]$ (say the lcm of the denominators of the coefficients of g).

But for large enough integers x the value of $\frac{f_1(x)}{f_2(x)}$ is a nonzero and has absolute value less than $\frac{1}{D}$. This is a contradiction. □

Remark. You can't drop the condition that g has rational (rather than integer) coefficients in the proof above; consider $g(x) = \frac{1}{2}x(x+1)$ for example.

A common wrong approach is to try to use the same logic on $\theta(x^n)/\theta(x^{n-1})$ for $n \ge 2$. This doesn't work since $\theta(x^n)$ and $\theta(x^{n-1})$ could have a common root for $n \ge 2$ and therefore the problem condition essentially says nothing.

Let C be an integer divisible by every denominator in the coefficients of g. Then apparently

$$h(x) = C^n \cdot g(x)$$

is a polynomial which only takes only nth powers as $x \in \mathbb{Z}$.

Claim (Polya and Szego)**.** Since h is a polynomial with integer coefficients whose only values are nth powers, it must itself be the nth power of a polynomial.

Proof. This is a classical folklore problem, but we prove it for completeness.

Decompose h into irreducible factors as

$$h(x) = c \cdot f_0(x)^{e_0} \cdot f_1(x)^{e_1} \cdot f_2(x)^{e_2} \cdot f_3(x)^{e_3} \cdot \dots \cdot f_m(x)^{e_m}$$

where the f_i are nonconstant and c is an integer, and $e_i > 0$ for all $i > 0$. We also assume $m > 0$.

We use the following facts:

- In general, if $A(x), B(x) \in \mathbb{Z}[x]$ are coprime, then $\gcd(A, B)$ is bounded by some constant $C_{A,B}$. This follows by Bezout lemma.
- If $A(x) \in \mathbb{Z}[x]$ is a nonconstant polynomial, then there are infinitely many primes dividing some element in the range of A. This is called Schur's theorem.
- Let $A(x) \in \mathbb{Z}[x]$ be an irreducible polynomial, and let $A'(x)$ be its derivative. Then if p is prime and $p > C_{A,A'}$, and p has root in $\mathbb{F}_p$, then there exists x with $\nu_p(A(x)) = 1$. This follows by Hensel lemma.

Now for the main proof. By the above facts and the Chinese remainder theorem (together with Dirichlet theorem), we can select enormous primes $p_1 < p_2 < \dots < p_m < q$ (exceeding c, e, $\max e_i$, $\max C_{f_i,x}$, $\max C_{f_i,f_j}$ for all i and j) and a single integer N satisfying the following constraints:

- $\nu_{p_i}(f_i(N)) = 1$ for all $i = 1, \dots, m$, by requiring $N \equiv t_i \pmod{p_i^2}$ for suitable constant t_i not divisible by p_i (because of Hensel lemma);
- $p_i \nmid f_j(N)$ whenever $i \neq j$; this follows by the fact that $p_i > C_{f_i,f_j}$;

Now look at the value of $f(N)$. It has

$$\begin{aligned} \nu_{p_1}(f(N)) &= e_1 \\ \nu_{p_2}(f(N)) &= e_2 \\ &\vdots \\ \nu_{p_m}(f(N)) &= e_m. \end{aligned}$$

Now $f(N)$ is a nth power so n divides all of $e_1, \dots, e_m$. Finally c must be an nth power too. □

So $h(x)$ is an nth power; thus so is $g(x)$. Let's write $g(x) = p(x)^n$ then. Since $g = f/r$ was supposed to take on all the values $\dots$, $(-2)^n$, $(-1)^n$, 0^n, 1^n, 2^n, $\dots$, it follows that for every $k \geq 0$, the of $p(x)$ contains either k or $-k$. For density reasons, this forces p to be linear, and actually of the form $p(x) = \pm x + c$ for some constant c.

Part 2. We have now shown $\theta(x^n) = (\pm x + c)^n r(x)$, for every n, for some sign and choice of c depending possibly on n. It remains to show that the choices of signs and constants are compatible across the different values of n. So let's verify this.

By applying a suitable transformation on x let's assume $\theta(x) = x$ for simplicity. Then look at $\theta(x^n + ax) = (\pm x + c)^n + ax$ for choices of integers a. This is apparently supposed to have a root for each choice of a, but if $c \neq 0$, this means $\frac{1}{x}(\pm x + c)^n$ can take any integer value, which is obviously not true for density reasons. This means $c = 0$, so it shows $\theta(x^n) = \pm x^n$ for any integer n.

Finally, by considering $\theta(x^n + x - 2) = \pm x^n - x + 2$, we see the sign must be $+$ for the RHS to have an integer root. This finishes the proof.

Second solution, outline (by contestants). The solution is like the previous one, but replaces the high-powered Polya and Szego with the following simpler result.

Claim (Odd-degree polynomials are determined by their range)**.** Let $P(x) \in \mathbb{Z}[x]$ be an odd-degree polynomial. Let $Q(x)$ be another polynomial with the same range as P over $\mathbb{Z}$. Then $P(x) = Q(\pm x + c)$ for some ± and c.

Proof. First, Q also has odd degree since it must be unbounded in both directions. By negating if needed, assume Q has positive leading coefficient.

Take a sufficiently large integer n_0 such that $P(x)$ and $Q(x)$ are both strictly increasing for $x \geq n_0$, and moreover $P(n_0) > \max_{x<n_0} P(x)$, $Q(n_0) > \max_{x<n_0} P(x)$. Then take an even larger integer $n_1 > n_0$ such that $\min(P(n_1), Q(n_1)) > \max(P(n_0), Q(n_0))$. Choose $n_2 > n_0$ such that $P(n_1) = Q(n_2)$. We find that this implies

$$\begin{aligned} P(n_1) &= Q(n_2) \\ P(n_1+1) &= Q(n_2+1) \\ P(n_1+2) &= Q(n_2+2) \\ P(n_1+3) &= Q(n_2+3) \end{aligned}$$

and so on. So P is a shift of Q as needed. □

This is enough to force $\theta(x^n) = (\pm x + c)^n r(x)$ when n is odd. When n is even, for each integer k one can consider

$$\theta(kx^{n+3} + x^n) = k\theta(x^{n+3}) + \theta(x^n)$$

and use the claim on $\theta(x^{n+3})$ and $\theta(kx^{n+3} + x^n)$ to pin down $\theta(x^n)$.

Third solution (from author). The answers are as before and we prove only the converse direction.

Lemma. Given two polynomials $P, Q \in \mathbb{Z}[x]$, if $P + nQ$ has an integer root for all n, then either P and Q share an integer root or $P(x) = \left(\frac{x+m}{k}\right) Q(x)$ for some integers m, k with $k \neq 0$.

Proof. Let $d = \gcd(P(0), Q(0))$ so $P(0) = dr$ and $Q(0) = ds$. Now, for an integer root k_n of $P + nQ$,

$$k_n | P(0) + nQ(0) = dr + nds = d(r + ns).$$

Let p be a prime $\equiv r \bmod s$, of which there are infinitely many by Dirichlet's theorem. Now, for $n = \frac{p-r}{s}$, we have

$$k_n | dp.$$

As the divisors of dp are exactly those of d times 1 or p, there exists a (not necessarily positive) divisor j of d and a $t \in \{1, p\}$ so that $k_n = dt$ for infinitely many n. In the first case, we have that $P(j) + nQ(j) = 0$ for infinitely many n and some fixed j, which implies that j is a root of both P and Q. In the second case, we have, noting $p = r + ns$, that

$$P(j(r + ns)) + nQ(j(r + ns)) = 0.$$

As this holds for infinitely many n, we may rewrite it as a polynomial equation

$$P(x) = (ax + b)Q(x)$$

for some rational a, b. Now, we know that $(ax + b + n)Q(x)$ has a rational root for all $n \in \mathbb{Z}$. If Q has an integer root then P does as well and we are in our first case; otherwise, $\frac{n+b}{a} \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. This implies that $1/a \in \mathbb{Z}$, let it be k. Then $b/a \in \mathbb{Z}$; let it be m. This finishes the proof. □

Now, let $P_n(x) = f(x^n)$. We claim that $P_1(x) = (\pm x + t)P_0(x)$ for some $t \in \mathbb{Z}$. Indeed, $P_1 + nP_0$ has an integer root for all n, so either P_1 and P_0 share an integer root or $P_1(x) = \left(\frac{x+m}{k}\right) P_0(x)$ for some $m, k \in \mathbb{Z}$. They clearly cannot share a root, since $P_0(x)$ cannot have any integer roots. Now,

$$kP_1(x) + P_0(x) = (x + m + k)P_0(x)$$

has an integer root, so $kx + 1$ must as well, and thus $k = \pm 1$, as desired. Now, we see that

$$\theta\left(a(x^n - c^n) + b(x - c)\right) = a\big(P_n(x) - c^n P_0(x)\big) + b\big(P_1(x) - cP_0(x)\big)$$

has an integer root for any c, a, b. Let $Q = P_n - c^n P_0$ and $R = P_1 - cP_0$. Since $aQ + bR$ has an integer root for all $a, b \in \mathbb{Z}$, we can apply our lemma on both the pair (Q, R) and (R, Q); if they do not share an integer root, then Q must be a linear polynomial times R and R must be a linear times Q, a contradiction unless they are both 0 (in which case they share any integer root). So, Q and R share an integer root. We have

$$R(x) = P_1(x) - cP_0(x) = (\pm x + t - c)P_0(x),$$

and P_0 has no integer root as 1 has no integer root, so we have that $\pm(c - t)$ is the only integer root of R and is thus also a root of Q; in particular

$$P_n(\pm(c - t)) = c^n P_0(\pm(c - t))$$

for all $c \in \mathbb{Z}$. This is a polynomial equation that holds for infinitely many c so we must have that

$$P_n(\pm(x - t)) = x^n P_0(\pm(x - t)) \implies P_n(x) = (\pm x + t)^n P_0(x).$$

Thus, if $Q(x) = \sum_{i=0}^{d} a_i x^i$,

$$\theta(Q(x)) = \theta\left(\sum_{i=0}^{d} a_i x^i\right) = \sum_{i=0}^{d} a_i(\pm x + t)^i P_0(x) = P_0(x)Q(\pm x + t),$$

finishing the proof.