Korea Winter 2019/3

Evan Chen

Twitch Solves ISL

Episode 160

Problem

Find all polynomials $P(x)$ with integer coefficients such that for all positive number n and prime p satisfying $p \nmid nP(n)$, the order of n modulo p is at least the order of $P(n)$ modulo p.

Video

https://youtu.be/uvcgiSAyjzc

External Link

https://aops.com/community/p11573483

Solution

The answer is $P(n) = n^d$ only for $d \geq 0$, which clearly works.

For the other direction, we assume P is nonconstant, and let ℓ be a large prime, say $\ell > 100(\deg P + 100)^2$.

Claim. For this prime ℓ, we have a divisibility of $\mathbb{Z}[X]$-polynomials

$$\Phi(X) \coloneqq X^{\ell-1} + X^{\ell-2} + \cdots + 1 \mid P(X)^\ell - 1.$$

Proof. Because Φ is irreducible and has large degree, it is coprime to both $P(n)$ and $P(n) \pm 1$. Then there exists a constant C such that

$$\gcd(\Phi(n), P(n)(P(n)^2 - 1)) \leq C$$

for all n, by Bezout.

Consider large primes $p > C$ such that

- $p \not\equiv 1 \pmod{q}$ for any prime $3 \leq q < \ell$,
- $p \equiv 1 \pmod{\ell}$.

There are infinitely many such primes by Dirichlet. For each such p, we can find n such that $p \mid \Phi(n)$, simply by taking g to be a primitive modulo p, and choosing $n = g^{\frac{p-1}{\ell}}$.

For that n we have $p \mid n^\ell - 1$, so the order of n is at most ℓ. Consequently, p divides

$$P(n) \cdot (P(n) - 1) \cdot (P(n)^2 - 1) \cdot \cdots \cdot (P(n)^\ell - 1).$$

Now p has to divide these factors. It doesn't divide $P(n)$ as $p > C$. And if it divided $P(n)^k - 1$ for some $k < \ell$, then the order of $P(n)$ modulo p would be a divisor of k. But it should also divide $\ell - 1$, and because of constraints on p this would be force the order to be at most 2. From $p > C$, that's impossible too. Hence p divides $P(n)^\ell - 1$, the last factor.

In other words, we have shown there are arbitrarily large primes such that p divides $\Phi(n)$ and $P(n)^\ell - 1$ for some ℓ. Hence (via the same Bezout argument) it follows $\Phi(X)$ is not coprime to $P(X)^\ell - 1$ and hence divides it. □

Now let ζ be a primitive ℓ^{th} root of unity. Then $P(\zeta)$ is an ℓ^{th} root of unity as well, so

$$P(\zeta) - \zeta^d = 0.$$

for some integer r, say $0 \leq d \leq \ell - 1$. However, $\Phi(X) \coloneqq X^{\ell-1} + X^{\ell-2} + \cdots + 1$ is the minimal polynomial of ζ, and $\deg P \ll \ell$. Reading the coefficients of our nonconstant P, this could only happen if $P(X) = X^d$ exactly, as desired.

Remark. The last step of the argument really uses the fact we have $P(X)^\ell - 1$. It would not work if we instead had $P(X)^k - 1$ for some $k < \ell$, because then the $\operatorname{lcm}(k, \ell)^{\text{th}}$ cyclotomic polynomial may not be so well-behaved. That's why in the proof of the claim we had to some modular condition on p (with $p \not\equiv 1 \pmod{q}$ for all q) to rule out the possibility that p divided any of the other factors. If one tries the argument at first with just generic large p dividing an element in the range of Φ, one would instead get $\Phi(X) \mid P(X)^k - 1$ for some k depending on ℓ, leading to the issue above.