USEMO 2022/5

Evan Chen

Twitch Solves ISL

Episode 103

Problem

Let $\tau(n)$ denote the number of positive integer divisors of a positive integer n (for example, $\tau(2022) = 8$). Given a polynomial $P(X)$ with integer coefficients, we define a sequence $a_1, a_2, \dots$ of nonnegative integers by setting

$$a_n = \begin{cases} \gcd\left(P(n),\ \tau(P(n))\right) & \text{if } P(n) > 0 \\ 0 & \text{if } P(n) \le 0 \end{cases}$$

for each positive integer n. We then say the sequence *has limit infinity* if every integer occurs in this sequence only finitely many times (possibly not at all).

Does there exist a choice of $P(X)$ for which the sequence $a_1, a_2, \dots$ has limit infinity?

Video

https://youtu.be/dC9VpiGVRqs

External Link

https://aops.com/community/p26379812

Solution

We claim the answer is no, such P does not exist.

Clearly we may assume P is nonconstant with positive leading coefficient. Fix P and fix constants $n_0, c > 0$ such that $c = P(n_0) > 0$. We are going to prove that infinitely many terms of the sequence are at most c.

We start with the following lemma.

Claim. For each integer $n \ge 2$, there exists an integer $r = r(n)$ such that

- For any prime p which is at most n, we have $\nu_p(P(r)) = \nu_p(c)$.
- We have
$$c \cdot \prod_{\text{prime } p \le n} \le r \le 2c \cdot \prod_{\text{prime } p \le n} p.$$

Proof. This follows by the Chinese remainder theorem: for each $p \le n$ we require $r \equiv n_0 \pmod{p^{\nu_p(c)+1}}$, which guarantees $\nu_p(P(r)) = \nu_p(P(n_0)) = \nu_p(c)$. Then there exists such an r modulo $\prod_{p \le n} p^{\nu_p(c)+1}$ as needed. $\square$

Assume for contradiction that all a_i are eventually larger than c. Take n large enough that $n > c$ and $r = r(n)$ has $a_r > c$. Then consider the term a_r:

- Using the conditions in the lemma it follows there exists a prime $p_n > n$ which divides $a_r = \gcd(P(r), \tau(P(r)))$ (otherwise a_r, which divides $P(r)$, is at most c).
- As p_n divides $\tau(P(r))$, this forces $P(r)$ to be divisible by (at least) $q_n^{p_n-1}$ for some prime q_n.
- For the small primes p at most n, we have $\nu_p(P(r)) = \nu_p(c) < c < n \le p_n - 1$. It follows that $q_n > n$.
- Ergo,
$$P(r) \ge q_n^{p_n-1} > n^n.$$

In other words, for large enough n, we have the asymptotic estimate

$$\begin{aligned} n^n < P(r) &= O(1) \cdot r^{\deg P} \\ &= O(1) \cdot c^{\deg P} \cdot \prod_{\text{prime } p \le n} p^{\deg p} \\ &< O(1) \cdot n^{\deg P \cdot \pi(n)} \end{aligned}$$

where $\pi(n)$ denotes the number of primes less than n. For large enough n this is impossible since the primes have zero density:

$$\lim_{n \to \infty} \frac{\pi(n)}{n} = 0.$$

Remark. For completeness, we outline a short elementary proof that $\lim_{n\to\infty} \frac{\pi(n)}{n} = 0$. For integers $M > 0$ define

$$\delta(M) := \prod_{p \le M} \left(1 - \frac{1}{p}\right).$$

Then $\pi(n) < \delta(M)n + \prod_{p \le M} p$, so it suffices to check that $\lim_{M\to\infty} \delta(M) = 0$. But

$$\frac{1}{\delta(M)} = \prod_{p \le M} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \le M} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) \ge 1 + \frac{1}{2} + \dots + \frac{1}{M}$$

which diverges for large M.