Non-constant $f(X) \in \mathbb{Z}[X]$ has Zeros in $\mathbb{Z}_p$ for Infinitely Many Primes p

S Kumaresan
Gitam Universsity
kumaresa@gmail.com

6/11/23

Let $f(X) = c_0 + c_1 X + \cdots + c_n X^n \in \mathbb{Z}[X]$ be a nonconstant polynomial with integral coefficients. Observe that $n \geq 1$ and $c_n \neq 0$. We say that $k \in \mathbb{Z}$ is a zero (or root) of f modulo N if $f(k) \equiv 0 \pmod{N}$. Recall that if R and S are commutative rings with identity and if $\varphi\colon \mathbb{R} \to S$ is a ring homomorphism, we have an induced homomorphism $\overline{\varphi}\colon R[X] \to S[X]$ defined by $\overline{\varphi}(f)(X) := \varphi_{c_0} + \varphi(c_1)X + \cdots + \varphi(c_n)X^n$. Using this notion, we see that f has aa zero modulo N iff $\varphi(f)$ has a zero in $\mathbb{Z}_N$.

Let $k \in \mathbb{Z}$ b a zero of f. Then f has a zero in $\mathbb{Z}_N$ for every $N \in \mathbb{N}$. (Why?)

Exercise 1. Prove that f has a zero in $\mathbb{Z}_N$ iff there exists $k \in \mathbb{Z}$ and $m \in \mathbb{Z}$ such that $f(k) = mN$.

Exercise 2. Let $m \in \mathbb{Z}$. Let $N := f(m) \in \mathbb{Z}$. Prove that f has a zero in $\mathbb{Z}_N$. Can we conclude that there exist infinitely many $N \in \mathbb{N}$ such that f has a zero in $\mathbb{Z}_N$? If you want to conclude this, what do you need to observe/prove

The next result strengthens the result of the last exercise.

Theorem 3. *Let $f(X) = c_0 + c_1 X + \cdots + c_n X^n \in \mathbb{Z}[X]$ be a nonconstant polynomial. Then there exist infinitely many primes p such that f has a zero in $\mathbb{Z}_p$.*

Proof. We may assume WLOG that f has not integral roots. (Why?) In particular, $c_0 \neq 0$. (Why?) Let p_i, $1 \leq i \leq r$ be the finite number of primes such that f has a zero modulo each p_i. We shall show show that there exists a prime p, different from each of the p_i's such that f has a zero modulo p. (Does this remind you of anything you learned earlier?)

Let $\alpha := p_1 \cdots p_r c_0$. We define a new polynomial $g(X) \in \mathbb{Z}[x]$ via the identity:

$$\begin{aligned} f(\alpha X) &= c_0 + c_1 \alpha X + \cdots + c_n (\alpha X)^n \\ &= c_0 g(X). \qquad \text{(Why is this possible?)} \end{aligned}$$

If we write $g(X) = d_0 + d_1 X + \cdots + d_n X^n$, then each of the coefficients of the nonconstant term $d_1, d_1, \ldots, d_n$ is divisible by $p_1 \ldots p_r$. (Why?) Since g is not a constant (Why?), there exists an integer $m \in \mathbb{Z}$ such that $g(m) \neq \pm 1$. (Why?) Let p be a prime divisor of $g(m)$. Note that $g(m) \equiv 1(\pmod{p}_i)$, $1 \leq i \leq r$. Hence $p \notin \{p_1, \ldots, p_r\}$. (Why?) We observe that p divides $c_g(m) = f(\alpha m)$. (Why?) Hence f has a zero modulo p. (Why?) $\square$