10 Number of solutions modulo a prime

Theorem *(Lagrange) Fix a prime p and integer $n \geq 1$. Let $f(x) = a_n x^n + \cdots + a_0$ be a polynomial with coefficients $a_i \in \mathbb{Z}$, such that some a_j is prime to p. Then the congruence*

$$f(x) \equiv 0 \,(mod\, p) \tag{1}$$

has at most n solutions mod p.

Proof: Suppose $n \equiv 1$. Then the congruence is $a_1 x \equiv -a_0 \,(\mathrm{mod}\, p)$. By hypothesis, either a_1 or a_0 is not divisible by p. The former case must happen as otherwise we would have $0 \equiv -a_0 \pmod{p}$, implying a_0 is also $\equiv 0$ (mod p), leading to a contradiction. Thus a_1 is invertible mod p; let a_1' be such that $a_1' a_1 \equiv 1 (\mathrm{mod}\, p)$. Multiplying $a_1 x \equiv -a_0 \,(\mathrm{mod}\, p)$ by a_1', get

$$(a_1' a_1)x \equiv x \equiv -a_1' a_0 (\mathrm{mod}\, p)$$

Thus we get a unique solution, and the Theorem is O.K. for $n = 1$.

Now let $n > 1$, and assume by induction that the Theorem holds for all $k < n$. Suppose (1) has no solutions mod p. Then there is nothing to prove. So we may assume that there is at least one solution, say $x \equiv x_1 \,(\mathrm{mod}\, p)$. Then we get

$$f(x_1) \equiv 0 \,(\mathrm{mod}\, p). \tag{2}$$

Subtracting (2) from (1), we get

$$f(x) - f(x_1) \equiv a_n(x^n - x_1^n) + a_{n-1}(x^{n-1} - x_1^{n-1}) + \cdots a_1(x - x_1) \equiv 0 \,(\mathrm{mod}\, p).$$

But for any $k \geq 1$, $(x - x_1) \mid (x^k - x_1^k)$, so $f(x) - f(x_1) = (x - x_1)g(x)$, where $g(x)$ is a polynomial in x of degree $k - 1$. Thus, $f(x) - f(x_1) \equiv 0 \,(\mathrm{mod}\, p)$ holds iff

$$(x - x_1)g(x) \equiv 0 \,(\mathrm{mod}\, p). \tag{3}$$

Then **either** $x - x_1 \equiv 0$ **or**

$$g(x) \equiv 0 \,(\mathrm{mod}\, p) \tag{4}$$

The coefficients of g cannot all be $\equiv 0$ (mod p), for otherwise $f(x)$ would be congruent to 0 (mod p). Since the degree of g is $< n$, we then have by the inductive hypothesis, that the number of solutions of (4) mod p is bounded above by $n-1$. Then the number of solutions mod p of (1) is $\leq 1 + n - 1 = n$.