Worksheet 5

1. Prove that for an integer polynomial $f(x)$ of degree n such that not all its coefficients are divisible by a fixed prime p, the congruence

$$I : f(x) \equiv 0 \mod p$$

has at most n roots.

Hint: Use the representation

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_k)q(x) + pr(x),$$

where $a_1, a_2, \cdots, a_k$ are roots of the congruence I.

2. The above result is famously called as "Lagrange's theorem". Lagrange theorem is false for prime power moduli i.e.

$$f(x) \equiv 0 \mod p^k.$$

Give an example of a polynomial $f(x)$, prime p and integer k to support the claim.

3. Solve the congruence equations

   (a) $x^3 + 4x \equiv 4 \mod 343$

   (b) $x^2 \equiv 0 \mod 12$

   (c) $x^3 + x + 2 \equiv 0 \mod 36$