Quadratic congruences: Conclusion

We extend Proposition 2 at the end of last lecture to give the number of solutions of a quadratic congruence (mod p^n).

Proposition 1. *Let $n \geq 1$, let p be an odd prime and let $a \in \mathbb{Z}$ be such that* $\gcd(a,p) = 1$. *Then, the number of distinct solutions of $x^2 \equiv a \pmod{p^n}$ is 2 or 0, depending on whether $(\frac{a}{p}) = 1$ or not.*

Proof. Denote by (C_n) the congruence $x^2 \equiv a(\pmod{p^n}$. It is sufficient to show that if $(\frac{a}{p}) = 1$, then (C_n) has exactly 2 distinct solutions (mod p^n). We use induction. Suppose that (C_n) has ≥ 3 distinct solutions (mod p^n) for some $n \geq 2$. By induction hypothesis, there exist two solutions x_1, x_2 of (C_n) such that $x_1 \equiv x_2 \pmod{p^{n-1}}$, that is, $x_2 = x_1 + tp^{n-1}$ where $1 \leq t \leq p-1$. It follows that $x_2^2 \equiv x_1^2 + 2x_1tp^{n-1} \pmod{p^n}$, that is, $p|x_1t$, which is impossible. □

Quadratic (and polynomial) congruences with respect to an arbitrary modulus are taken care of by the following extension of the Chinese Remainder Theorem (CRT).

Theorem 2. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial, let $m_1, m_2, \ldots, m_s$ be pairwise coprime integers ≥ 2, and let $m = m_1m_2 \ldots m_s$. Suppose that for each i, $1 \leq i \leq s$, the congruence $f(x) \equiv 0 \pmod{m_i}$ has exactly t_i pairwise incongruent solutions mod m_i. Then, the congruence $f(x) \equiv 0 \pmod{m}$ has exactly $t_1t_2 \ldots t_s$ mutually incongruent solutions modulo m.*

Proof. Each solution (mod m) of the system $f(x) \equiv 0 \pmod{m_i}$, $1 \leq i \leq s$, determines an s-tuple of solutions ($x \pmod{m_i}$; $1 \leq i \leq s$). Conversely, if x_i is (mod m_i) a solution of $f(x) \equiv 0 \pmod{m_i}$, then the s-tuple $(x_1, x_2, \ldots, x_s)$ determines a solution of the system (mod m). The method of the proof of (CRT) shows that this correspondence is one-to-one - supply the details! □

Despite the theory for deciding solvability of quadratic congruences, there is no good way of actually solving them in general. Small moduli, however, are accessible, even for systems of congruences.

Example 1. Consider the system of congruences $x^2 + x + 1 \equiv 0 \pmod{91}$, $x \equiv 3 \pmod{11}$. The quadratic congruence is equivalent to the pair $x^2+x+1 \equiv 0 \pmod{13}$ and $x^2+x+1 \equiv 0 \pmod{7}$. The first is equivalent to $(x-6)^2 \equiv 9 \pmod{13}$ and has solutions 3 and -4; the second is equivalent to $(x-3)^2 \equiv 1 \pmod{7}$ and has solutions 2 and 4. Combining the solutions gives four solutions $x = -17, -10, 9, 16 \pmod{91}$; combining these with $x \equiv 3 \pmod{11}$ yields the four final solutions $x = -283, -173, 256, 289 \pmod{1001}$.

We conclude with a result on the number of solutions of a polynomial congruence modulo a prime.

Lemma 3. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n and let p be a prime. Then, the congruence $f(x) \equiv 0 \pmod{p}$ has at most* $\min\{n, p\}$ *mutually incongruent solutions modulo p.*

Proof. Induction: Assume that the Lemma holds for all polynomials of degree less than n, where $n \geq 2$. For a contradiction, let $f(x)$ as above have at least $n+1$ solutions x_i, $1 \leq i \leq n+1$, incongruent mod p. Then, the polynomial $g(x) = f(x) - \prod_{1 \leq i \leq n}(x - x_i)$ has degree $< n$ and at least n roots. Since we are working mod p, we may w.l.o.g. assume that $g(x)$ is monic. By induction hypothesis, $g(x) \equiv 0 \pmod{p}$ for every $x \in \mathbb{Z}$. Hence $g(x_{n+1}) \equiv 0 \mod p$, that is, p divides $\prod_{1 \leq i \leq n}(x_{n+1} - x_i)$. This contradicts the assumption that the $n+1$ original solutions were incongruent mod p. And, clearly, there are at most p solutions. □