

Quadratic Reciprocity

• studied linear congruences

$$ax \equiv b \pmod{m}$$

• quadratic equations

$$x^2 \equiv a \pmod{p} \quad p \text{ prime.}$$

Thm. Let  $f(x) = a_n x^n + \dots + a_1 x + a_0$ ,  $p$  be a prime and  $(a_n, p) = 1$ . Then the congruence  $f(x) \equiv 0 \pmod{p}$  has at most  $n$  solutions.

Proof: Induction on  $n$ .

$$n=1: \quad a_1 x + a_0 \equiv 0 \pmod{p}, \quad (a_1, p) = 1$$

$$a_1 x \equiv -a_0 \pmod{p} \Rightarrow x \equiv -\bar{a}_1 a_0 \pmod{p}, \text{ which gives exactly 1 solution.}$$

Prove for  $n$  assuming true for a degrees  $< n$ .

Suppose not. Then  $u_1, \dots, u_m$  are distinct solutions, so

$$u_i \not\equiv u_j \pmod{p} \quad i \neq j$$

$$\text{Let } g(x) = f(x) - a_n(x-u_1)(x-u_2)\dots(x-u_n)$$

$$\deg g < n, \text{ since } g(x) = f(x) - (a_n x^n - a_n(u_1 + \dots + u_n)x^{n-1} + \dots)$$

$$g(u_i) \equiv 0 \pmod{p} \text{ for } i=1, \dots, n.$$

By induction, all coeff. of  $g$  are congruent to 0 (mod  $p$ ), since these are  $n$  distinct sol'n and degree  $g < n$ .

$$g(x) = b_m x^m + \dots + b_0, \quad \bar{g}(x) = \sum_{i=0}^m b_i x^i. \text{ For any } u, g(u) \equiv \bar{g}(u) \pmod{p}.$$

So  $\bar{g}$  has form of theorem, unless it's the zero poly,

and  $\bar{g}(u_i) \equiv 0 \pmod{p} \quad i=1, \dots, n$ . But since  $\deg g < n$ ,

this gives a contradiction unless  $\bar{g}(x)$  is zero poly.

Thus,  $g(a) \equiv 0 \pmod{p}$  for any  $a$ .

$$\text{In particular, } g(u_{n+1}) = f(u_{n+1}) + a_n(u_{n+1} - u_1)\dots(u_{n+1} - u_n) \equiv 0 - a_n(u_{n+1} - u_1)\dots(u_{n+1} - u_n) \equiv 0 \pmod{p}.$$

so  $p \mid a_n(u_{n+1} - u_1)\dots(u_{n+1} - u_n)$ , and since  $p \nmid a_n$ ,

$p \mid (u_{n+1} - u_i)$  for some  $i$ , which is a contradiction

since  $u_j$  were all distinct mod  $p$ .

Cor. The equation  $x^2 \equiv a \pmod{p}$  has  $\begin{cases} 2 \text{ or } 0 \text{ solutions if } (a, p) = 1 \\ 1 \text{ solution if } p \mid a \end{cases}$

Proof. If  $x$  is a sol,  $-x$  also solution, and if  $(p, a) = 1$ ,  $-x \not\equiv x \pmod{p}$

Def.  $p$  odd prime, the Legendre symbol  $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has sol, } (a, p) = 1 \\ 0 & \text{if } p \mid a \\ -1 & \text{otherwise} \end{cases}$

Thus, the cor reduces to  $x^2 \equiv a \pmod{p}$  has  $1 + \left(\frac{a}{p}\right)$  solns.

Def.  $m > 0$ ,  $(a, m) = 1$ . The order of  $a$  mod  $m$  is the smallest positive integer  $h$  for which  $a^h \equiv 1 \pmod{m}$

Thm.  $p$  prime. Then there are  $\phi(p-1)$  congruence classes  $a$  mod  $p$  of order  $p-1$ .

Remark:  $g$  is such an integer, then  $0, 1, g, g^2, \dots, g^{p-2}$  is a complete residue system mod  $p$ .

$$g^i \equiv g^j \pmod{p} \quad i > j \quad g^{i-j} \equiv 1 \pmod{p}$$

Proof: By 4 lemmas, which will be proved next time.

Lemma 1: If  $a$  has order  $h$  (mod  $m$ ), then those  $k$  for which  $a^k \equiv 1 \pmod{m}$  are precisely those for which  $h|k$ .

Proof:  $k = qh + r$ ,  $0 \leq r < h$ .  $a^k \equiv a^{qh} \cdot a^r \equiv a^r \pmod{m}$ , so  $a^r \equiv 1 \pmod{m}$ , which contradicts minimality of  $h$  unless  $r=0$ . Also,  $h|k \Rightarrow a^k \equiv a^{nh} = (a^h)^n \equiv 1 \pmod{m}$

Lemma 2: If  $a$  has order  $h$ , then  $a^k$  has order  $h/(h, k)$

Proof:

$$(a^k)^j \equiv 1 \pmod{m} \Leftrightarrow h|kj \text{ (by Lemma 1)} \Leftrightarrow \frac{h}{(h, k)} | \frac{k}{(h, k)} j$$