Math 412: Number Theory
Lecture 1~~6~~ quadratic residues and nonresidues

17

Gexin Yu
gyu@wm.edu

College of William and Mary

quadratic residue and nonresidue modulo p

- How to solve quadratic equations $ax^2 + bx + c \equiv 0 \pmod{m}$ where $(a, m) = 1$?

$$4a(ax^2+bx+c) \equiv 0 \pmod{m}$$

$$4a^2x^2 + 4abx + 4ac \equiv 0$$

$$(2ax)^2 + 2 \cdot 2ax \cdot b + b^2 - b^2 + 4ac \equiv 0$$

$$(2ax+b)^2 \equiv b^2 - 4ac$$

$$y^2 \equiv d \pmod{m}$$

quadratic residue and nonresidue modulo p

- How to solve quadratic equations $ax^2 + bx + c \equiv \pmod{m}$ where $(a, m) = 1$?
- We can simplify it to $y^2 \equiv d \pmod{m}$.

quadratic residue and nonresidue modulo p

- How to solve quadratic equations $ax^2 + bx + c \equiv \pmod{m}$ where $(a, m) = 1$?
- We can simplify it to $y^2 \equiv d \pmod{m}$.
- Or equivalently, we need to determine whether $x^2 \equiv d \pmod{m}$ has solution or not.

quadratic residue and nonresidue modulo p

- How to solve quadratic equations $ax^2 + bx + c \equiv \pmod{m}$ where $(a, m) = 1$?

$y = 2ax + b$

- We can simplify it to $y^2 \equiv d \pmod{m}$.
- Or equivalently, we need to determine whether $x^2 \equiv d \pmod{m}$ has solution or not.
- Def: let m be an integer and $(d, m) = 1$. Then d is a quadratic residue modulo m if $x^2 \equiv d \pmod{m}$ has a solution; d is quadratic nonresidue modulo m if it has no solution.

- Lem: let p be an odd prime and $(a,p)=1$. Then $x^2 \equiv a \pmod{p}$ has either no solution or exactly two solutions modulo p.

$x^2 - a \equiv 0 \pmod{p} \Longrightarrow$ has at most 2 solutions, by L. thm.

Let x_0 be a solution. Then $-x_0$ is also a solution.

But $x_0 \not\equiv -x_0 \pmod{p}$. (o/w, $p \mid 2x_0 \Rightarrow p \mid x_0$

$\Rightarrow x_0^2 \equiv 0 \pmod{p}$

$\equiv a$, a contradiction)

- Lem: let p be an odd prime and $(a, p) = 1$. Then $x^2 \equiv a \pmod{p}$ has either no solution or exactly two solutions modulo p.

1, 2, 4 are q.r. mod 7.
3, 5, 6 are q non-r. mod 7.

Ex: $\{\pm 1, \pm 2, \pm 3\} \longrightarrow 1^2 = 1,\ 2^2 = 4,\ 3^2 = 9 \equiv 2 \pmod 7$

- Thm: there are $(p-1)/2$ quadratic residues modulo p and $(p-1)/2$ quadratic nonresidues modulo p.

Ex: $p = 3$. $x^2 \equiv 1 \pmod 3$ has solutions. $\Rightarrow$ 1 is a q.r.
$x^2 \equiv 2 \pmod 3$ has no solution. $-1\,(2)$ is a q. non-r.

Pf: $U(p) = \{1, 2, \cdots, p-1\} = \{\pm 1, \pm 2, \cdots, \pm \frac{p-1}{2}\}$
but $(\pm 1)^2 = 1,\ (\pm 2)^2 = 4, \cdots, (\pm \frac{p-1}{2})^2$ give exactly $\frac{p-1}{2}$ different integers

Thm: let r be a primitive root of prime p, and $(a, p) = 1$. Then a is a quadratic residue of p if and only if $ind_r a$ is even.

$$ind_r a = \min\{t \in \mathbb{N} : r^t \equiv a \pmod p\} \in \{0, 1, 2, \cdots, p-1\}$$

pf: "$\Rightarrow$": a is a q.r. mod p $\Rightarrow$ $x^2 \equiv a \pmod p$ for some x.

$\Rightarrow$ $ind_r(x^2) \equiv ind_r(a)$ $\Rightarrow$ $ind_r(a) \equiv \underbrace{2\, ind_r(x)}_{\text{even}} \pmod{\cancel{p-1}\ \phi(p)}$

$\Rightarrow$ $ind_r(a)$ is even.

"$\Leftarrow$": $ind_r(a)$ is even. $\Rightarrow$ let x be $ind_r(x) = \underline{\dfrac{ind_r(a)}{2}} \in [p-1]$.

$\Rightarrow$ $a \equiv x^2 \pmod p$.

Legendre symbol

Legendre symbol of d modulo p: let p be an odd prime. Define the

$$\left(\frac{d}{p}\right) = \begin{cases} 1, & \text{if } d \text{ is a quadratic residue modulo } p \\ -1, & \text{if } d \text{ is a quadratic nonresidue modulo } p \\ 0, & \text{if } p \mid d \end{cases}$$

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1, \iff 1, 2, 4 \text{ are q.r. mod } 7.$$

$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

Thm (Euler Criterion): Let prime $p > 2$ and $p \nmid d$. Then

$$\left(\frac{d}{p}\right) \equiv d^{(p-1)/2} \pmod{p}.$$

pf: If d is a quadratic residue, then $d \equiv x_0^2 \pmod{p}$. Clearly $(p, x_0) = 1$.

$\Rightarrow \quad d^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} = \underline{x_0^{p-1} \equiv 1 \pmod{p}}$. (Euler Thm).

So $\quad 1 = \left(\frac{d}{p}\right) \equiv d^{\frac{p-1}{2}} \pmod{p}$.

If d is a q. non-residue, then for each integer $1 \le i \le p-1$, there exists a $j \in [1, p-1]$, $j \neq i$, s.t. $ij \equiv d \pmod{p}$.

$\Rightarrow \underbrace{1 \cdot 2 \cdot 3 \cdots (p-1)}_{= (p-1)! \equiv -1 \text{ (Wilson)}} \equiv \underbrace{d \cdot d \cdots d}_{(p-1)/2} = d^{\frac{p-1}{2}} \pmod{p}$

Thm (Euler Criterion): Let prime $p > 2$ and $p \nmid d$. Then

$$\left(\frac{d}{p}\right) \equiv d^{(p-1)/2} \pmod{p}.$$

Cor: -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 4$.

$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} = 1, \iff \frac{p-1}{2}$ is even. $\iff p \equiv 1 \pmod 4$.

Properties of Legendre symbol modulo p

- $\left(\frac{d}{p}\right) = \left(\frac{p+d}{p}\right)$

$$\left(\frac{d}{p}\right) \equiv d^{\frac{p-1}{2}} \equiv (d+p)^{\frac{p-1}{2}} \equiv \left(\frac{d+p}{p}\right) \pmod p$$

$$\Downarrow$$

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \text{ if } a \equiv b \pmod p.$$

Ex: $\left(\frac{100000}{7}\right) = \left(\frac{5}{7}\right) = -1.$

Properties of Legendre symbol modulo p

- $\left(\frac{d}{p}\right) = \left(\frac{p+d}{p}\right)$
- $\left(\frac{cd}{p}\right) = \left(\frac{c}{p}\right)\left(\frac{d}{p}\right)$

pf: $\left(\frac{cd}{p}\right) \equiv (cd)^{\frac{p-1}{2}} = c^{\frac{p-1}{2}} \cdot d^{\frac{p-1}{2}} \equiv \left(\frac{c}{p}\right) \cdot \left(\frac{d}{p}\right) \pmod p$.

$$\left(\frac{100000}{7}\right) = \left(\frac{10^5}{7}\right) = \left[\left(\frac{10}{7}\right)\right]^5 = \left(\left(\frac{3}{7}\right)\right)^5 = (-1)^5 = -1.$$

Properties of Legendre symbol modulo p

- $\left(\frac{d}{p}\right) = \left(\frac{p+d}{p}\right)$

- $\left(\frac{cd}{p}\right) = \left(\frac{c}{p}\right)\left(\frac{d}{p}\right)$

- If $p \nmid d$, then $\left(\frac{d^2}{p}\right) = 1$

pf1 definition

pf2 $\left(\frac{d^2}{p}\right) = \left(\frac{d}{p}\right)\cdot\left(\frac{d}{p}\right) = \left(\frac{d}{p}\right)^2 = 1$.

$n = 2^3 \cdot 3^5 \cdot 11^2 \cdot 13^3$

$\left(\frac{n}{7}\right) = \left(\frac{2^3}{7}\right)\cdot\left(\frac{3^5}{7}\right)\left(\frac{11^2}{7}\right)\left(\frac{13^3}{7}\right) = \left(\frac{2}{7}\right)\cdot\left(\frac{3}{7}\right)\left(\frac{13}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right)\left(\frac{6}{7}\right) = 1\cdot(-1)\cdot 1 = -1$.

Properties of Legendre symbol modulo p

- $\left(\frac{d}{p}\right) = \left(\frac{p+d}{p}\right)$

- $\left(\frac{cd}{p}\right) = \left(\frac{c}{p}\right)\left(\frac{d}{p}\right)$

- If $p \not| d$, then $\left(\frac{d^2}{p}\right) = 1$

- $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

$n = -123$

$= -1 \cdot 3 \cdot 41$

$\left(\frac{n}{7}\right) = \left(\frac{-123}{7}\right) = \left(\frac{-1}{7}\right) \cdot \left(\frac{3}{7}\right)\left(\frac{41}{7}\right) = \left(\frac{-1}{7}\right)\left(\frac{3}{7}\right) \cdot \left(\frac{6}{7}\right) = (-1) \cdot (-1) \cdot (-1)$

$= -1$.

Cor: Let p be odd prime and $p \nmid d_1, p \nmid d_2$. Then $d_1 d_2$ is a quadratic residue mod p if and only if both d_1 and d_2 are quadratic residues or nonresidues mod p.

Pf: $\left(\frac{d_1 d_2}{p}\right) = \left(\frac{d_1}{p}\right)\left(\frac{d_2}{p}\right)$

So $\left(\frac{d_1 d_2}{p}\right) = 1 \iff \left(\frac{d_1}{p}\right)$ & $\left(\frac{d_2}{p}\right)$ have the same sign.

$d_1 d_2$ is a q.r. $\iff$ both d_1 & d_2 are q.r.

or q. non-r.

Cor: Let p be odd prime and $p \not| d_1, p \not| d_2$. Then $d_1 d_2$ is a quadratic residue mod p if and only if both d_1 and d_2 are quadratic residues or nonresidues mod p.

So for any integer d, to compute $\left(\frac{d}{p}\right)$, we (just) need to know how to compute $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ and $\left(\frac{q}{p}\right)$.

Ex: determine the number of solutions to the following equations:

$$x^2 \equiv -2 \pmod{209} \quad 209 = 11 \cdot 19$$

$$\Longleftrightarrow \begin{cases} x^2 \equiv -2 \pmod{11} \\ x^2 \equiv -2 \pmod{19} \end{cases}$$

$$\left(\frac{-2}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{2}{11}\right) \equiv -\left(\frac{2}{11}\right) \equiv -2^{\frac{11-1}{2}} \equiv -2^5 \equiv -32 \equiv 1 \pmod{11}$$

because $11 \equiv 3 \pmod 4$

$\Longrightarrow$ $x^2 \equiv -2 \pmod{11}$ has two solutions.

$$\left(\frac{-2}{19}\right) = \left(\frac{-1}{19}\right)\left(\frac{2}{19}\right) \equiv -\left(\frac{2}{19}\right) \equiv -2^{\frac{19-1}{2}} \equiv -2^9 \equiv -1(2^4)(2^5) \pmod{19}$$

$$\equiv -(-3)(-6) \equiv -18 \equiv 1 \pmod{19}.$$

$\Longrightarrow$ $x^2 \equiv -2 \pmod{19}$ has two solutions.

So by CRT, $x^2 \equiv -2 \pmod{209}$ has 4 solutions.