QUADRATIC CONGRUENCES

$$\alpha y^2 + \beta y + \gamma \equiv 0 \pmod{m}$$

$\alpha, \beta, \gamma \in \mathbb{Z}$ $\quad m \in \mathbb{N}$

$\alpha \not\equiv 0 \pmod{m}$

$$\alpha y^2 + \beta y + \gamma \equiv 0 \pmod{p}$$

$p \in \mathbb{P}$, $p \neq 2$, $p \nmid \alpha$

can be rewritten as

$$\boxed{x^2 \equiv a \pmod{p}}$$

$$x \equiv y + \beta(2\alpha)^{-1} \pmod{p}$$

$$a \equiv (\beta^2 - 4\alpha\gamma)(4\alpha^2)^{-1} \pmod{p}$$

$p \nmid \alpha$

$\gcd(\alpha, p) = 1$

$p \neq 2$

$\gcd(2\alpha, p) = 1$

2α is invertible mod p.

(Defn) An integer a with $\gcd(a,p)=1$ is called

- a quadratic residue modulo p if $x^2 \equiv a \pmod p$ has a solution
- a quadratic non-residue modulo p otherwise.

If $p \mid a$, then a is neither a q.r nor a q.n.r

QR_p : set of all quadratic residues in $\mathbb{Z}_p$

QNR_p : set of all quadratic non-residues in $\mathbb{Z}_p$.

Example $\mathbb{Z}_{13} = \{0, 1, 2, \ldots, 12\}$

$1^2 \equiv 12^2 \equiv 1 \pmod{13}$

$2^2 \equiv 11^2 \equiv 4 \pmod{13}$

$3^2 \equiv 10^2 \equiv 9 \pmod{13}$

$4^2 \equiv 9^2 \equiv 3 \pmod{13}$

$5^2 \equiv 8^2 \equiv 12 \pmod{13}$

$6^2 \equiv 7^2 \equiv 10 \pmod{13}$

$QR_{13} = \{1, 3, 4, 9, 10, 12\}$

$QNR_{13} = \{2, 5, 6, 7, 8, 11\}$

$|QR_{13}| = |QNR_{13}| = 6 = \frac{13-1}{2}$

$$\boxed{\begin{aligned} &a \in \mathbb{Z}_p \setminus \{0\} \\ &(p-a)^2 = p^2 + a^2 - 2ap \\ &\qquad \equiv a^2 \pmod p \end{aligned}}$$

Thm $p \in \mathbb{P}$, p odd, $|QR_p| = |QNR_p| = (p-1)/2$

Proof: $a^2 \equiv (p-a)^2 \pmod p \quad \forall a \in \mathbb{Z}_p \setminus \{0\}$

$\#$ q.r.s $\leq \frac{p-1}{2}$

$a^2 \equiv b^2 \pmod p \qquad a, b \in \{1, 2, \ldots, \frac{p-1}{2}\}$, $a \neq b$.

$p \mid (a+b)(a-b)$

$p \mid (a+b)$ or $p \mid (a-b)$

$a \equiv \pm b \pmod p \to$ contradiction

$\Rightarrow 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are all distinct

i.e., $|QR_p| = \frac{p-1}{2}$

$|QNR_p| = p - \left(\frac{p-1}{2}\right) - 1 = \frac{p-1}{2}$

Legendre Symbol

(Defn) p : odd prime $\gcd(a,p)=1$, $a \in \mathbb{Z}$

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a q.r} \\ -1 & \text{if } a \text{ is a q.n.r} \end{cases}$$

Define $\left(\frac{a}{p}\right) = 0$ if $p \mid a$.

Properties

1. $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $\left(\frac{a}{p}\right) = \left(\frac{a \text{ rem } p}{p}\right)$
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
4. $\left(\frac{0}{p}\right) = 0$ $\left(\frac{1}{p}\right) = 1$
5. $\left(\frac{a^2}{p}\right) = 1$ if $p \nmid a$
6. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$
7. $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

Euler's Criterion

p: odd prime, $a \in \mathbb{Z}$

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

Proof: Suppose that $x^2 \equiv a \pmod{p}$ has a solution, say b.

$$a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} \equiv b^{(p-1)} \equiv 1 \pmod{p}$$ [Fermat's little thm]

i.e., when x is a q.r. $a^{(p-1)/2} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}$

$a^{p-1} \equiv 1 \pmod{p}$ has $(p-1)$ solutions in $\mathbb{Z}_p$.

Every element of $a \in \mathbb{Z}_p^*$ is invertible & satisfies

$$a^{p-1} \equiv 1 \pmod{p}$$

$p \mid (a^{p-1}-1)$ i.e., $p \mid (a^{(p-1)/2}+1)\underline{(a^{(p-1)/2}-1)}$

All elements of QR_p are roots of $(a^{(p-1)/2}-1) \bmod p$.

Roots of $\left(a^{(p-1)/2}+1\right)$ mod p must be $\mathbb{Z}_p^* \setminus QR_p = QNR_p$

i.e., $\forall\ a \in QNR_p$

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

Example.

$\mathbb{Z}_{397}$

$$12^{(397-1)/2} \equiv 12^{198} \equiv 1 \pmod{397}$$

12 is a q.r. modulo 397

$$13^{198} \equiv -1 \pmod{397}$$

Quadratic Reciprocity Law

p, q : odd primes

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \cdot \left(\frac{q}{p}\right)$$

Example

65 is a q. r. mod 397.

$$\left(\frac{65}{397}\right) = \left(\frac{13}{397}\right)\left(\frac{5}{397}\right)$$

$$\overset{QRL}{=} \underbrace{(-1)^{(397-1)(13-1)/4}}_{1} \cdot \left(\frac{397}{13}\right) \underbrace{(-1)^{(397-1)(5-1)/4}}_{1} \left(\frac{397}{5}\right)$$

$$= \left(\frac{397 \bmod 13}{13}\right)\left(\frac{397 \bmod 5}{5}\right)$$

$$= \left(\frac{7}{13}\right)\left(\frac{2}{5}\right) \overset{QRL}{=} (-1)^{(13-1)(7-1)/4} \cdot \left(\frac{13 \bmod 7}{7}\right) \left(\underbrace{2^{(5-1)/2} \bmod 5}_{-1 \bmod 5}\right)$$

$$= \left(\frac{6}{7}\right)(-1) = \left(\underbrace{6^{(7-1)/2} \bmod 7}_{-1 \bmod 7}\right)(-1) = +1$$

JACOBI SYMBOL

(Defn) Let b be an odd positive integer having the prime factorisation $p_1 p_2 \cdots p_r$ $p_i \in \mathbb{P} \setminus \{2\}$

For $a \in \mathbb{Z}$, the Jacobi symbol $\left(\frac{a}{b}\right)$ is given by

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)$$

legendre symbols

No relationship btw $\left(\frac{a}{b}\right)$ & the solvability of $x^2 \equiv a \pmod{b}$

Properties $\qquad b, b'$: odd +ve integers $\qquad a, a' \in \mathbb{Z}$

1. $\left(\dfrac{a a'}{b}\right) = \left(\dfrac{a}{b}\right)\left(\dfrac{a'}{b}\right)$

2. $\left(\dfrac{a}{b b'}\right) = \left(\dfrac{a}{b}\right)\left(\dfrac{a}{b'}\right)$

3. $a \equiv a' \pmod{b}$

$\Rightarrow \left(\dfrac{a}{b}\right) = \left(\dfrac{a'}{b}\right)$

4. $\left(\dfrac{a}{b}\right) = \left(\dfrac{a \text{ rem } b}{b}\right)$

5. $\left(\dfrac{-1}{b}\right) = (-1)^{(b-1)/2}$

6. $\left(\dfrac{2}{b}\right) = (-1)^{(b^2-1)/8}$

7. [Law of Quadratic Reciprocity]

$\left(\dfrac{b}{b'}\right) = (-1)^{(b-1)(b'-1)/4} \left(\dfrac{b'}{b}\right)$

$$\left(\frac{65}{397}\right) \overset{QRL}{=} \underbrace{(-1)^{(65-1)(397-1)/4}}_{1} \left(\frac{397}{65}\right)$$

$$= \left(\frac{397 \text{ rem } 65}{65}\right)$$

$$= \left(\frac{7}{65}\right)$$

$$\overset{QRL}{=} \underbrace{(-1)^{(7-1)(65-1)/4}}_{1} \cdot \left(\frac{65}{7}\right)$$

$$= \left(\frac{65 \text{ rem } 7}{7}\right)$$

$$= \left(\frac{2}{7}\right) = 2^{(7-1)/2} \pmod 7$$

$$= 1$$

Does $x^2 \equiv a \pmod p$ have a solution?

has exactly $1 + \left(\frac{a}{p}\right)$ solutions