Quadratic Residues

n is a positive integer and a is a unit in $\mathbb{Z}_n$. When do we have a solution to the congruence

$$x^2 \equiv a \pmod{n}$$

If there is a solution, then a is called a quadratic residue (QR). Otherwise, it will be called a quadratic non-residue (QNR) modulo n.

Examples: (1) $n = 4$. units $= 1, 3$

$1 \downarrow$ QR, $3 \downarrow$ QNR

(2) $n = 7$.

$1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 2 \pmod{7}$

$4^2 \equiv 2$, $5^2 \equiv 4$, $6^2 \equiv 1 \pmod{7}$

QR : 1, 2, 4 QNR : 3, 5, 6

(3) $n = 11$

$1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9$, $4^2 \equiv 5$, $5^2 \equiv 3 \pmod{11}$

$6^2 \equiv 3$, $7^2 \equiv 5$, $8^2 \equiv 9$, $9^2 \equiv 4$, $10^2 \equiv 1 \pmod{11}$

QR: 1, 3, 4, 5, 9 QNR: 2, 6, 7, 8, 10.

Is it always half and half? Not always.

(4) $n=8$. QR: 1 QNR: 3, 5, 7.

By CRT, we can reduce the problem

$$x^2 \equiv a \pmod{n} \qquad n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$$

to the prime power moduli $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_k^{\alpha_k}$.

$\Rightarrow$ We should focus on

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

By Hensel, this should also reduce to

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

i.e. understanding quadratic residues modulo prime p.

$f(x) = x^2 - a \Rightarrow f'(x) = 2x \equiv 0 \pmod{2}$. So, the cases $p=2$ and 2^k might be more complicated.

Quadratic Residues modulo odd prime p

Definition: The Legendre symbol of any integer a is

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a \\ 1, & \text{if } a \text{ is a QR} \\ -1, & \text{if } a \text{ is a QNR}. \end{cases}$$

- Definition depends only on $a \pmod{p}$.

For example,

$$\left(\frac{73}{7}\right) = \left(\frac{17}{7}\right) = \left(\frac{-4}{7}\right) = \left(\frac{3}{7}\right) = -1$$

Understanding QR in $\mathbb{Z}_p$ is easy using primitive roots.

Theorem: Let g be a primitive root of $\mathbb{Z}_p$, then we have

$(-1)^k$

$$\left(\frac{g^k}{p}\right) = \begin{cases} 1, & \text{if } k \text{ is even} \\ -1, & \text{if } k \text{ is odd}. \end{cases}$$

Proof: • If $k = 2\ell$ is even, then

$$g^k \equiv (g^\ell)^2 \pmod p$$

• Suppose g^k is a QR, then $x^2 \equiv g^k \pmod p$ for some x.

$x \equiv g^\ell \pmod p$ for some ℓ and hence

$$g^{2\ell} \equiv g^k \pmod p \Rightarrow 2\ell \equiv k \pmod{p-1}$$

$2 \cdot \frac{p-1}{2}$

$$\Rightarrow 2\ell \equiv k \pmod 2$$

$$\Rightarrow 0 \equiv k \pmod 2$$

Corollary: There are $\frac{p-1}{2}$ QR and $\frac{p-1}{2}$ QNR

$g^2, g^4, \ldots, g^{p-1}$ $g, g^3, g^5, \ldots, g^{p-2}$

Properties of Legendre Symbol

① $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

can generalize

$\left(\frac{abc}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \cdot \left(\frac{c}{p}\right)$

etc.

- If $p \mid a$ or $p \mid b \Rightarrow 0 = 0$
- Suppose $p \nmid a$, $p \nmid b$.

Write $a \equiv g^k$, $b \equiv g^\ell \pmod{p}$

$\Rightarrow ab \equiv g^{k+\ell} \pmod{p}$ and

$$(-1)^{k+\ell} = (-1)^k \cdot (-1)^\ell \quad \checkmark$$

This means: QR × QR = QR

QNR × QNR = QR

QR × QNR = QNR

② $\left(\frac{1}{p}\right) = 1$, i.e. 1 is a QR

③ a is a unit. $\left(\frac{a^{-1}}{p}\right) = \left(\frac{a}{p}\right)$

- $1 = \left(\frac{1}{p}\right) = \left(\frac{a \cdot a^{-1}}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a^{-1}}{p}\right)$

$(QR)^{-1} = QR \qquad (QNR)^{-1} = QNR.$

④ If a is a unit, then $\left(\frac{a^2}{p}\right) = 1$

⑤ If a is a unit, then $\left(\frac{a^2 \cdot b}{p}\right) = \left(\frac{b}{p}\right)$

⑥ (Euler's Criterion) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

- $a \equiv 0 \pmod p \Rightarrow 0 \equiv 0 \pmod p$
- $a \equiv g^{2k} \pmod p \Rightarrow a^{\frac{p-1}{2}} \equiv g^{2k \cdot \frac{p-1}{2}}$
  $\equiv (g^{p-1})^k \equiv 1 \pmod p$
- $a \equiv g^{2k+1} \pmod p \Rightarrow a^{\frac{p-1}{2}} \equiv g^{(2k+1) \cdot \frac{p-1}{2}}$
  $\equiv (g^{p-1})^k \cdot g^{\frac{p-1}{2}}$
  $\equiv g^{\frac{p-1}{2}} \equiv -1 \pmod p$

proved in Lecture 17

⑦ $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$

-1 is a QR $\iff \frac{p-1}{2}$ even $\iff p \equiv 1 \pmod 4$