<u>Recall</u> : Let $a$ be a unit of $\mathbb{Z}_n$

quadratic residue : $x^2 \equiv a \pmod{n}$ has a solution

quadratic non-residue : $x^2 \equiv a \pmod{n}$ has no solution.

Let $p$ be an odd prime.

Legendre symbol $\left(\frac{a}{p}\right)$ : $1$ if <u>QR</u> ; $-1$ if <u>QNR</u> ; $0$ if <u>$0 \pmod{p}$</u>

- $g$ primitive root. $\left(\frac{g^k}{p}\right) = (-1)^k$
- $\frac{p-1}{2}$ QR and $\frac{p-1}{2}$ QNR.
- $\left(\frac{1}{p}\right) = 1$ • $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ • $\left(\frac{a}{p}\right) = \left(\frac{a^{-1}}{p}\right)$
- $a$ unit $\Rightarrow \left(\frac{a^2}{p}\right) = 1$ and $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$

<u>Euler's Criterion</u> : $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

$a$ unit

call $x$

$x^2 \equiv a^{p-1} \equiv 1 \pmod{p}$

$x \equiv \pm 1 \pmod{p}$

- $p \equiv 1 \pmod{4} \Rightarrow -1$ is a QR
- $p \equiv 3 \pmod{4} \Rightarrow -1$ is a QNR

---

Two types of questions :

- What are the quadratic residues modulo $\overset{p}{17}$ ?

$1^2 \equiv 1$ , $2^2 \equiv 4$ , $3^2 \equiv 9$ , $4^2 \equiv 16$ , $5^2 \equiv 8$ , $6^2 \equiv 2$ , $7^2 \equiv 15$ , $\underset{\frac{p-1}{2}}{8}{}^2 \equiv 13$

no need to check the rest because $9 \equiv -8$ , $10 \equiv -7$ , ...

- Is $7$ a quadratic residue modulo $23$ ?

We use Euler's criterion.

$7^2 \equiv 3$ , $7^4 \equiv 9$ , $7^8 \equiv 12$ $\Rightarrow 7^{11} \equiv 12 \cdot 3 \cdot 7 \equiv 13 \cdot 7 \equiv -1$

So, $\left(\frac{7}{23}\right) = -1$ .

<u>An application:</u> There are infinitely many primes of the form $4k+1$.

Suppose not, call them $p_1, p_2, \dots, p_n$.

Consider $m = (2p_1 p_2 \cdots p_n)^2 + 1$ .

If $p \mid m$ , then $(2p_1 p_2 \cdots p_n)^2 \equiv -1 \pmod{p}$

$$\Rightarrow \left(\frac{-1}{p}\right) = 1$$

$$\Rightarrow p \equiv 1 \pmod{4}$$

$p_1, p_2, \dots, p_n \nmid m$ , contradiction.

Can we compute $a^{\frac{p-1}{2}} \pmod{p}$ using the idea in the proof of Fermat's theorem? $(a, p) = 1$

Consider $\left\{ a, 2a, 3a, \dots, \frac{p-1}{2} \cdot a \right\} = S$

<u>Examples:</u> $p = 7$ , $a = 3$ $\left(\frac{3}{7}\right) = -1$

$$\{3, 6, 9\} \equiv \{2, 3, 6\} \equiv \{-1, 2, 3\}$$

$p = 13$ , $a = 2$ $\qquad \left(\frac{2}{13}\right) = -1$

$$\{2, 4, 6, 8, 10, 12\} \equiv \{-1, 2, -3, 4, -5, 6\}$$

$p = 13$ $\quad a = 5$ $\qquad \left(\frac{5}{13}\right) = -1$

$$\{5, 10, 15, 20, 25, 30\} \equiv \{2, 4, 5, 7, 10, 12\}$$

$$\equiv \{-1, 2, -3, 4, 5, -6\}$$

The elements of $S$ all different mod $p$:

$$i \cdot a \not\equiv j \cdot a \quad \text{for} \quad 1 \leq i, j \leq \frac{p-1}{2}$$

we also cannot have $\quad ia \equiv -ja$

$\Rightarrow$ $S$ contains

- $1$ or $-1$
- $2$ or $-2$

$\vdots$

- $\frac{p-1}{2}$ or $-\frac{p-1}{2}$ .

Suppose there are $n$ negative signs when we write $S$ like that. The product of the elements will be

$$\left(\frac{p-1}{2}\right)! \; a^{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)! \, (-1)^n \pmod p$$

<u>Gauss' Lemma:</u> Suppose $a$ is a unit modulo $p$. Write each of $a, 2a, \ldots, \frac{p-1}{2} \cdot a$ between $-\frac{p-1}{2}$ and $\frac{p-1}{2}$ modulo $p$ and say there are $n$ negative signs. Then, $\left(\frac{a}{p}\right) = (-1)^n$.

<u>An application:</u> $a = 2$, $p$ an odd prime.

We consider $S = \{2, 4, 6, \ldots, p-1\}$

<u>Case I:</u> $p = 4k+1$.

$$S \equiv \{2, 4, 6, \ldots, 2k, 2k+2, 2k+4, \ldots, 4k\}$$

$$\equiv \{2, 4, 6, \ldots, 2k, -(2k-1), -(2k-3), \ldots, -1\}$$

$\Rightarrow n = k$

$\left(\frac{2}{p}\right) = 1$ if $\overset{=2m}{k}$ is even, i.e. $\overset{p=8m+1}{p \equiv 1 \pmod 8}$

$\left(\frac{2}{p}\right) = -1$ if $\overset{=2m+1}{k}$ is odd, i.e. $\overset{p=8m+5}{p \equiv 5 \pmod 8}$

<u>Case II:</u> $p = 4k+3$

$$S \equiv \{2, 4, 6, \ldots, 4k+2\}$$

$$\equiv \{2, 4, 6, \ldots, 2k, -(2k+1), -(2k-1), \ldots, -1\}$$

$\Rightarrow n = k+1$

$$\left(\frac{2}{p}\right) = 1 \quad \text{if} \quad \underset{}{k}^{=2m+1} \text{ is odd, i.e. } p \equiv 7 \pmod 8 \quad (p = 8m+7)$$

$$\left(\frac{2}{p}\right) = -1 \quad \text{if} \quad k^{=2m} \text{ is even, i.e. } p \equiv 3 \pmod 8 \quad (p = 8m+3)$$

<u>Conclusion:</u>

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 7 \pmod 8 \\ -1, & \text{if } p \equiv 3, 5 \pmod 8 \end{cases}$$

<u>Exercise:</u> Can you compute $\left(\frac{3}{p}\right)$ similarly?

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 11 \pmod{12} \\ -1, & \text{if } p \equiv 5, 7 \pmod{12} \\ 0, & \text{if } p = 3 \end{cases}$$

We still don't have a very fast way to compute $\left(\frac{a}{p}\right)$ for large numbers other than Euler's criterion.

Consider $\left(\frac{2^3 \cdot 17^2 \cdot 19 \cdot 23^3}{71}\right)$

$$= \underbrace{\left(\frac{2^2 \cdot 17^2 \cdot 23^2}{71}\right)}_{1} \cdot \underbrace{\left(\frac{2}{71}\right)}_{1} \cdot \left(\frac{19}{71}\right) \cdot \left(\frac{23}{71}\right)$$

$$= \left(\frac{19}{71}\right) \cdot \left(\frac{23}{71}\right)$$

Enough to compute $\left(\frac{q}{p}\right)$ for odd primes $p, q$.

## Law of Quadratic Reciprocity

Suppose $p \neq q$ are odd primes, then

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

If $p$ or $q$ or both $\equiv 1 \pmod 4$ $\Rightarrow \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$

If $p \equiv q \equiv 3 \pmod 4$ $\Rightarrow \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$

We'll prove it on Wednesday.

How to use it?

1. $\left(\frac{83}{103}\right) = ?$

$$\left(\frac{83}{103}\right) = -\left(\frac{103}{83}\right) = -\left(\frac{20}{83}\right) = -\left(\frac{4}{83}\right)\cdot\left(\frac{5}{83}\right)$$

$$= -\left(\frac{5}{83}\right) = -\left(\frac{83}{5}\right) = -\left(\frac{3}{5}\right) = -(-1) = 1.$$

2. $\left(\frac{219}{383}\right) = ?$

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right)\cdot\left(\frac{73}{383}\right) = 1.$$

- $\left(\frac{3}{383}\right) = -\left(\frac{383}{3}\right) = -\left(\frac{2}{3}\right) = 1.$
- $\left(\frac{73}{383}\right) = \left(\frac{383}{73}\right) = \left(\frac{18}{73}\right) = \left(\frac{2}{73}\right) = 1$

③ $\left(\frac{-42}{61}\right) = ?$

$$\left(\frac{-42}{61}\right) = \underbrace{\left(\frac{-1}{61}\right)}_{1} \cdot \underbrace{\left(\frac{2}{61}\right)}_{-1} \cdot \left(\frac{3}{61}\right) \cdot \left(\frac{7}{61}\right)$$

$$= 1 \cdot (-1) \cdot \left(\frac{61}{3}\right) \cdot \left(\frac{61}{7}\right)$$

$$= - \underbrace{\left(\frac{1}{3}\right)}_{1} \cdot \left(\frac{5}{7}\right)$$

$$= -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right) = 1 .$$

Alternatively,

$$\left(\frac{-42}{61}\right) = \left(\frac{19}{61}\right) = \left(\frac{61}{19}\right) = \left(\frac{4}{19}\right) = 1 .$$

Can we obtain results like

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 11 \pmod{12} \\ -1, & \text{if } p \equiv 5, 7 \pmod{12} \\ 0, & \text{if } p = 3 \end{cases}$$

using Law of Quadratic Reciprocity?

- $\left(\frac{7}{p}\right) = ?$

Case I : $p \equiv 1 \pmod 4 \implies \left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$

$p \equiv 1, 2, 4 \pmod 7 \Rightarrow \left(\frac{7}{p}\right) = 1$

$p \equiv 3, 5, 6 \pmod 7 \Rightarrow \left(\frac{7}{p}\right) = -1$

Combining with $p \equiv 1 \pmod 4$ by CRT,

$$\left(\frac{7}{p}\right) = \begin{cases} 1, & \text{if } 1, 9, 25 \pmod{28} \\ -1, & \text{if } 5, 13, 17 \pmod{28} \end{cases}$$

<u>Case II :</u> $p \equiv 3 \pmod 4 \Rightarrow \left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$

$p \equiv 1, 2, 4 \pmod 7 \Rightarrow \left(\frac{7}{p}\right) = -1$

$p \equiv 3, 5, 6 \pmod 7 \Rightarrow \left(\frac{7}{p}\right) = 1$ .

Combining with $p \equiv 3 \pmod 4$ by CRT,

$$\left(\frac{7}{p}\right) = \begin{cases} 1, & \text{if } 3, 19, 27 \pmod{28} \\ -1, & \text{if } 11, 15, 23 \pmod{28} \end{cases}$$

To summarize,

$$\left(\frac{7}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 3, 9, 19, 25, 27 \pmod{28} \text{ or } p = 2 \\ -1, & \text{if } p \equiv 5, 11, 13, 15, 17, 23 \pmod{28} \\ 0, & p = 7 \end{cases}$$

• $\left(\frac{-3}{p}\right) = ?$

$1$

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}}$$

$$= \left(\frac{p}{3}\right)$$

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 3 \\ -1, & \text{if } p \equiv 2 \pmod 3 \\ 0, & \text{if } p = 3 \end{cases}$$

We are done with odd prime $p$ case.

## Passing to $p^k$

Suppose $p$ is odd and $(a, p) = 1$.

When $x^2 \equiv a \pmod{p^k}$ has a solution?

① Solve $x^2 \equiv a \pmod p$ first. If there is no solution, then no solution $\pmod{p^k}$ as well.

② If there is a solution, then we can lift uniquely to $\pmod{p^k}$

$f(x) = x^2 - a$ and $f'(x) = 2x \not\equiv 0 \pmod p$ because $p \neq 2$ and $x \not\equiv 0 \pmod p$ (otherwise $a$ is also $0 \pmod p$).

Conclusion: $a$ is a QR mod $p^k$ if and only if it is a QR mod $p$

How many QR in $\mathbb{Z}_{p^k}$?

$$\frac{p-1}{2} \cdot p^{k-1} \text{ QR and } \frac{p-1}{2} \cdot p^{k-1} \text{ QNR}$$