Let p be an odd prime number, and let a be an integer.

In the following several sections, we want to study the solutions for the (quadratic) congruent equation:

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

Definition: If the equation above has a solution, then a is said to be <u>congruent to a square modulo p</u> or a <u>quadratic residue mod p</u>.

Suppose that $\gcd(a,p)=1$.

We use the abbreviation: QR.

If the equation above has no solution, then a is said to be <u>not congruent to a square modulo p</u> or a <u>quadratic nonresidue mod p</u>.

We use the abbreviation: NR.

Example: 3 is not congruent to a square modulo 7

i.e. 3 is a NR mod 7

To show that, we consider the equation:

$$x^2 \equiv 3 \pmod 7$$

$$0^2 \equiv 0 \pmod 7$$
$$1^2 \equiv 1 \pmod 7$$
$$2^2 \equiv 4 \pmod 7$$
$$3^2 \equiv 2 \pmod 7$$
$$4^2 \equiv 2 \pmod 7$$
$$5^2 \equiv 4 \pmod 7$$
$$6^2 \equiv 1 \pmod 7$$

Therefore, $x^2 \equiv 3 \pmod 7$ has no solution.

This implies: 3 is a NR mod 7.

Lemma: $(p-a)^2 \equiv a^2 \pmod p$

Proof: $(p-a)^2 = p^2 - 2p + a^2 \equiv a^2 \pmod p$ $\square$

This lemma tells us: if we want to list all QR,

we only need to investigate:

$1^2 \pmod p, \ 2^2 \pmod p, \ \cdots \ \left(\frac{p-1}{2}\right)^2 \pmod p$ (*)

Theorem (20.1) Let p be an odd prime. Then there are exactly $\frac{p-1}{2}$ QR mod p. and exactly $\frac{p-1}{2}$ NR mod p.

Proof: Claim: (*) gives all distinct QR mod p.

Proof of the claim: we choose $b_1 \neq b_2 \in \{1, 2, 3, \cdots \frac{p-1}{2}\}$

(Proof by contradiction) Suppose that $b_1^2 \equiv b_2 \pmod p$

Then $p \mid b_1^2 - b_2^2 = (b_1 - b_2)(b_1 + b_2)$

This implies: $p \mid (b_1 - b_2)$ or $p \mid (b_1 + b_2)$

$b_1, b_2 \in \{1, 2, \cdots \frac{p-1}{2}\}$,

$\Rightarrow |b_1 - b_2| < \frac{p-1}{2}$ and $b_1 \neq b_2 \neq 0. \Rightarrow p \nmid (b_1 - b_2)$

$\Rightarrow 2 \leq b_1 + b_2 \leq p-1 \qquad \Rightarrow p \nmid (b_1 + b_2)$

A contradiction.

This implies, $b_1^2 \not\equiv b_2^2 \pmod p$

Therefore, $1^2, 2^2, \cdots \left(\frac{p-1}{2}\right)^2$ are distinct QR mod p.

However, $1^2, 2^2, 3^2, \cdots \left(\frac{p-1}{2}\right)^2, \left(\frac{p+1}{2}\right)^2, \cdots (p-1)^2$

are all QR mod p.

By the lemma,

$$1^2 \equiv (p-1)^2 \pmod p$$

$$2^2 \equiv (p-2)^2 \pmod p$$

$$\cdots$$

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

Therefore, $1^2, 2^2, \cdots \left(\frac{p-1}{2}\right)^2$ are all distinct QR mod p.

Next, we finish the proof of the theorem:

We have:

$$1, 2, 3, \cdots p-1$$

$p-1$ numbers in total.

We have $\frac{p-1}{2}$ QR $\pmod p$

Then we have $p-1-\frac{p-1}{2} = \frac{p-1}{2}$ NR $\pmod p$. $\square$

Theorem 20.2. (Quadratic Residue Multiplication Rule, Version I)

Let p be an odd prime.

(1) The produt of two qudratic residues (mod p) is a qudratic residue. $QR \times QR = QR$.

(2) The produt of a qudratic residue and a nonresidue is a non residue $QR \times NR = NR$.

(3) The produt of two nonresidues (mod p) is a qudratic residue. $NR \times NR = QR$.

The symbol QR be haves like "$+1$"

The symbol NR be haves like "-1"!

We define the following Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a } QR \pmod p \\ -1 & a \text{ is a } NR \pmod p \end{cases}$$

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

Theorem (Qudratic Residue Multiplication Rule, version 2)

Let p be an odd prime, and let a, b be integers satisfying $\gcd(ab, p) = 1$. Then

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

Remark: we can drop the condition $\gcd(ab, p) = 1$ if we further assume that

$$\left(\frac{a}{p}\right) = 0 \quad \text{if} \quad \gcd(p, a) > 1$$