Quadratic Residue:

Let p be a prime number.

Consider $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$.

We call an element $y \in \mathbb{Z}_p^*$ is a quadratic residue if $\exists\, x \in \mathbb{Z}_p^*$ such that $y = x^2 \bmod p$.

x: Square root of y.

$y \in \mathbb{Z}_p^*$ is called a quadratic non-residue if there is no square root of y.

Prop: Let $p > 2$ be a prime. Every quadratic residue in $\mathbb{Z}_p^*$ has exactly two square roots.

Pf: Suppose x is a soln to $y = x^2 \bmod p$.
then $(-x) \bmod p$ is also a root

$x \bmod p$ and $-x \bmod p$ are two distinct elements.

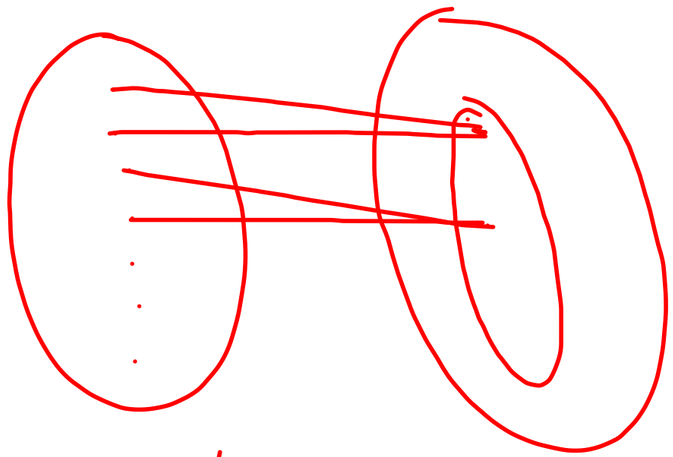
$x \not\equiv -x \bmod p$

This shows that y has at least two square roots.

$Sq_p : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$

$Sq_p(x) = x^2 \bmod p$.

Sq_p is a 2-1 fn.



There are exactly $\left(\frac{p-1}{2}\right)$ quadratic residues modulo p and the remaining $\frac{p-1}{2}$ elements of $\mathbb{Z}_p^*$ are quadratic non-residues.

$QR_p = \{x : x \text{ is a quadratic residue modulo } p\}$.

$QNR_p = \{x : x \text{ is a quadratic non-residue}\}$.

$$|QR_p| = |QNR_p| = \frac{(p-1)}{2}.$$

Jacobi Symbol:

for every $x \in \mathbb{Z}_p^*$

$$J_p(x) = \begin{cases} +1 & \text{if } x \in QR_p. \\ -1 & \text{if } x \in QNR_p. \end{cases}$$

Characterization of Quadratic Residue.

We want to decide efficiently, whether an element $x \in \mathbb{Z}_p^*$ is quadratic residue or not.

Lemma: Let $p > 2$ be a prime. Then $J_p(x) = x^{\frac{p-1}{2}} \bmod p$.

Pf: $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$.

$$\mathbb{Z}_p^* = \{g^0, g^1, \ldots g^{\frac{p-1}{2}-1}, g^{\frac{p-1}{2}}, g^{\frac{p-1}{2}+1}, \ldots g^{p-2}\}.$$

By taking the square of every element in $\mathbb{Z}_p^*$ yields the li

$$\{g^0, g^2, g^4, \ldots g^{p-3}, g^{p-1}, \ldots g^0, g^2, \ldots g^{p-1}\}.$$

Every $y \in QR_p$. we can express y as.

$$y = g^{\alpha}, \text{ where } \alpha \text{ is an even integer.}$$

- Let $x \in QR_p$.

Therefore, $x = g^{2i}$. $x^{\frac{p-1}{2}} = \left(g^{p-1}\right)^{i} = 1 \bmod p$.

Therefore $J_p(x) = x^{\frac{p-1}{2}}$.

- Let $x \in QNR_p$.

Every $y \in QR_p$. we can express y as.

$$y = g^{\alpha}, \text{ where } \alpha \text{ is an even integer.}$$

- Let $x \in QR_p$.

Therefore, $x = g^{2i}$. $x^{\frac{p-1}{2}} = \left(g^{p-1}\right)^{i} = 1 \bmod p$.

Therefore $J_p(x) = x^{\frac{p-1}{2}}$.

- Let $x \in QNR_p$. Therefore $x = g^{(2i+1)}$

$$x^{\frac{p-1}{2}} = \left(g^{2i+1}\right)^{\frac{p-1}{2}} = \left(g^{p-1}\right)^{i} g^{\frac{p-1}{2}} = g^{\frac{p-1}{2}}.$$

$$x^{\frac{p-1}{2}} = g^{\frac{p-1}{2}}.$$

$$\left(x^{\frac{p-1}{2}}\right)^2 = \left(g^{\frac{p-1}{2}}\right)^2 = g^{p-1} = 1$$

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

$$g^{\frac{p-1}{2}} = 1 \mod p. \quad (X).$$

$$g^{\frac{p-1}{2}} = -1 \mod p. \quad \smile.$$

$$x^{\frac{p-1}{2}} = g^{\frac{p-1}{2}}.$$

$$\left(x^{\frac{p-1}{2}}\right)^2 = \left(g^{\frac{p-1}{2}}\right)^2 \sim g^{p-1} = 1$$

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

$$g^{\frac{p-1}{2}} = 1 \bmod p. \quad (X).$$

$$g^{\frac{p-1}{2}} = -1 \bmod p. \quad \checkmark$$

$$\Rightarrow x^{\frac{p-1}{2}} = -1 \bmod p. \quad \text{Therefore } J_p(x) = x^{\frac{p-1}{2}}$$

Conclusion:

x is a quadratic residue $\Rightarrow x^{\frac{p-1}{2}} = 1$

x is a quadratic non-residue $\Rightarrow x^{\frac{p-1}{2}} = -1$.

How to decide whether $x \in \mathbb{Z}_p^*$ is a quadratic residue or not:

Compute $x^{\frac{p-1}{2}}$.

If the result is 1, then $x \in QR_p$.

If the result is -1, then $x \in QNR_p$.

Prof: Let $p>2$ be a prime. Then for $x, y \in \mathbb{Z}_p^*$.

$$J_p(xy) = J_p(x) \cdot J_p(y).$$

Prof: Let $p>2$ be a prime. Let $x, x' \in QR_p$ and $y, y' \in QNR_p$.

(i) $xx' \bmod p \in QR_p$.

(ii) $yy' \bmod p \in QR_p$.

(iii) $xy \bmod p \in QNR_p$.

Quadratic Residuosity over a composite number.

$N = p \cdot q$.

By the result of CRT, we know that

$$\mathbb{Z}_N^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*.$$

Therefore for any $y \in \mathbb{Z}_N^*$, an unique element.

$(y_p, y_q) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. where $y_p = y \bmod p$, $y_q = y \bmod q$.

Defn: An element $y \in \mathbb{Z}_N^*$ is called a quadratic residue if $\exists\, x \in \mathbb{Z}_N^*$ such that

$$y = x^2 \bmod N.$$

x → square root of y.

$QR_N = \{x : x \text{ is a quadratic residue modulo } N\}$.

So for $x \in \mathbb{Z}_N^*$, $x \leftrightarrow (x_p, x_q)$.

$$x^2 \leftrightarrow (x_p, x_q)^2 = \left([x \bmod p]^2,\ [x \bmod q]^2\right).$$

y has exactly four square roots, namely

$(x \bmod p,\ x \bmod q)$

$(x \bmod p,\ -x \bmod q)$

$(-x \bmod p,\ x \bmod q)$

$(-x \bmod p,\ -x \bmod q)$

$Sq_N : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ defined by

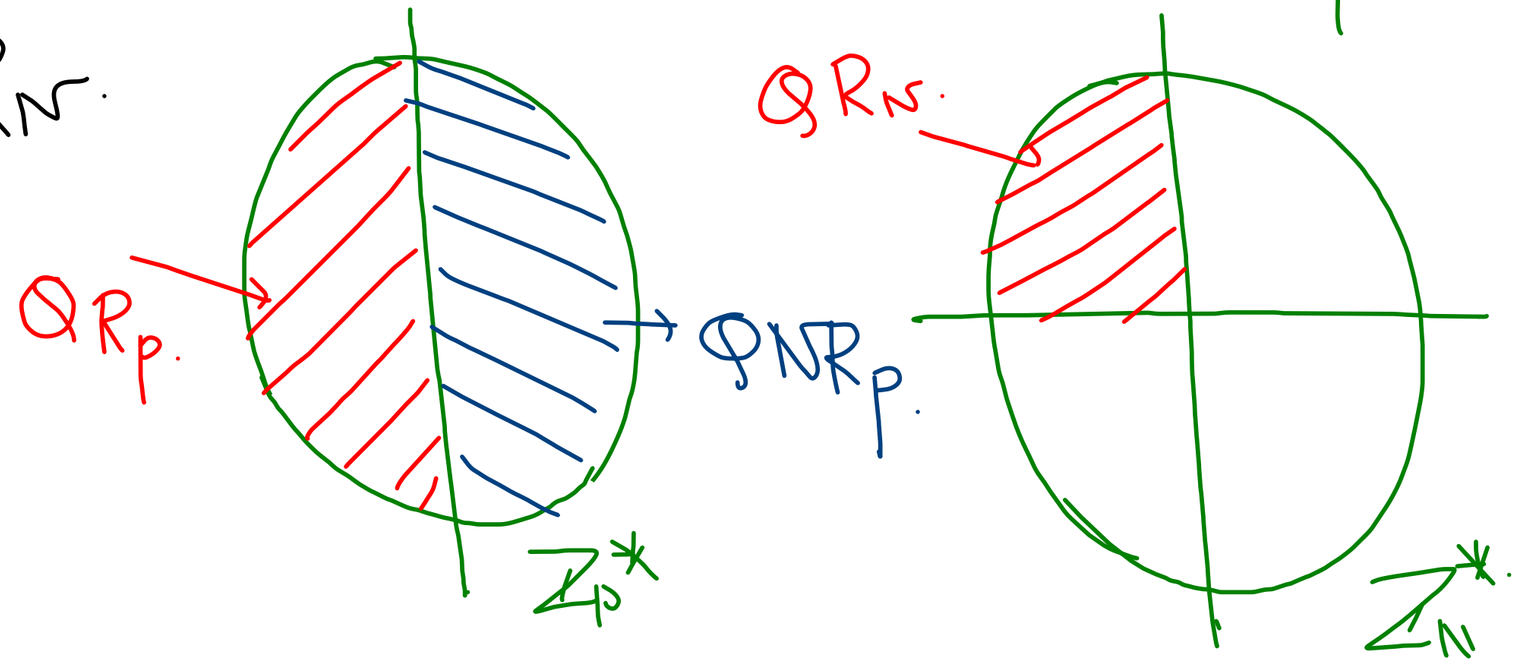
$Sq_N(x) = x^2 \bmod N$ is a 4-1 fn.

Therefore, $|QR_N| = \frac{|\mathbb{Z}_N^*|}{4} = \frac{(p-1)(q-1)}{4}$.

Since there is a bijection between QR_N and $(QR_p \times QR_q)$.

$$|QR_N| = |QR_p| \times |QR_q| = \frac{p-1}{2} \times \frac{q-1}{2} = \frac{|Z_N^*|}{4}.$$

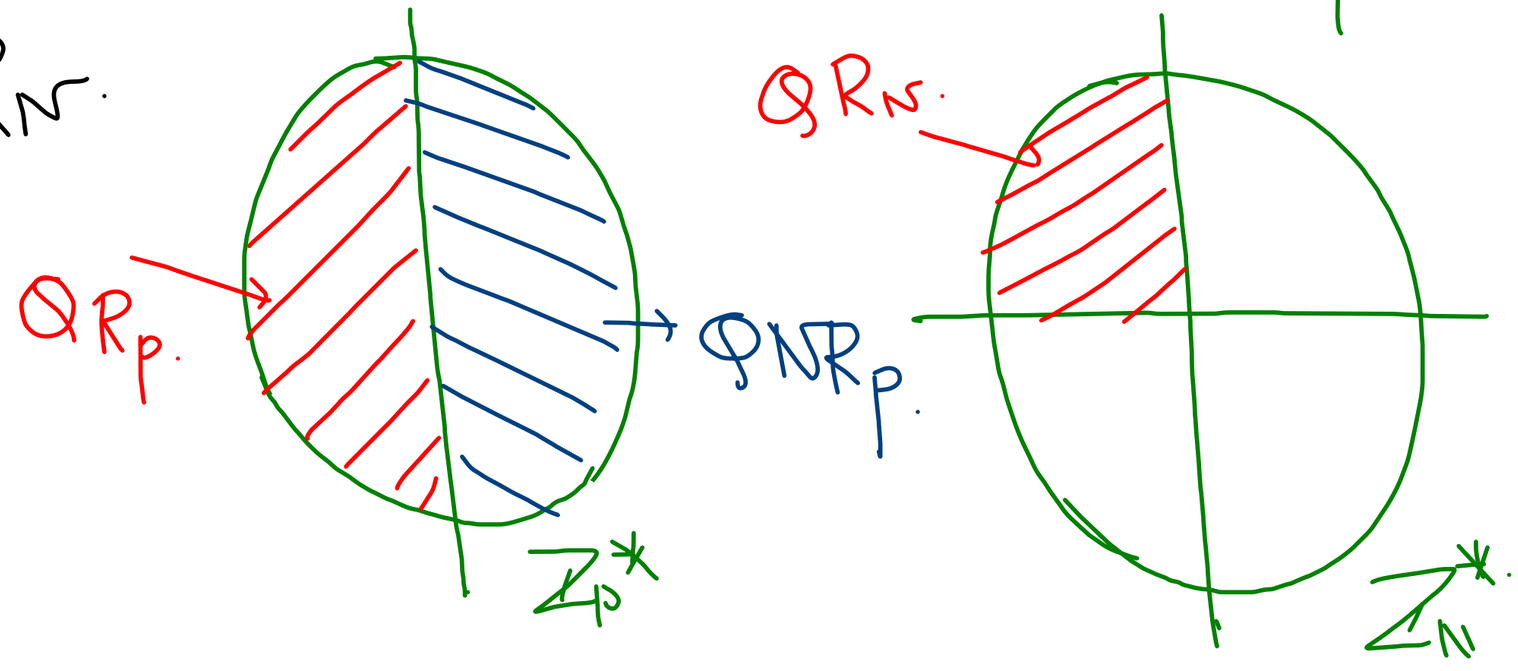
Suppose $y \in QR_N$.



Since there is a bijection between QR_N and $(QR_p \times QR_q)$.

$$|QR_N| = |QR_p| \times |QR_q| = \frac{p-1}{2} \times \frac{q-1}{2} = \frac{|Z_N^*|}{4}.$$

Suppose $y \in QR_N$.



Jacobi Symbol:

for any $x \in \mathbb{Z}_N^*$. we define.

$$J_N(x) := J_p(x) \cdot J_q(x)$$

$$= J_p(x \bmod p) \cdot J_p(x \bmod q).$$

Prop: Let p, q be two distinct odd primes. and $N = pq$. Let $y \in \mathbb{Z}_N^*$ with $y \leftrightarrow (y_p, y_q)$. Then y is a quadratic residue modulo N iff y_p is a quadratic residue modulo p and y_q is a quadratic residue modulo q.

y_p is a quadratic residue modulo $p \Rightarrow$.

$\exists\, x_p \in \mathbb{Z}_p^*$ such that

$$y_p = x_p^2 \bmod p \quad \text{— (i)}$$

Similarly, $y_q = x_q^2 \bmod q$ — (ii).

for (i), $\exists$ two roots $-x_p \bmod p$, $x_p \bmod p$.

for (ii) $\exists$ " " $-x_q \bmod q$, $x_q \bmod q$.

From the above proposition, we see that $y \in QR_N$ iff.

$J_p(y) = +1$ and $J_q(y) = +1$.

As we know that

$J_N(y) = J_p(y) \cdot J_q(y)$.

Therefore if y is a quadratic residue modulo N

then $J_N(y) = 1$.

$QNR_N^{+1} = \{ y \in \mathbb{Z}_N^* : J_N(y) = 1$ but y is not a quadratic residue$\}$.

We define $J_N^{+1}(x) = \{ x \in \mathbb{Z}_N^* : J_N(x) = +1 \}$.

" " $J_N^{-1}(x) = \{ x \in \mathbb{Z}_N^* : J_N(x) = -1 \}$

Pwf: $|J_N^{+1}| = |\mathbb{Z}_N^*|/2$

$|J_N^{-1}| = |\mathbb{Z}_N^*|/2$.

Pwf: Let $N = pq$ with p, q distinct odd primes.

(i) Then exactly half of the elements of $\mathbb{Z}_N^*$ are in J_N^{+1}

(ii) $QR_N \subseteq J_N^{+1}$

(iii) exactly half of the elements of J_N^{+1} are in QR_N and the other half in QNR_N^{+1}.

Pf:

$$J_N^{+1} = \{x \in \mathbb{Z}_N^* : J_N(x) = +1\}.$$

$$J_N(x) = J_p(x) \cdot J_q(x).$$

$J_N(x) = +1$, when both $J_p(x) = J_q(x) = +1$, $\rightarrow \frac{p-1}{2} \times \frac{q-1}{2}$

Or " $J_p(x) = J_q(x) = -1 \rightarrow \frac{p-1}{2} \times \frac{q-1}{2}$.

$$|J_N^{+1}| = \frac{|\mathbb{Z}_N^*|}{2}$$

$$\frac{|\mathbb{Z}_N^*|}{2} = \frac{(p-1)(q-1)}{2}.$$

$$|QR_N| = \frac{|\mathbb{Z}_N^*|}{4} \Rightarrow |QR_N| = \frac{|J_N^{+1}|}{2}.$$

Pf:

$$J_N^{+1} = \{x \in \mathbb{Z}_N^* : J_N(x) = +1\}.$$

$$J_N(x) = J_p(x) \cdot J_q(x).$$

$J_N(x) = +1$, when both $J_p(x) = J_q(x) = +1$, $\rightarrow \frac{p-1}{2} \times \frac{q-1}{2}$

Or " $J_p(x) = J_q(x) = -1 \rightarrow \frac{p-1}{2} \times \frac{q-1}{2}$.

$$|J_N^{+1}| = \frac{|\mathbb{Z}_N^*|}{2}$$

$$\frac{|\mathbb{Z}_N^*|}{2} = \frac{(p-1)(q-1)}{2}.$$

$$|QR_N| = \frac{|\mathbb{Z}_N^*|}{4} \Rightarrow |QR_N| = \frac{|J_N^{+1}|}{2}.$$

Prop: Let $N = pq$ be a product of two distinct odd primes. Then for any $x, y \in \mathbb{Z}_N^*$, we have

$$J_N(xy) = J_N(x) \cdot J_N(y).$$

Pf: $J_N(xy) = J_p(xy) \cdot J_q(xy)$

$$= J_p(x) \cdot J_q(x) \cdot J_p(y) \cdot J_q(y)$$

$$= J_N(x) \cdot J_N(y).$$

Corollary: Let $N = pq$ be a product of two distinct odd primes. Then for any $x, x' \in QR_N$ and $y, y' \in QNR_N^{+1}$.

we have

(i) $x x' \bmod N \in QR_N$.

(ii) $y y' \bmod N \in QR_N$.

(iii) $xy \bmod N \in QNR_N^{+1}$.

we have

(i) $x x' \bmod N \in Q R_N$.

(ii) $y y' \bmod N \in Q R_N$.

(iii) $xy \bmod N \in Q N R_N^{+1}$.

Pf (i) $J_N(xx') = J_N(x) \cdot J_N(x')$.

$= J_p(x) \cdot J_q(x) \cdot J_p(x') \cdot J_q(x') = J_p(xx') \cdot J_q(xx')$

$J_p(x) = 1$, $J_q(x) = 1$

(ii) $J_N(yy') = J_N(y) \cdot J_N(y')$.

we have to show that $J_p(yy') = 1$, $J_q(yy') = 1$.

$J_p(yy') = J_p(y) \cdot J_p(y') = +1$ (−1, −1)

$J_q(yy') = J_q(y) \cdot J_q(y') = +1$ (−1, −1)

$J_N(yy') = J_N(y) \cdot J_N(y')$.

not a quadratic residue mod p and q

$yy' \in QNR_N$ $\Rightarrow$ Jacobi $+1$.

(iii) $J_N(xy) = J_p(xy) \cdot J_q(xy)$ (+1, −1)

$= -1 \cdot -1 = +1$.

$J_p(xy) = J_p(x) \cdot J_p(y) = -1$

$J_q(xy) = J_q(x) \cdot J_q(y) = -1$

(+1, −1) (+1, −1)

$J_N(yy') = J_p(yy') \cdot J_q(yy')$

$= J_p(y) \cdot J_p(y') \cdot J_q(y) \cdot J_q(y')$

$= +1 \cdot -1 \cdot +1 \cdot -1$

Remark: $y, y' \in QNR_p$, then $yy' \in QR_p$. $\Rightarrow J_p(yy') = -1$

Suppose $y, y' \in QNR_N$ $\Rightarrow J_p(y) = +1$, $J_q(y) = -1$ $\Rightarrow J_q(yy') = -1$.

$\Rightarrow J_p(y') = -1$, $J_q(y') = +1$.