Speedrun Quadratic Residue

Cryptography Breaks

Buce-Ithon

11$^{\text{th}}$ January, 2025

Contents

1 Unique Section

The definition of quadratic remainder comes from the expansion of perfect square numbers(x^2) in the integer system into the multiplicative group modulo q.

Definition 1.1. ***Quadratic Residue***
$\forall$ prime number p,$a \in \mathbb{Z}_p$, a is a quadratic residue modulo p if $\exists$ integer x such that $x^2 \equiv a \pmod{p}$. Otherwise, a is a quadratic non-residue modulo p.

Definition 1.2. ***Legendre Symbol***
$\forall$ odd prime number p,$a \in \mathbb{Z}_p$, the Legendre symbol is defined as:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \ mod\ p \equiv \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \\ 0 & \text{if } a \equiv 0 \pmod{p} \end{cases}$$

Property.
1. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
2. *If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$*

Theorem 1.1. ***Gauss Law of Quadratic Reciprocity***
$\forall$ odd prime numbers p and q, the Legendre symbol satisfies:

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

Definition 1.3. ***Jacobi Symbol***
$\forall$ odd integer n and $a \in \mathbb{Z}_n$, $gcd(n, a) = 1$, the Jacobi symbol is defined as:

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$$

where $n = \prod_{i=1}^{k} p_i^{e_i}$ is the prime factorization of n.

Moreover, 2 important theorems should be mentioned here.

Theorem 1.2. *Euler's Theorem*
$\forall$ integer a and n, $gcd(a, n) = 1$, then:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Theorem 1.3. *(Collary)Fermat's Little Theorem*
$\forall$ prime number p and integer a, then:

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

Last but not least, let's come back to cryptography, looking at some applications of Legendre symbol.

Theorem 1.4. ***Solovay-Strassen Primality Test***

1. *$\forall$ odd prime p, then $\forall$ integer a, we have $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ mod p.*

2. *$\forall$ odd composite n, then there are at least 50% integer a, s.t. $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}$ mod n is false.*