QUADRATIC RESIDUE

JUDE GAO

1. Introduction

Definition 1.1. a is said to be a *quadratic residue* if there exists non-zero $x \in \mathbb{Z}$ such that

$$x^2 \equiv a \mod p$$

Otherwise, if x is non-zero, a is said to be a *quadratic non-residue*.

Note that we are excluding the case where $a \equiv 0 \mod p$. In such case, a is neither a quadratic residue nor a quadratic non-residue.

It turns out that there is an interesting connection between quadratic residues and primitive roots, as in the following example.

Example 1.1. Consider the quadratic residues modulus 11. Let $1 \leq x < 11$.

x	x^2 mod 11
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

Already, an interesting feature of quadratic residues reveals, namely, the symmetry of quadratic residues. It is clearly not a coincidence since if $x^2 \equiv a \mod p$, then $(-x)^2 \equiv a \mod p$ for all a.

Thus, the set of complete representatives of quadratic residues modulus 11 is

$$\{1, 3, 4, 5, 9\}$$

Now let's investigate the connection between quadratic residues and primitive roots. We know that 2 is a primitive root modulus 11. Consider 2^λ for $1 \leq \lambda < 11$.

λ	$2^\lambda \mod 11$
1	2
2	4
3	8
4	5
5	10
6	9
7	7
8	3
9	6
10	1

Concentrate on the even powers of 2. They are $4, 5, 9, 3, 1$. Exactly, every quadratic residue appears in the even powers of a primitive root. This motivates the following theorem.

Theorem 1.1. Let g be any primitive root modulus p. Then,

$$a \equiv g^\alpha \text{ is a quadratic residue}$$

$$\text{iff}$$

$$\alpha \text{ is even}$$

Proof. Suppose $x^2 \equiv a \mod p$. Let

$$a \equiv g^\alpha \mod p$$
$$x \equiv g^\lambda \mod p$$

(**Exercise.** Explain why we can write x and a in terms of g.)
where

$$\begin{aligned} x^2 \equiv a &\implies g^{2\lambda} \equiv g^\alpha \\ &\implies p-1 \mid 2\lambda - \alpha \qquad \text{(Why?)} \\ (2 \mid p-1) &\implies 2 \mid 2\lambda - \alpha \\ &\implies 2 \mid \alpha \end{aligned}$$

Let $\alpha = 2\alpha_0$ for some $\alpha \in \mathbb{Z}$. Then

$$a \equiv (g^{\alpha_0})^2 \mod p$$

Any of $x \equiv \pm g^{\alpha_0} \mod p$ works.

□

It follows immediately that the number of quadratic residues is half of $p-1$ (except for $p = 2$). Thus, the corollary:

Corollary 1.1. Let p be an odd prime. The number of quadratic residues amongst $1 \leq a < p$ equals $\frac{p-1}{2}$.

2. Multiplication law of quadratic residue

We will see that multiplying quadratic residues will give another quadratic residue, and this is referred to as **the multiplication law of quadratic residue**.

Let a, b be two quadratic residues modulus p. Let g be any primitive root modulus p. Theorem 1.1 tells that for some even α and β, we have that

$$a \equiv g^{\alpha} \mod p \tag{1}$$

$$b \equiv g^{\beta} \mod p \tag{2}$$

Multiplying (1) and (2) gives

$$ab \equiv g^{\alpha+\beta} \mod p$$

Since α and β are even, it is clear that $\alpha + \beta$ is even. By Theorem 1.1, ab must be another quadratic residue.

Clearly, one can henceforth deduce that if α and β are odd, then ab is also a quadratic residue. When one of α and β is even and the other one is odd, ab can not be a quadratic residue.

The multiplication law motivates **Legendre's Symbol**.

Definition 2.1. Let p be an odd prime. Let $a \in \mathbb{Z}$. Define

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

Previously, we saw that to verify if some a is a quadratic residue, we have to make use of primitive roots, but it often involves large computations. However, the following theorem gives another characteristics of quadratic residues without primitive roots.

Theorem 2.1 (Euler's Criterion)**.** Let p be an odd prime and $a \in \mathbb{Z}$. Then,

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

Proof. If $a \equiv 0 \mod p$, then both sides are zero. Thus, assume $a \not\equiv 0 \mod p$. Let g be a primitive root modulus p.

Then, Theorem 1.1 suggests that we consider

$$a \equiv g^{\alpha} \mod p$$

If $\left(\frac{a}{p}\right) = 1$, then α is even. It implies

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv \left(g^{2\alpha_0}\right)^{\frac{p-1}{2}} \mod p \\ &\equiv \left(g^{p-1}\right)^{\alpha_0} \\ &\equiv 1 \qquad \text{(By Fermat)} \end{aligned}$$

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

If $\left(\frac{a}{p}\right) = -1$, then $\alpha = 2\alpha_0 + 1$ is odd. Then,

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv \left(g^{2\alpha_0+1}\right)^{\frac{p-1}{2}} \\ &\equiv \left(g^{p-1}\right)^{\alpha_0} \cdot g^{\frac{p-1}{2}} \\ &\equiv g^{\frac{p-1}{2}} \mod p \qquad \text{(By Fermat)} \end{aligned}$$

But, $g^{p-1} \equiv 1 \mod p$ by Fermat. It implies

$$\begin{aligned} p \mid g^{p-1} - 1 &\implies p \mid \left(g^{\frac{p-1}{2}} - 1\right)\left(g^{\frac{p-1}{2}} + 1\right) \\ &\implies g \mid g^{\frac{p-1}{2}} + 1 \qquad \text{(Why } p \text{ does not divide } g^{\frac{p-1}{2}} - 1\text{?)} \\ &\implies g^{\frac{p-1}{2}} \equiv -1 \mod p \end{aligned}$$

Hence, $a^{\frac{p-1}{2}} \equiv -1 \mod p$. □