4. Quadratic Residues

We study quadratic residues and non-residues. In this part we are mainly interested in deciding whether a given integer a is a quadratic residue modulo an odd prime p. We will introduce quadratic reciprocity, whose proof will be given in next part.

4.1. **Quadratic residues and the Legendre symbol.** First we recall the definition of quadratic residues and non-residues.

Definition 4.1. For integers a and m, $m \neq 0$, $\mathrm{hcf}(a, m) = 1$, a is called a *quadratic residue* modulo m if the congruence $x^2 \equiv a \pmod{m}$ has a solution. Otherwise a is called a *quadratic non-residue* modulo m.

Given any fixed positive integer m, it is possible to determine the quadratic residues by simply listing the positive integers less than and coprime to m, squaring them, and reducing modulo m. But we prefer to have a more convenient way to determine whether a given integer a coprime to m is a quadratic residue modulo m. At the moment we are mostly interested in the case that m is an odd prime p. An example of a composite m will be given in Exercise 5.3.

The Legendre symbol is a very simple yet powerful tool in studying this problem. Roughly speaking, it is the indication function for quadratic residues. We recall its definition:

Definition 4.2. Let p be an odd prime. The *Legendre symbol* $\left(\frac{a}{p}\right)$ takes value 1 if a is a quadratic residue modulo p, or -1 if a is a quadratic non-residue modulo p, or 0 if p divides a.

Therefore the problem reduces to the computation of the Legendre symbol. There are a series of rules which help with the computation. We introduce them in four groups.

The first group of properties are simple consequences of the definition.

Proposition 4.3. *Let p be an odd prime.*

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

(2) *If $p \nmid a$, then $\left(\frac{a^2}{p}\right) = 1$.*

Proof. Both statements are clear by definition. □

Next group of properties are more interesting. The proof essentially use the existence of primitive roots.

Proposition 4.4. *Let p be an odd prime.*

(1) (Euler's criterion). $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

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

Proof. For (1), both sides are congruent to 0 if $p \mid a$. Now we assume $p \nmid a$. Notice that $a^{p-1} \equiv 1 \pmod{p}$ by Corollary 2.11. Hence $(a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) \equiv 0 \pmod{p}$, so $a^{\frac{p-1}{2}} \equiv 1$ or $-1 \pmod{p}$.

If a is a quadratic residue modulo p, assume $a \equiv x^2 \pmod{p}$. Then $p \nmid x$, and $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$ by Corollary 2.11 again. If a is a quadratic non-residue modulo p, it suffices to show $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. Let g be a primitive root modulo p, then $a \equiv g^r \pmod{p}$ for some $r \in \mathbb{Z}$. We observe that r must be odd, otherwise $a \equiv (g^{\frac{r}{2}})^2 \pmod{p}$ is a quadratic residue. Hence we can write $r = 2k + 1$ for some $k \in \mathbb{Z}$. Then we have $a^{\frac{p-1}{2}} \equiv g^{(2k+1)\cdot\frac{p-1}{2}} \equiv g^{(p-1)k} \cdot g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ because the order of g modulo p is $p - 1$.

For (2), by (1) we can get $(\frac{ab}{p}) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (\frac{a}{p})(\frac{b}{p}) \pmod{p}$. Since both sides can only take values in $\{-1, 0, 1\}$, they must be equal. □

We characterise those primes for which -1 or 2 is a quadratic residue by the follow proposition. We remind the reader that if n is an odd integer, then $n - 1$ is always a multiple of 2 and $n^2 - 1$ is always a multiple of 8 (we have seen this fact in the proof of Proposition 3.6).

Proposition 4.5. *Let p be an odd prime.*

(1) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv -1 \pmod{4}. \end{cases}$

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

Proof. Part (1) follows immediately from of Proposition 4.4 (1). There are different ways of proving part (2). We provide an elementary proof here. Consider the following $\frac{p-1}{2}$

congruences

$$\begin{aligned} p-1 &\equiv 1\cdot(-1)^1 \pmod p \\ 2 &\equiv 2\cdot(-1)^2 \pmod p \\ p-3 &\equiv 3\cdot(-1)^3 \pmod p \\ &\vdots \\ \frac{p-1}{2} \text{ or } p-\frac{p-1}{2} &\equiv \frac{p-1}{2}\cdot(-1)^{\frac{p-1}{2}} \pmod p. \end{aligned}$$

The pattern on the left-hand side: for every $i = 1, 2, \cdots, \frac{p-1}{2}$, we put i if i is even, or $p-i$ if i is odd. So the left-hand side of the above congruences has exhausted all even numbers between 1 and p. We multiply all of the congruences together to get

$$2\cdot 4\cdot 6\cdots(p-3)\cdot(p-1) \equiv \left(\frac{p-1}{2}\right)!\cdot(-1)^{1+2+\cdots+\frac{p-1}{2}} \pmod p.$$

Therefore we have

$$2^{\frac{p-1}{2}}\cdot\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!\cdot(-1)^{\frac{p^2-1}{8}} \pmod p.$$

Since p does not divide $\left(\frac{p-1}{2}\right)!$, we can cancel it on both sides to get

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod p.$$

By Proposition 4.4 (1) we get

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

since they both take values 1 or -1.

Finally, if $p \equiv \pm 1 \pmod 8$, then we can write $p = 8k \pm 1$ for some $k \in \mathbb{Z}$. Hence $\frac{p^2-1}{8} = 8k^2 \pm 2k$ is an even number. If $p \equiv \pm 3 \pmod 8$, then we can write $p = 8k \pm 3$ for some $k \in \mathbb{Z}$. Hence $\frac{p^2-1}{8} = 8k^2 \pm 6k + 1$ is an odd number. This proves

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8, \end{cases}$$

as desired. □

Finally, we state the law of quadratic reciprocity. This is a deep result which has great influence in the modern number theory. The proof will be postponed to next part.

Theorem 4.6 (Law of Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then*

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

Remark 4.7. We can state the quadratic reciprocity in a slightly different way: for odd primes p and q, we have $(\frac{q}{p}) = \pm(\frac{p}{q})$. We take the positive sign if either p or q is congruent to 1 modulo 4, or the negative sign if both p and q are congruent to -1 modulo 4.

The law of quadratic reciprocity can be used in conjunction with the previous propositions to compute the Legendre symbol. Very roughly speaking, given a Legendre symbol $(\frac{a}{p})$, after replacing a by the remainder of a modulo p if possible, we use the prime factorisation of a to write $(\frac{a}{p})$ as the product of several Legendre symbols, some of which can be immediately evaluated. Then we use the quadratic reciprocity for the other factors and repeat this process. We give an example:

Example 4.8. We calculate $(\frac{79}{101})$. Since $101 \equiv 1 \pmod 4$ we have $(\frac{79}{101}) = (\frac{101}{79}) = (\frac{22}{79})$. Then we factor as $(\frac{22}{79}) = (\frac{2}{79})(\frac{11}{79})$. Now $79 \equiv 7 \pmod 8$, thus $(\frac{2}{79}) = 1$. Since both 11 and 79 are congruent to 3 modulo 4 we have $(\frac{11}{79}) = -(\frac{79}{11}) = -(\frac{2}{11})$. Finally $11 \equiv 3 \pmod 8$ implies that $(\frac{2}{11}) = -1$. Therefore $(\frac{79}{101}) = 1$; i.e. 79 is a quadratic residue modulo 101. Indeed, we can check $33^2 \equiv 79 \pmod{101}$.