5. Quadratic Reciprocity

We introduce yet another way of computing Legendre symbol due to Gauss and give a proof of the law of quadratic reciprocity.

5.1. **Gauss' lemma.** For any odd prime p and any integer a not divisible by p, Euler's criterion Proposition 4.4 (1) gives a characterisation of the Legendre symbol. Next we introduce another characterisation of the Legendre symbol due to Gauss, usually named as Gauss' lemma.

For simplicity we write $r = \frac{p-1}{2}$. We consider the set

$$S = \{-r, -(r-1), \cdots, -2, -1, 1, 2, \cdots, r-1, r\}.$$

Any integer n not divisible by p is congruent to one element in S, which is called the *least residue* of n modulo p. If $p \nmid a$, let μ be the number of integers among $a, 2a, \cdots, ra$ which have negative least residues modulo p. For example, let $p = 7$ and $a = 4$. Then $r = 3$, and the residues of $1 \cdot 4, 2 \cdot 4, 3 \cdot 4$ are $-3, 1, -2$ respectively. Thus in this case $\mu = 2$.

Gauss' lemma is the following very simple yet very powerful result:

Lemma 5.1 (Gauss' Lemma). *Let p be an odd prime, $r = \frac{p-1}{2}$, $p \nmid a$, and μ the number of integers among $a, 2a, \cdots, ra$ which have negative least residues modulo p. Then $\left(\frac{a}{p}\right) = (-1)^\mu$.*

Proof. Let m_l or $-m_l$ be the least residue of la modulo p, where m_l is positive. As l ranges between 1 and r, μ is clearly the number of minus signs that occur in this way. We claim that $m_l \neq m_k$ for any $l \neq k$ and $1 \leqslant l, k \leqslant r$. For, if $m_l = m_k$, then $la \equiv \pm ka \pmod p$, and since $p \nmid a$ this implies that $l \pm k \equiv 0 \pmod p$. The latter congruence is impossible since $l \neq k$ and $|l \pm k| \leqslant |l| + |k| \leqslant p - 1$. It follows that the sets $\{1, 2, \cdots, r\}$ and $\{m_1, m_2, \cdots, m_r\}$ coincide. Multiply the congruences

$$\begin{aligned}
1 \cdot a &\equiv \pm m_1 \pmod p, \\
2 \cdot a &\equiv \pm m_2 \pmod p, \\
&\vdots, \\
r \cdot a &\equiv \pm m_r \pmod p.
\end{aligned}$$

Notice that the number of negative signs on the right hand sides is μ, we obtain

$$r! \cdot a^r \equiv (-1)^\mu \cdot r! \pmod p.$$

Since $p \nmid r!$, this yields

$$a^r \equiv (-1)^\mu \pmod p.$$

By Euler's criterion $a^r = a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$ and the result follows. $\square$

We use Gauss' lemma to give another characterisation of the Legendre symbol, which will be used in the proof of quadratic reciprocity.

For later convenience, we introduce the so-called *floor function*. For any real number x, we define the symbol $[x]$ to be the largest integer less than or equal to x, which is sometimes also called the *integral part* of x. But pay attention when x is negative. For example, $[3] = [3.2] = 3$, $[-3] = -3$ but $[-3.2] = -4$.

If $a, b \in \mathbb{Z}$ and $b \neq 0$, we know that there is a unique way to write $a = bq + c$ for some $q, c \in \mathbb{Z}$ and $0 \leqslant c < |b|$, where q is called the *quotient* and c is called the *remainder* (or *Euclidean residue*). If we assume $b > 0$, then q is the integral part of the fraction $\frac{a}{b}$; i.e. $\left[\frac{a}{b}\right] = q$. In other words we can write $a = b\left[\frac{a}{b}\right] + c$.

Lemma 5.2. *Let p be an odd prime, a an odd integer not divisible by p. Let*

$$t = \sum_{l=1}^{\frac{p-1}{2}} \left[\frac{la}{p}\right].$$

Then $\left(\dfrac{a}{p}\right) = (-1)^t$.

Proof. For simplicity we write $r = \frac{p-1}{2}$. For each $l = 1, 2, \cdots, r$, we can write

$$la = p\left[\frac{la}{p}\right] + c_l,$$

where $0 \leqslant c_l \leqslant p-1$. We take the sum of the l equations and get

$$a \cdot \sum_{l=1}^{r} l = pt + \sum_{l=1}^{r} c_l. \tag{5.1}$$

Recall we wrote $\pm m_l$ for the least residue in the proof of Lemma 5.1. It is clear that

$$c_l = \begin{cases} m_l & \text{if the sign in front of } m_l \text{ is positive;} \\ -m_l + p & \text{if the sign in front of } m_l \text{ is negative.} \end{cases}$$

Modulo 2 we get

$$c_l \equiv \begin{cases} m_l \pmod 2 & \text{if the sign in front of } m_l \text{ is positive;} \\ m_l + p \pmod 2 & \text{if the sign in front of } m_l \text{ is negative.} \end{cases}$$

Now we take the sum of the l congruences and keep in mind that the negative sign in front of m_l appears exactly μ times:

$$\sum_{l=1}^{r} c_l \equiv \sum_{l=1}^{r} m_l + p\mu \pmod 2.$$

We also know that $\{m_1, m_2, \cdots, m_r\}$ is simply a permutation of $\{1, 2, \cdots, r\}$, hence

$$\sum_{l=1}^{r} c_l \equiv \sum_{l=1}^{r} l + p\mu \pmod 2. \tag{5.2}$$

Now we use (5.2) to rewrite (5.1) as

$$a \cdot \sum_{l=1}^{r} l \equiv pt + \sum_{l=1}^{r} l + p\mu \pmod 2.$$

Since a is odd, we get $pt + p\mu \equiv 0 \pmod 2$. Since p is also odd, we get $t + \mu \equiv 0 \pmod 2$; that is $t \equiv \mu \pmod 2$. By Lemma 5.1 we have

$$\left(\frac{a}{p}\right) = (-1)^{\mu} = (-1)^{t},$$

as desired. □