Chapter 10

Quadratic Reciprocity

10.1 Gauss' Law of Quadratic Reciprocity

This has been described as 'the most beautiful result in Number Theory'.

Theorem 10.1. *Suppose p, q are distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} -1 & \text{if } p \equiv q \equiv 3 \bmod 4 \\ 1 & \text{otherwise.} \end{cases}$$

More than 200 proofs of this have been given. Gauss himself gave 11.

We give a short proof of the Theorem below. It is due to Rousseau, and is fairly recent (1989), although it is said to be based on Gauss' 5th proof. It is subtle, but requires nothing we have not met.

10.2 Wilson's Theorem

We start with a preliminary result which is not really necessary, but which simplifies the formulae in the proof.

Proposition 10.1. *If p is an odd prime then*

$$(p-1)! \equiv -1 \bmod p.$$

Proof. Consider the numbers $1, 2, \ldots, p-1$. Each number x has a reciprocal $x^{-1} \mod p$ in this set. The number x is equal to its reciprocal if and only if

$$x^2 \equiv 1 \implies x \equiv \pm 1 \bmod p.$$

It follows that the remaining $p-3$ numbers divide into pairs, each with product $1 \mod p$. Hence the product of all $p-1$ numbers is

$$1 \cdot -1 = -1 \bmod p.$$

□

We shall find our formulae are simplified if we set

$$P = (p-1)/2,\ Q = (q-1)/2.$$

Corollary 10.1. $(P!)^2 \equiv (-1)^{P+1} \bmod p$.

Proof. This follows from Wilson's Theorem on replacing the numbers $\{P+1, \ldots, p-1\}$ by $\{-1, -2, ..., -P \bmod p\}$. □

Recall the definition of the quotient-group G/H, where H is a normal subgroup of G. (We will only be interested in abelian groups, in which case every subgroup is normal.) The elements of G/H are the cosets of H in G. If we write $x' \sim x$ to mean that x', x are in the same H-coset, ie $x' = xh$ for some $h \in H$, then the basic step in defining the product operation on G/H is to show that

$$x' \sim x,\ y' \sim y \implies x'y' \sim xy.$$

It follows from this that if we take representatives $x_1, \ldots, x_r$ of all the cosets of H then the coset containing the product $x_1 \cdots x_r$ is independent of the choice of representatives:

$$x_i' \sim x_i \text{ for } 1 \le i \le r \implies x_i' \cdots x_r' \sim x_1 \cdots x_r,$$

ie

$$x_i' \cdots x_r' = (x_1 \cdots x_r)h,$$

for some $h \in H$.

10.3 Rousseau's proof

Proof. Recall that the Chinese Remainder Theorem establishes a group-isomorphism

$$(\mathbb{Z}/pq)^\times = (\mathbb{Z}/p)^\times \times (\mathbb{Z}/q)^\times,$$

under which

$$n \bmod pq \mapsto (n \bmod p, n \bmod q)$$

for n coprime to pq. We can identify the product-group on the right with the pairs

$$\{(x, y) : x \in \{1, \ldots, p-1\},\ y \in \{1, \ldots, q-1\}\}.$$

We are going to consider the quotient of this group by the subgroup

$$\{\pm 1\} = C_2.$$

In other words, we are going to divide the group into pairings $\{(x, y), (-x, -y)\}$. The group has order $(p-1)(q-1) = 4PQ$, so there are $2PQ$ pairings.

We are going to choose one representative from each pairing, in two different ways. In each case we will form the product of these representatives. by the argument above, the two products will differ by a factor ± 1.

For our first division, let us take the first half of $(\mathbb{Z}/p)^\times$, and the whole of $(\mathbb{Z}/q)^\times$. In other words, we take the representatives

$$\{(x, y) :\ 1 \le x \le P,\ 1 \le y \le q-1\}.$$

We want to compute the product of these elements.

The x-components are $1, 2, \ldots, P$, repeated $q-1$ times. Their product is

$$(P!)^{q-1} = ((P!)^2)^Q \equiv (-1)^{(P+1)Q} \bmod p,$$

by the Corollary to Wilson's Theorem.

The y-components are $1, 2, \ldots, q-1$, repeated P times. By Wilson's Theorem, their product is

$$(-1)^P \bmod q.$$

Thus the product of the representatives is

$$((-1)^{(P+1)Q} \bmod p,\ (-1)^P \bmod q).$$

We could equally well choose representatives by taking the whole of $(\mathbb{Z}/p)^\times$ and the first half of $(\mathbb{Z}/q)^\times$. The product of these representatives would be

$$((-1)^Q \bmod p,\ (-1)^{P(Q+1)} \bmod q).$$

However, what we need is a third way of choosing representatives, by choosing the first half of $(\mathbb{Z}/pq)^\times$. By this we mean the pairs ($n \mod p$, $n \mod q$), where n runs through the numbers $1, \ldots, (pq-1)/2$ not divisible by p or q, ie the set of numbers $A \setminus B$, where

$$A = \{1, 2, \ldots, p-1, p+1, p_2, \ldots, 2p-1, \ldots, Qp+1, \ldots, Qp+P\},$$

while B denotes the numbers in this set divisible by q, ie

$$B = \{q, 2q, \ldots, Pq\}.$$

Again, we compute the product ($X \bmod p$, $Y \bmod q$) of these representatives. The first component $X \mod p$ is

$$((p-1)!)^Q \cdot P!/q^P \cdot P! = ((p-1)!)^Q/q^P \equiv (-1)^Q/q^P \bmod p.$$

But by Eisenstein's criterion,

$$q^P = \left(\frac{q}{p}\right) \bmod p.$$

Thus

$$X = (-1)^Q \left(\frac{q}{p}\right) \bmod p.$$

Similarly, the second component $Y \mod q$ is

$$Y = (-1)^P \left(\frac{p}{q}\right) \bmod q.$$

Comparing the products of the two choices of representatives,

$$((-1)^{(P+1)Q} \bmod p,\ (-1)^P \bmod q) = \pm((-1)^Q \left(\frac{q}{p}\right) \bmod p, (-1)^P \left(\frac{p}{q}\right) \bmod q).$$

From the second components, the factor ± 1 is actually $\left(\frac{p}{q}\right)$. Hence from the first components,

$$(-1)^{(P+1)Q} = (-1)^Q \left(\frac{q}{p}\right)\left(\frac{p}{q}\right),$$

ie

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

which is the Reciprocity Theorem.

□