5. Quadratic Reciprocity

5.1. **Introduction.** Recall that the Legendre symbol $\left(\frac{a}{p}\right)$ is defined for an odd prime p and integer a coprime to p as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a quadratic residue} \pmod p; \\ -1 \text{ otherwise;} \end{cases}$$

Recall too that for a, b coprime to p

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

(easily proved by writing a, b as powers of a primitive root), and that, by Euler's Criterion,

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

Theorem 5.1 (Law of Quadratic Reciprocity (Legendre, Gauss))**.** *For distinct odd primes p and q we have*

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

(Thus $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless p and q are both $\equiv -1 \pmod 4$, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.)

There are now 240 recorded proofs of this (not all different), including six by Gauss – see

`http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`.

We'll give one of Gauss's proofs, using

Lemma 5.2 (Gauss's Lemma)**.** *For an odd prime p, put $p' = \frac{p-1}{2}$, and let a be an integer coprime to p. Consider the sequence*

$$a, 2a, 3a, ..., p'a,$$

reduced $\bmod p$ *to lie in* $(-\frac{p}{2}, \frac{p}{2})$*. Then* $\left(\frac{a}{p}\right) = (-1)^\nu$*, where ν is the number of negative numbers in this sequence.*

Proof. Now all of $a, 2a, 3a, ..., p'a$ are $\equiv \pmod p$ to one of $\pm 1, \pm 2, \ldots, \pm p'$. Further,

- no two are equal, as $ia \equiv ja \pmod p \Rightarrow i \equiv j \pmod p$;
- none is minus another, as $ia \equiv -ja \pmod p \Rightarrow i + j \equiv 0 \pmod p$.

So they must be $\pm 1, \pm 2, \ldots, \pm p'$, with each of $1, 2, \ldots, p'$ occurring with a *definite sign.* Hence

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot p'a \equiv (\pm 1) \cdot (\pm 2) \cdot \ldots \cdot (\pm p') \pmod p,$$

giving

$$a^{p'}(p')! \equiv (-1)^\nu (p')! \pmod p,$$

and so, as $(p')!$ is coprime to p, that

$$a^{p'} \equiv (-1)^\nu \pmod{p}.$$

Finally, using Euler's criterion (Prop. 2.8), we have

$$\left(\frac{a}{p}\right) \equiv a^{p'} \equiv (-1)^\nu \pmod{p}.$$

Hence $\left(\frac{a}{p}\right) = (-1)^\nu$. □

We can use Gauss's Lemma to evaluate $\left(\frac{2}{p}\right)$.

Proposition 5.3. *For p an odd prime we have $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.*

(This is equal to 1 when $p \equiv \pm 1 \pmod 8$, and to -1 when $p \equiv \pm 3 \pmod 8$.)

Proof. There are four similar cases, depending on $p \pmod 8$. We give the details for $p \equiv 3 \pmod 8$, $p = 8\ell + 3$ say. Then $p' = 4\ell + 1$, and, taking $a = 2$ in Gauss's Lemma, we see that for the sequence

$$2, 4, 6, \ldots, 4\ell, 4\ell + 2, \ldots, 8\ell + 2$$

that this becomes

$$2, 4, 6, \ldots, 4\ell, -(4\ell + 1), -(4\ell - 1), \ldots, -3, -1$$

when reduced $\pmod p$ into the range $(-\frac{p}{2}, \frac{p}{2})$. This clearly has 2ℓ positive members, and hence $\nu = p' - 2\ell = 2\ell + 1$ negative members. Hence $\left(\frac{2}{p}\right) = (-1)^{2\ell+1} = -1$. □

Doing the other three cases would be a good exercise!

We now use Gauss's Lemma with $a = q$ to prove the Law of Quadratic Reciprocity.

Proof of Theorem 5.1. Take distinct odd primes p and q. For $k = 1, 2, \ldots, p'$ write (one step of the Euclidean algorithm)

$$kq = q_k p + r_k \tag{1}$$

say, where $1 \le r_k \le p - 1$ and

$$q_k = \left\lfloor \frac{kq}{p} \right\rfloor. \tag{2}$$

Now, working in $\mathbb{F}_p$ we have

$$\{q, 2q, \ldots, p'q\} = \{r_1, r_2, \ldots, r_{p'}\} = \{a_1, a_2, \ldots, a_t\} \cup \{-b_1, -b_2, \ldots, -b_\nu\},$$

as in Gauss's Lemma. So the a_i's are in $(0, \frac{p}{2})$ and the $-b_i$'s are in $(-\frac{p}{2}, 0)$. (In fact $t = p' - \nu$, but not needed.) Now put

$$a = \sum_{i=1}^{t} a_i, \qquad b = \sum_{i=1}^{\nu} b_i.$$

So, by the definition of the a_i's and $-b_i$'s we have

$$\sum_{k=1}^{p'} r_k = a - b + \nu p. \tag{3}$$

Now, in the proof of Gauss's Lemma we saw that

$$\{a_1, a_2, \ldots, a_t\} \cup \{b_1, b_2, \ldots, b_\nu\} = \{1, 2, \ldots, p'\},$$

so that

$$\frac{p^2-1}{8} = 1 + 2 + \cdots + p' = a + b. \tag{4}$$

and

$$\begin{aligned} \frac{p^2-1}{8} q &= \sum_{k=1}^{p'} kq \\ &= p \sum_{k=1}^{p'} q_k + \sum_{k=1}^{p'} r_k \qquad \text{(using (1))} \\ &= p \sum_{k=1}^{p'} q_k + a - b + \nu p, \qquad \text{(using (3).)} \end{aligned} \tag{5}$$

Next, on subtracting (5) from (4) we get

$$\frac{p^2-1}{8}(q-1) = p \sum_{k=1}^{p'} q_k - 2b + \nu p.$$

Reducing this modulo 2 we have $0 \equiv \sum_{k=1}^{p'} q_k - \nu \pmod 2$, or $\nu \equiv \sum_{k=1}^{p'} q_k \pmod 2$. Thus Gauss's Lemma gives

$$\left(\frac{q}{p}\right) = (-1)^\nu = (-1)^{\sum_{k=1}^{p'} q_k} = (-1)^{\sum_{k=1}^{p'} \left\lfloor \frac{kq}{p} \right\rfloor},$$

using (2).

Now, reversing the rôles of p and q we immediately get

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{\ell=1}^{q'} \left\lfloor \frac{\ell p}{q} \right\rfloor},$$

where of course $q' = (q-1)/2$, and we've replaced the dummy variable k by ℓ. So

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\left\{\sum_{k=1}^{p'} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{\ell=1}^{q'} \left\lfloor \frac{\ell p}{q} \right\rfloor\right\}},$$

which equals $(-1)^{p'q'}$, by Prop. 1.4. □