Appendix 8A. Eisenstein's proof of quadratic reciprocity

8.10. Eisenstein elegant proof, 1844

A lemma of Gauss gives a complicated but useful formula to determine (a/p):

Theorem 8.6 (Gauss's Lemma). *Given an integer a which is not divisible by odd prime p, define r_n to be the absolutely least residue of an* (mod p)*, and then define the set $\mathcal{N} := \{1 \le n \le \frac{p-1}{2} :\ r_n < 0\}$. Then $\left(\frac{a}{p}\right) = (-1)^{|\mathcal{N}|}$.*

For example, if $a = 3$ and $p = 7$ then $r_1 = 3, r_2 = -1, r_3 = 2$ so that $\mathcal{N} = \{2\}$ and therefore $\left(\frac{3}{7}\right) = (-1)^1 = -1$.

Proof. For each $m, 1 \le m \le \frac{p-1}{2}$ there is exactly one integer $n,\ 1 \le n \le \frac{p-1}{2}$ such that $r_n = m$ or $-m \pmod p$ (for if $an \equiv \pm an' \pmod p$ then $p|a(n \mp n')$, and so $p|n \mp n'$, which is possible in this range only if $n = n'$). Therefore

$$\left(\frac{p-1}{2}\right)! = \prod_{1\le m\le \frac{p-1}{2}} m = \prod_{\substack{1\le n\le \frac{p-1}{2}\\ n\notin\mathcal{N}}} r_n \cdot \prod_{\substack{1\le n\le \frac{p-1}{2}\\ n\in\mathcal{N}}} (-r_n)$$

$$\equiv \prod_{\substack{1\le n\le \frac{p-1}{2}\\ n\notin\mathcal{N}}} (an) \cdot \prod_{\substack{1\le n\le \frac{p-1}{2}\\ n\in\mathcal{N}}} (-an) = a^{\frac{p-1}{2}} (-1)^{|\mathcal{N}|} \cdot \left(\frac{p-1}{2}\right)! \pmod p.$$

Cancelling out the $\left(\frac{p-1}{2}\right)!$ from both sides, the result then follows from Euler's criterion. □

This proof is a clever generalization of the proof of Theorem 8.4.

Exercise 8.10.1.† Use Gauss's Lemma to determine the values of (a) $(-1/p)$; and (b) $(3/p)$, for all primes $p > 3$.

Exercise 8.10.2.† Let r be the absolutely least residue of $N \pmod p$. Prove that the least non-negative residue of $N \pmod p$ is given by

$$N - p\left[\frac{N}{p}\right] = \begin{cases} r & \text{if } r \geq 0; \\ p + r & \text{if } r < 0. \end{cases}$$

Corollary 8.10.1. *If p is a prime > 2 and a is an odd integer not divisible by p, then*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{n=1}^{\frac{p-1}{2}} \left[\frac{an}{p}\right]} . \tag{8.10.1}$$

Proof. (Gauss) By exercise 8.10.2 we have

$$\sum_{n=1}^{\frac{p-1}{2}} \left(an - p\left[\frac{an}{p}\right]\right) = \sum_{\substack{n=1 \\ n \notin \mathcal{N}}}^{\frac{p-1}{2}} r_n + \sum_{\substack{n=1 \\ n \in \mathcal{N}}}^{\frac{p-1}{2}} (p + r_n) = \sum_{n=1}^{\frac{p-1}{2}} r_n + p|\mathcal{N}|. \tag{8.10.2}$$

In the proof of Gauss's Lemma we saw that for each $m, 1 \leq m \leq \frac{p-1}{2}$ there is exactly one integer $n,\ 1 \leq n \leq \frac{p-1}{2}$ such that $r_n = m$ or $-m$, and so $r_n \equiv m \pmod 2$. Therefore, as a and p are odd, (8.10.2) implies that

$$|\mathcal{N}| \equiv \sum_{n=1}^{\frac{p-1}{2}} \left[\frac{an}{p}\right] \pmod 2 \text{ as } \sum_{n=1}^{\frac{p-1}{2}} r_n \equiv \sum_{m=1}^{\frac{p-1}{2}} m \equiv a \sum_{n=1}^{\frac{p-1}{2}} n \pmod 2.$$

We now deduce (8.10.1) from Gauss's lemma. □

The exponent $\sum_{n=1}^{\frac{p-1}{2}} \left[\frac{an}{p}\right]$ on the right-hand side of (8.10.1) looks excessively complicated. However it arises in a different context that is easier to work with:

Lemma 8.10.1. *Suppose that a and b are odd, coprime positive integers. There are*

$$\sum_{n=1}^{\frac{b-1}{2}} \left[\frac{an}{b}\right]$$

lattice points $(n, m) \in \mathbb{Z}^2$ for which $bm < an$ with $0 < n < b/2$.

Proof. We seek the number of lattice points (n, m) inside the triangle bounded by the lines $y = 0$, $x = \frac{b}{2}$ and $by = ax$. For such a lattice point, n can be any integer in the range $1 \leq n \leq \frac{b-1}{2}$. For a given value of n, the triangle contains the lattice points (n, m) where m is any integer in the range $0 < m < \frac{an}{b}$. These are the lattice points in the shaded rectangle in figure 1.

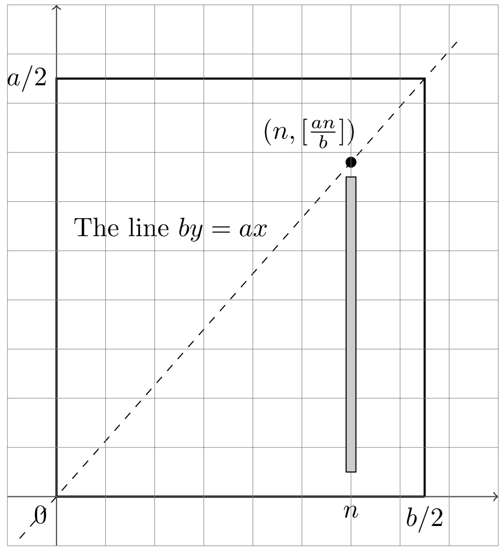

Figure 1. The shaded rectangle covers the lattice points (n, m) with $1 \le m \le [\frac{an}{b}]$

Evidently m ranges from 1 to $[\frac{an}{b}]$, and so there are $[\frac{an}{b}]$ such lattice points. Summing this up over the possible values of n, gives the lemma. ☐

Corollary 8.10.2. *If a and b are odd coprime positive integers then*

$$\sum_{n=1}^{\frac{b-1}{2}} \left[\frac{an}{b}\right] + \sum_{m=1}^{\frac{a-1}{2}} \left[\frac{bm}{a}\right] = \frac{(a-1)(b-1)}{2}.$$

Proof. The idea is to split the triangle

$$R := \left\{(x, y) : \ 0 < x < \frac{b}{2} \text{ and } 0 < y < \frac{a}{2}\right\},$$

into two parts: The points in R on or below the line $by = ax$; that is, in the region

$$A := \{(x, y) : \ 0 < x < b/2 \text{ and } 0 < y \le ax/b\};$$

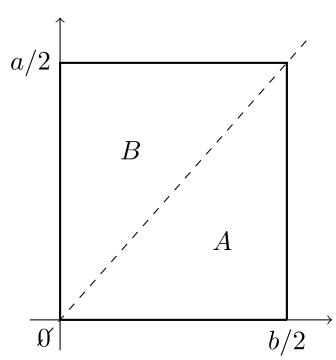

Figure 2. Splitting the rectangle R into two parts

and the points in R above the line $by = ax$; that is, in the region

$$B := \{(x, y) :\ 0 < x < by/a \text{ and } 0 < y < a/2\}.$$

We count the lattice points (that is, the points with integer co-ordinates) in R and then in A and B together. To begin with

$$R \cap \mathbb{Z}^2 = \left\{(n, m) \in \mathbb{Z}^2 :\ 1 \le n \le \frac{b-1}{2} \text{ and } 1 \le m \le \frac{a-1}{2}\right\},$$

so that $|R \cap \mathbb{Z}^2| = \frac{a-1}{2} \cdot \frac{b-1}{2}$.

Since there are no lattice points in R on the line $by = ax$, as $(a, b) = 1$, therefore

$$A \cap \mathbb{Z}^2 = \left\{(n, m) \in \mathbb{Z}^2 :\ 0 < n < b/2 \text{ and } bm < an\right\},$$

and so $|A \cap \mathbb{Z}^2| = \sum_{n=1}^{\frac{b-1}{2}} \left[\frac{an}{b}\right]$ by Lemma 8.10.1. Similarly

$$B \cap \mathbb{Z}^2 = \left\{(n, m) \in \mathbb{Z}^2 :\ 0 < m < a/2 \text{ and } an < bm\right\},$$

and so $|B \cap \mathbb{Z}^2| = \sum_{m=1}^{\frac{a-1}{2}} \left[\frac{bm}{a}\right]$ by Lemma 8.10.1 (with the roles of a and b interchanged). The result then follows from the observation that $A \cap \mathbb{Z}^2$ and $B \cap \mathbb{Z}^2$ partition $R \cap \mathbb{Z}^2$. $\square$

Eisenstein's proof of the law of quadratic reciprocity. By Corollary 8.10.1 with $a = q$, and then with the roles of p and q reversed, and then by Corollary 8.10.2, we deduce the desired law of quadratic reciprocity:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{n=1}^{\frac{p-1}{2}} \left[\frac{qn}{p}\right]} \cdot (-1)^{\sum_{m=1}^{\frac{q-1}{2}} \left[\frac{pm}{q}\right]} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}. \qquad \square$$