The Law of Quadratic Reciprocity

R. C. Daileda

Trinity University

Number Theory

Recall

Goal: Evaluate the Legendre symbol $\left(\frac{a}{p}\right)$, where p is an odd prime and $p \nmid a$, and thereby determine if a is a quadratic residue of p.

Reduction: Using the multiplicative property of $\left(\frac{\cdot}{p}\right)$, we must be able to evaluate $\left(\frac{q}{p}\right)$ for primes $q \neq p$.

The *Law of Quadratic Reciprocity* (which we have yet to state) will enable us to do the latter efficiently.

Number theorists love Quadratic Reciprocity: there are over 100 different proofs.

Gauss gave the first proof, in 1801. We will give one due to Eisenstein, one of Gauss' students.

Preliminary Lemma

Our main ingredient will be a reformulation of Gauss' Lemma.

Lemma (Eisenstein's Lemma)

Let p be an odd prime and $a \in \mathbb{Z}$ odd with $p \nmid a$. Let

$$R_a = \left\{ a, 2a, 3a, \ldots, \frac{p-1}{2}a \right\}.$$

Then

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{r \in R_a} \left\lfloor \frac{r}{p} \right\rfloor}.$$

Proof. Recall Gauss' Lemma: for each $r \in R_a$ there is a unique $-\frac{p-1}{2} \leq s_r \leq \frac{p-1}{2}$ so that $r \equiv s_r \pmod{p}$, and $\left(\frac{a}{p}\right) = (-1)^{\nu}$ where ν is the number of $s_r < 0$.

Moreover, the proof of Gauss' Lemma showed that, up to ν negative signs, $\{s_r \mid r \in R_a\}$ is $\left\{1, 2, 3, \ldots, \frac{p-1}{2}\right\}$.

To prove the current lemma it suffices to show that

$$\sum_{r \in R_a} \left\lfloor \frac{r}{p} \right\rfloor \equiv \nu \pmod{2}.$$

Begin by writing

$$r = q_r p + r_p, \;\; 0 \leq r_p < p$$

for $r \in R_a$. Notice that

$$\frac{r}{p} = q_r + \frac{r_p}{p}, \;\; 0 \leq \frac{r_p}{p} < 1 \;\; \Rightarrow \;\; \left\lfloor \frac{r}{p} \right\rfloor = q_r \;\; \Rightarrow \;\; r = \left\lfloor \frac{r}{p} \right\rfloor p + r_p.$$

We have

- $r_p < \frac{p}{2} \;\Rightarrow\; r_p = s_r > 0$;
- $r_p > \frac{p}{2} \;\Rightarrow\; -\frac{p}{2} < r_p - p < 0$ and $r = \left(\left\lfloor \frac{r}{p} \right\rfloor + 1\right) p + (r_p - p)$

$$\Rightarrow r_p - p = s_r < 0.$$

Summing over R_a we obtain

$$\sum_{r \in R_a} r = p \sum_{r \in R_a} \left\lfloor \frac{r}{p} \right\rfloor + \sum_{\substack{r \in R_a \\ s_r > 0}} s_r + \sum_{\substack{r \in R_a \\ s_r < 0}} (p + s_r)$$

$$a \sum_{k=1}^{(p-1)/2} k = p \sum_{r \in R_a} \left\lfloor \frac{r}{p} \right\rfloor + \sum_{\substack{r \in R_a \\ s_r > 0}} s_r + \sum_{\substack{r \in R_a \\ s_r < 0}} s_r + \nu p.$$

According to the proof of Gauss' Lemma

$$\sum_{k=1}^{(p-1)/2} k = \sum_{\substack{r \in R_a \\ s_r > 0}} s_r - \sum_{\substack{r \in R_a \\ s_r < 0}} s_r .$$

If we add this equation to the previous one we find that

$$(a+1) \sum_{k=1}^{(p-1)/2} k = p \sum_{r \in R_a} \left\lfloor \frac{r}{p} \right\rfloor + 2 \sum_{\substack{r \in R_a \\ s_r > 0}} s_r + \nu p.$$

Since a and p are both odd, if we consider this equation modulo 2 we get

$$0 \equiv \sum_{r \in R_a} \left\lfloor \frac{r}{p} \right\rfloor + \nu \pmod{2},$$

which is equivalent to what we wanted to show. $\square$

Example

Remark: This result simply expresses $\left(\frac{a}{p}\right)$ in terms of the *quotients* obtained when the elements of R_a are divided by p, as opposed to Gauss' Lemma which uses the *remainders*.

Example

Use the lemma above to evaluate $\left(\frac{7}{13}\right)$.

We have $R_7 = \{7, 14, 21, 28, 35, 42\}$ and

$$\begin{aligned}
7 &= 0 \cdot 13 + 7,\\
14 &= 1 \cdot 13 + 1,\\
21 &= 1 \cdot 13 + 8,\\
28 &= 2 \cdot 13 + 2,\\
35 &= 2 \cdot 13 + 9,\\
42 &= 3 \cdot 13 + 3.
\end{aligned}$$

Quadratic Reciprocity

Hence

$$\left(\frac{7}{13}\right) = (-1)^{0+1+1+2+2+3} = -1$$

so that 7 is a quadratic nonresidue of 13.

We are finally ready to state and prove our main result.

Theorem (The Law of Quadratic Reciprocity)

Let p and q be odd primes. Then

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

Proof. Since $\left(\frac{q}{p}\right) = \pm 1$, it is its own inverse. Hence it suffices to prove that

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

We will achieve this by counting the points of $\mathbb{N} \times \mathbb{N}$ (*lattice points*) in the rectangle $\mathcal{R}_{p,q} = [0, p/2] \times [0, q/2]$ in two ways.

Because there are $\frac{p-1}{2}$ naturals in the first interval and $\frac{q-1}{2}$ in the second, there are

$$\frac{p-1}{2} \cdot \frac{q-1}{2}$$

lattice points in $\mathcal{R}_{p,q}$.

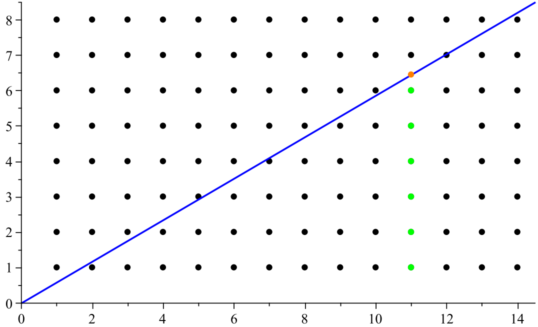
Now consider the diagonal D of $\mathcal{R}_{p,q}$, the line $y = \frac{q}{p}x$. Note that no lattice point in $\mathcal{R}_{p,q}$ lies on D (why?).

Thus $\#\{$lattice points in $\mathcal{R}_{p,q}\}$ is

$$\#\{\text{lattice points below } D\} + \#\{\text{lattice points above } D\}.$$

We count points below D by columns, and points above D by rows.

Given $1 \leq k \leq \frac{p-1}{2}$, the lattice points above $(k, 0)$ and below D have the form (k, ℓ) where $1 \leq \ell \leq \lfloor \frac{qk}{p} \rfloor$. For example:



Here $p = 29$, $q = 17$, $k = 11$. The orange point is $(11, 11q/p)$, and the number of green points is $\left\lfloor \frac{11q}{p} \right\rfloor$.

Hence

$$\#\{\text{lattice points below } D\} = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor .$$

Likewise, counting lattice points in rows above D gives

$$\#\{\text{lattice points above } D\} = \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{pk}{q} \right\rfloor .$$

Therefore, according to Eisenstein's Lemma, we have

$$\begin{aligned}
(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} &= (-1)^{\sum_{k=1}^{(p-1)/2}\left\lfloor \frac{qk}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2}\left\lfloor \frac{pk}{q} \right\rfloor} \\
&= (-1)^{\sum_{k=1}^{(p-1)/2}\left\lfloor \frac{qk}{p} \right\rfloor}(-1)^{\sum_{k=1}^{(q-1)/2}\left\lfloor \frac{pk}{q} \right\rfloor} \\
&= \left(\frac{q}{p}\right)\left(\frac{p}{q}\right).
\end{aligned}$$

Remark

Notice that if $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$, then the exponent $\frac{p-1}{2} \cdot \frac{q-1}{2}$ is even.

It is odd if and only if $p \equiv q \equiv 3 \pmod{4}$.

We can therefore state the Law of Quadratic Reciprocity as

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4}, \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod{4}. \end{cases}$$

Example 1

Let's compute $\left(\frac{-1234}{4567}\right)$ using quadratic reciprocity. First of all

$$\begin{aligned}\left(\frac{-1234}{4567}\right) &= \left(\frac{-2\cdot 617}{4567}\right)\\ &= \left(\frac{-1}{4567}\right)\left(\frac{2}{4567}\right)\left(\frac{617}{4567}\right)\\ &= (-1)\cdot(1)\cdot(1)\left(\frac{4567}{617}\right),\end{aligned}$$

where we have used the facts that $4567 \equiv -1 \pmod 8$ and $617 \equiv 1 \pmod 4$ to evaluate the powers of -1.

We have already observed that $\left(\frac{a}{p}\right)$ is p-periodic in a. We can therefore reduce 4567 modulo 617.

Hence

$$
\begin{aligned}
\left(\frac{-1234}{4567}\right) &= -\left(\frac{248}{617}\right) = -\left(\frac{8\cdot 31}{617}\right)\\
&= -\left(\frac{2}{617}\right)\left(\frac{31}{617}\right) = -\left(\frac{617}{31}\right)\\
&= -\left(\frac{28}{31}\right) = -\left(\frac{4\cdot 7}{31}\right) = \left(\frac{31}{7}\right)\\
&= \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = \boxed{-1}.
\end{aligned}
$$

since $617 \equiv 1 \pmod 8$ and $31 \equiv 7 \equiv 3 \pmod 4$.

Therefore -1234 is a quadratic nonresidue of 4567.

Example 2

Determine the primes p for which 7 is a quadratic residue of p. We want

$$1 = \left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{7}\right)$$

which happens if and only if

$$(-1)^{\frac{p-1}{2}} = \left(\frac{p}{7}\right) = 1 \quad \text{or} \quad (-1)^{\frac{p-1}{2}} = \left(\frac{p}{7}\right) = -1.$$

By direct computation we find these to be equivalent to

$$\begin{array}{ccc} p \equiv 1 \pmod 4, & & p \equiv 3 \pmod 4, \\ & \text{or} & \\ p \equiv 1, 2, 4 \pmod 7; & & p \equiv 3, 5, 6 \pmod 7. \end{array}$$

The CRT yields the equivalents $\boxed{p \equiv \pm 1, \pm 3, \pm 9 \pmod{28}}$.