

Quadratic Reciprocity

We have seen earlier that the following result is true.

Theorem (EULER'S CRITERION). Let $p > 2$ be a prime, and let a be an integer not divisible by p . Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \quad \square$$

Corollary. Let $p > 2$ be a prime. Then

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

Using Euler's Criterion and the following lemma, we'll obtain a proof of Quadratic Reciprocity.

Lemma (GAUSS'S LEMMA). Let $p > 2$ be a prime, and let a be an integer not divisible by p . Put

$$\mathcal{R}_p = \{x \in \mathbb{Z} : 0 < x < p \text{ and } x \equiv at \pmod{p} \text{ for some positive integer } t \leq \frac{p-1}{2}\}.$$

If n denotes the number of elements of \mathcal{R}_p that are greater than $\frac{p}{2}$, then

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

Proof. Let u_1, u_2, \dots, u_m denote the (distinct) elements of \mathcal{R}_p that are less than $\frac{p}{2}$, and let v_1, v_2, \dots, v_n denote the (distinct) elements of \mathcal{R}_p that are greater than $\frac{p}{2}$. (So $\mathcal{R}_p = \{u_1, u_2, \dots, u_m, v_1, v_2, \dots, v_n\}$ and $m + n = \#\mathcal{R}_p = \frac{p-1}{2}$.) Multiplying the elements of \mathcal{R}_p together, we find

$$\prod_{i=1}^m u_i \prod_{j=1}^n v_j = \prod_{x \in \mathcal{R}_p} x \equiv \prod_{t=1}^{\frac{p-1}{2}} at \equiv a^{\frac{p-1}{2}} \prod_{t=1}^{\frac{p-1}{2}} t \equiv a^{\frac{p-1}{2}} \left[\frac{p-1}{2}\right]! \pmod{p}.$$

Now consider the following list of integers:

$$\mathcal{L}_p = u_1, u_2, \dots, u_m, p - v_1, p - v_2, \dots, p - v_n.$$

Each integer in the list is positive and less than $\frac{p}{2}$. If these integers are distinct, then they are precisely the integers $1, 2, \dots, \frac{p-1}{2}$ in some order. In order to show that they are distinct, it suffices to show that we cannot have $u_i = p - v_j$ for any choice of i and j . Suppose we do have $u_i = p - v_j$. Since u_i and v_j are elements of \mathcal{R}_p , (and clearly $u_i \neq v_j$), we know there are positive integers $t_i \neq t_j$, with each less than $\frac{p}{2}$, such that $u_i \equiv at_i \pmod{p}$ and $v_j \equiv at_j \pmod{p}$. But then

$$at_i \equiv u_i = p - v_j \equiv p - at_j \equiv -at_j \pmod{p},$$

which implies (since a has a multiplicative inverse modulo p)

$$t_i \equiv -t_j \pmod{p}.$$

Since, t_i and t_j are positive and less than $\frac{p}{2}$, this is impossible. We have shown that the integers in the list \mathcal{L}_p are distinct, and hence \mathcal{L}_p is some permutation of the list $1, 2, \dots, \frac{p-1}{2}$. From this we conclude that

$$\prod_{i=1}^m u_i \prod_{j=1}^n (p - v_j) = \prod_{x \in \mathcal{L}_p} x = \left[\frac{p-1}{2} \right]!$$

Combining this with our previous conclusion about the product of the elements of \mathcal{R}_p , we obtain

$$\left[\frac{p-1}{2} \right]! \equiv \prod_{i=1}^m u_i \prod_{j=1}^n (p - v_j) \equiv \prod_{i=1}^m u_i \prod_{j=1}^n (-v_j) \equiv (-1)^n \prod_{i=1}^m u_i \prod_{j=1}^n v_j \equiv (-1)^n a^{\frac{p-1}{2}} \left[\frac{p-1}{2} \right]! \pmod{p}.$$

Noting that $\left[\frac{p-1}{2} \right]!$ is relatively prime to p , we may use its multiplicative inverse modulo p to conclude $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$. The lemma now follows from Euler's Criterion. \square

Corollary. Let $p \neq q$ be odd primes and let a be an integer relatively prime to each of p and q . If either $p - q$ or $p + q$ is divisible by $4a$, then $\left(\frac{a}{q} \right) = \left(\frac{a}{p} \right)$.

Proof. From Gauss's Lemma, we have

$$\left(\frac{a}{p} \right) = (-1)^{n_p} \quad \text{and} \quad \left(\frac{a}{q} \right) = (-1)^{n_q},$$

where n_p is the number of elements of \mathcal{R}_p that are greater than $\frac{p}{2}$ and n_q is the number of elements of \mathcal{R}_q that are greater than $\frac{q}{2}$. To obtain the desired conclusion, it will suffice to show that n_p and n_q have the same parity.

To find n_p , recall that the elements of \mathcal{R}_p are the remainders modulo p of certain multiples of a . Note that if at is such a multiple of a , then at has a remainder modulo p that is greater than $\frac{p}{2}$ if and only if it satisfies $\frac{(2k-1)p}{2} < at < kp$ for some positive integer $k \leq \lfloor \frac{p}{2a} \rfloor$. Hence, the remainder of at modulo p is greater than $\frac{p}{2}$ if and only if $\frac{(2k-1)p}{2a} < t < \frac{kp}{a}$ for some positive integer $k \leq \lfloor \frac{p}{2a} \rfloor$. Therefore, n_p is the cardinality

$$n_p = \# \left(\bigcup_{k=1}^{\lfloor \frac{p}{2a} \rfloor} \left\{ t \in \mathbb{Z} : \frac{(2k-1)p}{2a} < t < \frac{kp}{a} \right\} \right) = \sum_{k=1}^{\lfloor \frac{p}{2a} \rfloor} \# \left\{ t \in \mathbb{Z} : \frac{(2k-1)p}{2a} < t < \frac{kp}{a} \right\}.$$

Similarly, for n_q we have

$$n_q = \sum_{k=1}^{\lfloor \frac{q}{2a} \rfloor} \# \left\{ t \in \mathbb{Z} : \frac{(2k-1)q}{2a} < t < \frac{kq}{a} \right\}.$$

Now suppose $4a$ divides $p - q$; so $q = p + 4ay$ for some integer y . Then

$$\begin{aligned} n_q &= \sum_{k=1}^{\lfloor \frac{q}{2a} \rfloor} \# \left\{ t \in \mathbb{Z} : \frac{(2k-1)(p+4ay)}{2a} < t < \frac{k(p+4ay)}{a} \right\} \\ &= \sum_{k=1}^{\lfloor \frac{q}{2a} \rfloor} \# \left\{ t \in \mathbb{Z} : \frac{(2k-1)p}{2a} + 2(2k-1)y < t < \frac{kp}{a} + 4ky \right\}. \end{aligned}$$

For a fixed value of k , the cardinality of the set $\left\{ t \in \mathbb{Z} : \frac{(2k-1)p}{2a} + 2(2k-1)y < t < \frac{kp}{a} + 4ky \right\}$ differs from the cardinality of the set $\left\{ t \in \mathbb{Z} : \frac{(2k-1)p}{2a} < t < \frac{kp}{a} \right\}$ by an even integer, (this is because the respective endpoints differ by even integers). Hence n_q and n_p differ by an even integer.

The proof for the case when $4a$ divides $p + q$ is similar. \square

Now we are ready to prove the main result.

Theorem (THE LAW OF QUADRATIC RECIPROCITY). Let $p \neq q$ be odd primes. Then

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

Proof. Since p and q are both odd, there are two cases: either $q \equiv p \pmod{4}$ or $q \equiv -p \pmod{4}$.

Case 1. Suppose $q \equiv p \pmod{4}$. There is some integer c such that $q = p + 4c$. Note that c must be relatively prime to each of p and q , since otherwise the equation $q = p + 4c$ would force p and q to have a non-trivial GCD. Thus

$$\left(\frac{q}{p}\right) = \left(\frac{p+4c}{p}\right) = \left(\frac{4c}{p}\right) = \left(\frac{c}{p}\right),$$

and similarly

$$\left(\frac{p}{q}\right) = \left(\frac{q-4c}{q}\right) = \left(\frac{-4c}{q}\right) = \left(\frac{-c}{q}\right) = \left(\frac{-1}{q}\right) \left(\frac{c}{q}\right).$$

From the above computations and the corollary to Euler's Criterion, we obtain

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

The corollary to Gauss's Lemma gives $\left(\frac{c}{q}\right) \left(\frac{c}{p}\right) = 1$, whence

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

Case 2. Suppose $q \equiv -p \pmod{4}$. There is some integer d such that $q = -p + 4d$. Note that d must be relatively prime to each of p and q . Thus

$$\left(\frac{q}{p}\right) = \left(\frac{-p+4d}{p}\right) = \left(\frac{4d}{p}\right) = \left(\frac{d}{p}\right),$$

and similarly

$$\left(\frac{p}{q}\right) = \left(\frac{-q+4d}{q}\right) = \left(\frac{4d}{q}\right) = \left(\frac{d}{q}\right).$$

From the above computations, we obtain

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = \left(\frac{d}{q}\right) \left(\frac{d}{p}\right).$$

The corollary to Gauss's Lemma gives $\left(\frac{d}{q}\right) \left(\frac{d}{p}\right) = 1$, whence

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

(The last equality is true since one of p or q is congruent to 1 modulo 4, so that either $\frac{p-1}{2}$ or $\frac{q-1}{2}$ is even.) \square