

Quadratic Reciprocity by Group Theory

Tim Kunisky[†]

Livingston High School '10

Livingston, NJ 07039

tkunisky@gmail.com

For p a prime, consider $(\mathbb{Z}/p\mathbb{Z})^\times$, the multiplicative group of the nonzero integers modulo p . We know that exactly half of the elements are squares, and want to find them. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 1 if a is a square in $(\mathbb{Z}/p\mathbb{Z})^\times$, -1 otherwise. Besides simply squaring the integers from 1 to $p-1$ to see if $\left(\frac{a}{p}\right) = 1$, we can also use Euler's Criterion, which states that $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$. However, the most elegant way uses the law of quadratic reciprocity, first proven by Gauss. It states that if p and q are odd primes then

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

We will prove this result using elementary group theory. Consider the group $G = (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ for p, q odd primes. Note that $A = \{(1, 1), (-1, -1)\}$ is a normal subgroup of G , and let $H = G/A$ be the quotient group. We will find two equivalent expressions for the product of all elements of H by considering coset representatives for A .

Any $(a, b) \in G$ can be written uniquely as $(a, \pm b')$ where $1 \leq a \leq p-1$ and $1 \leq b' \leq \frac{q-1}{2}$. Since negating a does not change the possibilities for the first coordinate, $S = \{(x, y) \mid 1 \leq x \leq p-1, 1 \leq y \leq \frac{q-1}{2}\}$ is a set of coset representatives for A . Taking the product of all elements of this set gives

$$\left((p-1)!^{\frac{q-1}{2}}, \left(\frac{q-1}{2}\right)!^{p-1}\right)$$

but we know that in $\mathbb{Z}/q\mathbb{Z}$

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

and therefore

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

So the product can be rewritten as

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

[†]Currently, Tim is in his junior year at Livingston High School in Livingston, New Jersey. Largely influenced by his time at PROMYS, his mathematical interests have been oriented towards number theory along with algebra, though he has made attempts at studying analysis independently more recently as well. His first experience with extracurricular study was a deeper exploration of calculus, but his interests have shifted significantly to more foundational branches, including abstract algebra and set theory. Tim is fascinated with elegant proofs of simple or well-known theorems—a passion that resulted in the creation of this proof. In the next few years, he hopes to narrow his interests and pursue mathematics in college and beyond.

Next, we apply the Chinese Remainder Theorem to find another set of coset representatives, namely the set

$$T = \{(k \bmod p, k \bmod q) \mid k = 1, 2, \dots, \frac{pq-1}{2}; (k, pq) = 1\}.$$

Clearly under multiplication by $(-1, -1)$ the elements of $\mathbb{Z}/pq\mathbb{Z}$ over $\frac{pq-1}{2}$ are included, and generate all elements of G that are not in T . Therefore, this is a second set of coset representatives.

Denote the product of these ordered pairs by (r, s) . Then, r is the product of all k taken modulo p , and s is the same product but modulo q . Since we require $(k, pq) = 1$, to calculate r we may exclude all multiples of p , then divide out all multiples of q :

$$r = \frac{\left(\prod_{i=1}^{p-1} i\right) \left(\prod_{i=1}^{p-1} p+i\right) \cdots \left(\prod_{i=1}^{p-1} \left(\frac{q-1}{2} - 1\right) p+i\right) \left(\prod_{i=1}^{\frac{p-1}{2}} \frac{q-1}{2} p+i\right)}{(1 \cdot q)(2 \cdot q) \cdots \left(\frac{p-1}{2} \cdot q\right)}$$

By manipulating the terms and applying Euler's Criterion, we find:

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

We also have a symmetric expression for s :

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

So by equating this with the product from the previous calculation we find:

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

Therefore,

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

Since we have been working in G/A , this is only accurate up to sign. But if we multiply the components of the ordered pairs together having both negative will make no difference, so we have the desired equation:

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