QUADRATIC RECIPROCITY

LEO GOLDMAKHER

Quadratic Reciprocity is arguably the most important theorem taught in an elementary number theory course. Since Gauss' original 1796 proof (by induction!) appeared, more than 100 different proofs have been discovered. Here I present one proof which is not particularly well-known, due to George Rousseau [2]. (The proof was rediscovered more recently by (then) high-schooler Tim Kunisky [1].) Although not the shortest proof, it is the easiest to remember of all the elementary proofs I have encountered. In particular, it does not rely on Gauss' Lemma, or lattice counting, or Gauss sums; the only ingredients used in the proof are the Chinese Remainder Theorem, Wilson's Theorem, and Euler's Criterion. After proving Quadratic Reciprocity for the case of two odd primes, I'll show how to derive the 'supplementary' laws directly from the classical case.

1. Quadratic Reciprocity for odd primes

Let p and q be distinct odd primes. The Chinese Remainder Theorem asserts that the map

$$\sigma : (\mathbb{Z}/pq\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$$

defined by $\sigma(k) := (k, k)$ is a bijection. It follows that if we took half of $(\mathbb{Z}/pq\mathbb{Z})^\times$, it would get mapped to half of $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. For example, set

$$L := \left\{k \in (\mathbb{Z}/pq\mathbb{Z})^\times : 1 \le k < \frac{pq}{2}\right\} \quad \text{and} \quad R := \left\{(a,b) \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times : 1 \le b < \frac{q}{2}\right\}.$$

A bit of thought shows that for each $(a, b) \in R$, there exists a unique $k \in L$ such that $\sigma(k) = \pm(a, b)$. Thus we have

$$\prod_{(a,b)\in R} (a,b) = \epsilon \prod_{k\in L} (k,k), \tag{1}$$

where $\epsilon = \pm 1$ and the products are taken in the group $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$.

Both sides of (1) simplify quite nicely. For brevity, set $P := \frac{p-1}{2}$ and $Q := \frac{q-1}{2}$. We have:

$$\begin{aligned}\prod_{(a,b)\in R} (a,b) = \prod_{\substack{a<p\\ b<q/2}} (a,b) &= \Big((p-1)!^Q, Q!^{2P}\Big) \\ &= \Big((-1)^Q, \big((q-1)!(-1)^Q\big)^P\Big) \\ &= \Big((-1)^Q, (-1)^P(-1)^{PQ}\Big).\end{aligned}$$

The right hand side of (1) is slightly more involved, and we compute the two coordinates separately. First, observe that in $(\mathbb{Z}/p\mathbb{Z})^\times$ we have

$$\begin{aligned}\prod_{k\in L} k = \prod_{\substack{k<pq/2\\(k,pq)=1}} k &= \left(\prod_{\substack{k<pq/2\\p|k}} k\right)\cdot\left(\prod_{\substack{k<pq/2\\q|k}} k\right)^{-1}\\ &= \left(\prod_{0<k<p} k\right)\left(\prod_{p<k<2p} k\right)\cdots\left(\prod_{(Q-1)p<k<Qp} k\right)\left(\prod_{Qp<k<pq/2} k\right)\cdot\left(\prod_{\substack{k<pq/2\\q|k}} k\right)^{-1}\\ &= \frac{(p-1)!^Q\cdot P!}{(q)(2q)(3q)\cdots(Pq)}\\ &= \frac{(-1)^Q}{q^P}\\ &= (-1)^Q\left(\frac{q}{p}\right).\end{aligned}$$

By symmetry, in $(\mathbb{Z}/q\mathbb{Z})^\times$ we have

$$\prod_{k\in L} k = (-1)^P\left(\frac{p}{q}\right).$$

Thus, equation (1) becomes

$$\left((-1)^Q, (-1)^P(-1)^{PQ}\right) = \epsilon\cdot\left((-1)^Q\left(\frac{q}{p}\right), (-1)^P\left(\frac{p}{q}\right)\right)$$

or in other words,

$$\left(\frac{q}{p}\right)\cdot\epsilon \equiv 1 \pmod p \qquad \text{and} \qquad \left(\frac{p}{q}\right)\cdot\epsilon \equiv (-1)^{PQ} \pmod q.$$

The former congruence implies that $\epsilon = \left(\frac{q}{p}\right)$; plugging this into the latter congruence yields the Quadratic Reciprocity law.

2. Extensions of Quadratic Reciprocity

Quadratic Reciprocity allows us to calculate Legendre symbols like $\left(\frac{3}{47}\right)$. But what about $\left(\frac{10}{47}\right)$? In this section, we'll prove two results which will allow us to evaluate such symbols as well. The first is a multiplicative property of the Legendre symbol:

Proposition 1. *For any two integers a, b and any odd prime p,*

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

Proof. This is an immediate consequence of Euler's Criterion. □

Thus, $\left(\frac{10}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{5}{47}\right)$. The second factor can now be evaluated by Quadratic Reciprocity, so the only remaining question is a formula for $\left(\frac{2}{p}\right)$. We will prove:

Theorem 2. *Given any odd prime p, we have*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

Our approach to this theorem relies on the observation that $\left(\frac{2}{p}\right) = \left(\frac{2-p}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p-2}{p}\right)$. The advantage here is that $p-2$ is odd, so we can now apply multiplicativity to split $p-2$ into its prime factors and then apply quadratic reciprocity.[1] For example, $\left(\frac{2}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{9}{11}\right) = -1 \cdot 1 = -1$. This gives an algorithmic solution to the problem of determining $\left(\frac{2}{p}\right)$, but doesn't yield the clean formula of Theorem 2. Try applying this algorithm to evaluate $\left(\frac{2}{19}\right)$ to get a better feel for it.

To prove Theorem 2, we introduce a generalization of the Legendre symbol which is interesting in its own right: the *Jacobi symbol* $\left(\frac{a}{n}\right)$, which is defined for any odd integer $n \geq 3$ and any $a \in \mathbb{Z}$.[2] The symbol $\left(\frac{a}{n}\right)$ is already defined if n is an odd prime. If $n \geq 3$ is composite, then n can be written as a product of primes, say $n = p_1 p_2 \cdots p_k$ (the p_i are not necessarily distinct). Then we define

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right).$$

The following properties of the Jacobi symbol are straightforward consequences of the corresponding properties of the Legendre symbol:

Theorem 3. *Given $m \geq 3$ odd. Then*

(1) *For any $a, b \in \mathbb{Z}$, we have* $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$.
(2) $\left(\frac{a}{m}\right)\left(\frac{m}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{m-1}{2}}$ *for any odd integer $a \geq 3$.*
(3) *If $a, b \in \mathbb{Z}$ and $a \equiv b \pmod m$, then* $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.
(4) *We have* $\left(\frac{-1}{m}\right) = \begin{cases} 1 & \text{if } m \equiv 1 \pmod 4 \\ -1 & \text{if } m \equiv -1 \pmod 4 \end{cases}$

Using these properties, we can now evaluate $\left(\frac{2}{n}\right)$ with relative ease for any odd $n \geq 3$. In this context, our first observation from above reads:

$$\left(\frac{2}{n}\right) = \left(\frac{2-n}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{n-2}{n}\right) \tag{2}$$

Now observe that for any odd $k \geq 3$, we have

$$\left(\frac{k-2}{k}\right) = \left(\frac{k}{k-2}\right) = \left(\frac{k-2(k-2)}{k-2}\right) = \left(\frac{-1}{k-2}\right)\left(\frac{k-4}{k-2}\right).$$

---

[1] The first factor, $\left(\frac{-1}{p}\right)$, is easily evaluated by Euler's Criterion: $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv -1 \pmod 4 \end{cases}$

[2] This can be extended fairly easily to *all* odd integers n, and (with a bit more work) to arbitrary integers n; the latter extension is called the Kronecker symbol.

Applying this relation to (2) and iterating yields

$$\begin{aligned}\left(\frac{2}{n}\right) &= \left(\frac{-1}{n}\right)\left(\frac{n-2}{n}\right)\\ &= \left(\frac{-1}{n}\right)\left(\frac{-1}{n-2}\right)\left(\frac{n-4}{n-2}\right)\\ &= \cdots\\ &= \left(\frac{-1}{n}\right)\left(\frac{-1}{n-2}\right)\cdots\left(\frac{-1}{3}\right)\left(\frac{1}{3}\right).\end{aligned}$$

Now $\left(\frac{1}{3}\right)$ is simply 1, and from Theorem 3 we see that $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$ for any odd $m \geq 3$. Thus,

$$\left(\frac{2}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{-1}{n-2}\right)\cdots\left(\frac{-1}{3}\right) = (-1)^{\frac{n-1}{2}+\frac{n-3}{2}+\cdots+\frac{3-1}{2}} = (-1)^{1+2+\cdots+\frac{n-1}{2}} = (-1)^{\frac{n^2-1}{8}}.$$

It follows immediately that

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod 8 \\ -1 & \text{if } n \equiv \pm 3 \pmod 8 \end{cases}$$

which concludes the proof of Theorem 2. QED

Acknowledgements. I learned about Rousseau's argument thanks to a post by Noah Snyder on mathoverflow [3]. I am also grateful to John Friedlander, Wei Ho, Youness Lamzouri, and Carl Pomerance for helpful discussions.

REFERENCES

[1] T. Kunisky, *Quadratic Reciprocity by Group Theory*, Harvard College Math. Review, Vol. 2, no. 2 (2008), 75–76.
[2] G. Rousseau, *On the Quadratic Reciprocity Law*, J. Austral. Math. Soc. Ser. A **51** (1991), no. 3, 423–425.
[3] http://mathoverflow.net/questions/1420/whats-the-best-proof-of-quadratic-reciprocity

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO
40 ST. GEORGE STREET, ROOM 6290
TORONTO, M5S 2E4, CANADA

E-mail address: lgoldmak@math.toronto.edu