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 [1]. (The proof was rediscovered more recently by high-schooler Tim Kunisky.) 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. I'll recall these, and the statement of Quadratic Reciprocity, in the first section. In the second section, I'll explain Rousseau's proof. In the third and final section, I discuss the Jacobi symbol and the supplement to Quadratic Reciprocity.

1. PRELIMINARIES

Recall that $\mathbb{Z}_n^\times$ is defined to be the set of all integers between 1 and n which are relatively prime to n. Actually, an element $k \in \mathbb{Z}_n^\times$ doesn't merely refer to the number k, but to the arithmetic progression $k + n\mathbb{Z}$. It will be convenient to refer to elements of $\mathbb{Z}_n^\times$ using the name of one of the terms in the corresponding arithmetic progression. For example, strictly speaking 9 isn't an element of $\mathbb{Z}_5^\times$, but we will allow the symbol 9 as an alternative name for the element $4 \in \mathbb{Z}_5^\times$.

Recall that the *Legendre symbol*, denoted $\left(\frac{a}{p}\right)$, measures whether or not a is a square $\pmod p$. More precisely, it is defined as follows: for any integer a and any odd prime p,

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } a \equiv 0 \pmod p \\ 1 & \text{if } \exists x \in \mathbb{Z}_p^\times \text{ such that } x^2 \equiv a \pmod p \\ -1 & \text{otherwise.} \end{cases}$$

Thus, $\left(\frac{1}{3}\right)$ is 1 and $\left(\frac{2}{3}\right)$ is -1. If $\left(\frac{a}{p}\right)$ is 1 (i.e. a is a square $\pmod p$), we say a is a *quadratic residue* modulo p. If $\left(\frac{a}{p}\right)$ is -1, we say a is a quadratic non-residue.

The following result, an easy consequence of the existence of a primitive root modulo p, is a very useful tool in studying the Legendre symbol.

Theorem (Euler's Criterion)**.** *Given any odd prime p and any $a \in \mathbb{Z}$, we have*

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

Thus, for example,

$$\left(\frac{-1}{7}\right) \equiv (-1)^3 \pmod 7,$$

whence -1 is not a square $\pmod 7$. This example generalizes quite nicely:

Corollary. *Given an odd prime p, we have*

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

Are there similar general formulas for $\left(\frac{a}{p}\right)$ for other choices of a? Some experimentation will convince the reader that the answer is yes; however, it's not at all obvious how to write down a master formula for the general a and p. The Law of Quadratic Reciprocity solves this problem in the case that a is an odd prime:

Theorem (Quadratic Reciprocity)**.** *Given distinct odd primes p and q. Then*

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

For example, this allows us to figure out a formula for $\left(\frac{3}{p}\right)$: by QR, we have

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right).$$

Since $\left(\frac{p}{3}\right)$ is completely determined by the reduction of $p \pmod 3$, and $(-1)^{\frac{p-1}{2}}$ is determined by the reduction of $p \pmod 4$, we deduce the following formula:

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

We can use QR to obtain similar formulas for $\left(\frac{5}{p}\right)$, or $\left(\frac{7}{p}\right)$, or more generally for $\left(\frac{q}{p}\right)$ for any odd prime q. But what about for other choices of top entry? Is there a formula for $\left(\frac{2}{p}\right)$, or for $\left(\frac{15}{p}\right)$? As we shall see (in the third section), just by playing around with QR a bit one can derive formulas for all of these, and more generally, for $\left(\frac{a}{p}\right)$ for any fixed integer a.

Our proof of QR relies crucially on the following result:

Theorem (Chinese Remainder Theorem)**.** *Given positive relatively prime integers m, n. The following map is a bijection:*

$$\begin{aligned} \sigma : \mathbb{Z}_{mn}^{\times} &\longrightarrow \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times} \\ k &\longmapsto (k, k) \end{aligned}$$

In other words, for all $(a, b) \in \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$ there exists a unique $k \in \mathbb{Z}_{mn}^{\times}$ such that $\sigma(k) = (a, b)$.

I strongly encourage the reader to compute $\sigma(k)$ for all $k \in \mathbb{Z}_{15}^{\times}$, with $m = 3$ and $n = 5$, to get a sense of how this works. For example, with these choices of m and n, we have $\sigma(7) = (1, 2)$.

We are now in a position to prove Quadratic Reciprocity, which we do in the next section. In the third and final section, we discuss extensions of QR.

2. Proof

Consider the sets

$$A := \left\{(a,b) \in \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times : 1 \le b < \frac{q}{2}\right\} \qquad \text{and} \qquad K := \left\{k \in \mathbb{Z}_{pq}^\times : 1 \le k < \frac{pq}{2}\right\}.$$

A is half of $\mathbb{Z}_p^\times \times \mathbb{Z}_q^\times$, while K is half of $\mathbb{Z}_{pq}^\times$. Our first move is to adapt the Chinese Remainder Theorem to compare these two sets.

Lemma 1. *For each $(a,b) \in A$, there exists a unique $k \in K$ such that $\sigma(k) = \pm(a,b)$.*

I strongly encourage the reader to experiment with the case $p = 3, q = 5$ to get a feel for this result.

Lemma 1 implies that

$$\prod_{(a,b)\in A} (a,b) = \prod_{k\in K} \pm\sigma(k) = \pm \prod_{k\in K} (k,k).$$

In other words, there exists $\epsilon = \pm 1$ such that the following congruences simultaneously hold:

$$\prod_{a\in\mathbb{Z}_p^\times} \prod_{b<q/2} a \equiv \epsilon \prod_{\substack{k<pq/2 \\ (k,pq)=1}} k \pmod p \tag{1}$$

and

$$\prod_{a\in\mathbb{Z}_p^\times} \prod_{b<q/2} b \equiv \epsilon \prod_{\substack{k<pq/2 \\ (k,pq)=1}} k \pmod q. \tag{2}$$

Evaluating these products isn't too difficult, as we shall see (after finishing the proof of QR). We will show:

Lemma 2. *Let $P := \frac{p-1}{2}$ and $Q := \frac{q-1}{2}$. Then*

$$\prod_{a\in\mathbb{Z}_p^\times} \prod_{b<q/2} a \equiv (-1)^Q \pmod p \qquad \prod_{\substack{k<pq/2 \\ (k,pq)=1}} k \equiv \frac{(-1)^Q}{q^P} \pmod p$$

$$\prod_{a\in\mathbb{Z}_p^\times} \prod_{b<q/2} b \equiv (-1)^P(-1)^{PQ} \pmod q \qquad \prod_{\substack{k<pq/2 \\ (k,pq)=1}} k \equiv \frac{(-1)^P}{p^Q} \pmod q$$

By Euler's Criterion,

$$q^P \equiv \left(\frac{q}{p}\right) \pmod p \qquad \text{and} \qquad p^Q \equiv \left(\frac{p}{q}\right) \pmod q.$$

Plugging this into Lemma 2 and equation (1) shows that $\epsilon = \left(\frac{q}{p}\right)$. Substituting this into congruence (2) and applying Lemma 2 yields

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

Multiplying both sides by $\left(\frac{p}{q}\right)$ concludes the proof. QED

The above is an overview of the proof of Quadratic Reciprocity. To complete the proof, it suffices to prove the two lemmas. I leave the first lemma as an exercise to the reader. The second lemma consists of four congruences, which we prove now.

Let's start with the easiest of the four. We have

$$\prod_{a\in\mathbb{Z}_p^\times}\prod_{b<q/2} a = \prod_{a\in\mathbb{Z}_p^\times} a^Q = (p-1)!^Q.$$

By Wilson's theorem, $(p-1)! \equiv -1 \pmod p$, whence

$$\prod_{a\in\mathbb{Z}_p^\times}\prod_{b<q/2} a \equiv (-1)^Q \pmod p$$

as claimed.

Next, we have

$$\begin{aligned}\prod_{a\in\mathbb{Z}_p^\times}\prod_{b<q/2} b = (Q!)^{p-1} = (Q!^2)^P &= \Big(Q!\cdot(-1)(-2)\cdots(-Q)\cdot(-1)^Q\Big)^P \\ &\equiv \Big((q-1)!(-1)^Q\Big)^P \pmod q \\ &\equiv (-1)^P(-1)^{PQ} \pmod q.\end{aligned}$$

Finally, we will compute

$$\prod_{\substack{k<pq/2\\(k,pq)=1}} k \pmod p. \tag{3}$$

We're multiplying together all the integers between 1 and $pq/2$ which are not multiples of p or q. To gain some intuition, we start by writing down a table of *all* integers between 1 and $pq/2$:

$$\begin{array}{ccccccc} 1 & 2 & 3 & & & \cdots & p \\ p+1 & p+2 & p+3 & & & \cdots & 2p \\ 2p+1 & 2p+2 & 2p+3 & & & \cdots & 3p \\ \vdots & \vdots & \vdots & & & & \vdots \\ (Q-1)p+1 & (Q-1)p+2 & (Q-1)p+3 & & & \cdots & Qp \\ Qp+1 & Qp+2 & Qp+3 & \cdots & \frac{pq-1}{2} & & \end{array}$$

This is a $(Q\times p)$ table, plus an incomplete $(Q+1)$st row. (Prove this!) To compute the product (3) we need to remove all multiples of p and q from the table, and multiply the rest of the elements together. The multiples of p are easy to remove. Once that's done, here's how we proceed:

- each complete row contributes $(p-1)! \pmod p$ to the product, and there are Q complete rows;
- the incomplete row contributes $P! \pmod p$ to the product (why?); and
- there are precisely P multiples of q in the table, namely $q, 2q, 3q, \ldots, Pq$. (Prove this!)

Thus, we find

$$\prod_{\substack{k\le pq/2\\(k,pq)=1}} k \equiv \frac{(p-1)!^Q\cdot P!}{(q)(2q)(3q)\cdots(Pq)} \pmod p$$
$$\equiv \frac{(-1)^Q\cdot P!}{P!\cdot q^P} \pmod p$$
$$\equiv \frac{(-1)^Q}{q^P} \pmod p.$$

The fourth congruence, which is the evaluation of the same product as above but modulo q, follows from the above computation by switching the roles of p and q.

3. Extensions

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 3. *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 4. *Given any odd prime p, we have*

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

To fully appreciate this result (as well as Quadratic Reciprocity itself), I urge the reader to put away this document and spend the next hour (or more!) trying to prove Theorem 4.

There are many ways to prove the theorem. Our approach 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 of this rewriting 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. 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 give the clean formula of Theorem 4. Try applying this algorithm to evaluate $\left(\frac{2}{19}\right)$ to get a better feel for it.

To prove Theorem 4, 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 $a \in \mathbb{Z}$.[1] 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

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

For example,

$$\left(\frac{-1}{45}\right) = \left(\frac{-1}{3\cdot 3\cdot 5}\right) = \left(\frac{-1}{3}\right)\left(\frac{-1}{3}\right)\left(\frac{-1}{5}\right) = 1.$$

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

Theorem 5. *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:

$$\left(\frac{2}{n}\right) = \left(\frac{2-n}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{n-2}{n}\right) \tag{4}$$

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

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

Applying this relation to (4) 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 5 we see that $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$ for any odd $m \geq 3$. Thus,

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

[1] 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.

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 4. QED

Acknowledgements. I learned about Rousseau's argument thanks to a post by Noah Snyder on mathoverflow [2]. I am also grateful to John Friedlander, Wei Ho, Youness Lamzouri, and Carl Pomerance for helpful discussions.

REFERENCES

[1] G. Rousseau, *On the Quadratic Reciprocity Law*, J. Austral. Math. Soc. Ser. A **51** (1991), no. 3, 423–425.
[2] 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