The law of quadratic reciprocity

Chapter 5

Carl Friedrich Gauss

Which famous mathematical theorem has been proved most often? Pythagoras would certainly be a good candidate or the fundamental theorem of algebra, but the champion is without doubt the law of quadratic reciprocity in number theory. In an admirable monograph Franz Lemmermeyer lists as of the year 2000 no fewer than 196 proofs. Many of them are of course only slight variations of others, but the array of different ideas is still impressive, as is the list of contributors. Carl Friedrich Gauss gave the first complete proof in 1801 and followed up with seven more. A little later Ferdinand Gotthold Eisenstein added five more — and the ongoing list of provers reads like a Who is Who of mathematics.

With so many proofs present the question which of them belongs in the Book can have no easy answer. Is it the shortest, the most unexpected, or should one look for the proof that had the greatest potential for generalizations to other and deeper reciprocity laws? We have chosen two proofs (based on Gauss' third and sixth proofs), of which the first may be the simplest and most pleasing, while the other is the starting point for fundamental results in more general structures.

As in the previous chapter we work "modulo p", where p is an odd prime; $\mathbb{Z}_p$ is the field of residues upon division by p, and we usually (but not always) take these residues as $0, 1, \ldots, p-1$. Consider some $a \not\equiv 0 \pmod p$, that is, $p \nmid a$. We call a a *quadratic residue* modulo p if $a \equiv b^2 \pmod p$ for some b, and a *quadratic nonresidue* otherwise. The quadratic residues are therefore $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$, and so there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic nonresidues. Indeed, if $i^2 \equiv j^2 \pmod p$ with $1 \le i, j \le \frac{p-1}{2}$, then $p \mid i^2 - j^2 = (i-j)(i+j)$. As $2 \le i+j \le p-1$ we have $p \mid i-j$, that is, $i \equiv j \pmod p$.

For $p = 13$, the quadratic residues are $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9$, $4^2 \equiv 3$, $5^2 \equiv 12$, and $6^2 \equiv 10$; the nonresidues are $2, 5, 6, 7, 8, 11$.

At this point it is convenient to introduce the so-called *Legendre symbol*. Let $a \not\equiv 0 \pmod p$, then

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue,} \\ -1 & \text{if } a \text{ is a quadratic nonresidue.} \end{cases}$$

The story begins with Fermat's "little theorem": For $a \not\equiv 0 \pmod p$,

$$a^{p-1} \equiv 1 \pmod p. \tag{1}$$

In fact, since $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ is a group with multiplication, the set $\{1a, 2a, 3a, \ldots, (p-1)a\}$ runs again through all nonzero residues,

$$(1a)(2a)\cdots((p-1)a) \equiv 1 \cdot 2 \cdots (p-1) \pmod p,$$

and hence by dividing by $(p-1)!$, we get $a^{p-1} \equiv 1 \pmod p$.

Alternatively, this is just $a^{|G|} = 1$ for the group $G = \mathbb{Z}_p^*$ (see the box on Lagrange's theorem, p. 4).

M. Aigner, G. M. Ziegler, *Proofs from THE BOOK*, https://doi.org/10.1007/978-3-662-57265-8_5

In other words, the *polynomial* $x^{p-1} - 1 \in \mathbb{Z}_p[x]$ has as roots all nonzero residues. Next we note that

$$x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1).$$

Suppose $a \equiv b^2 \pmod p$ is a quadratic residue. Then by Fermat's little theorem $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod p$. Hence the quadratic residues are precisely the roots of the first factor $x^{\frac{p-1}{2}} - 1$, and the $\frac{p-1}{2}$ nonresidues must thus be the roots of the second factor $x^{\frac{p-1}{2}} + 1$. Comparing this to the definition of the Legendre symbol, we obtain the following important tool.

For example, for $p = 17$ and $a = 3$ we have $3^8 = (3^4)^2 = 81^2 \equiv (-4)^2 \equiv -1 \pmod{17}$, while for $a = 2$ we get $2^8 = (2^4)^2 \equiv (-1)^2 \equiv 1 \pmod{17}$. Hence 2 is a quadratic residue, while 3 is a nonresidue.

Euler's criterion. *For $a \not\equiv 0 \pmod p$,*

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

This gives us at once the important *product rule*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right), \tag{2}$$

since this obviously holds for the right-hand side of Euler's criterion. The product rule is extremely helpful when one tries to compute Legendre symbols: Since any integer is a product of ± 1 and primes we only have to compute $(\frac{-1}{p})$, $(\frac{2}{p})$, and $(\frac{q}{p})$ for odd primes q.

By Euler's criterion $(\frac{-1}{p}) = 1$ if $p \equiv 1 \pmod 4$, and $(\frac{-1}{p}) = -1$ if $p \equiv 3 \pmod 4$, something we have already seen in the previous chapter. The case $(\frac{2}{p})$ will follow from the Lemma of Gauss below: $(\frac{2}{p}) = 1$ if $p \equiv \pm 1 \pmod 8$, while $(\frac{2}{p}) = -1$ if $p \equiv \pm 3 \pmod 8$.

Euler, Legendre, and Gauss did lots of calculations with quadratic residues and, in particular, studied the relations between q being a quadratic residue modulo p and p being a quadratic residue modulo q, when p and q are odd primes. Euler and Legendre thus discovered the following remarkable theorem, but they managed to prove it only in special cases. However, Gauss was successful: On April 8, 1796 he was proud to record in his diary the first full proof.

Law of quadratic reciprocity. *Let p and q be different odd primes. Then*

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

If $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then $\frac{p-1}{2}$ (resp. $\frac{q-1}{2}$) is even, and therefore $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$; thus $(\frac{q}{p}) = (\frac{p}{q})$. When $p \equiv q \equiv 3 \pmod 4$, we have $(\frac{p}{q}) = -(\frac{q}{p})$. Thus for odd primes we get $(\frac{p}{q}) = (\frac{q}{p})$ unless *both* p and q are congruent to $3 \pmod 4$.

Example: $(\frac{3}{17}) = (\frac{17}{3}) = (\frac{2}{3}) = -1$, so 3 is a nonresidue mod 17.

First proof. The key to our first proof (which is Gauss' third) is a counting formula that soon came to be called the *Lemma of Gauss*:

> **Lemma of Gauss.** *Suppose* $a \not\equiv 0 \pmod p$. *Take the numbers* $1a, 2a, \ldots, \frac{p-1}{2}a$ *and reduce them modulo* p *to the residue system smallest in absolute value,* $ia \equiv r_i \pmod p$ *with* $-\frac{p-1}{2} \le r_i \le \frac{p-1}{2}$ *for all* i. *Then*
>
> $$(\frac{a}{p}) = (-1)^s, \text{ where } s = \#\{i : r_i < 0\}.$$

■ **Proof.** Suppose $u_1, \ldots, u_s$ are the residues smaller than 0, and that $v_1, \ldots, v_{\frac{p-1}{2}-s}$ are those greater than 0. Then the numbers $-u_1, \ldots, -u_s$ are between 1 and $\frac{p-1}{2}$, and are all different from the v_js (see the margin); hence $\{-u_1, \ldots, -u_s, v_1, \ldots, v_{\frac{p-1}{2}-s}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. Therefore

$$\prod_i (-u_i) \prod_j v_j = \tfrac{p-1}{2}!,$$

If $-u_i = v_j$, then $u_i + v_j \equiv 0 \pmod p$. Now $u_i \equiv ka$, $v_j \equiv \ell a \pmod p$ implies $p \mid (k+\ell)a$. As p and a are relatively prime, p must divide $k + \ell$ which is impossible, since $k + \ell \le p - 1$.

which implies

$$(-1)^s \prod_i u_i \prod_j v_j \equiv \tfrac{p-1}{2}! \pmod p.$$

Now remember how we obtained the numbers u_i and v_j; they are the residues of $1a, \cdots, \frac{p-1}{2}a$. Hence

$$\tfrac{p-1}{2}! \equiv (-1)^s \prod_i u_i \prod_j v_j \equiv (-1)^s \tfrac{p-1}{2}!\, a^{\frac{p-1}{2}} \pmod p.$$

Cancelling $\frac{p-1}{2}!$ together with Euler's criterion gives

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \equiv (-1)^s \pmod p,$$

and therefore $(\frac{a}{p}) = (-1)^s$, since p is odd. □

With this we can easily compute $(\frac{2}{p})$: Since $1 \cdot 2, 2 \cdot 2, \ldots, \frac{p-1}{2} \cdot 2$ are all between 1 and $p-1$, we have

$$s = \#\{i : \tfrac{p-1}{2} < 2i \le p-1\} = \tfrac{p-1}{2} - \#\{i : 2i \le \tfrac{p-1}{2}\} = \lceil \tfrac{p-1}{4} \rceil.$$

Check that s is even precisely for $p = 8k \pm 1$.

The Lemma of Gauss is the basis for many of the published proofs of the quadratic reciprocity law. The most elegant may be the one suggested by Ferdinand Gotthold Eisenstein, who had learned number theory from Gauss' famous *Disquisitiones Arithmeticae* and made important contributions to "higher reciprocity theorems" before his premature death at age 29. His proof is just counting lattice points!

Let p and q be odd primes, and consider $(\frac{q}{p})$. Suppose iq is a multiple of q that reduces to a negative residue $r_i < 0$ in the Lemma of Gauss. This means that there is a unique integer j such that $-\frac{p}{2} < iq - jp < 0$. Note that $0 < j < \frac{q}{2}$ since $0 < i < \frac{p}{2}$. In other words, $(\frac{q}{p}) = (-1)^s$, where s is the number of lattice points (x, y), that is, pairs of integers x, y satisfying

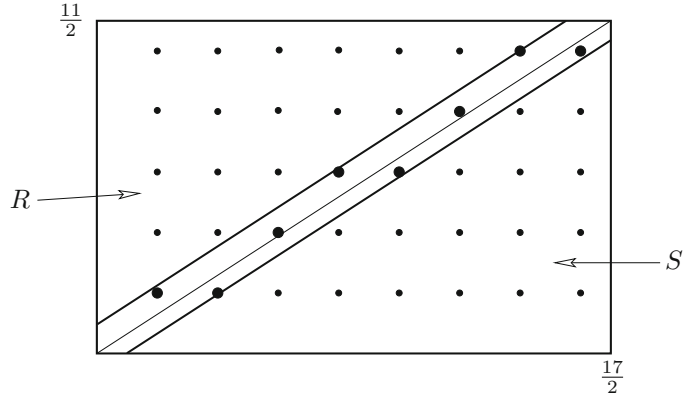
$$0 < py - qx < \frac{p}{2},\ 0 < x < \frac{p}{2},\ 0 < y < \frac{q}{2}\,. \tag{3}$$

Similarly, $(\frac{p}{q}) = (-1)^t$ where t is the number of lattice points (x, y) with

$$0 < qx - py < \frac{q}{2},\ 0 < x < \frac{p}{2},\ 0 < y < \frac{q}{2}\,. \tag{4}$$

Now look at the rectangle with side lengths $\frac{p}{2}$, $\frac{q}{2}$, and draw the two lines parallel to the diagonal $py = qx$, $y = \frac{q}{p}x + \frac{1}{2}$ or $py - qx = \frac{p}{2}$, respectively, $y = \frac{q}{p}(x - \frac{1}{2})$ or $qx - py = \frac{q}{2}$.
The figure shows the situation for $p = 17$, $q = 11$.

$p = 17 \quad q = 11$
$s = 5 \quad t = 3$
$(\frac{q}{p}) = (-1)^5 = -1$
$(\frac{p}{q}) = (-1)^3 = -1$



The proof is now quickly completed by the following three observations:

1. There are no lattice points on the diagonal and the two parallels. This is so because $py = qx$ would imply $p|x$, which cannot be. For the parallels observe that $py - qx$ is an integer while $\frac{p}{2}$ and $\frac{q}{2}$ are not.

2. The lattice points observing (3) are precisely the points in the upper strip $0 < py - qx < \frac{p}{2}$, and those of (4) the points in the lower strip $0 < qx - py < \frac{q}{2}$. Hence the number of lattice points in the two strips is $s + t$.

3. The outer regions $R : py - qx > \frac{p}{2}$ and $S : qx - py > \frac{q}{2}$ contain the *same* number of points. To see this consider the map $\varphi : R \to S$ which maps (x, y) to $(\frac{p+1}{2} - x, \frac{q+1}{2} - y)$ and check that φ is an involution.

Since the total number of lattice points in the rectangle is $\frac{p-1}{2} \cdot \frac{q-1}{2}$, we infer that $s + t$ and $\frac{p-1}{2} \cdot \frac{q-1}{2}$ have the same parity, and so

$$(\tfrac{q}{p})(\tfrac{p}{q}) \;=\; (-1)^{s+t} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \qquad \square$$

Second proof. Our second choice does not use Gauss' lemma, instead it employs so-called "Gauss sums" in finite fields. Gauss invented them in his study of the equation $x^p - 1 = 0$ and the arithmetical properties of the field $\mathbb{Q}(\zeta)$ (called cyclotomic field), where ζ is a p-th root of unity. They have been the starting point for the search for higher reciprocity laws in general number fields.

Let us first collect a few facts about finite fields.

A. Let p and q be different odd primes, and consider the finite field F with q^{p-1} elements. Its prime field is $\mathbb{Z}_q$, whence $qa = 0$ for any $a \in F$. This implies that $(a+b)^q = a^q + b^q$, since any binomial coefficient $\binom{q}{i}$ is a multiple of q for $0 < i < q$, and thus 0 in F. Note that Euler's criterion is an *equation* $(\frac{p}{q}) = p^{\frac{q-1}{2}}$ in the prime field $\mathbb{Z}_q$.

B. The multiplicative group $F^* = F \setminus \{0\}$ is cyclic of size $q^{p-1} - 1$ (see the box on the next page). Since by Fermat's little theorem p is a divisor of $q^{p-1} - 1$, there exists an element $\zeta \in F$ of order p, that is, $\zeta^p = 1$, and ζ generates the subgroup $\{\zeta, \zeta^2, \ldots, \zeta^p = 1\}$ of F^*. Note that any ζ^i $(i \neq p)$ is again a generator. Hence we obtain the polynomial decomposition $x^p - 1 = (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^p)$.

Now we can go to work. Consider the *Gauss sum*

$$G \;\coloneqq\; \sum_{i=1}^{p-1} \big(\frac{i}{p}\big)\, \zeta^i \;\in\; F,$$

where $(\frac{i}{p})$ is the Legendre symbol. For the proof we derive two different expressions for G^q and then set them equal.

First expression. We have

$$G^q \;=\; \sum_{i=1}^{p-1} (\frac{i}{p})^q \zeta^{iq} \;=\; \sum_{i=1}^{p-1} (\frac{i}{p}) \zeta^{iq} \;=\; (\frac{q}{p}) \sum_{i=1}^{p-1} (\frac{iq}{p}) \zeta^{iq} \;=\; (\frac{q}{p}) G, \qquad (5)$$

where the first equality follows from $(a+b)^q = a^q + b^q$, the second uses that $(\frac{i}{p})^q = (\frac{i}{p})$ since q is odd, the third one is derived from (2), which yields $(\frac{i}{p}) = (\frac{q}{p})(\frac{iq}{p})$, and the last one holds since iq runs with i through all nonzero residues modulo p.

Example: Take $p = 3$, $q = 5$. Then $G = \zeta - \zeta^2$ and $G^5 = \zeta^5 - \zeta^{10} = \zeta^2 - \zeta = -(\zeta - \zeta^2) = -G$, corresponding to $(\frac{5}{3}) = (\frac{2}{3}) = -1$.

Second expression. Suppose we can prove

$$G^2 = (-1)^{\frac{p-1}{2}} p\,, \qquad (6)$$

then we are quickly done. Indeed,

$$G^q = G(G^2)^{\frac{q-1}{2}} = G(-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} = G(\frac{p}{q})(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\,. \qquad (7)$$

Equating the expressions in (5) and (7) and cancelling G, which is nonzero by (6), we find $(\frac{q}{p}) = (\frac{p}{q})(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, and thus

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

The multiplicative group of a finite field is cyclic

Let F^* be the multiplicative group of the field F, with $|F^*| = n$. Writing $\mathrm{ord}(a)$ for the order of an element, that is, the smallest positive integer k such that $a^k = 1$, we want to find an element $a \in F^*$ with $\mathrm{ord}(a) = n$. If $\mathrm{ord}(b) = d$, then by Lagrange's theorem, d divides n (see the margin on page 4). Classifying the elements according to their order, we have

$$n = \sum_{d\,|\,n} \psi(d), \text{ where } \psi(d) = \#\{b \in F^* : \mathrm{ord}(b) = d\}. \quad (8)$$

If $\mathrm{ord}(b) = d$, then every element b^i $(i = 1, \ldots, d)$ satisfies $(b^i)^d = 1$ and is therefore a root of the polynomial $x^d - 1$. But, since F is a field, $x^d - 1$ has at most d roots, and so the elements $b, b^2, \ldots, b^d = 1$ are precisely these roots. In particular, every element of order d is of the form b^i.

On the other hand, it is easily checked that $\mathrm{ord}(b^i) = \frac{d}{(i,d)}$, where (i, d) denotes the greatest common divisor of i and d. Hence $\mathrm{ord}(b^i) = d$ if and only if $(i, d) = 1$, that is, if i and d are relatively prime. Denoting *Euler's function* by $\varphi(d) = \#\{i : 1 \le i \le d, (i, d) = 1\}$, we thus have $\psi(d) = \varphi(d)$ whenever $\psi(d) > 0$. Looking at (8) we find

$$n = \sum_{d\,|\,n} \psi(d) \le \sum_{d\,|\,n} \varphi(d)\,.$$

But, as we are going to show that

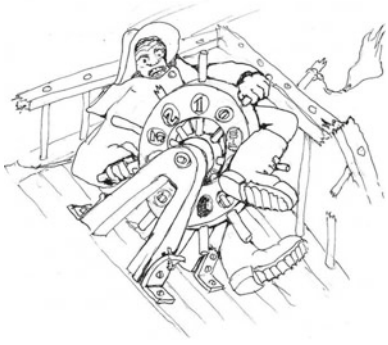
$$\sum_{d\,|\,n} \varphi(d) \;=\; n, \quad (9)$$

we must have $\psi(d) = \varphi(d)$ for all d. In particular, $\psi(n) = \varphi(n) \ge 1$, and so there is an element of order n.

The following (folklore) proof of (9) belongs in the Book as well. Consider the n fractions

$$\tfrac{1}{n}, \tfrac{2}{n}, \ldots, \tfrac{k}{n}, \ldots, \tfrac{n}{n},$$

reduce them to lowest terms $\frac{k}{n} = \frac{i}{d}$ with $1 \le i \le d$, $(i, d) = 1$, $d\,|\,n$, and check that the denominator d appears precisely $\varphi(d)$ times.



"Even in total chaos we can hang on to the cyclic group"

It remains to verify (6), and for this we first make two simple observations:

- $\sum_{i=1}^{p} \zeta^i = 0$ and thus $\sum_{i=1}^{p-1} \zeta^i = -1$. Just note that $-\sum_{i=1}^{p} \zeta^i$ is the coefficient of x^{p-1} in $x^p - 1 = \prod_{i=1}^{p}(x - \zeta^i)$, and thus 0.
- $\sum_{k=1}^{p-1}(\frac{k}{p}) = 0$ and thus $\sum_{k=1}^{p-2}(\frac{k}{p}) = -(\frac{-1}{p})$, since there are equally many quadratic residues and nonresidues.

We have

$$G^2 \;=\; \Big(\sum_{i=1}^{p-1} \big(\frac{i}{p}\big)\,\zeta^i\Big)\,\Big(\sum_{j=1}^{p-1} \big(\frac{j}{p}\big)\,\zeta^j\Big) \;=\; \sum_{i,j} \big(\frac{ij}{p}\big)\,\zeta^{i+j}.$$

Setting $j \equiv ik \,(\mathrm{mod}\, p)$ we find

$$G^2 \;=\; \sum_{i,k} \big(\frac{k}{p}\big)\,\zeta^{i(1+k)} \;=\; \sum_{k=1}^{p-1} \big(\frac{k}{p}\big) \sum_{i=1}^{p-1} \zeta^{(1+k)i}.$$

For $k = p-1 \equiv -1 \,(\mathrm{mod}\, p)$ this gives $(\frac{-1}{p})(p-1)$, since $\zeta^{1+k} = 1$. Move $k = p-1$ in front and write

$$G^2 \;=\; \big(\frac{-1}{p}\big)(p-1) + \sum_{k=1}^{p-2} \big(\frac{k}{p}\big) \sum_{i=1}^{p-1} \zeta^{(1+k)i}.$$

Euler's criterion: $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$

Since ζ^{1+k} is a generator of the group for $k \neq p-1$, the inner sum equals $\sum_{i=1}^{p-1} \zeta^i = -1$ for all $k \neq p-1$ by our first observation. Hence the second summand is $-\sum_{k=1}^{p-2}(\frac{k}{p}) = (\frac{-1}{p})$ by our second observation. It follows that $G^2 = (\frac{-1}{p})p$ and thus with Euler's criterion $G^2 = (-1)^{\frac{p-1}{2}} p$, which completes the proof. □

For $p = 3$, $q = 5$, $G^2 = (\zeta - \zeta^2)^2 = \zeta^2 - 2\zeta^3 + \zeta^4 = \zeta^2 - 2 + \zeta = -3 = (-1)^{\frac{3-1}{2}} 3$, since $1 + \zeta + \zeta^2 = 0$.

References

[1] A. BAKER: *A Concise Introduction to the Theory of Numbers,* Cambridge University Press, Cambridge 1984.

[2] F. G. EISENSTEIN: *Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste,* J. Reine Angewandte Mathematik **28** (1844), 186-191.

[3] C. F. GAUSS: *Theorema arithmetici demonstratio nova,* Comment. Soc. regiae sci. Göttingen **XVI** (1808), 69; Werke II, 1-8 (contains the 3rd proof).

[4] C. F. GAUSS: *Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et amplicationes novae (1818),* Werke II, 47-64 (contains the 6th proof).

[5] F. LEMMERMEYER: *Reciprocity Laws,* Springer-Verlag, Berlin 2000.

"What's up?"

"I'm pushing 196 proofs
for quadratic reciprocity"