WON Series in Discrete Mathematics and Modern Algebra Volume 8

THE QUADRATIC RECIPROCITY LAW

Amin Witno

Abstract

We discuss four detailed proofs of the quadratic reciprocity law. The first proof, right off Euler's criterion, follows the path of Gauss' lemma and Eisenstein's lattice counting. Relying on the lemma again, we then give a second proof via an equivalent law that was conjectured by Euler, as well as a third, due to Eisenstein, involving some properties of complex functions. For a fourth proof, we employ Gauss sum and results from finite fields.

These notes have been prepared as a supplementary reading assignment for my Number Theory students (Math 313) at Philadelphia University, Jordan.[1] Outline notes are more like a revision. No student is expected to fully benefit from these notes unless they have regularly attended the lectures.

1 Prelude

Throughout this article, p stands for an odd prime, and a an arbitrary integer but not a multiple of p. Any other number variable, if undeclared, is understood integer.

Definition. We call a a *quadratic residue* or *non-residue* modulo p, depending whether the congruence $x^2 \equiv a \pmod{p}$ has a solution or no solution, respectively. The *Legendre symbol* of a mod p is the quantity $\left(\frac{a}{p}\right)$ defined by

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

The well-known reciprocity law is commonly stated as follows.

The Quadratic Reciprocity Law. If q is another odd prime, distinct from p, then

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

Equivalently, the law can be rephrased based on the two classes of primes mod 4:

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p\,\%\,4 = 1 \text{ or if } q\,\%\,4 = 1 \\ -\left(\frac{p}{q}\right) & \text{if } p\,\%\,4 = 3 \text{ and } q\,\%\,4 = 3 \end{cases}$$

Last Revision: 17–01–2019
awitno@gmail.com

The notation (%) here represents residue mod operator, given by the formula

$$m \,\%\, n \;=\; m - \left\lfloor \frac{m}{n} \right\rfloor \times n$$

and where $\lfloor \cdot \rfloor$ indicates the greatest integer function.

More than 300 proofs of the reciprocity law have been published, many of which rely on the so-called Gauss' lemma. Our goal for now is to establish the following result of Euler, of which Gauss' lemma is a close consequence.

Theorem 1 (Euler's Criterion)**.** The Legendre symbol $\left(\frac{a}{p}\right)$ satisfies the congruence

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

Exercise 1. We ask you first to show that Euler's criterion gives the identity

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

and the formula

$$\left(\frac{-1}{p}\right) \;=\; (-1)^{\frac{p-1}{2}} \;=\; \begin{cases} +1 & \text{if } p \,\%\, 4 = 1 \\ -1 & \text{if } p \,\%\, 4 = 3 \end{cases}$$

Definition. A *full system* modulo p if any set of $p-1$ integers representing distinct non-zero residue classes modulo p. In other words, S is a full system if and only if $|S| = p-1$ and $\{x \,\%\, p \mid x \in S\} = \{1, 2, \ldots, p-1\}$.

Theorem 2. Let S be a full system modulo p, and let $p \nmid a$. Then $aS := \{ax \mid x \in S\}$ is also a full system modulo p.

Proof. It is clear there is no zero residue in aS, so it suffices to see that its elements are distinct modulo p. Well, if $ax \equiv ay \pmod{p}$ for some $x, y \in S$, then p divides $ax - ay = a(x-y)$. Since $p \nmid a$ and p is a prime, then we would have $p \mid x - y$, i.e., $x \equiv y \pmod{p}$, which is not possible in S by design. ▽

The term *cancellation law* refers to the proposition that $ax \equiv ay \pmod{p}$ implies $x \equiv y \pmod{p}$, under the condition $p \nmid a$. We mention this because we will encounter this law again next.

Theorem 3 (Fermat's Little Theorem)**.** If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Let us have two sets of full system modulo p, i.e., $S = \{1, 2, \ldots, p-1\}$ and the other one aS. They yield the congruence

$$1 \times 2 \times \cdots \times (p-1) \;\equiv\; a \times 2a \times \cdots \times (p-1)a \pmod{p}$$

Since $p \nmid (p-1)!$, the cancellation law applies, and $1 \equiv a^{p-1} \pmod{p}$. ▽

Suppose for the moment that $\left(\frac{a}{p}\right) = +1$, which means that we have an integer x for which $x^2 \equiv a \pmod{p}$. It is clear that $p \nmid x$, hence by Fermat's little theorem,

$$a^{\frac{p-1}{2}} \;\equiv\; x^{p-1} \;\equiv\; 1 \pmod{p}$$

And that is Euler's criterion. As for the case $\left(\frac{a}{p}\right) = -1$, we shall see shortly.

Theorem 4 (Wilson's Theorem)**.** We have $(p-1)\,!\equiv -1 \pmod p$.

Proof. Let $S=\{1,2,\ldots,p-1\}$. We have demonstrated that for each $x\in S$, the set xS is a full system modulo p. In particular, there is a unique $y\in S$ such that $xy\equiv 1 \pmod p$. Occasionally, we might have $y=x$, i.e., when $x^2\equiv 1 \pmod p$, but that can happen if and only if p divides $x^2-1=(x-1)(x+1)$, i.e., $x\equiv \pm 1 \pmod p$. In other words, the elements of S can be paired two by two of the form $\{x,y\}$ with $xy\equiv 1 \pmod p$, except for $x=1$ and $x=p-1$. Thus

$$(p-2)\,! \;=\; 2\times 3\times\cdots\times(p-2) \;=\; \prod_{xy\equiv 1}(x\times y) \;\equiv\; 1 \pmod p$$

and multiplying by $(p-1)$ gives the result $(p-1)\,!\equiv -1 \pmod p$. ▽

In the proof of Fermat's little theorem earlier, observe that the displayed congruence simplifies to $-1\equiv -a^{p-1} \pmod p$ by Wilson's theorem, bypassing the cancellation law. However, we did not want to imply that Fermat's theorem stands upon Wilson's. And by the way, despite its name, it was Lagrange who proved Wilson's theorem.

By similar reasoning, for each $x\in S$, there is a unique $y\in S$ for which $xy\equiv a \pmod p$. Hence, if $\left(\frac{a}{p}\right)=-1$, then it is not allowed to have $y=x$. In that case, the elements of S can be paired two by two of the form $\{x,y\}$ with $xy\equiv a \pmod p$. Thus by Wilson's theorem,

$$-1 \;\equiv\; (p-1)\,! \;=\; 1\times 2\times\cdots\times(p-1) \;=\; \prod_{xy\equiv a}(x\times y) \;\equiv\; a^{\frac{p-1}{2}} \pmod p$$

which completes Euler's criterion for both cases.

2 Gauss, Proof Nº 3

Gauss himself wrote eight different proofs of the reciprocity law. His third seems to be the most popular as a basis of other later proofs, including a modified version we put together here, initially introduced by Eisenstein.

Definition. A set H of $\frac{p-1}{2}$ integers is called a *half system* modulo p if and only if the set $\{\pm x \mid x\in H\}$ is a full system modulo p.

Theorem 5. Let H be a half system modulo p, and let $p\nmid a$. Then aH is also a half system modulo p.

Proof. The relation $ax\equiv \pm ay \pmod p$ implies $x\equiv \pm y \pmod p$. Hence, if the elements in the set $\{\pm x \mid x\in H\}$ are distinct modulo p, so are those in $\{\pm ax \mid x\in H\}$. ▽

So let us have two sets of half system modulo p, i.e., $H=\{1,2,\ldots,\frac{p-1}{2}\}$ and aH. This implies that we have a one-to-one correspondence between $x\in aH$ and $r\in H$, in such a way that $x\equiv \pm r \pmod p$. Hence, if we let $\gamma:=\gamma(a,p)$ denote the number of occurrences with negative signs, then we may have the congruence

$$(-1)^\gamma\times 1\times 2\times\cdots\times\frac{p-1}{2} \;\equiv\; a\times 2a\times\cdots\times\frac{p-1}{2}\,a \pmod p$$

Cancellation law gives us $(-1)^\gamma \equiv a^{\frac{p-1}{2}} \pmod p$, which, by Euler's criterion, becomes

$$\left(\frac{a}{p}\right) \;=\; (-1)^{\gamma(a,p)}$$

Exercise 2. This last identity is a formula known as Gauss' lemma. At this point, your part is to apply Gauss' lemma and establish another formula,

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

by letting $a = 2$ and evaluating $\gamma(2, p)$ accordingly. Solution is provided at the end of this article, but it really is worth your effort.

We next claim that if a is an odd number, then $\left(\frac{a}{p}\right) = (-1)^{\Gamma(a,p)}$, where we define

$$\Gamma(a,p) \;:=\; \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor$$

by showing that $\gamma(a, p)$ and $\Gamma(a, p)$ are of the same parity, i.e., that

$$\gamma(a,p) \;\equiv\; \Gamma(a,p) \pmod 2$$

Now being odd, $p \equiv 1 \pmod 2$, so we may write

$$\Gamma(a,p) \;=\; \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor \;\equiv\; \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor \; p \pmod 2$$

Then we recall our mod operator formula, $ak \,\%\, p = ak - \left\lfloor \frac{ak}{p} \right\rfloor p$, and obtain

$$\Gamma(a,p) \;\equiv\; \sum_{k=1}^{\frac{p-1}{2}} ak - \sum_{k=1}^{\frac{p-1}{2}} ak \,\%\, p \pmod 2$$

But the second sum here has its summands from the set $\{x \,\%\, p \mid x \in aH\}$, where for each $x \in aH$, there is a unique $r \in H$ such that, either $x \,\%\, p = r$ or else $x \equiv -r \pmod p$. For the latter case, we have $x \,\%\, p = p - r$, and a total of γ such cases. Therefore, if we reorder the set H by labeling these γ elements first, then

$$\Gamma(a,p) \;\equiv\; \sum_{k=1}^{\frac{p-1}{2}} ak - \left(\sum_{i=1}^{\gamma} (p - r_i) + \sum_{i=\gamma+1}^{\frac{p-1}{2}} r_i \right) \pmod 2$$

Note that as $-1 \equiv 1 \pmod 2$, we may as well replace every minus sign with plus sign:

$$\Gamma(a,p) \;\equiv\; \sum_{k=1}^{\frac{p-1}{2}} ak + \sum_{i=1}^{\gamma} p + \sum_{i=1}^{\gamma} r_i + \sum_{i=\gamma+1}^{\frac{p-1}{2}} r_i \;=\; \gamma\, p + \sum_{k=1}^{\frac{p-1}{2}} ak + \sum_{i=1}^{\frac{p-1}{2}} r_i \pmod 2$$

And since the summands r_i run through all the elements of H, then we have

$$\sum_{i=1}^{\frac{p-1}{2}} r_i \;=\; \sum_{k=1}^{\frac{p-1}{2}} k$$

and therefore,

$$\Gamma(a,p) \;\equiv\; \gamma\, p + \sum_{k=1}^{\frac{p-1}{2}} (a+1)k \pmod 2$$

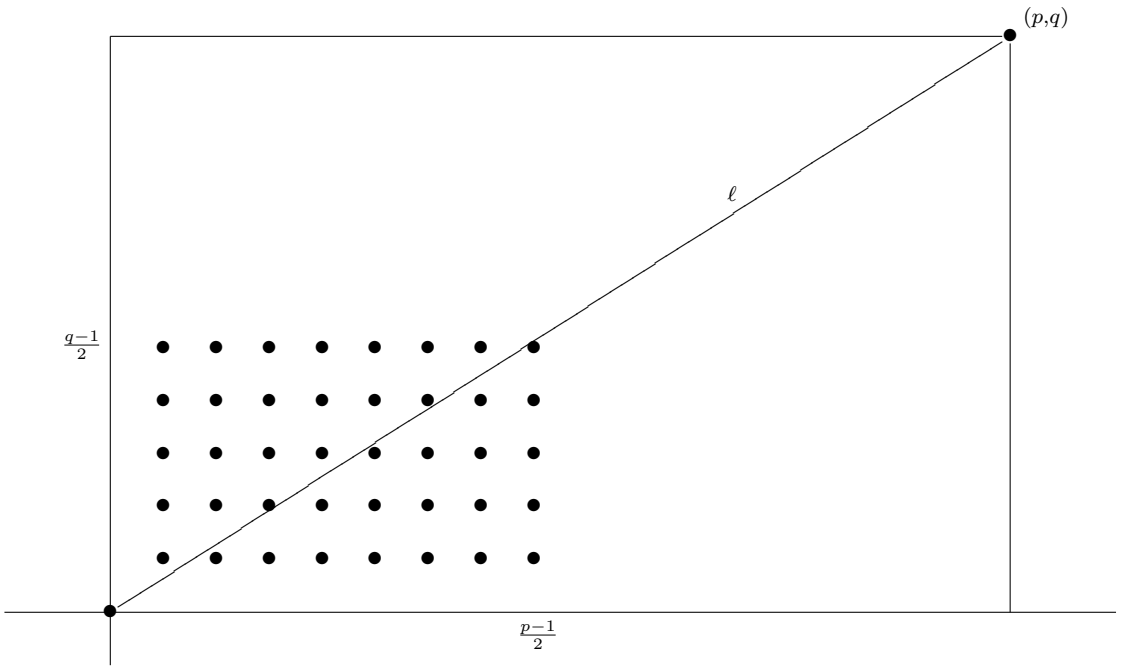
This is where we want a to be odd, so that $a+1 \equiv 0 \pmod 2$ and $\Gamma(a,p) \equiv \gamma\, p \equiv \gamma \pmod 2$ as desired.

In particular, now we are going to let $a = q$, which stands for another odd prime number distinct from p. Thus we have demonstrated that

$$\left(\frac{q}{p}\right) \;=\; (-1)^{\Gamma(q,p)}$$

The rest of the proof is an observation from basic analytic geometry.

Consider the straight line ℓ on the xy-plane given by the equation $y = \frac{q}{p}x$, as well as the region R bounded by $1 \le x \le \frac{p-1}{2}$ and $1 \le y \le \frac{q-1}{2}$. Since the fraction $\frac{q}{p}$, i.e., the slope of ℓ, is in reduced form, there are no integral lattice points lying on ℓ between $(0,0)$ and (p,q). In particular, none of the $\frac{p-1}{2} \times \frac{q-1}{2}$ lattice points in R lies on ℓ.



Let us count how many lattice points in R lie below ℓ. Well, for a fixed integer $x \in \left[1, \frac{p-1}{2}\right]$, we have a lattice point (x,y) corresponding to the values $y = 1$, $y = 2, \ldots,$ up to $y = \left\lfloor \frac{qx}{p} \right\rfloor$. Summing over x gives us the total:

$$\sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor \;=\; \Gamma(q,p)$$

By symmetry, we can also say that the number of lattice points in R above ℓ is $\Gamma(p,q)$. Hence, in all, the number of lattice points in R is given in two ways:

$$\Gamma(q,p) \;+\; \Gamma(p,q) \;=\; \frac{p-1}{2} \;\times\; \frac{q-1}{2}$$

From here, it follows that

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \;=\; (-1)^{\Gamma(q,p)}\,(-1)^{\Gamma(p,q)} \;=\; (-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}$$

which is an equivalent form of the quadratic reciprocity law. ▽

3 Interlude

Before Gauss, Euler had actually discovered the reciprocity law but was unable to prove it—thus named a conjecture. His version of the law, however, looked quite different from what we are familiar with today.

Theorem 6 (Euler's Conjecture)**.** Let p and q be distinct odd prime numbers. If a is a positive integer such that $p \equiv \pm q \pmod{4a}$, then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Exercise 3. Your job now is to prove that Euler's conjecture is indeed equivalent to the quadratic reciprocity law proved in the preceding section. Solution is provided at the end. For a start, try first to obtain $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ given that a is prime.

For the sake of completion, in this section we shall demonstrate how Euler could have proved his conjecture had he known the lemma of Gauss. And here we go.

We wish to show that if $p \equiv \pm q \pmod{4a}$, then $(-1)^{\gamma(a,p)} = (-1)^{\gamma(a,q)}$. Thus the key is proving that $\gamma(a,p)$ and $\gamma(a,q)$ are of the same parity.

Recall that $\gamma(a,p)$ counts the number of elements $x \in aH$ for which $x \equiv -r \pmod{p}$ with $r \in H = \{1, 2, \ldots, \frac{p-1}{2}\}$, i.e., for which $\frac{p}{2} < x \,\%\, p < p$. So if we let $\left\lfloor \frac{ar}{p} \right\rfloor = k-1$, then this remainder condition is equivalent to having $\left(k-\frac{1}{2}\right)p \;<\; ar \;<\; kp$, or

$$\frac{\left(k-\frac{1}{2}\right)p}{a} \;<\; r \;<\; \frac{kp}{a}$$

In other words, we count the number of $r \in H$ which meets this compound inequality with any value of $k \geq 1$. Since $r \leq \frac{p-1}{2}$, the left-hand inequality implies that $k \leq \left\lfloor \frac{a}{2} \right\rfloor$. Conversely, if $k \leq \left\lfloor \frac{a}{2} \right\rfloor$, then $\frac{kp}{a} < \frac{p-1}{2} + 1$. This observation enables us to enumerate such r by evaluating $\left\lfloor \frac{kp}{a} \right\rfloor - \left\lfloor \frac{(k-\frac{1}{2})p}{a} \right\rfloor$ for all k in the range $1 \leq k \leq \left\lfloor \frac{a}{2} \right\rfloor$, i.e.,

$$\gamma(a,p) \;=\; \sum_{k=1}^{\lfloor \frac{a}{2} \rfloor} \left(\left\lfloor \frac{kp}{a} \right\rfloor - \left\lfloor \frac{(k-\frac{1}{2})p}{a} \right\rfloor \right)$$

Now we substitute $p = 4am + n$, where $0 < n < 4a$, and check that this sum becomes

$$\gamma(a,p) \;=\; \sum_{k=1}^{\lfloor \frac{a}{2} \rfloor} \left(2m + \left\lfloor \frac{kn}{a} \right\rfloor - \left\lfloor \frac{(k-\frac{1}{2})n}{a} \right\rfloor \right)$$

Therefore, if $p \equiv q \pmod{4a}$, then we may write $q = 4am' + n$, and similarly we get

$$\gamma(a,q) \;=\; \sum_{k=1}^{\lfloor \frac{a}{2} \rfloor} \left(2m' + \left\lfloor \frac{kn}{a} \right\rfloor - \left\lfloor \frac{(k-\frac{1}{2})n}{a} \right\rfloor \right)$$

That gives us $\gamma(a,p) \equiv \gamma(a,q) \pmod 2$ as desired. Meanwhile, if $p \equiv -q \pmod{4a}$, then we write $q = 4am'' + (4a-n)$ with $0 < 4a-n < 4a$. In this case, similarly,

$$\gamma(a,q) \;=\; \sum_{k=1}^{\lfloor \frac{a}{2} \rfloor} \left(2m'' + 2 + \left\lfloor \frac{k(-n)}{a} \right\rfloor - \left\lfloor \frac{(k-\frac{1}{2})(-n)}{a} \right\rfloor \right)$$

If we observe that $\lfloor -t \rfloor = -\lfloor t \rfloor - 1$ for any non-integer rational number t, then

$$\gamma(a,q) \;=\; \sum_{k=1}^{\lfloor \frac{a}{2} \rfloor} \left(2m'' + 2 - \left\lfloor \frac{kn}{a} \right\rfloor + \left\lfloor \frac{(k-\frac{1}{2})n}{a} \right\rfloor \right)$$

And once again, we have $\gamma(a,q) \equiv \gamma(a,p) \pmod 2$.

4 Eisenstein, A Proof in $\mathbb{C}$

This next proof requires some familiarity with complex numbers and functions, e.g., Euler's formula $e^{ix} = \cos x + i \sin x$, where $x \in \mathbb{R}$, measured in radian.

Definition. Set $\zeta := e^{2\pi i/n} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$, i.e., a primitive n-th root of unity.

It is known that the geometric sequence $\{\zeta^k\}$ is cyclic with period n. In particular, we have $\zeta^n = 1$ and $\zeta^m = \zeta^{m \,\%\, n}$ for any $m \in \mathbb{Z}$. Moreover, the fact that $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ are all distinct zeros of $z^n - 1$ gives us the polynomial factorization $z^n - 1 = \prod (z - \zeta^k)$ over $\mathbb{C}$, where k can vary within any complete residue system modulo n.

Theorem 7. If $n \in \mathbb{N}$ and is odd, then for all $v, w \in \mathbb{C}$,

$$v^n - w^n \;=\; \prod_{k=0}^{n-1} \left(\zeta^k v - \zeta^{-k} w \right)$$

Proof. Note that the claimed identity holds for $w = 0$, where $\prod \zeta^k v = v^n (\zeta^n)^{\frac{n-1}{2}} = v^n$. Assuming $w \neq 0$, then

$$v^n - w^n \;=\; w^n \left(\left(\frac{v}{w} \right)^n - 1 \right) \;=\; w^n \prod_{k=0}^{n-1} \left(\frac{v}{w} - \zeta^k \right) \;=\; \prod_{k=0}^{n-1} \left(v - \zeta^k w \right)$$

Now we need the fact that if $\gcd(a,n) = 1$, then $ab \equiv ac \pmod n$ implies $b \equiv c \pmod n$, (This is a generalization of the cancellation law we have seen in Section 1, also known as Euclid's lemma.) from which we get $\{ak \,\%\, n \mid 0 \leq k \leq n-1\} = \{0, 1, \ldots, n-1\}$. Hence, ζ^k and ζ^{ak} run through the same set of values in the above product. In particular, since n is odd, we choose $a = -2k$:

$$v^n - w^n = \prod_{k=0}^{n-1} \left(v - \zeta^{-2k} w \right) = \prod_{k=0}^{n-1} \zeta^{-k} \prod_{k=0}^{n-1} \zeta^k \left(v - \zeta^{-2k} w \right) = (\zeta^{-n})^{\frac{n-1}{2}} \prod_{k=0}^{n-1} \left(\zeta^k v - \zeta^{-k} w \right)$$

and the result follows as $\zeta^{-n} = 1$. ▽

Definition. We consider the complex function $f(z) := e^{2\pi i z} - e^{-2\pi i z}$ for all $z \in \mathbb{C}$.

Observe that $f(-z) = -f(z)$ and that $f(z+1) = e^{2\pi iz}e^{2\pi i} - e^{-2\pi iz}e^{-2\pi i} = f(z)$, due to the fact that $e^{2\pi i} = 1$. By induction, it then follows that $f(z+m) = f(z)$ for all $m \in \mathbb{Z}$. Moreover, recall the complex trigonometric function $\sin z = \frac{e^{iz}-e^{-iz}}{2i}$ and check that $f(z) = 2i \sin 2\pi z$. So if $x \in \mathbb{R}$, then $f(x) = 0$ if and only if $2x \in \mathbb{Z}$.

Exercise 4. Granted that you have not seen $\sin z$ before, but are comfortable with Euler's formula. Then write $z = x + iy$ with $x, y \in \mathbb{R}$, and define $e^z = e^{x+iy} := e^x e^{iy} = e^x(\cos y + i \sin y)$. Try this approach and prove that $f(x) = 0$ if and only if $2x \in \mathbb{Z}$.

Theorem 8. If $n \in \mathbb{N}$ and is odd, then for all $z \in \mathbb{C}$,

$$f(nz) \;=\; f(z) \prod_{k=1}^{\frac{n-1}{2}} f\left(z + \frac{k}{n}\right)\, f\left(z - \frac{k}{n}\right)$$

Proof. If we let $v = e^{2\pi iz}$ and $w = e^{-2\pi iz}$, then $f(nz) = v^n - w^n$, so we apply the preceding theorem, noting that $\zeta^k v - \zeta^{-k} w = e^{2\pi i(z+k/n)} - e^{-2\pi i(z+k/n)} = f(z + k/n)$:

$$f(nz) \;=\; \prod_{k=0}^{n-1} f\left(z + \frac{k}{n}\right) \;=\; f(z) \prod_{k=1}^{\frac{n-1}{2}} f\left(z + \frac{k}{n}\right) \prod_{k=\frac{n+1}{2}}^{n-1} f\left(z + \frac{k}{n}\right)$$

Now it remains to show that the very last product can be expressed as

$$\prod_{k=\frac{n+1}{2}}^{n-1} f\left(z + \frac{k}{n}\right) \;=\; \prod_{k=1}^{\frac{n-1}{2}} f\left(z - \frac{k}{n}\right)$$

To see this, observe that $f(z + \frac{k}{n}) = f(z + \frac{k}{n} - 1) = f(z - \frac{n-k}{n})$, and that as k goes from $\frac{n+1}{2}$ to $n-1$, the value of $n-k$ goes from 1 to $\frac{n-1}{2}$ in the reverse order. $\triangledown$

At this point we go back to Gauss' lemma: Let $H = \{1, 2, \ldots, \frac{p-1}{2}\}$, where we have a one-to-one correspondence between $x \in aH$ and $r \in H$, i.e., that $x \equiv \pm r \pmod p$, with exactly $\gamma(a,p)$ of these needing the negative sign, and where $(-1)^{\gamma(a,p)} = \left(\frac{a}{p}\right)$.

For such pair (x, r), the stated congruence implies that $\frac{x}{p} \mp \frac{r}{p} \in \mathbb{Z}$. Therefore, the relation $f(z+m) = f(z)$ gives us $f(\frac{x}{p}) = f(\pm\frac{r}{p})$, which then, since $f(-z) = -f(z)$, becomes $f(\frac{x}{p}) = \pm f(\frac{r}{p})$. Now letting $a = q$, we take the product of such equality over all $r \in H$:

$$\prod_{r=1}^{\frac{p-1}{2}} f\left(\frac{qr}{p}\right) \;=\; (-1)^{\gamma(q,p)} \prod_{r=1}^{\frac{p-1}{2}} f\left(\frac{r}{p}\right) \;=\; \left(\frac{q}{p}\right) \prod_{r=1}^{\frac{p-1}{2}} f\left(\frac{r}{p}\right)$$

On the other hand, if we take similar product with $f(nz)$ in the preceding theorem, with $n = q$ and $z = r/p$, then we get

$$\prod_{r=1}^{\frac{p-1}{2}} f\left(\frac{qr}{p}\right) \;=\; \prod_{r=1}^{\frac{p-1}{2}} f\left(\frac{r}{p}\right) \prod_{r=1}^{\frac{p-1}{2}} \prod_{k=1}^{\frac{q-1}{2}} f\left(\frac{r}{p} + \frac{k}{q}\right)\, f\left(\frac{r}{p} - \frac{k}{q}\right)$$

We substitute the left-hand side by $\left(\frac{q}{p}\right)\prod f(\frac{r}{p})$ and, noting that $f(\frac{r}{p}) \neq 0$ since $p \nmid 2r$, we cancel $\prod f(\frac{r}{p})$ off both sides to obtain

$$\left(\frac{q}{p}\right) \;=\; \prod_{r=1}^{\frac{p-1}{2}} \prod_{k=1}^{\frac{q-1}{2}} f\left(\frac{r}{p}+\frac{k}{q}\right)\; f\left(\frac{r}{p}-\frac{k}{q}\right)$$

Of course, we now reverse the roles of p and q (as well as the indices r and k for convenience) and employ the relation $f(-z) = -f(z)$ once again:

$$\left(\frac{p}{q}\right) = \prod_{k=1}^{\frac{q-1}{2}} \prod_{r=1}^{\frac{p-1}{2}} f\left(\frac{k}{q}+\frac{r}{p}\right)\; f\left(\frac{k}{q}-\frac{r}{p}\right) = \prod_{k=1}^{\frac{q-1}{2}} \prod_{r=1}^{\frac{p-1}{2}} f\left(\frac{k}{q}+\frac{r}{p}\right)\; f\left(\frac{r}{p}-\frac{k}{q}\right)\; (-1)$$

Without the factor of (-1), this product would be $\left(\frac{q}{p}\right)$ in the form given earlier, i.e.,

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

and that gives the reciprocity law. ▽

5 Gauss, Proof Nº 6 in $\mathbb{F}$

This proof relies on some knowledge about finite fields.

Definition. Let $\mathbb{F}$ denote the finite field of order q^{p-1}, i.e., an extension of degree $p-1$ over the prime field $\mathbb{Z}_q$. We know that the multiplicative group $\mathbb{F}^*$ is cyclic of order $q^{p-1}-1$ which, according to Fermat's little theorem, is a multiple of p. Hence, there exists an element $\eta \in \mathbb{F}$ of multiplicative order p, and we use this to define

$$G \;:=\; \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \eta^k$$

This G is an element of $\mathbb{F}$ which is called *Gauss sum.*

Theorem 9. We have $G^2 \in \mathbb{Z}_q$. More precisely,

$$G^2 \;=\; \left(\frac{-1}{p}\right) p$$

Proof. By its definition,

$$G^2 \;=\; \left(\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \eta^k\right) \left(\sum_{l=1}^{p-1} \left(\frac{l}{p}\right) \eta^l\right) \;=\; \sum_{k=1}^{p-1} \sum_{l=1}^{p-1} \left(\frac{kl}{p}\right) \eta^{k+l}$$

If k is fixed, then for each $m \in S := \{1, 2, \ldots, p-1\}$, there exists $l \in S$ such that $l \equiv km \pmod p$. And according to Theorem 2, as m runs through the full system S,

so does km. Moreover, since η has order p, we have $\eta^l = \eta^{km}$. These facts allow us to substitute the index l by m for the inner sum:

$$G^2 \;=\; \sum_{k=1}^{p-1} \sum_{m=1}^{p-1} \left(\frac{k^2 m}{p}\right) \eta^{k+km} \;=\; \sum_{k=1}^{p-1} \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \eta^{k(1+m)}$$

Then we regroup the summands by switching the indices k and m:

$$G^2 \;=\; \sum_{m=1}^{p-1} \sum_{k=1}^{p-1} \left(\frac{m}{p}\right) \eta^{k(1+m)} \;=\; \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \sum_{k=1}^{p-1} \eta^{k(1+m)}$$

Now the summand corresponding to $m = p-1$ is $\left(\frac{-1}{p}\right) \sum_{k=1}^{p-1} \eta^{kp} = \left(\frac{-1}{p}\right)(p-1)$ since $\eta^p = 1$. Hence, it suffices to show that the remaining summands add up to $\left(\frac{-1}{p}\right)$, i.e., that

$$\sum_{m=1}^{p-2} \left(\frac{m}{p}\right) \sum_{k=1}^{p-1} \eta^{k(1+m)} \;=\; \left(\frac{-1}{p}\right)$$

To establish this last identity, first note that $p \nmid (1+m)$ as m goes from 1 to $p-2$, hence by Theorem 2 again, both k and $k(1+m)$ run through a full system modulo p. And again, combined with the fact that η is of order p, this implies that

$$\sum_{m=1}^{p-2} \left(\frac{m}{p}\right) \sum_{k=1}^{p-1} \eta^{k(1+m)} \;=\; \sum_{m=1}^{p-2} \left(\frac{m}{p}\right) \sum_{k=1}^{p-1} \eta^{k}$$

Since the elements $1, \eta, \eta^2, \ldots, \eta^{p-1}$ are distinct zeros of $x^p - 1$, we have the polynomial factorization $x^p - 1 = \prod_{k=0}^{p-1}(x - \eta^k)$ over $\mathbb{F}$. In particular, equating the coefficient of x^{p-1} from each side yields $0 = -\sum_{k=0}^{p-1} \eta^k$, which implies that $\sum_{k=1}^{p-1} \eta^k = -\eta^0 = -1$. So now it remains for us to show that

$$\sum_{m=1}^{p-2} \left(\frac{m}{p}\right) \;=\; -\left(\frac{-1}{p}\right)$$

and this readily follows from a rather well-known identity, i.e., that $\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) = 0$. For the sake of completion, we ask you to prove this fact as a last exercise. $\bigtriangledown$

Exercise 5. You are to demonstrate that

$$\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \;=\; 0$$

by proving that quadratic residues and non-residues are equally many in a given full system modulo p.

Recall that $\mathbb{F}$, being a field of characteristic q, enjoys the formula $(x+y)^q = x^q + y^q$ for all $x, y \in \mathbb{F}$ (since the middle terms, being "multiples" of q, all vanish). By this, and noting that q is odd,

$$G^q \;=\; \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)^q \eta^{qk} \;=\; \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \eta^{qk} \;=\; \sum_{k=1}^{p-1} \left(\frac{q}{p}\right)^2 \left(\frac{k}{p}\right) \eta^{qk} \;=\; \left(\frac{q}{p}\right) \sum_{k=1}^{p-1} \left(\frac{qk}{p}\right) \eta^{qk}$$

But both k and qk vary through a full system modulo p, and η is of order p, so we are allowed to replace the term qk by k without changing the value of the sum:

$$G^q \;=\; \left(\frac{q}{p}\right) \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \eta^k \;=\; \left(\frac{q}{p}\right) G$$

Furthermore, the preceding theorem implicitly implies that G is not the zero element, hence invertible, and that gives us

$$\left(\frac{q}{p}\right) \;=\; G^{q-1}$$

Finally, we apply the theorem once more, plus Euler's criterion and $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$:

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

where the last equality (instead of a congruence) is justified in the prime field $\mathbb{Z}_q$. $\bigtriangledown$

6 Postlude

Solution 1. It is clear that $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$. However, both sides of the congruence are either 1 or -1, and their difference is divisible by $p > 2$. That is possible only when both are equal. Similarly also, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. And since odd primes come in the form $p = 4n + 1$ or $p = 4n + 3$, we easily check that $\frac{p-1}{2}$ is even or odd, respectively, according to these two classes.

Solution 2. We have $2H = \{2, 4, \ldots, p-1\}$. Those congruent to $r \in H$ are 2, 4, ... up to $2\left\lfloor\frac{p-1}{4}\right\rfloor$, while the rest to $-r$. Hence,

$$n \;=\; \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor$$

We show that $(-1)^n = (-1)^{\frac{p^2-1}{8}}$ by comparing the parity of n and of $\frac{p^2-1}{8}$ in the four cases that complete the proof:

1. Let $p = 8k + 1$. Then $n = 4k - 2k$ is even and so is $\frac{p^2-1}{8} = 8k^2 + 2k$.
2. Let $p = 8k + 3$. Then $n = (4k + 1) - 2k$ is odd and so is $\frac{p^2-1}{8} = 8k^2 + 6k + 1$.
3. Let $p = 8k + 5$. Then $n = (4k + 2) - (2k + 1)$ is odd as is $\frac{p^2-1}{8} = 8k^2 + 10k + 3$.
4. Let $p = 8k + 7$. Then $n = (4k + 3) - (2k + 1)$ is even as is $\frac{p^2-1}{8} = 8k^2 + 14k + 6$.

Solution 3. Let us assume that if $p \equiv \pm q \pmod{4a}$, then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. There are four cases in which we must verify that the reciprocity law holds:

1. Let $p \,\%\, 4 = 1$ and $q \,\%\, 4 = 1$, so that $p - q = 4a$. Then

$$\left(\tfrac{q}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{q}{p}\right) = \left(\tfrac{-q}{p}\right) = \left(\tfrac{p-q}{p}\right) = \left(\tfrac{4a}{p}\right) = \left(\tfrac{a}{p}\right) = \left(\tfrac{a}{q}\right) = \left(\tfrac{4a}{q}\right) = \left(\tfrac{p-q}{q}\right) = \left(\tfrac{p}{q}\right)$$

2. Let $p \,\%\, 4 = 1$ and $q \,\%\, 4 = 3$, so that $p + q = 4a$. Then
$$\left(\tfrac{q}{p}\right) = \left(\tfrac{p+q}{p}\right) = \left(\tfrac{4a}{p}\right) = \left(\tfrac{a}{p}\right) = \left(\tfrac{a}{q}\right) = \left(\tfrac{4a}{q}\right) = \left(\tfrac{p+q}{q}\right) = \left(\tfrac{p}{q}\right)$$
3. Let $p \,\%\, 4 = 3$ and $q \,\%\, 4 = 1$, so that $p + q = 4a$. Then
$$\left(\tfrac{q}{p}\right) = \left(\tfrac{p+q}{p}\right) = \left(\tfrac{4a}{p}\right) = \left(\tfrac{a}{p}\right) = \left(\tfrac{a}{q}\right) = \left(\tfrac{4a}{q}\right) = \left(\tfrac{p+q}{q}\right) = \left(\tfrac{p}{q}\right)$$
4. Let $p \,\%\, 4 = 3$ and $q \,\%\, 4 = 3$, so that $p - q = 4a$. Then
$$-\left(\tfrac{q}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{q}{p}\right) = \left(\tfrac{-q}{p}\right) = \left(\tfrac{p-q}{p}\right) = \left(\tfrac{4a}{p}\right) = \left(\tfrac{a}{p}\right) = \left(\tfrac{a}{q}\right) = \left(\tfrac{4a}{q}\right) = \left(\tfrac{p-q}{q}\right) = \left(\tfrac{p}{q}\right)$$

Conversely, let us assume the reciprocity law, and suppose that $p \equiv \pm q \pmod{4a}$. To show $\left(\tfrac{a}{p}\right) = \left(\tfrac{a}{q}\right)$, it suffices to consider a a prime number, due to the multiplicative property of the Legendre symbol proved in Exercise 1. Moreover, the case $a = 2$ is already done in Exercise 2, hence we now assume that a is an odd prime. Note that $p \equiv \pm q \pmod{a}$ and $p \equiv \pm q \pmod{4}$, so we consider the four cases again:

1. Let $p \,\%\, 4 = 1$ and $q \,\%\, 4 = 1$, so that $p \equiv q \pmod{a}$. Then
$$\left(\tfrac{a}{p}\right) = \left(\tfrac{p}{a}\right) = \left(\tfrac{q}{a}\right) = \left(\tfrac{a}{q}\right)$$
2. Let $p \,\%\, 4 = 1$ and $q \,\%\, 4 = 3$, so that $p \equiv -q \pmod{a}$. Then
$$\left(\tfrac{a}{p}\right) = \left(\tfrac{p}{a}\right) = \left(\tfrac{-q}{a}\right) = \left(\tfrac{-1}{a}\right)\left(\tfrac{q}{a}\right) = (-1)^{\frac{a-1}{2}}\left(\tfrac{a}{q}\right)(-1)^{\frac{a-1}{2}} = \left(\tfrac{a}{q}\right)$$
3. Let $p \,\%\, 4 = 3$ and $q \,\%\, 4 = 1$, so that $p \equiv -q \pmod{a}$. Then
$$\left(\tfrac{a}{q}\right) = \left(\tfrac{q}{a}\right) = \left(\tfrac{-p}{a}\right) = \left(\tfrac{-1}{a}\right)\left(\tfrac{p}{a}\right) = (-1)^{\frac{a-1}{2}}\left(\tfrac{a}{p}\right)(-1)^{\frac{a-1}{2}} = \left(\tfrac{a}{p}\right)$$
4. Let $p \,\%\, 4 = 3$ and $q \,\%\, 4 = 3$, so that $p \equiv q \pmod{a}$. Then
$$\left(\tfrac{a}{p}\right) = \left(\tfrac{p}{a}\right)(-1)^{\frac{a-1}{2}} = \left(\tfrac{q}{a}\right)(-1)^{\frac{a-1}{2}} = \left(\tfrac{a}{q}\right)(-1)^{\frac{a-1}{2}}(-1)^{\frac{a-1}{2}} = \left(\tfrac{a}{q}\right)$$

Solution 4. The fact that $\cos x$ is an even function while $\sin x$ is odd gives us
$$e^{2\pi ix} - e^{-2\pi ix} = \cos 2\pi x + i \sin 2\pi x - \cos(-2\pi x) - i \sin(-2\pi x) = 2i \sin 2\pi x$$
Hence $f(x) = 0$ if and only if $\sin 2\pi x = 0$, i.e., $2x \in \mathbb{Z}$.

Solution 5. Choose the full system $S = \{\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\}$ modulo p. We know that $x^2 \equiv m \pmod{p}$ has a solution if and only if $m \in \{x^2 \mid x \in S\}$. Since $(\pm x)^2 = x^2$, we can have at most $\frac{p-1}{2}$ quadratic residues. On the other hand, $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ are all distinct modulo p, because with p being a prime, $x^2 \equiv y^2 \pmod{p}$ implies $x \equiv \pm y \pmod{p}$ for any $x, y \in S$. Hence, there are exactly $\frac{p-1}{2}$ quadratic residues.

7 In Memoriam

Fermat	(1601–1665)
Euler	(1707–1783)
Lagrange	(1736–1855)
Legendre	(1752–1833)
Gauss	(1777–1855)
Eisenstein	(1823–1852)