Let $p$ be an odd prime and $\zeta$ be a primitive $p^{th}$-root of unity. For any integer $a$ prime to $p$, let $(\frac{a}{p})$ denote the Legendre symbol, which is 1 if $a$ is a square mod $p$, and is $-1$ otherwise. Using Euler’s Criterion that $a^{(p-1)/2} = (\frac{a}{p}) \mod p$, it follows that the Legendre symbol gives a homomorphism from the multiplicative group of nonzero elements $\mathbb{F}_p^*$ of $F_p = \mathbb{Z}/p\mathbb{Z}$ to $\{\pm 1\}$. Gauss’s law of quadratic reciprocity states that for any other odd prime $q$,

$$(\frac{q}{p})(\frac{p}{q}) = (-1)^{(p-1)(q-1)/4}.$$ 

A table describing the multitude of proofs of this cherished result over the past two centuries is given in Appendix B of [10], which shows that the starting point of many of the proofs (including one of Gauss’s) is the quadratic Gauss sum,

$g = \sum_{a=1}^{p-1} (\frac{a}{p}) \zeta^a.$

and Gauss’s calculation that

$g^2 = (\frac{-1}{p})p.$ \hspace{1cm} (1)

The purpose of this note is to present a variety of proofs of (1) (some well known and others perhaps less so), using techniques from different branches of number theory, each providing its own insight.

Let $\phi(x) = (x^p - 1)/(x - 1) = x^{p-1} + \cdots + 1$. Identifying $x$ with $\zeta$, we can view (1) as an equality in the cyclotomic field $K = \mathbb{Q}[x]/(\phi(x))$. The Galois group $D$ of $K$ over $\mathbb{Q}$ consists of the automorphisms $\{\sigma_b | b \in \mathbb{F}_p^*\}$ of $K$ defined by $\sigma_b(\zeta) = \zeta^b$. By the multiplicativity of the Legendre symbol, if we let $g_b = \sigma_b(g)$, then

$$g_b = \sum_{a=1}^{p-1} (\frac{a}{p}) \zeta^{ab} = (\frac{b}{p}) \sum_{a=1}^{p-1} (\frac{ab}{p}) \zeta^{ab} = (\frac{b}{p})g.$$ 

So it follows that $g^2$ is fixed by $D$ and hence by Galois theory is a rational number. The crux of (1) therefore is in determining which rational number. The “standard” approach to proving (1) is lovely in its own right (see, e.g., [10], Proposition 3.19), and it is hard to find a slicker proof than those given in [7, Proposition 6.3.2] and [3, Theorem 1.14(a)].
A pretty proof of (1) comes from noting that since $\zeta$ is a root of $\phi$, $$0 = \sum_{a=0}^{p-1} \zeta^a.$$ (2)

So, if inspired by Euler’s Criterion, we set $(\frac{a}{p}) = 0$ when $a$ is a multiple of $p$, we then have $$g = \sum_{a=0}^{p-1} (1 + (\frac{a}{p})) \zeta^a = \sum_{b=0}^{p-1} \zeta^{b^2},$$ (3) since $(1 + (\frac{a}{p})) \zeta^a$ is 1 if $a = 0 \mod p$, vanishes if $a$ is not a square mod $p$, and is $\zeta^{b^2} + \zeta^{(-b)^2}$ if $a = b^2 \neq 0 \mod p$. From (3) we get $$gg^{-1} = \sum_{r=0}^{p-1} n_r \zeta^r,$$

where $n_r$ is the number of solutions to $x^2 - y^2 = (x-y)(x+y) = r$ for $x, y \in \mathbb{F}_p$. Since $n_0 = 2p - 1$, and $n_r = p - 1$ for $0 < r < p$, applying (2) now gives $$gg^{-1} = p,$$ (1′)

which is equivalent to (1).

Considerably more difficult than (1) is finding the argument of $g$ as a complex number when we take $\zeta = e^{2\pi i/p}$. Gauss proved that $$g = \sqrt{p} \text{ if } p = 1 \mod 4, \text{ and } g = i\sqrt{p} \text{ if } p = 3 \mod 4.$$ (4)

(Here $\sqrt{p}$ denotes the positive square root of $p$.) Proofs of (4) using the calculus of residues and Fourier analysis are given in [9] and [3] (the definitive survey of the various work on (4) is [2]). There is a particularly lovely proof of (4) by Schur (given in [9]) that uses only linear algebra, which adapts to give a miraculous proof of (1) (see also [12]). Let $S$ be the $p \times p$ matrix whose $ij^{th}$ entry is $\zeta^{ij}$ for $0 \leq i, j < p$. Then, if we let a bar denote complex conjugation, (2) implies that $SS^\dagger$ is $p$ times the identity matrix. Hence, since $S$ is symmetric, $S/\sqrt{p}$ is a unitary matrix, so each of its eigenvalues $\lambda$ has complex absolute value $|\lambda| = 1$. Let $v$ be the column vector whose $a^{th}$ component, for $0 \leq a < p$, is $(\frac{a}{p})$, and $[g(a)]$ be the column vector whose $a^{th}$ component, for $0 \leq a < p$, is $g_a$. Then $$Sv = [g(a)] = gv.$$ Therefore $g/\sqrt{p}$ is an eigenvalue of $S/\sqrt{p}$, and so $$|g|^2 = gg^\dagger = p,$$ (1′′) which is equivalent to (1′) since $\bar{g} = g_{-1}$.

One algebraic number theoretic approach to (1) is to realize that in any field $F$ of characteristic not $p$ containing a primitive $p^{th}$-root of unity $\zeta$, the
group characters $\chi_a: \langle \zeta \rangle \to F^*$ defined by $\chi_a(\zeta) = \zeta^a$ are distinct for $a = 1, ..., p - 1$, and hence by a Theorem of Dedekind [4, Chpt. 14, Thm. 7] are linearly independent functions over $F$. Hence $\sum_{a=1}^{p-1}(\frac{a}{p})\chi_a$ is not identically 0 as a function on $\langle \zeta \rangle$, so for some $b$, $\sum_{a=1}^{p-1}(\frac{a}{p})\chi_a(\zeta^b) = gb \neq 0$ in $F$. Since

$$\sum_{a=1}^{p-1}(\frac{a}{p}) = 0,$$

(the homomorphism from $F_p^*$ to itself given by $x \to x^2$ has kernel $\pm 1$, so has an image which is a subgroup of $F_p^*$ of index 2), necessarily $b \neq 0$. Therefore $g = \pm gb$, and we have $g \neq 0$ in $F$. Now considering $g$ as an element in the ring of integers $\mathbb{Z}[\zeta]$ of $K$, its reduction modulo any maximal ideal $\mathfrak{q}$ of $\mathbb{Z}[\zeta]$ is in a field of characteristic not $p$ that contains a primitive $p^h$-root of unity, so long as $\mathfrak{q}$ is not the ideal $\mathfrak{p}$ generated by $1 - \zeta$ (the lone prime ideal of $\mathbb{Z}[\zeta]$ dividing $p$). Therefore, $g$ is not 0 mod $\mathfrak{q}$ for $\mathfrak{q} \neq \mathfrak{p}$, and on the other hand, by (5), $g$ is 0 mod $\mathfrak{p}$. Hence, $g$ is a unit in $\mathbb{Z}[\zeta]$ times a nontrivial power of $1 - \zeta$. Therefore, $g\bar{g} \in \mathbb{Z}$ is a nontrivial power of $p$. The elementary bound $|g| < p$ then establishes $1''$.

Pedro Berrizbeitia showed us a lovely proof of (1) using that $F_p^*$ is a cyclic group of even order. On the one hand this shows that there is a $b \in F_p^*$ which is not a square, and hence that $D$ is cyclic. Hence $K$ contains a unique quadratic field $L$. Then, since $g \in K$ and $g^2 \in \mathbb{Q}$, $\sigma_b(g) = -g$ means $L = \mathbb{Q}(g)$. From $\rho = \phi(1) = \prod_{i=1}^{(p-1)/2}(\zeta^i - \zeta^{-i})$, an easy manipulation gives that $\rho^2 = (\frac{-1}{p})p$, where $\rho = \prod_{i=1}^{(p-1)/2}(\zeta^i - \zeta^{-i})$. Since $\rho \in K$, this gives that $L = \mathbb{Q}(\rho)$, so $g/\rho$ is a rational number $r$. But $g^2$ is an algebraic integer and hence in $\mathbb{Z}$, so by the unique factorization of integers into the product of primes, $g^2/(\frac{-1}{p})p = r^2$ implies that $r$ is an integer. But $g/r$ is an algebraic integer in $\mathbb{Z}[\zeta]$, and since $g/\zeta$ is a polynomial in $\zeta$ of degree less than $p - 1$ with coefficients of $\pm 1$, this is impossible unless $r = \pm 1$. Then $g^2 = (\frac{-1}{p})pr^2$ gives (1).

To see how analytic number theory aids in our understanding of (1), we can (as in [5]) use the Dirichlet $L$-Series $L(s) = \sum_{n \geq 1}(\frac{n}{p})/n^s$, which (just using $|\langle \frac{a}{p} \rangle| \leq 1$) defines an analytic function where the real part of $s$ is greater than 1. But $L(s)$ has an analytic continuation to the whole complex $s$-plane, and satisfies the functional equation [1, Thm 12.11],

$$L(1-s) = \frac{g^{p-1}\Gamma(s)}{(2\pi)^s}(e^{-\pi is/2} + (\frac{-1}{p})e^{\pi is/2})L(s),$$

where $\Gamma(s)$ is the Gamma function. Note that (6) gives one relation between $L(s)$ and $L(1-s)$, and plugging in $1-s$ for $s$ in (6) gives another. Using these equations to eliminate $L(s)$ and $L(s-1)$, and employing Euler’s reflection formula for the Gamma function, $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$, yields (1). (For references on the analogy (noticed by Jacobi) between this reflection formula and (1), see [10, p. 139].)

An arithmetic geometer might say the “reason” (1) is true is that Hasse and Davenport showed that $-1/g$ is a zero of the congruence zeta function for
the curve $y^p - y = x^2$ defined over $\mathbb{F}_p[6]$, so by Weil’s proof of the Riemann Hypothesis for curves over a finite field [13], $g$ must be an algebraic integer of absolute value $\sqrt{p}$ in every embedding into the complex numbers, i.e., $(1')$ holds.

At the risk of filling the proverbial (and apocryphal [8]) much-needed gap in the literature, we provide one more elementary proof of $(1)$, inspired by the theory of cyclic codes (see [11, Chapter 7]).

If $F$ is a finite field and $n$ is a positive integer, then an $F$-vector subspace $C$ of $F^n$ is called a **linear code of length** $n$, and $C$ is called cyclic if $(x_1, \ldots, x_n) \in C$ implies that $(x_2, \ldots, x_n, x_1) \in C$. Cyclic codes of length $n$ are in one-to-one correspondence with the ideals in $R = F[x]/(x^n - 1)$. When $n = p$ and $F = \mathbb{F}_q$ for some other prime $q$ such that $(\frac{q}{p}) = 1$, an important example of such cyclic codes are the quadratic residue codes, which make use of analogues of Gauss sums in $\mathbb{Q}$. By transporting this circle of ideas to the $\mathbb{Q}$-algebra $A = \mathbb{Q}[x]/(x^p - 1)$, we will get a simple proof to $(1)$.

Of course $A$ is the “wrong ring” in which to work, since it is not a field like $K$ is. However, there is still something of a Galois theory for $A$, which is quite explicit. For any positive integer $b$, since $x^p - 1$ divides $x^b p - 1$, there is a $\mathbb{Q}$-algebra endomorphism $\tau_b$ of $A$ induced by $x \to x^b$, that only depends on $b$ mod $p$. Since $\tau_b \tau_c = \tau_{bc}$, when $b$ is invertible mod $p$, $\tau_b$ is a $\mathbb{Q}$-algebra automorphism of $A$. The map $b \to \tau_b$ then gives an action of $\mathbb{F}_p^*$ on $A$. Let $A_0$ be the sub $\mathbb{Q}$-algebra of $A$ fixed under this action. Since the action is transitive on the set $\{x, x^2, \ldots, x^{p-1}\}$, an element

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_{p-1} x^{p-1} \mod x^p - 1, c_i \in \mathbb{Q}, 1 \leq i \leq p - 1,$$

is fixed if and only if $c_1 = c_2 = \cdots = c_{p-1}$. Hence $A_0$ is spanned as a $\mathbb{Q}$-vector space by $1$ and $\phi(x)$.

Let $G = \sum_{a=1}^{p-1}(\frac{a}{p})x^a$ in $A$. Then $G = g \mod \phi(x)$. Again, by the multiplicativity of the Legendre symbol, $\tau_b(G) = (\frac{b}{p})G$, so $G^2$ lies in $A_0$. Hence, there are rational numbers $m$ and $n$ such that

$$m + n \phi(x) = G^2. \quad (7)$$

Taking $(7)$ mod $\phi(x)$ gives $g^2 = m$. To find $m$, we will now find 2 equations in $m$ and $n$. Using $(5)$ and taking $(7)$ mod $x - 1$ gives

$$m + np = 0. \quad (8)$$

Comparing constant terms in $(7)$ gives

$$m + n = \sum_{a=1}^{p-1}(\frac{a}{p}) \left( \frac{p - a}{p} \right) = \sum_{a=1}^{p-1}(\frac{a}{p}) \left( \frac{-a}{p} \right) = (\frac{-1}{p})(p - 1). \quad (9)$$

(This is the calculation which is easier to do in $A$ than in $K$, and so the motivation for this approach.) Solving $(8)$ and $(9)$ gives $m = (\frac{-1}{p})p$. 

4
References


Department of Mathematics, University of Colorado at Boulder, Boulder, CO 80309–0395
grant@colorado.edu