Squares and Nonsquares mod p

Let $\mathbb{F}_p$ be a field of odd prime order p, i.e. the integers mod p. We write $\mathbb{F}_p^\times$ for the set of nonzero elements of $\mathbb{F}_p$, so that $|\mathbb{F}_p^\times| = p-1$. A *square* in $\mathbb{F}_p$ is an element of the form b^2 for some $b \in \mathbb{F}_p^\times$. Such an element has exactly two square roots since the solutions of $x^2 = b^2$ satisfy

$$0 = x^2 - b^2 = (x+b)(x-b) \ \Rightarrow\ x = \pm b.$$

It follows that the map $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto x^2$ is exactly two-to-one, so $\mathbb{F}_p^\times$ has exactly $\frac{p-1}{2}$ squares and (by process of elimination) also $\frac{p-1}{2}$ nonsquares. The *Legendre symbol* is defined for every integer a and odd prime p, by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } a \equiv 0 \mod p; \\ 1, & \text{if } a \text{ is a nonzero square mod } p; \\ -1, & \text{if } a \text{ is a nonsquare mod } p. \end{cases}$$

(Squares and nonsquares are also called quadratic residues and nonquadratic residues; but unfortunately the latter is often abbreviated to nonresidues, a misnomer. We will simply speak of squares and nonsquares.) The strict definition of the Legendre symbol usually excludes the case $a \equiv 0$ mod p; but a natural generalization of $\left(\frac{a}{p}\right)$ called the *Jacobi symbol* allows this case, and so do we.

By Fermat's Little Theorem, every $a \in \mathbb{F}_p$ is a root of the polynomial

$$x^p - x \ =\ x\big(x^{\frac{p-1}{2}} - 1\big)\big(x^{\frac{p-1}{2}} + 1\big) \ \in\ \mathbb{F}_p[x].$$

Every square in $\mathbb{F}_p^\times$ is a root of the second factor $x^{\frac{p-1}{2}} - 1$ since

$$(b^2)^{\frac{p-1}{2}} - 1 \ =\ b^{p-1} - 1 \ =\ 0$$

whenever $b \in \mathbb{F}_p^\times$; so by process of elimination, the roots of $x^{\frac{p-1}{2}} + 1$ are precisely the nonsquares. This gives Euler's Criterion:

$$(1) \qquad \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \text{ mod } p \text{ for every integer } a.$$

An immediate consequence of (1) is the multiplicativity of the Legendre symbol: $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{(p-1)/2}b^{(p-1)/2} \equiv (ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right)$ mod p, so

$$(2) \qquad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \text{ for all integers } a, b.$$

The formula (1) is most useful in computer calculation of the Legendre symbol; when working by hand with smaller examples of two or three digits, a more convenient approach is the following:

Theorem. Let p and q be distinct odd primes. Then

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

(ii) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \mod 8; \\ -1, & \text{if } p \equiv \pm 3 \mod 4; \end{cases}$

(iii) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} = \begin{cases} 1, & \text{if \textit{at least one} of } p, q \text{ is} \equiv 1 \mod 4; \\ -1, & \text{if } p \equiv q \equiv 3 \mod 4. \end{cases}$

Part (iii) is properly known as the*Law of Quadratic Reciprocity*; and we include (i) and (ii) for completeness. There are currently hundreds of proofs of this result known—probably more proofs than any result other than the Theorem of Pythagoras. A current census lists 246 distinct proofs:

`http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html`

Gauss himself gave many different proofs; and the proof we give here is his sixth proof, although it has been rediscovered by many others since then. In order to prove this result, we first note that

$$(3) \qquad \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \;=\; \left(\frac{0}{p}\right) + \left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) \;=\; 0$$

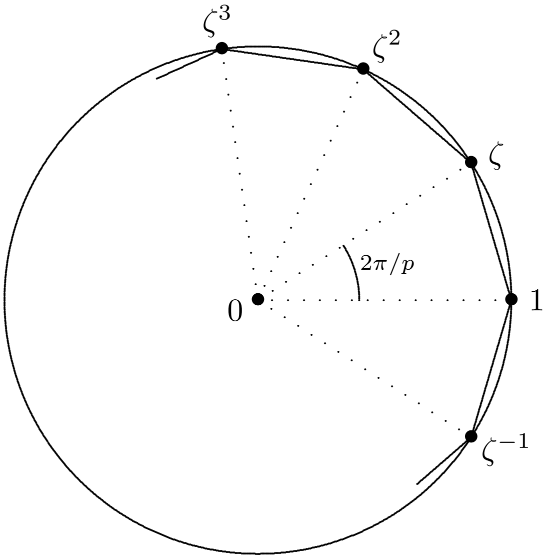
since the sum includes one 0 term, $\frac{p-1}{2}$ terms equal to $+1$, and $\frac{p-1}{2}$ terms equal to -1. Next we consider the factorization

$$(4) \qquad \begin{aligned} z^p - 1 &= (z-1)(z^{p-1} + z^{p-2} + \cdots + z + 1) \\ &= (z-1)(z-\zeta)(z-\zeta^2)\cdots(z-\zeta^{p-1}) \end{aligned}$$

where $\zeta = e^{2\pi i/p}$ is a p-th root of unity in $\mathbb{C}$. By (4), ζ is a root of the polynomial $z^{p-1} + z^{p-2} + \cdots + z + 1$, i.e.

$$(5) \qquad 1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} = 0.$$

Alternatively, (5) follows from the fact that $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$ are the vertices of a regular p-gon inscribed in the unit circle in $\mathbb{C}$, so that (5) follows by symmetry, considering $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$ as unit vectors in the plane symmetrically arranged about the origin:



More generally, if $a \not\equiv 0 \mod p$ then

$$\text{(5a)} \qquad 1 + \zeta^a + \zeta^{2a} + \cdots + \zeta^{(p-1)a} = 0$$

since $0, a, 2a, \ldots, (p-1)a$ are congruent to $0, 1, 2, \ldots, p-1 \mod p$ in some order.

Gauss considered sums of the form

$$\text{(6)} \qquad S = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \zeta^k = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k;$$

thus for example $S = \zeta - \zeta^2 - \zeta^3 + \zeta^4$ when $p = 5$. Sums of the form (6) are called *quadratic Gauss sums*. Gauss himself proved

Lemma. $S^2 = \left(\frac{-1}{p}\right) p = \begin{cases} p, & \text{if } p \equiv 1 \mod 4; \\ -p, & \text{if } p \equiv 3 \mod 4. \end{cases}$

Proof.

$$\begin{aligned}
S^2 &= \left[\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta^k\right]\left[\sum_{\ell=0}^{p-1}\left(\frac{\ell}{p}\right)\zeta^\ell\right] \\
&= \sum_{k=1}^{p-1}\sum_{\ell=0}^{p-1}\left(\frac{k}{p}\right)\left(\frac{\ell}{p}\right)\zeta^{k+\ell} \\
&= \sum_{k=1}^{p-1}\sum_{\ell=0}^{p-1}\left(\frac{k\ell}{p}\right)\zeta^{k+\ell} \qquad \text{(by (2))} \\
&= \sum_{k=1}^{p-1}\sum_{m=0}^{p-1}\left(\frac{k^2m}{p}\right)\zeta^{k+km} \qquad \text{(substituting } \ell = km\text{)} \\
&= \sum_{k=1}^{p-1}\sum_{m=0}^{p-1}\left(\frac{m}{p}\right)\zeta^{(1+m)k} \\
&= \sum_{m=0}^{p-1}\left(\frac{m}{p}\right)\left[\sum_{k=1}^{p-1}\zeta^{(1+m)k}\right].
\end{aligned}$$

Now if $m \neq p{-}1$ then the inner sum $\sum_{k=1}^{p-1}\zeta^{(1+m)k} = -1$ by (5a), whereas if $m = p{-}1$ we have $\sum_{k=1}^{p-1}\zeta^{(1+m)k} = \sum_{k=1}^{p-1} 1 = p{-}1$. This leaves

$$\begin{aligned}
S^2 &= -\sum_{m=0}^{p-2}\left(\frac{m}{p}\right) + \left(\frac{p-1}{p}\right)(p-1) \\
&= \left(\frac{p-1}{p}\right) + \left(\frac{p-1}{p}\right)(p-1) \qquad \text{by (3)} \\
&= \left(\frac{p-1}{p}\right)p.
\end{aligned}$$

□

By the Lemma,

$$S = \begin{cases} \pm\sqrt{p}, & \text{if } p \equiv 1 \mod 4, \\ \pm i\sqrt{p}, & \text{if } p \equiv 3 \mod 4. \end{cases}$$

The question of resolving the ambiguous signs in this formula is an obvious problem, and one which perplexed Gauss for years before finally the answer came to him. As Gauss wrote to a friend in 1805:

> The determination of the sign of the root has vexed me for many years. This deficiency overshadowed everything that I found: over the last four years, there was rarely a week that I did not make one or another attempt, unsuccessfully, to untie the knot. I succeeded—but not as a result of my search but rather, I should say, through the mercy of God. As lightning strikes, the riddle has solved itself.

The precise result, as Gauss showed, has '+' in place of each of the signs '±' above; however for our purposes the less explicit version of the Lemma above suffices.

Before proceeding further, we need to recall another fact usually presented in Math 3500 or 4510:

(7) For every prime q, $(x+y)^q \equiv x^q + y^q \bmod q$.

This follows from the binomial expansion

$$(x+y)^q = x^q + qx^{q-1}y + \frac{q(q-1)}{2}x^{q-2}y^2 + \cdots + qxy^{q-1} + y^q$$

since the coefficient of $x^{q-k}y^k$ is $\binom{q}{k} = \frac{q!}{k!(q-k)!}$ which has a factor of q in the numerator and no factors of q in the denominator to cancel it, for $k = 1, 2, \ldots, q-1$. The relation (7) is to be understood as a congruence in the ring $\mathbb{Z}[x,y]$ of all polynomials in x and y with integer coefficients; and it is often refered to as *Freshman's Dream*.

We are ready to proceed with the proof of the Law of Quadratic Reciprocity. Let p, q be distinct odd primes, and consider the Gauss sum $S = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right)\zeta^k$ as in (6), where $\zeta = e^{2\pi i/p}$ as in (4). Taking the $\frac{q-1}{2}$ power of the relation in the Lemma gives

$$S^{q-1} \;=\; (S^2)^{(q-1)/2} \;=\; \left(\frac{-1}{p}\right)^{(q-1)/2} p^{(q-1)/2} \;\equiv\; (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right) \bmod q.$$

Multiplying both sides by S gives

$$\begin{aligned}
(-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)S &\equiv S^q \\
&\equiv \sum_{k=0}^{q-1}\left(\frac{k}{p}\right)^q \zeta^{qk} \quad \text{(by (7))} \\
&\equiv \sum_{k=0}^{q-1}\left(\frac{k}{p}\right)\zeta^{qk} \quad \text{(since } q \text{ is odd)} \\
&\equiv \sum_{k=0}^{q-1}\left(\frac{kq^2}{p}\right)\zeta^{qk} \quad \text{(since } q \text{ is odd)} \\
&\equiv \sum_{\ell=0}^{q-1}\left(\frac{\ell q}{p}\right)\zeta^{\ell} \quad \text{(substituting } \ell = kq\text{)} \\
&\equiv \sum_{\ell=0}^{q-1}\left(\frac{\ell}{q}\right)\left(\frac{q}{p}\right)\zeta^{\ell} \quad \text{(by (2))} \\
&\equiv \left(\frac{q}{p}\right)S \bmod q.
\end{aligned}$$

Again we multiply both sides by S to obtain

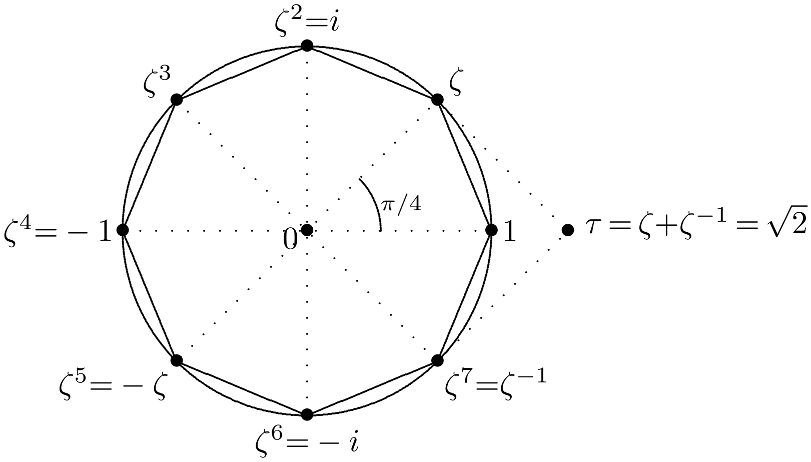
$$(-1)^{(p-1)(q-1)/4}\Big(\frac{p}{q}\Big)S^2 \;\equiv\; \Big(\frac{q}{p}\Big)S^2 \mod q$$

and since $S^2 = \big(\frac{-1}{p}\big)p$, which is an integer relatively prime to q, this gives

$$(-1)^{(p-1)(q-1)/4}\Big(\frac{p}{q}\Big) \;\equiv\; \Big(\frac{q}{p}\Big) \mod q.$$

All factors on both sides of this expression are ±1 so this gives part (iii) of the Theorem.

Part (i) of the Theorem follows immediately from Euler's Criterion (2). Although we have given a proof of (ii), here is a faster proof, also using roots of unity. This time we let $\zeta = e^{\pi i/4} = \frac{1+i}{\sqrt{2}}$, an eighth root of unity in $\mathbb{C}$; and let $\tau = \zeta + \zeta^{-1} = \sqrt{2}$.



By Euler's Criterion (1),

$$\Big(\frac{2}{p}\Big) \;\equiv\; 2^{(p-1)/2} \;\equiv\; \tau^{p-1} \mod p$$

so by (7),

$$\Big(\frac{2}{p}\Big)\tau \;\equiv\; \tau^p \equiv (\zeta + \zeta^{-1})^p \;\equiv\; \zeta^p + \zeta^{-p} \mod p.$$

Since ζ is an eighth root of unity, we obtain

$$\Big(\frac{2}{p}\Big)\tau \;\equiv\; (-1)^{(p^2-1)/8}\tau \mod p$$

where

$$(-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \mod 8; \\ -1, & \text{if } p \equiv \pm 3 \mod 8. \end{cases}$$

Multiplying both sides by τ gives $2\left(\frac{2}{p}\right) \equiv (-1)^{(p^2-1)/8}2 \mod p$; and since 2 is relatively prime to p, (ii) follows.

In our proofs of (ii) and (iii), we swept one detail under the rug: we are working not in $\mathbb{Z}$ but in the larger ring

$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-2}\zeta^{p-2} \ : \ a_0, a_1, \ldots, a_{p-2} \in \mathbb{Z}\}.$$

However for our proofs, not much specialized knowledge of $\mathbb{Z}[\zeta]$ is required; all that one needs is the fact that if $a, b \in \mathbb{Z}$ satisfy $a \equiv b \mod p$ in $\mathbb{Z}[\zeta]$, then $a \equiv b \mod p$ in $\mathbb{Z}$. This however follows from $\mathbb{Z} \cap p\mathbb{Z}[\zeta] = p\mathbb{Z}$, which is easily verified.