Quadratic reciprocity

Robin Chapman
8 December 2003

Let $p$ be an odd prime number. We consider which numbers $a \neq 0$ are squares modulo $p$. If $a \equiv b^2$ then $a \equiv (-b)^2$ and as $b \neq -b \pmod{p}$ then $x^2 \equiv a \pmod{p}$ has precisely the two solutions $x \equiv \pm b \pmod{p}$. It follows that there are exactly $\frac{1}{2}(p-1)$ such $a$ up to congruence modulo $p$, which are $1^2, 2^2, \ldots, \left[\frac{1}{2}(p-1)\right]^2$. These are the quadratic residues modulo $p$. The $\frac{1}{2}(p-1)$ remaining values modulo $p$, for which the congruence $x^2 \equiv a \pmod{p}$ is insoluble are the quadratic nonresidues modulo $p$. We define the Legendre symbol $\left(\frac{a}{p}\right)$ as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

The Legendre symbol $\left(\frac{a}{p}\right)$ depends only on $a$ modulo $p$, that is,

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \quad \text{whenever } a \equiv b \pmod{p}.$$

**Theorem 1 (Euler’s criterion)** Let $p$ be an odd prime and let $a \in \mathbb{Z}$. Then

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

**Proof** If $p \mid a$ then both sides of $(\ast)$ are zero modulo $p$. We may thus suppose that $p \nmid a$. Let $g$ be a primitive root modulo $p$. Then $g^{(p-1)/2} \not\equiv 1 \pmod{p}$ but $[g^{(p-1)/2}]^2 = g^{p-1} \equiv 1 \pmod{p}$. It follows that $g^{(p-1)/2} \equiv -1 \pmod{p}$. Now $a \equiv g^k \pmod{p}$ for some integer $k \geq 0$ and so

$$a^{(p-1)/2} \equiv g^{k(p-1)/2} \equiv [g^{(p-1)/2}]^k \equiv (-1)^k \equiv \begin{cases} 1 & \text{if } k \text{ is even}, \\ -1 & \text{if } k \text{ is odd.} \end{cases}$$
Let us attempt to solve the congruence $x^2 \equiv a \equiv g^k \pmod{p}$. The solution must have the form $x \equiv g^r \pmod{p}$ and so $g^{2r} \equiv g^k \pmod{p}$. This is equivalent to the congruence $2r \equiv k \pmod{p-1}$. As $2 \mid (p-1)$ this linear congruence is soluble if and only if $k$ is even. Hence if $a$ is a quadratic residue then $k$ is even and $a^{(p-1)/2} \equiv 1 = \left(\frac{a}{p}\right)$, while if $a$ is a quadratic nonresidue then $k$ is odd and $a^{(p-1)/2} \equiv -1 = \left(\frac{a}{p}\right)$. \hfill \Box

**Corollary 1** Let $p$ be an odd prime, and let $a, b \in \mathbb{Z}$. Then

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

In particular if $a$ and $b$ are both quadratic residues modulo $p$ or both quadratic nonresidues modulo $p$, then $ab$ is a quadratic residue modulo $p$, while if one of $a$ and $b$ is a quadratic residue modulo $p$ and the other is a quadratic nonresidue modulo $p$, then $ab$ is a quadratic nonresidue modulo $p$.

**Proof** By Euler’s criterion

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

Both sides of this congruence lie in the set $\{-1, 0, 1\}$ and as $p \geq 3$ no two distinct elements of this set are congruent modulo $p$. Hence we have equality, not just congruence:

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

\hfill \Box

**Corollary 2** Let $p$ be an odd prime. Then

$$\left(\frac{-1}{p}\right) = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{4}, \\
-1 & \text{if } p \equiv 3 \pmod{4}.
\end{cases}$$

**Proof** By Euler’s criterion

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

If $p \equiv 1 \pmod{4}$ then $(p-1)/2$ is even, and so $\left(\frac{-1}{p}\right) \equiv 1 \pmod{p}$; consequently $\left(\frac{-1}{p}\right) = 1$. If $p \equiv 3 \pmod{4}$ then $(p-1)/2$ is odd, and so $\left(\frac{-1}{p}\right) \equiv -1 \pmod{p}$; consequently $\left(\frac{-1}{p}\right) = -1$. \hfill \Box

We now prove Gauss’s lemma, which gives a useful if opaque characterization of the Legendre symbol.
Theorem 2 (Gauss’s lemma) Let $p$ be an odd prime and let $a$ be an integer coprime to $p$. Let $R = \{ j \in \mathbb{N} : 0 < j < p/2 \}$ and $S = \{ j \in \mathbb{N} : p/2 < j < p \}$. Then $\left( \frac{a}{p} \right) = (-1)^\mu$ where $\mu$ is the number of $j \in R$ for which the least nonnegative residue of $aj$ modulo $p$ lies in $S$.

**Proof** It is convenient to introduce some notation. If $m$ is an integer, it is congruent modulo $p$ to exactly one integer between $-p/2$ and $p/2$. Let $\langle m \rangle$ denote this integer: that is, $\langle m \rangle \equiv m \pmod{p}$ and $|\langle m \rangle| < p/2$. Then $m$ is congruent modulo $p$ to an element of $S$ if and only if $\langle m \rangle < 0$.

We consider the numbers $\langle aj \rangle$ for $j \in R$. Then $\mu$ is the number of $j \in R$ for which $\langle aj \rangle < 0$. Let us write $\langle aj \rangle = \varepsilon_j b_j$ where $\varepsilon_j = \pm 1$ and $b_j = \langle \langle aj \rangle \rangle$. Then $(-1)^\mu = \prod_{j=1}^{(p-1)/2} \varepsilon_j$. I claim that the numbers $b_1, \ldots, b_{(p-1)/2}$ are the same as the numbers in $R$ in some order. Certainly $b_j \neq 0$ for if $b_j = 0$ then $p \mid aj$ contrary to Euclid’s lemma ($p \nmid a$ and $p \nmid j$). Suppose there were integers $j$ and $k$ with $0 < j < k < p/2$ and $b_j = b_k$. Then $ak \equiv \varepsilon_k b_k = \varepsilon_j b_j \equiv \varepsilon_j \varepsilon_k a_j \pmod{p}$. So $p \mid a(k \pm j)$ and as $p \nmid a$ then $p \mid (k \pm j)$. But $0 < k + j < p$ and $0 < k - j < p/2$. Neither $k + j$ nor $k - j$ is a multiple of $p$. This contradiction shows that all the $b_j$ are distinct, and so the $b_j$ are the elements of $R$ in some order.

It follows that $\prod_{j=1}^{(p-1)/2} b_j = \left( \frac{1}{2} (p - 1) \right)!$ and so

$$a^{(p-1)/2} \left( \frac{p - 1}{2} \right)! = \prod_{j=1}^{(p-1)/2} (aj) \equiv \prod_{j=1}^{(p-1)/2} (\varepsilon_j b_j) = (-1)^\mu \left( \frac{p - 1}{2} \right)! \pmod{p}. $$

As $\left( \frac{1}{2} (p - 1) \right)!$ is coprime to $p$, we may cancel it and get $a^{(p-1)/2} \equiv (-1)^\mu \pmod{p}$. Applying Euler’s criterion gives $\left( \frac{a}{p} \right) = (-1)^\mu$. $\square$

In the proof of the following theorem, we adopt the following notation. If $x < y$ then $N(x, y)$ denotes the number of integers $n$ with $x < n < y$. It is useful to note several simple properties of $N(x, y)$.

- $N(x, y) = N(-y, -x)$;
- if $a$ is an integer, then $N(x + a, y + a) = N(x, y)$;
- if $a$ is a positive integer, then $N(x, y + a) = N(x, y) + a$;
- if $a$ is a positive integer, and $x$ is not an integer, then $N(x, x + a) = a$;
- if $x < y < z$ and $y$ is not an integer, then $N(x, z) = N(x, y) + N(y, z)$.

The proofs of all of these are straightforward, and left as exercises.
Theorem 3 Let $a \in \mathbb{N}$, and let $p$ and $q$ be distinct odd primes, each coprime to $a$. If $q \equiv \pm p \pmod{4a}$ then \( \left( \frac{a}{q} \right) = \left( \frac{a}{p} \right) \).

Proof By Gauss’s lemma, \( \left( \frac{a}{p} \right) = (-1)^{\mu} \) where $\mu$ is the number of integers $j \in (0, p/2)$ and with $aj$ having least positive residue modulo $p$ in the interval $(p/2, p)$. If $0 < j < p/2$ then $0 < aj < ap/2$ and so $\mu$ is the number of integers $j$ with

$$aj \in \bigcup_{k=1}^{b} \left( \left( k - \frac{1}{2} \right) p, kp \right)$$

where $b = a/2$ or $b = (a - 1)/2$ according to whether $b$ is even or $b$ is odd. Hence $\mu$ is the number of integers in the set

$$\bigcup_{k=1}^{b} \left( \frac{(2k-1)p}{2a}, \frac{kp}{a} \right),$$

that is

$$\mu = \sum_{k=1}^{b} N \left( \frac{(2k-1)p}{2a}, \frac{kp}{a} \right).$$

Similarly \( \left( \frac{a}{q} \right) = (-1)^{\nu} \) where

$$\nu = \sum_{k=1}^{b} N \left( \frac{(2k-1)q}{2a}, \frac{kq}{a} \right).$$

Suppose first that $q \equiv p \pmod{4a}$. Without loss of generality, $q > p$, and we may write $q = p + 4ar$ with $r \in \mathbb{N}$. Then

$$\nu = \sum_{k=1}^{b} N \left( \frac{(2k-1)p}{2a} + (4k-2)r, \frac{kp}{a} + 4kr \right)$$

$$= \sum_{k=1}^{b} N \left( \frac{(2k-1)p}{2a} + 2r, \frac{kp}{a} + 2r \right)$$

$$= \sum_{k=1}^{b} \left[ N \left( \frac{(2k-1)p}{2a}, \frac{kp}{a} \right) + 2r \right]$$

$$= \mu + 2rb.$$ Consequently

$$\left( \frac{a}{q} \right) = (-1)^{\nu} = (-1)^{\mu + 2rb} = (-1)^{\mu} = \left( \frac{a}{p} \right).$$
Now suppose that \( q \equiv -p \pmod{4} \). Then \( p + q = 4as \) with \( s \) an integer. Thus

\[
\nu = \sum_{k=1}^{b} N\left(\frac{(4k-2)s - \frac{(2k-1)p}{2a}, 4ks - \frac{kp}{a}}{2a}\right)
\]

\[
= \sum_{k=1}^{b} N\left(\frac{kp}{a} - 4ks, \frac{(2k-1)p}{2a} - (4k-2)s\right)
\]

\[
= \sum_{k=1}^{b} N\left(\frac{kp}{a}, \frac{(2k-1)p}{2a} + 2s\right).
\]

Hence

\[
\mu + \nu = \sum_{k=1}^{b} \left[ N\left(\frac{(2k-1)p}{2a}, \frac{kp}{a}\right) + N\left(\frac{kp}{a}, \frac{(2k-1)p}{2a} + 2s\right)\right]
\]

\[
= \sum_{k=1}^{b} N\left(\frac{(2k-1)p}{2a}, \frac{(2k-1)p}{2a} + 2s\right)
\]

\[
= 2sb.
\]

Consequently

\[
\left(\frac{a}{q}\right) = (-1)^\nu = (-1)^{-\mu + 2sk} = (-1)^\mu = \left(\frac{a}{p}\right).
\]

We can now prove the law of quadratic reciprocity

**Theorem 4 (Quadratic reciprocity)** Let \( p \) and \( q \) be distinct odd primes. Then

\[
\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)
\]

unless \( p \equiv q \equiv 3 \pmod{4} \) in which case

\[
\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).
\]

**Proof** Suppose first that \( p \equiv q \pmod{4} \). Without loss of generality, \( q > p \) so that \( q = p + 4a \) with \( a \in \mathbb{N} \). Then

\[
\left(\frac{q}{p}\right) = \left(\frac{p + 4a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{a}{p}\right)
\]

\[
\left(\frac{a}{p}\right)
\]
and
\[
\left( \frac{p}{q} \right) = \left( \frac{q - 4a}{q} \right) = \left( \frac{-4a}{q} \right) = \left( \frac{-1}{q} \right) \left( \frac{a}{q} \right).
\]

By Theorem 3
\[
\left( \frac{a}{p} \right) = \left( \frac{a}{q} \right)
\]
and then
\[
\left( \frac{q}{p} \right) = \left( \frac{-1}{q} \right) \left( \frac{a}{q} \right).
\]

Thus if \( p \equiv q \equiv 1 \) (mod 4) then
\[
\left( \frac{q}{p} \right) = \left( \frac{-1}{q} \right) \left( \frac{p}{q} \right) = \left( \frac{p}{q} \right)
\]
while if \( p \equiv q \equiv 3 \) (mod 4) then
\[
\left( \frac{q}{p} \right) = \left( \frac{-1}{q} \right) \left( \frac{p}{q} \right) = - \left( \frac{p}{q} \right).
\]

Now suppose that \( p \equiv -q \) (mod 4). Then \( p + q = 4a \) with \( a \in \mathbb{N} \). Then
\[
\left( \frac{q}{p} \right) = \left( \frac{4a - p}{p} \right) = \left( \frac{4a}{p} \right) = \left( \frac{a}{p} \right)
\]
and
\[
\left( \frac{p}{q} \right) = \left( \frac{4a - q}{q} \right) = \left( \frac{4a}{q} \right) = \left( \frac{a}{q} \right).
\]

By Theorem 3
\[
\left( \frac{a}{p} \right) = \left( \frac{a}{q} \right)
\]
and then
\[
\left( \frac{q}{p} \right) = \left( \frac{p}{q} \right).
\]

When applying quadratic reciprocity, it is useful to have a version involving the Jacobi symbol. This is denoted by \( (\frac{a}{n}) \), like the Legendre symbol, but in the Legendre symbol the number \( n \) must be an odd prime, in the Jacobi symbol \( n \) can be any positive odd integer and \( a \) any integer at all. We define the Jacobi symbol as follows: if \( n \) is a positive odd integer, write \( n = p_1 \ldots p_k \) with the \( p_j \) prime. Then set
\[
(\frac{a}{n}) = \prod_{j=1}^{k} (\frac{a}{p_j}).
\]
It is immediate that the Jacobi symbol shares some of the formal properties of the Legendre symbol:

- \((\frac{a}{n}) = \pm 1\) if \(a\) and \(n\) are coprime and \((\frac{a}{n}) = 0\) otherwise,
- \((\frac{a}{n}) = (\frac{b}{n})\) whenever \(a \equiv b \pmod{n}\),
- \((\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})\) and \((\frac{a}{mn}) = (\frac{a}{m})(\frac{a}{n})\).

The most convenient property is that quadratic reciprocity is true for the Jacobi symbol too. Let \(m\) and \(n\) be coprime odd positive integers. Write \(m = p_1 \cdots p_r\) and \(n = q_1 \cdots q_s\) where the \(p_j\) and \(q_k\) are primes. By quadratic reciprocity,

\[
(\frac{m}{n}) = \prod_{j=1}^{r} \prod_{k=1}^{s} (\frac{p_j}{q_k}) = \prod_{j=1}^{r} \prod_{k=1}^{s} \varepsilon_{j,k} (\frac{q_k}{p_j}) = (-1)^\mu (\frac{n}{m})
\]

where \(\varepsilon_{j,k} = 1\) unless \(p_j \equiv q_j \equiv 3 \pmod{4}\) in which case \(\varepsilon_{j,k} = -1\) and \(\mu\) is the number of pairs \((j, k)\) with \(\varepsilon_{j,k} = -1\). But \(\mu = ab\) where \(a\) is the number of \(p_j\) which are 3 modulo 4 and \(b\) is the number of \(q_k\) which are 3 modulo 4. Then \(m \equiv 3^a \equiv (-1)^a \pmod{4}\) and \(n \equiv 3^b \equiv (-1)^b \pmod{4}\). Then \((-1)^{ab} = 1\) unless both \(a\) and \(b\) are odd when \((-1)^\mu = -1\). Thus \((-1)^\mu = -1\) if and only if \(m \equiv n \equiv 3 \pmod{4}\):

\[
(\frac{m}{n}) = (\frac{n}{m})
\]

unless \(m \equiv n \equiv 3 \pmod{4}\) in which case

\[
(\frac{m}{n}) = - (\frac{n}{m}).
\]

(This even holds when \(m\) and \(n\) are non-coprime positive odd integers, for then both sides are zero.)