**Quadratic Reciprocity**

To be able to determine the quadratic character of an arbitrary number mod $p$ ($p$ an odd prime), we need to be able to evaluate $\left( \frac{q}{p} \right)$ for any prime $q$.

The first (and most delicate) case concerns $\left( \frac{2}{p} \right)$.

**Proposition** Let $p$ be an odd prime.

(1) $p \equiv 1 \pmod{8} \Rightarrow \left( \frac{-2}{p} \right) = 1$

(2) $p \equiv \pm 3 \pmod{8} \Rightarrow \left( \frac{2}{p} \right) = -1$

(3) $p \equiv -1 \pmod{8} \Rightarrow \left( \frac{-2}{p} \right) = -1$

**Proof** (1) Let $p = 8k + 1$. By FLT, $x^{8k} - 1 \equiv (x^{4k} - 1)(x^{4k} + 1) \equiv 0 \pmod{p}$ has $8k$ solutions, whence by Lagrange’s Theorem, each of the factor polynomials $x^{4k} \pm 1 \equiv 0 \pmod{p}$ must have $4k$ solutions. Since $k$ must be positive, there must exist some integer $a$ (necessarily prime to $p$) that satisfies $a^{4k} + 1 \equiv 0 \pmod{p}$. But then

$$ (a^{2k} - 1)^2 + 2(a^k)^2 \equiv a^{4k} + 1 \equiv 0 \pmod{p}, $$
so \((a^{2k} - 1)^2 \equiv -2(a^k)^2 \) (mod \(p\)). Multiplication (twice) by the inverse of \(a^k\) yields \((a^{2k} - 1)(a^k)^{-1}\)^2 \equiv -2 \) (mod \(p\)), whence \(-2\) is a quadratic residue.

(2) If \(p \equiv \pm 3 \) (mod \(8\)) but \(2\) is a quadratic residue mod \(p\), then there must be an integer \(a\) \((0 < a < p)\) which satisfies the congruence \(x^2 \equiv 2\) (mod \(p\)). Indeed, we may assume that \(a\) is odd, else we can replace \(a\) with \(p - a\), which also satisfies this congruence and must have opposite parity from \(a\). Then \(a^2 - 2 = pk\) for some odd number \(k\). As \(pk = a^2 - 2 < a^2 < p^2\), it follows that \(k < p\). Now, for any prime factor \(q\) of \(k\) — which is also smaller than \(p\) — we must have \(a^2 \equiv 2\) (mod \(q\)). If \(q \equiv \pm 3\) (mod \(8\)), then we can apply this same argument to find an even smaller prime for which \(2\) is a quadratic residue; by this process, eventually we must come to the smallest prime congruent to \(\pm 3\) (mod \(8\)) for which \(2\) is a quadratic residue. For simplicity, let us suppose it was \(p\) itself. Then every prime factor \(q\) of \(k\) referred to above is not congruent to \(\pm 3\) (mod \(8\)). So \(q \equiv \pm 1\) (mod \(8\)) for all such \(q\), whence \(k \equiv \pm 1\) (mod \(8\)) as well. Therefore, \(a^2 - 2 \equiv pk \equiv \pm 3 \cdot \pm 1 \equiv \pm 3\) (mod \(8\)) \(\Rightarrow a^2 \equiv 5, -1\) (mod \(8\)). But this is impossible, since neither \(5\) nor \(-1\) is a quadratic residue mod \(8\). This contradiction shows that \(2\) must be a quadratic nonresidue mod \(p\).
(3) As in the argument in (2) above, assume that $p = -1 \pmod{8}$ but that $-2$ is a quadratic residue mod $p$; then there must be an integer $a$ $(0 < a < p)$ which satisfies the congruence $x^2 \equiv -2 \pmod{p}$ and is odd (else we can replace it with $p - a$). As before, $a^2 + 2 = pk$ for some odd $k$. As $pk = a^2 + 2 < (p - 1)^2 - 2 < p^2$, it follows that $k < p$. Thus, for any prime factor $q$ of $k$ — which must be smaller than $p$ — we must have $a^2 \equiv -2 \pmod{q}$. We may assume that $p$ is the smallest prime factor of $a^2 + 2$ of the form $8k - 1$, else we can transfer this argument to whichever prime does satisfy this property. So we have that every prime factor $q$ of $k$ referred to above is not congruent to $-1 \pmod{8}$. If $q \equiv -3 \pmod{8}$, then $a^2 \equiv -2 \pmod{q} \Rightarrow \left( \frac{-2}{q} \right) = 1$, but $\left( \frac{-1}{q} \right) = q \equiv 1 \pmod{4}$, so $\left( \frac{2}{q} \right) = \left( \frac{-1}{q} \right) \left( \frac{-2}{q} \right) = 1$, contradicting (2) above. So it must be that $q \equiv 1$ or $3 \pmod{8}$. But the product of primes of this type is also of this type, so $k \equiv 1$ or $3 \pmod{8}$ and it follows that $a^2 + 2 = pk \equiv (-1)k \equiv -1$ or $-3 \pmod{8}$. But then $a^2 \equiv -3, -5 \equiv \pm 3 \pmod{8}$, which is impossible since $3$ and $-3$ are both quadratic nonresidues mod $8$. //
**Corollary** If $p$ is an odd prime, \( \left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8} \).

**Proof** Left as an exercise. //

There are a number of interesting consequences that flow from knowing the quadratic character of $2$ mod $p$.

**Corollary** There are infinitely many primes $p \equiv 3 \pmod{8}$.

**Proof** Suppose there are only finitely many, namely the primes $p_1, p_2, \ldots, p_k$. Let $N = (p_1 p_2 \cdots p_k)^2 + 2$. Then any prime $q$ that divides $N$ satisfies $(p_1 p_2 \cdots p_k)^2 + 2 \equiv 0 \pmod{q}$, whence $-2$ is a quadratic residue mod $q$. It follows that $q \equiv 1$ or $3 \pmod{8}$. If all the prime factors of $N$ were of the form $q \equiv 1 \pmod{8}$, then $N \equiv 1 \pmod{8}$, but this would mean that $(p_1 p_2 \cdots p_k)^2 + 2 \equiv 1 \pmod{8} \Rightarrow (p_1 p_2 \cdots p_k)^2 \equiv -1 \pmod{8}$, contradicting that $-1$ is a quadratic nonresidue mod $8$. So at least one of the prime factors $q$ of $N$, which is necessarily not one of $p_1, p_2, \ldots, p_k$, must be congruent to $3 \pmod{8}$, contradicting the fact that we had already listed all primes of this type among the $p$’s. //
**Corollary** Let $p$ be a Germain prime, i.e., a prime for which $q = 2p + 1$ is also prime (named after Sophie Germain, 1776-1831, a student of Gauss and Legendre). If also $p > 3$ and $p \equiv 3 \pmod{4}$, then the Mersenne number $M_p = 2^p - 1$ is composite.

**Proof** Since $p = 4k + 3$ for some $k$, $q = 8k + 7$, 2 is a quadratic residue mod $q$. By Euler’s Criterion, $2^{(q-1)/2} \equiv 1 \pmod{q}$, so $q | 2^{(q-1)/2} - 1 = 2^p - 1 = M_p$.

Since $p > 3$, we have $2^{p-1} > p + 1$ (true for all integers $p > 3$, not just for primes), so $2^p > 2p + 2 \Rightarrow M_p > q$. Thus, $M_p$ is composite. //

Now let’s consider the quadratic character of the prime 3 mod $p$.

**Proposition** If $p > 3$ is prime, $\left(\frac{-3}{p}\right) = p \pmod{3}$.

**Proof** If $p \equiv 1 \pmod{3}$, then $p = 3k + 1$ for some $k$ and so

\[
4(x^{3k} - 1) = (x^k - 1)(4x^{2k} + 4x^k + 4) = (x^k - 1)((2x^k + 1)^2 + 3)
\]

Working mod $p$, we know that the polynomial on the left has $3k$ roots (FellT) so the two factors on the
right have a full complement of roots as well. In particular, the congruence \((2x^k+1)^2 \equiv -3 \pmod{p}\) has \(2k\) solutions. Since \(2x^k+1 \equiv 0 \pmod{p}\) can have at most \(k\) solutions, there must be a non-zero solution \(y \equiv 2x^k+1 \pmod{p}\) to \(y^2 \equiv -3 \pmod{p}\).

On the other hand, if \(\left(\frac{-3}{p}\right)=1\), then there is a non-zero solution to \(y^2 \equiv -3 \pmod{p}\). As there are two solutions of opposite parity, we may take \(y\) to be the odd one. If \(y=2z+1\), then

\[
4(z^2 + z + 1) \equiv (2z+1)^2 + 3 \equiv y^2 + 3 \equiv 0 \pmod{p}
\]

whence \(z^2 + z + 1 \equiv 0 \pmod{p} \Rightarrow z^3 - 1 \equiv 0 \pmod{p}\). That is, \(z\) has order 3 mod \(p\). But then \(3 \mid p - 1\), so \(p \equiv 1 \pmod{3}\). //

**Corollary** \(\left(\frac{3}{p}\right)=1\) iff \(p \equiv \pm 1 \pmod{12}\).

**Proof** \(\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-3}{p}\right) = 1\) when \(\left(\frac{-1}{p}\right) = \left(\frac{-3}{p}\right)\). These two symbols are both equal to 1 when \(p\) is congruent to 1 modulo 3 and 4, and both equal –1 when \(p\) is congruent to –1 modulo 3 and 4. //