Quadratic Residues

- a is a **quadratic residue** mod m if $x^2 = a \pmod{m}$. Otherwise, a is a **quadratic nonresidue**.
- **Quadratic Reciprocity** relates the solvability of the congruence $x^2 = p \pmod{q}$ to the solvability of the congruence $x^2 = q \pmod{p}$, where p and q are distinct odd primes.
- If p is an odd prime, there are equal numbers of quadratic residues and quadratic nonresidues among $\{1, 2, \ldots, p-1\}$.
- If p is an odd prime, $a > 0$, and $(a, p) = 1$, the **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined by

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

- Legendre symbols provide a computational tool for determining whether a quadratic congruence has a solution.
- **Euler's theorem** says that if p is an odd prime, $a > 0$, and $(a, p) = 1$, then

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

Gauss considered the proofs he gave of quadratic reciprocity one of his crowning achievements; in fact, he gave 6 distinct proofs during his lifetime. Reciprocity is a deep result: Proofs eluded both Euler and Legendre.

The reciprocity law is simple to state. For p and q odd primes, it relates solutions to the two congruences

$$x^2 = p \pmod{q} \quad \text{and} \quad x^2 = q \pmod{p}.$$

(Note how p and q switch places: This explains why it's called a *reciprocity* law.) The law of quadratic reciprocity says:

> The congruences are either both solvable or both unsolvable, unless both primes are congruent to 3 mod 4. In that case, one is solvable while the other is not.

Gauss first gave a proof of this when he was 19!

Gauss's masterwork, the *Disquisitiones Arithmeticae*, was published in 1801 when Gauss was 24. It changed the course of number theory, collecting scattered results into a unified theory.

Definition. Let $(a, m) = 1$, $m > 0$. a is a **quadratic residue** mod m if

$$x^2 = a \pmod{m}$$

has a solution. Otherwise, a is a **quadratic nonresidue** mod m.

Example. 8 is a quadratic residue mod 17, since

$$5^2 = 8 \pmod{17}.$$

However, 8 is a quadratic nonresidue mod 11:

$$x^2 = 8 \pmod{11}$$

has no solutions.

n	0	1	2	3	4	5	6	7	8	9	10
$n^2 \pmod{11}$	0	1	4	9	5	3	3	5	9	4	1

As the table shows, 1, 3, 4, 5, and 9 are quadratic residues mod 11. (0 is not considered a quadratic residue, since $(0, 11) = 11 \neq 1$.) But 8 is a quadratic nonresidue mod 11.

Notice the symmetry in the nonzero elements of the table. Do you see why this is happening? □

Lemma. Let p be an odd prime. The congruence

$$x^2 = a \pmod{p}$$

has:

(a) Only the solution $x = 0$ if $a = 0$.

(b) Exactly 0 or 2 solutions if $p \nmid a$.

Proof. $x = 0$ solves $x^2 = 0 \pmod{p}$. Conversely, if $x^2 = 0 \pmod{p}$, then $p \mid x^2$, so $p \mid x$, and hence $x = 0 \pmod{p}$.

Suppose $p \nmid a$. To show there are 0 or 2 solutions, suppose there is at least one solution b. Then $b^2 = a \pmod{p}$, so $(-b)^2 = a \pmod{p}$. I claim that b and $-b$ are distinct.

If not, then $b = -b \pmod{p}$, so $p \mid 2b$. p is an odd prime, so $p \nmid 2$. Therefore, $p \mid b$, $b = 0 \pmod{p}$, $b^2 = 0 \pmod{p}$, and finally $a = 0 \pmod{p}$ — contradicting $p \nmid a$. Hence, $b \neq -b \pmod{p}$.

Now I have two distinct solutions; since a quadratic equation mod p has at most two solutions (Prove it!), there are exactly two. □

Example. $x^2 = 8 \pmod{17}$ has 5 and 12 as solutions, and $5 = -12 \pmod{17}$.

But note that the result is false if $p = 2$: $x^2 = 1 \pmod{2}$ has exactly one solution ($x = 1 \pmod{2}$). □

Example. Take $p = 7$.

k	0	1	2	3	4	5	6
$k^2 \pmod{7}$	0	1	4	2	2	4	1

Thus, 1, 2, 4 are quadratic residues mod 7. Notice that there are equal numbers of residues and nonresidues. □

Corollary. Let p be an odd prime. There are $\dfrac{p-1}{2}$ quadratic residues and $\dfrac{p-1}{2}$ quadratic nonresidues mod p in $\{1, \ldots, p-1\}$.

Proof. k and $-k = p - k$ have the same square mod p. That is, 1 and $p-1$ have the same square, 2 and $p-2$ have the same square, ..., and $\frac{p-1}{2}$ and $\frac{p-1}{2}+1$ have the same square.

Thus, the number of different squares is $\frac{p-1}{2}$ — these squares are the quadratic residues, and the other $\frac{p-1}{2}$ numbers in $\{1, 2, \ldots, p-1\}$ are quadratic nonresidues. □

The fact observed in the first sentence of the proof explains the symmetries in the table of squares mod 11 and mod 7 that I gave above.

Definition. Let p be an odd prime, and let $(a, p) = 1$. The **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined by

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

Note that $a = 0$ is disallowed (since $(0, p) = p \neq 1$) even though $x^2 = 0 \pmod{p}$ has a solution.

Example. $(5, 11) = 1$. $\left(\frac{5}{11}\right) = 1$, since $4^2 = 5 \pmod{11}$. Likewise, $\left(\frac{11}{5}\right) = 1$, since $6^2 = 11 \pmod{5}$.

Note that 5 is congruent to 1 mod 4; as predicted by reciprocity, both the congruences

$$x^2 = 5 \pmod{11} \quad \text{and} \quad x^2 = 11 \pmod{5}$$

have solutions. □

You might wonder about the case where $p = 2$, or the case where the modulus is composite. For $p = 2$, there are only two quadratic congruences:

$$x^2 = 0 \pmod{2} \quad \text{and} \quad x^2 = 1 \pmod{2}.$$

These have the solutions $x = 0 \pmod{2}$ and $x = 1 \pmod{2}$ — nothing much is going on.

If the modulus has prime factorization $n = p_1^{r_1} \cdots p_k^{r_k}$, then relative primality implies that it's enough to solve the congruences $x^2 = a \pmod{p_i^{r_i}}$ for each i. It turns out that solving such a congruence reduces to determining whether a is a quadratic residue mod p_i. Therefore, there is little harm in concentrating on the case of a single prime.

Example. $x^2 = 14 \pmod{35}$ can be reduced to the simultaneous congruences

$$x^2 = 14 \pmod{5} \quad \text{and} \quad x^2 = 14 \pmod{7}.$$

These can be rewritten as

$$x^2 = 4 \pmod{5} \quad \text{and} \quad x^2 = 0 \pmod{7}.$$

The first equation has solutions $x = 2 \pmod{5}$ or $x = 3 \pmod{5}$. The second equation has the single solution $x = 0 \pmod{7}$. So I have two cases.

If $x = 2 \pmod{5}$ and $x = 0 \pmod{7}$, the Chinese Remainder Theorem gives $x = 7 \pmod{35}$.

If $x = 3 \pmod{5}$ and $x = 0 \pmod{7}$, the Chinese Remainder Theorem gives $x = 28 \pmod{35}$.

Thus, I have two solutions mod 35 to the original quadratic congruence. □

Here are some tools for computing Legendre symbols.

Theorem. (Euler) Let p be an odd prime, $a > 0$, $(a, p) = 1$. Then

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

Proof. There are two cases. Suppose that $\left(\frac{a}{p}\right) = 1$. Then there is a number b such that $b^2 = a \pmod{p}$. So

$$(b^2)^{(p-1)/2} = a^{(p-1)/2} \pmod{p}, \quad b^{p-1} = a^{(p-1)/2} \pmod{p}.$$

If $p \mid b$, then $p \mid b^2 = a$ ↯. So $p \nmid b$, and little Fermat implies that $b^{p-1} = 1 \pmod{p}$. So

$$a^{(p-1)/2} = 1 \pmod{p}, \quad \text{and} \quad \left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}.$$

The other possibility is $\left(\frac{a}{p}\right) = -1$. In this case, consider the set $\{1, 2, \ldots, p-1\}$. I claim that these integers occur in pairs s, t, such that $st = a$.

First, if $s \in \{1, 2, \ldots, p-1\}$, then s is invertible mod p. So I can write $s(s^{-1}a) = a$, and the pair s, $s^{-1}a$, multiplies to a.

Moreover, s and $s^{-1}a$ are distinct. If not, $s = s^{-1}a$, or $s^2 = a$, which contradicts $\left(\frac{a}{p}\right) = -1$.

Since the integers $\{1, 2, \ldots, p-1\}$ divide up into pairs, each multiplying to a, and since there are $\frac{p-1}{2}$ pairs, I have

$$1 \cdot 2 \cdots (p-1) = a^{(p-1)/2} \pmod{p}.$$

By Wilson's theorem,

$$-1 = a^{(p-1)/2} \pmod{p}, \quad \text{so} \quad \left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}. \quad \square$$

Example. Suppose $p = 13$ and $a = 10$. Then

$$a^{(p-1)/2} = 10^{12} = 100^6 = 9^6 = 81^3 = 3^3 = 1 \pmod{13}.$$

Hence, $\left(\frac{10}{13}\right) = 1$, and $x^2 = 10 \pmod{13}$ should have a solution. Indeed,

$$7^2 = 49 = 10 \pmod{13}. \quad \square$$

Lemma. If $a = b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Proof. If $a = b \pmod{p}$, then $x^2 = a \pmod{p}$ if and only if $x^2 = b \pmod{p}$. Thus, one of these equations is solvable or not solvable if and only if the same is true for the other — which means $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. $\square$

Note that I can use this result to apply Euler's formula to $\left(\frac{a}{p}\right)$ for $a < 0$ by simply replacing a with $b > 0$ such that $a = b \pmod{p}$.

Lemma. Let p be an odd prime, $a, b > 0$, $(a, p) = (b, p) = 1$. Then

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

Proof. By Euler,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{(p-1)/2}b^{(p-1)/2} \pmod p, \quad \text{and} \quad \left(\frac{ab}{p}\right) = (ab)^{(p-1)/2} \pmod p.$$

Therefore,

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

The two sides of this equation are ± 1. Since p is an odd prime, the two sides can't differ by 2. Hence, they must be *equal as integers*:

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

Corollary. Let p be an odd prime, $a > 0$, $(a, p) = 1$. Then

$$\left(\frac{a^2}{p}\right) = 1. \quad \square$$

You can use the results above to compute $\left(\frac{a}{p}\right)$ for specific values of a and arbitrary p.

Lemma.

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

Proof. By Euler's formula,

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

$$\begin{cases} (-1)^{2k} & \text{if } p = 4k+1 \\ (-1)^{2k+1} & \text{if p = 4k + 3} \end{cases} = \begin{cases} 1 & \text{if } p = 4k+1 \\ -1 & \text{if p = 4k + 3} \end{cases}. \quad \square$$

Using Gauss's lemma, which I'll prove shortly, you can also show that

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Note that the exponent on the right is actually an integer: Since $p = 2k + 1$, $p^2 - 1 = 4k(k + 1)$. And $4k(k + 1)$ is divisible by 8, because one of k, $k + 1$, must be even.

Example. $\left(\frac{-1}{13}\right) = 1$, because $13 = 4 \cdot 3 + 1$. Thus, $x^2 = -1 \pmod{13}$ has solutions. And in fact,

$$5^2 = 25 = 12 = -1 \pmod{13}.$$

Likewise, $\left(\frac{-1}{23}\right) = -1$, because $23 = 4 \cdot 5 + 3$. Hence, $x^2 = -1 \pmod{23}$ has no solutions. Finally,

$$\left(\frac{2}{7}\right) = (-1)^{(7^2-1)/8} = 1.$$

Therefore, $x^2 = 2 \pmod 7$ has solutions. $x = 3$ works, for instance. $\square$

Quadratic Reciprocity

- **Quadratic reciprocity** relates solutions to $x^2 = p \pmod{q}$ to solutions to $x^2 = q \pmod{p}$, where p and q are distinct odd primes. The equations are both solvable or both unsolvable if either p or q has the form $4k+1$; one is solvable and one is unsolvable if both primes have the form $4k+3$.
- Quadratic reciprocity can be expressed in terms of Legendre symbols: If p and q are distinct odd primes, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if either p or q has the form $4k+1$, whereas $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ if both primes have the form $4k+3$.

Lemma. (Gauss) Let p be an odd prime, $(a,p)=1$. Let k be the number of least positive residues of

$$a, 2a, \ldots, \frac{p-1}{2}a$$

that are greater than $\frac{p}{2}$. Then

$$\left(\frac{a}{p}\right) = (-1)^k.$$

Proof. Since p is odd, $\frac{p}{2}$ is not an integer. Hence, every residue of a, $2a$, $\ldots$, $\frac{p-1}{2}a$ is either less than $\frac{p}{2}$ or greater than $\frac{p}{2}$. Label these two sets:

$$a_1, \ldots, a_j < \frac{p}{2}, \quad b_1, \ldots, b_k > \frac{p}{2}.$$

Thus, $j + k = \frac{p-1}{2}$.

Step 1 $\{p - b_1, \ldots, p - b_k, a_1, \ldots, a_j\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$.

The a_i's are contained in $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, because the a_i's are less than $\frac{p}{2}$ (so less than or equal to $\frac{p-1}{2}$).

What about the $p - b_i$'s?

$$b_i > \frac{p}{2}, \quad \text{so} \quad p - b_i < p - \frac{p}{2} = \frac{p}{2}.$$

Since $p - b_i$ is an integer and $\frac{p}{2}$ is an integer plus one-half, I have $p - b_i \leq \frac{p-1}{2}$. This shows that the $p - b_i$'s are contained in $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ as well.

There are $\frac{p-1}{2}$ elements in $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, and $j + k = \frac{p-1}{2}$. So if the a_i's and $p - b_i$'s are all distinct, I'll know the two sets are equal.

Each a_i has the form ra, where $1 \leq r \leq \frac{p-1}{2}$. So if ra and sa are the same, then

$$ra = sa \pmod{p}, \quad \text{so} \quad p \mid (r-s)a.$$

$p \not| a$, so $p \mid (r-s)$. This is impossible for $1 \leq r, s \leq \frac{p-1}{2}$ unless $r = s$ — which implies $ra = sa$ to begin with.

A similar argument shows that the b_i's, and hence the $p - b_i$'s, are distinct.
Could $a_i = p - b_h$? $a_i = ra$ and $p - b_h = p - sa$ for $1 \le r, s \le \dfrac{p-1}{2}$, so

$$p - sa = ra \pmod p, \quad ra + sa = 0 \pmod p, \quad p \mid (r+s)a.$$

Again, $p \not| a$, so $p \mid (r+s)$. But $1 \le r, s \le \dfrac{p-1}{2}$ implies $2 \le r + s \le p - 1$, so $p \mid (r+s)$ is impossible.
This finishes the proof that $\{p - b_1, \ldots, p - b_k, a_1, \ldots, a_j\} = \left\{1, 2, \ldots, \dfrac{p-1}{2}\right\}$.

Step 2 Since the two sets are the same, the products of the elements in the two sets are the same:

$$(p - b_1) \cdots (p - b_k) \cdot a_1 \cdots a_j = \left(\frac{p-1}{2}\right)! \pmod p.$$

Now $p - b_i = -b_i \pmod p$, so

$$(-1)^k b_1 \cdots b_k \cdot a_1 \cdots a_j = \left(\frac{p-1}{2}\right)! \pmod p.$$

But the a's and b's are exactly the residues of the numbers $a, 2a, \ldots, \dfrac{p-1}{2}a$, so I may replace the product of the a's and b's with the product of $a, 2a, \ldots, \dfrac{p-1}{2}a$:

$$(-1)^k a \cdot 2a \cdots \left(\frac{p-1}{2}\right) a = \left(\frac{p-1}{2}\right)! \pmod p,$$

$$(-1)^k a^{(p-1)/2} \left(\frac{p-1}{2}\right)! = \left(\frac{p-1}{2}\right)! \pmod p.$$

Now $\left(p, \dfrac{p-1}{2}\right) = 1$, so I can cancel the $\left(\dfrac{p-1}{2}\right)!$ terms from both sides. Then applying Euler's theorem, I get

$$(-1)^k a^{(p-1)/2} = 1 \pmod p, \quad (-1)^k \left(\frac{a}{p}\right) = 1 \pmod p, \quad \left(\frac{a}{p}\right) = (-1)^k \pmod p.$$

I made the last step by multiplying both sides by $(-1)^k$ and using the fact that $(-1)^{2k} = 1$. □

Example. I'll use Gauss's lemma to compute $\left(\dfrac{6}{7}\right)$.

Since $p = 7$, $\dfrac{p}{2} = 3.5$ and $\dfrac{p-1}{2} = 3$. Look at the residues $1 \cdot 6 = 6$, $2 \cdot 6 = 5$, and $3 \cdot 6 = 4$. All three are greater than 3.5 — they're b_i's, in the notation of the proof of Gauss's lemma — so Gauss says

$$\left(\frac{6}{7}\right) = (-1)^3 = -1.$$

As a check, Euler's theorem gives $\left(\dfrac{6}{7}\right) = 6^3 = -1 \pmod 7$. □

Lemma. Let $a, b > 0$, where b is an odd integer. Then

$$a = b \cdot \left(\left[\frac{a}{b}\right] + e\right) + (-1)^e \cdot r,$$

where $e = 0$ or 1 and $0 \le r \le \dfrac{b-1}{2}$.

Here $\left[\cdot\right]$ denotes the greatest integer function and $\left[\dfrac{a}{b}\right] + e$ is the integer closest to $\dfrac{a}{b}$.

Proof. By the Division Algorithm,

$$a = bq + r, \text{ where } 0 \le r < b.$$

Now $\dfrac{b}{2}$ is not an integer, so either $r < \dfrac{b}{2}$ or $r > \dfrac{b}{2}$.

(For example, if $a = 11$ and $b = 3$, then $r = 2 > \dfrac{3}{2} = \dfrac{b}{2}$, while if $a = 11$ and $b = 5$, $r = 1 < \dfrac{5}{2} = \dfrac{b}{2}$.)

Consider the two cases.

Case 1: $r < \dfrac{b}{2}$.

Write

$$a = b \cdot \left(\left[\frac{a}{b}\right] + 0\right) + (-1)^0 \cdot r.$$

Here $e = 0$, and $\left[\dfrac{a}{b}\right] + 0$ is the integer closest to $\dfrac{a}{b}$. $r < \dfrac{b}{2}$, but $\dfrac{b}{2}$ is not an integer, so $r \le \dfrac{b-1}{2}$, and $0 \le r \le \dfrac{b-1}{2}$.

Case 2: $r > \dfrac{b}{2}$.

Write

$$a = b \cdot \left(\left[\frac{a}{b}\right] + 1\right) + (r - b) = b \cdot \left(\left[\frac{a}{b}\right] + 1\right) + (-1)^1(b - r).$$

Here $e = 1$, and $\left[\dfrac{a}{b}\right] + 1$ is the integer closest to $\dfrac{a}{b}$. $r < b$, so $b - r > 0$. $r > \dfrac{b}{2}$, so $-r < -\dfrac{b}{2}$, or $b - r < b - \dfrac{b}{2} = \dfrac{b}{2}$. Since $\dfrac{b}{2}$ is not an integer, $b - r \le \dfrac{b-1}{2}$. Therefore, $0 \le r \le \dfrac{b-1}{2}$. ∎

Example. Take $a = 42$ and $b = 17$. $\dfrac{42}{17} \approx 2.47$, so the integer closest to $\dfrac{42}{17}$ is 2.

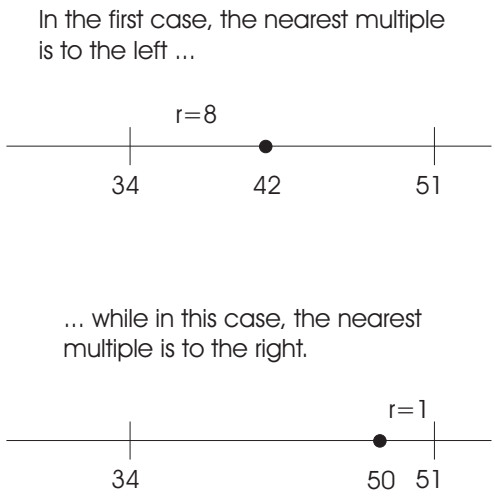
$$42 = 17 \cdot 2 + 8,$$

and $0 \le 8 \le \dfrac{17-1}{2}$.

Take $a = 50$ and $b = 17$. $\dfrac{50}{17} = 2.94$, so the integer closest to $\dfrac{50}{17}$ is 3.

$$50 = 17 \cdot 3 + (-1) \cdot 1.$$

In other words, the r in the lemma represents the distance from a to the *nearest* multiple of b.



The $\pm$ is needed depending on whether the nearest multiple is less than or greater than a. □

I'll use the lemma to give an ingenious proof of Quadratic Reciprocity due to J.S. Frame [1].

Theorem. (**Quadratic Reciprocity**) Let p and q be distinct odd primes.

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

Proof. To simplify the writing, let $p' = \dfrac{p-1}{2}$ and $q' = \dfrac{q-1}{2}$.

Let $1 \le n \le q'$. Apply the Lemma with $a = np$ and $b = q$:

$$np = q \cdot \left(\left[\frac{np}{q}\right] + e_n\right) + (-1)^{e_n} r_n,$$

where $1 \le r_n \le q'$ and $e_n = 0$ or 1.

The first thing I will show is that the remainders r_n are just a permutation of the integers $1, \ldots, q'$.

If I take the initial equation and go mod q, I get

$$np = (-1)^{e_n} r_n \pmod{q}.$$

Can two of the r's be equal? Suppose $r_m = r_n$, where $1 \le m, n \le q'$. Then

$$0 = r_m - r_n = ((-1)^{e_m} m - (-1)^{e_n} n)\, p \pmod{q}.$$

In other words, $q \mid ((-1)^{e_m} m - (-1)^{e_n} n)\, p$. But $m + n \le 2q' = q - 1$, so $(-1)^{e_m} m - (-1)^{e_n} n$ is surely smaller than q in absolute value. Since $q \not| p$, this is impossible unless $(-1)^{e_m} m - (-1)^{e_n} n = 0$. This in turn is impossible unless $m = n$. Thus, the r's are distinct. Since there are q' of them, and since they're all in the range $[1, q']$, they must be some permutation of the numbers $1, \ldots, q'$.

As a preliminary to the next computation, take the first equation and go mod 2. p and q are odd, so they equal 1 mod 2; $(-1)^{e_n} = \pm 1$, so either way it equals 1 mod 2. Therefore,

$$n = \left[\frac{np}{q}\right] + e_n + r_n \pmod{2}.$$

(I'm going to use this in an exponent of -1 in a second!)

Now let $1 \le m \le p'$, $1 \le n \le q'$. Then $mq - np \neq 0$, for $mq = np$ implies $p \div m$ — impossible, because $1 \le m \le p' = \dfrac{p-1}{2}$.

Now here's the heart of the proof. The idea will be to define a weird product which turns out to be the Legendre symbol. Define

$$f(p,q) = \prod_{m=1}^{p'} \prod_{n=1}^{q'} \frac{mq - np}{|mq - np|}.$$

Notice that $\dfrac{mq-np}{|mq-np|}$ is a fancy way of expressing the *sign* of $mq - np$ — $+1$ when it's positive, -1 when it's negative.

When is $mq - np$ negative? $mq < np$ gives $m < \dfrac{np}{q}$, or $m \le \left[\dfrac{np}{q}\right]$. That is, $mq - np$ is negative for $m = 1, \ldots, \left[\dfrac{np}{q}\right]$. So the product (for fixed n) has $\left[\dfrac{np}{q}\right]$ -1's, and

$$f(p,q) = \prod_{n=1}^{q'} (-1)^{[np/q]}.$$

$n = \left[\dfrac{np}{q}\right] + e_n + r_n \pmod 2$, so $n - r_n - e_n = \left[\dfrac{np}{q}\right] \pmod 2$. In fact, $-e_n = e_n \pmod 2$, so $n - r_n + e_n = \left[\dfrac{np}{q}\right] \pmod 2$. Since things which are equal mod 2 give the same power of -1,

$$f(p,q) = \prod_{n=1}^{q'} (-1)^{n-r_n+e_n} = \prod_{n=1}^{q'} (-1)^{n-r_n}(-1)^{e_n} = (-1)^{\sum_{n=1}^{q'}(n-r_n)} \prod_{n=1}^{q'} (-1)^{e_n}.$$

Since the r_n's are just the integers from 1 to q' and since n runs from 1 to q', $\displaystyle\sum_{n=1}^{q'}(n - r_n) = 0$! So now I have

$$f(p,q) = \prod_{n=1}^{q'} (-1)^{e_n}.$$

If I take the very first equation and go mod q, I get

$$np = (-1)^{e_n} r_n \pmod q, \quad \text{or} \quad \frac{np}{r_n} = (-1)^{e_n} \pmod q.$$

(r_n is invertible mod q, so the fraction makes sense.) So now

$$f(p,q) = \prod_{n=1}^{q'} \frac{np}{r_n} \pmod q.$$

But $\displaystyle\prod_{n=1}^{q'} \frac{n}{r_n} = 1$, because as n runs over the numbers from 1 to q', so does r_n. So finally

$$f(p,q) = \prod_{n=1}^{q'} p = p^{q'} = \left(\frac{p}{q}\right)$$

by Euler's theorem.

Notice that

$$f(q,p) = \prod_{m=1}^{q'} \prod_{n=1}^{p'} \frac{mp - nq}{|mp - nq|} = \prod_{m=1}^{p'} \prod_{n=1}^{q'} \frac{np - mq}{|np - mq|}.$$

I got the second product by swapping m and n in the first.
Whew! The rest is easy — fortunately!

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = f(p,q)f(q,p) = \prod_{m=1}^{p'} \prod_{n=1}^{q'} \frac{mq - np}{|mq - np|}\frac{np - mq}{|np - mq|} = \prod_{m=1}^{p'} \prod_{n=1}^{q'} (-1) = (-1)^{p'q'}.$$

Since $p' = \dfrac{p-1}{2}$ and $q' = \dfrac{q-1}{2}$, I'm done! □

As complicated as this proof is, it's actually no worse than most proofs of this result.

Before giving an example, I want to discuss what reciprocity tells you about solutions to quadratic congruences.

An odd prime p is congruent to 1 or to 3 mod 4.
If $p = 4k+1$, then $\dfrac{p-1}{2} = 2k$, an even number. If $p = 4k+3$, then $\dfrac{p-1}{2} = 2k+1$, an odd number.
Since an even number times anything is even,

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \begin{cases} \text{even} & \text{if } p \text{ or } q = 1 \pmod 4 \\ \text{odd} & \text{if } p \text{ and } q = 3 \pmod 4 \end{cases}$$

Therefore,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} +1 & \text{if } p \text{ or } q = 1 \pmod 4 \\ -1 & \text{if } p \text{ and } q = 3 \pmod 4 \end{cases}$$

However,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = +1 \text{ means } \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1 \quad \text{or} \quad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = -1$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1 \text{ means one of } \left(\frac{p}{q}\right), \left(\frac{q}{p}\right) \text{ is } +1 \text{ and the other is } -1$$

In terms of the congruences

$$x^2 = p \pmod q \quad \text{and} \quad x^2 = q \pmod p$$

this means:

1. If at least one of p, q is congruent to 1 mod 4, then both equations are solvable or both equations are unsolvable.
2. If both p and q are congruent to 3 mod 4, then one equation is solvable and the other is unsolvable.

Corollary. Let p and q be distinct odd primes.

(a) If at least one of p, q is congruent to 1 mod 4, then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

(b) If both p and q are congruent to 3 mod 4, then

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right). \quad \square$$

Example. Compute $\left(\frac{17}{71}\right)$.

$17 = 1 \pmod 4$, so

$$\left(\frac{17}{71}\right) = \left(\frac{71}{17}\right) = \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = 2^{(3-1)/2} = 2 = -1 \pmod 3.$$

In other words, $x^2 = 17 \pmod{71}$ does not have any solutions. □

Example. Compute $\left(\frac{299}{359}\right)$.

$\left(\frac{299}{359}\right) = \left(\frac{13}{359}\right)\left(\frac{23}{359}\right)$; I'll compute $\left(\frac{13}{359}\right)$ and $\left(\frac{23}{359}\right)$.

$$\left(\frac{13}{359}\right) = \left(\frac{359}{13}\right) = \left(\frac{8}{13}\right) = 8^{(13-1)/2} = 8^6 = 262144 = -1 \pmod{13},$$

$$\left(\frac{23}{359}\right) = -\left(\frac{359}{23}\right) = -\left(\frac{14}{23}\right) = -\left(\frac{2}{23}\right)\left(\frac{7}{23}\right).$$

Next, I'll compute $\left(\frac{2}{23}\right)$ and $\left(\frac{7}{23}\right)$.

$$\left(\frac{2}{23}\right) = 2^{(23-1)/2} = 2^{11} = 2048 = 1 \pmod{23},$$

$$\left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -(2^{(7-1)/2}) = -8 = -1 \pmod 7.$$

Therefore, $\left(\frac{23}{359}\right) = -(1)(-1) = 1$, and

$$\left(\frac{299}{359}\right) = (-1)(1) = -1.$$

The congruence $x^2 = 299 \pmod{359}$ does not have a solution. □

---

[1] J.S. Frame, A short proof of quadratic reciprocity, *Amer. Math. Monthly*, 85(10)(1978), 818–819.