Quadratic Reciprocity

We now turn our attention to the problem of solving quadratic congruences. That is, we want to know if there are any values of x such that

$$x^2 \equiv b \pmod{m}$$

To make things a little easier, we'll only consider congruences modulo a prime p. In fact, we'll only look at odd primes, because the case when $p=2$ is a bit boring.

Notice that some of these quadratic congruences have solutions — $x^2 \equiv 8 \pmod{17}$ has a solution $x=5$, $5^2=25=17+8$ — but some do not — there is no value of x such that $x^2 \equiv 10 \pmod{17}$.

So, given values b and p, how can we determine if $x^2 \equiv b \pmod{p}$ has any solutions? Answering this question will take some time, and will require that we learn a bit of terminology, notation, and some technical tools along the way.

First some vocabulary. If $x^2 \equiv b \pmod{p}$ has a solution (and $p \nmid b$), then we say that b is a *quadratic residue modulo p*. If $x^2 \equiv b \pmod{p}$ has no solutions, then we say b is a *quadratic non-residue modulo p*. (By convention, 0 is neither a quadratic residue nor a quadratic non-residue.)

To save ourselves some writing, we'll abbreviate "quadratic residue" as QR, and "quadratic non-residue" as NR.

For example, we can calculate all the QR's modulo p by making a table of x and x^2 for each $1 \leq x \leq p-1$. For $p=17$ this gives

x	x^2
1	1
2	4
3	9
4	16
5	8
6	2
7	15
8	13
9	13
10	15
11	2
12	8
13	16
14	9
15	4
16	1

This table tells us the QR's mod 17 are 1, 2, 4, 8, 9, 13, 15, 16, and the NR's mod 17 are 3, 5, 6, 7, 10, 11, 12, 14.

Notice our table above was symmetric: $x^2 \equiv (17-x^2)$ (mod 17). This is true for every prime:

<u>Lemma</u>

For each odd prime p and each $1 \leq x < p$,

$$x^2 \equiv (p-x)^2 \pmod{p}$$

<u>Pf</u>

Note $(p-x)^2 = p^2 - 2px + x^2$, but p^2 and $-2px$ are bothe congruent to 0 modulo p. □

Notice there were 8 QR's mod 17 and 8 NR's mod 17. It's easy to show this happens in general: there are just as many QR's mod p as there are NR's mod p.

<u>Lemma</u>

If p is an odd prime, then there are exactly $\frac{p-1}{2}$ QR's and NR's mod p

Pf

By definition, the QR's mod p are the congruence classes of $1^2, 2^2, 3^2, \ldots, (p-1)^2$. However, by symmetry, we can only get half of these, $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$. We need to show these congruence classes are distinct for there to be $\frac{p-1}{2}$ QR's.

If they weren't, then for some a and b between 1 and $\frac{p-1}{2}$, we'd have

$$a^2 \equiv b^2 \pmod{p}$$
$$\Rightarrow a^2 - b^2 \equiv 0 \pmod{p}$$
$$\Rightarrow (a-b)(a+b) \equiv 0 \pmod{p}$$
$$\Rightarrow p \mid (a-b)\cdot(a+b)$$
$$\Rightarrow p \mid (a-b) \quad \text{or} \quad p \mid (a+b)$$

Since $1 \leq a, b \leq \frac{p-1}{2}$, note $2 \leq a+b \leq p-1$, so p can't divide $a+b$. Hence $p \mid (a-b)$. But

$$-\frac{p-1}{2} < a-b < +\frac{p-1}{2}$$

The only value in this range which p divides is 0, so $a-b=0$ meaning $a=b$. □

To help us study quadratic residues we'll introduce some surprisingly useful notation. Given an odd prime p and a value a with $p \nmid a$, we define the Legendre symbol of a modulo p, denoted $\left(\frac{a}{p}\right)$, to be 1 if a is QR mod p, and -1 if a is NR mod p.

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

What makes Legendre symbols helpful is that the satisfy a multiplicative law.

Theorem

Suppose $p \nmid a$, $p \nmid b$, and $p > 2$ is prime.
Then

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

Pf
There are 3 cases to consider.

Case 1 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$

Here a and b are both quadratic residues modulo p. This means there are values x and y such that

$$x^2 \equiv a \pmod{p}$$
$$y^2 \equiv b \pmod{p}.$$

Notice

$$(xy)^2 = x^2y^2 \equiv ab \pmod{p}$$

so ab is a QR mod p, and $\left(\frac{ab}{p}\right)=1$.

<u>Case 2</u> $\left(\frac{a}{p}\right)=1$, $\left(\frac{b}{p}\right)=-1$

Since a is QR mod p, $x^2 \equiv a \pmod{p}$ for some x. We need to show $\left(\frac{ab}{p}\right)=-1$, so we'll show $\left(\frac{ab}{p}\right)=1$ is impossible. If $\left(\frac{ab}{p}\right)=1$, then there exists some y such that $y^2 \equiv ab \pmod{p}$, which we could write as $y^2 = x^2b \pmod{p}$. As $p \nmid a$, $p \nmid x$ either. This means x has a multiplicative inverse: there exists a z such that $xz \equiv 1 \pmod{p}$. Hence

$$\begin{aligned} y^2 &\equiv x^2 b \pmod{p} \\ \Rightarrow z^2y^2 &\equiv z^2x^2b \pmod{p} \\ &\equiv (zx)^2 b \pmod{p} \\ &\equiv b \pmod{p} \end{aligned}$$

But this is impossible because $\left(\frac{b}{p}\right)=-1$! So it must be the case that $\left(\frac{ab}{p}\right)=-1$, as desired.

Case 3 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$

Notice that the following sets are equal

$$\{1, 2, 3, \ldots, p-1\} = \{a, 2a, 3a, \ldots, (p-1)a\}$$

because there are only $p-1$ congruence classes and no two of ia, ja are congruent mod p for $1 \leq i, j \leq p-1$ unless $i=j$. Of these $p-1$ values in

$$\{a, 2a, 3a, \ldots, (p-1)a\}$$

exactly $\frac{p-1}{2}$ are QR's, and $\frac{p-1}{2}$ are NR's. We've already seen that the product of a QR with an NR must be an NR (this was Case 2 above), and this accounts for all of the non-residues of

$$\{a, 2a, 3a, \ldots, (p-1)a\}$$

as a is an NR. Hence the remaining values (which are non-residues times a) must give the QR's □

Notice this theorem really says

$$QR \cdot QR = QR$$

$$QR \cdot NR = NR$$

$$NR \cdot NR = QR$$

This is just like multiplying positives and negatives, with QR's playing the role of positive, and NR playing the role of negative.

How are Legendre symbols helpful? Well, they let us reduce the problem of determining if a given value is a quadratic residue or not, to determining if the primes dividing that number are QR's or not.

For example is 612 a quadratic residue mod 17? The prime factorization of 612 is $612 = 2^2 \cdot 3^2 \cdot 7$, so

$$\begin{aligned}\left(\frac{612}{17}\right) &= \left(\frac{2}{17}\right)\left(\frac{2}{17}\right)\left(\frac{3}{17}\right)\left(\frac{3}{17}\right)\left(\frac{7}{17}\right)\\ &= 1 \cdot 1 \cdot -1 \cdot -1 \cdot -1\\ &= -1\end{aligned}$$

so 612 is a non-residue mod 17.

Now, back to our general problem. Given a and p, how do we figure out if $\left(\frac{a}{p}\right) = \pm 1$? To answer this problem we'll actually answer a related question: if we fix a, for which primes p is a a quadratic residue?

Ultimately we'll want to answer this for prime values of a, since this would tell us how to compute Legendre symbols. To get started, we suppose $a=-1$. So, our question is basically for which (odd) primes p does -1 have a square root modulo p?

We begin by gathering some data. Using Sage, it's relatively easy to create a list of primes, and for each prime determine if there are any solutions to $x^2 \equiv -1 \pmod{p}$. For the table we'll generate we can do this in the naïve way: for each $1 \le x \le p$, see if $x^2 \equiv p-1 \equiv -1 \pmod{p}$. If there are any solutions, the Legendre symbol $\left(\frac{-1}{p}\right)$ is 1, and otherwise it's -1. Here is the list I generated with Sage (code on the website:

p	$\left(\frac{-1}{p}\right)$	Solutions to $x^2 \equiv -1 \pmod{p}$
3	-1	—
5	1	2, 3
7	-1	—
11	-1	—
13	1	5, 8
17	1	4, 13
19	-1	—
23	-1	—
29	1	12, 17

At first glance there may not be an obvious pattern, but notice we're partitioning the odd primes into two categories. We have another way of putting the odd primes into two families — those congruent to 1 mod 4, and those congruent to 3 mod 4. How do these compare to the primes where $\left(\frac{-1}{p}\right) = \pm 1$?

We can easily modify our Sage code to add this information to our table

p	p mod 4	$\left(\frac{-1}{p}\right)$	Solutions to $x^2 \equiv -1 \pmod{p}$
3	3	−1	—
5	1	1	2, 3
7	3	−1	—
11	3	−1	—
13	1	1	5, 8
17	1	1	4, 13
19	3	−1	—
23	3	−1	—
29	1	1	12, 17

From the little bit of data we have, we might conjecture that $\left(\frac{-1}{p}\right) = 1$ iff $p \equiv 1 \pmod{4}$.

Any good conjecture should be testable, so let's put our conjecture to the test by picking some large primes congruent to 1 or 3 mod 4, and seeing if $x^2 \equiv -1 \pmod{p}$ has roots or not. The values 911 and 929 are prime (we could generate a list with some "big" prime using the sieves of Eratosthenes or Sundaram), and

$$911 \equiv 3 \pmod{4}$$
$$929 \equiv 1 \pmod{4}$$

Naively testing to see if -1 has any square roots, we have that there are no roots mod 911, but 324 and 605 are roots mod 929.

How can we prove our conjecture? Well, first let's notice that we're trying to square something and get -1. If we were to square again, we'd get 1. So as a first step, let's try to find all the things that square to 1:

$$A^2 \equiv 1 \pmod{p}$$
$$\Rightarrow A^2 - 1 \equiv 0 \pmod{p}$$
$$\Rightarrow (A+1)(A-1) \equiv 0 \pmod{p}$$
$$\Rightarrow A+1 \equiv 0 \pmod{p} \text{ or } A-1 \equiv 0 \pmod{p}$$

This step depends heavily on p being prime

$$\Rightarrow A \equiv -1 \pmod{p} \text{ or } A \equiv 1 \pmod{p}$$

So if we can square A and get $1 \pmod{p}$, A must be congruent to $\pm 1 \pmod{p}$.

However, given any $1 \leq a < p$, we know one thing (besides 1) we can square to get $1 \pmod{p}$: thanks to Fermat's little theorem,

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

Thus $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. So for each value of a, we're associating ± 1 by computing the congruence class of $a^{\frac{p-1}{2}}$. But we have another way of associating ± 1 to a — the Legendre symbol $\left(\frac{a}{p}\right)$. Could $a^{\frac{p-1}{2}}$ be related to $\left(\frac{a}{p}\right)$?

Using Sage we can easily build a table for a big collection of primes p, comparing $a^{\frac{p-1}{2}}$ and $\left(\frac{a}{p}\right)$ for each $1 \leq a < p$.

p	a	$a^{\frac{p-1}{2}}$	$\left(\frac{a}{p}\right)$
3	2	−1	−1
5	2	−1	−1
5	3	−1	−1
5	4	1	1
7	2	1	1
7	3	−1	−1
7	4	1	1
7	5	−1	−1
7	6	−1	−1
	2	−1	−1
11	3	1	1
11	4	1	1
11	5	1	1
11	6	1	1

It certainly appears that $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$, and this is known as Euler's criterion:

Thm (Euler's criterion)
If $p \nmid a$, then $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$, where p is an odd prime.

Pf
If $\left(\frac{a}{p}\right) = 1$, then a is a quadratic residue modulo p. Hence $x^2 \equiv a \pmod p$ for some x. Thus

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$$

where the right-most congruence follows from Fermat's little theorem. So the theorem is true when a is QR. Now we need to show if a is NR, $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

We've shown that every quadratic residue must satisfy the congruence

$$y^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$$

Notice this is a polynomial congruence equation, and we've seen that polynomial congruences of degree d has at most d solutions.

There are $\frac{p-1}{2}$ QR's, all of which are solutions

So if a is NR, it can not solve

$$y^{\frac{p-1}{2}} - 1 \equiv 0$$

However we know each $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$, and so it must be that $a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod{p}$. □

With Euler's criterion at our disposal, it is extremely easy to calculate $\left(\frac{-1}{p}\right)$ because we know

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

and $(-1)^{\frac{p-1}{2}}$ is 1 if $\frac{p-1}{2}$ is even, and -1 if $\frac{p-1}{2}$ is odd.

For example,

$$\left(\frac{-1}{17}\right) \equiv (-1)^{\frac{17-1}{2}} \equiv (-1)^{8} \equiv 1 \pmod{p}$$

$$\left(\frac{-1}{911}\right) \equiv (-1)^{\frac{911-1}{2}} \equiv (-1)^{455} \equiv -1 \pmod{p}$$

We had originally conjectured $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{4}$, and we can now prove this using Euler's criterion.

Thm (Quadratic Reciprocity, pt. 1)

Let $p>2$ be prime. Then

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

Pf

By Euler's criterion, $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$.

- If $p \equiv 1 \pmod 4$, then $p = 4m+1$ for some m. Hence

$$\frac{p-1}{2} = \frac{4m+1-1}{2} = 2m$$

and $(-1)^{\frac{p-1}{2}} = 1$.

- If $p \equiv 3 \pmod 4$, then $p = 4m+3$, and

$$\frac{p-1}{2} = \frac{4m+3-1}{2} = \frac{4m+2}{2} = 2m+1$$

and $(-1)^{\frac{p-1}{2}} = -1$. □

We had previously shown there were infinitely many primes congruent to 3 (mod 4) using a variation of Euclid's proof there were infinitely-many primes. We are now finally able to show there are infinitely-many primes congruent to 1 (mod 4).

Thm

There are infinitely-many primes congruent to 1 (mod 4).

Pf

Suppose there were only finitely-many primes congruent to 1 (mod 4) — say

$$p_1, p_2, \dots, p_m$$

Consider the number

$$A = 4p_1^2 p_2^2 \cdots p_m^2 + 1$$

We will show there must exist a prime congruent to 1 (mod 4) ~~but~~ dividing A, but which is not on our list.

First note that A is congruent to 1 (mod 4), and none of $p_1, \dots, p_m$ divide A as dividing any p_i into A will result in a remainder of 1.

Now let $A = q_1 q_2 \cdots q_n$ be the prime factorization of A. Note no q_i is on our list $p_1, p_2, \dots, p_m$. If we can show at least one q_i is congruent to 1 (mod 4), we'll be done.

As A is odd, all the q_i must be odd.

For each q_i,

$$A \equiv 0 \pmod{q_i}$$
$$\Rightarrow 4p_1^2 p_2^2 \cdots p_m^2 + 1 \equiv 0 \pmod{q_i}$$
$$\Rightarrow (2p_1 p_2 \cdots p_m)^2 \equiv -1 \pmod{q_i}$$

So $2p_1 p_2 \cdots p_m$ solves $x^2 \equiv -1 \pmod{q_i}$ for each q_i — $\left(\frac{-1}{q_i}\right) = 1$. But if $\left(\frac{-1}{q_i}\right) = 1$, then $q_i \equiv 1 \pmod{4}$. □

We now move on to our next stepping stone for quadratic residues.

Ultimately, we'd like to determine $\left(\frac{q}{p}\right)$ for every prime pair, q and p. If we knew these Legendre symbols, we could figure out any other Legendre symbol.

Let's first consider $\left(\frac{2}{p}\right)$ — for which primes p is 2 a quadratic residue modulo p? I.e., when does $x^2 \equiv 2 \pmod{p}$ have a solution?

Let's first gather some data, naively asking Sage to find solutions to $x^2 \equiv 2 \pmod{p}$ for several values of p.

Our Sage code (which is on the website) tells us the first few primes where 2 is QR are

7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 87

and when 2 is NR,

3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67, 83

There's no obvious pattern here, but maybe a pattern will emerge if we consider congruence classes.

Looking at our primes modulo 4, our lists of QR's and NR's become

QR's: 3, 1, 3, 3, 1, 3, 3, 1, 3, 1, 1
NR's: 3, 1, 3, 1, 3, 1, 1, 3, 1, 3, 1, 3, 3

So congruences modulo 4 don't seem helpful — but maybe congruences modulo another number would be. If we mod out by 8, our lists become

QR's: 7, 1, 7, 7, 1, 7, 7, 1, 7, 1, 1
NR's: 3, 5, 3, 5, 3, 5, 5, 3, 5, 3, 5, 3, 3

Now this is something we might be able to work with.

Based on the little bit of data we have, we might conjecture

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \end{cases}$$

We'd like to use something like Euler's criterion to apply here, which would tell us

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

So what we need is an easy way to determine the congruence class of $2^{\frac{p-1}{2}} \pmod p$.

The following idea is due to Gauss:

① Consider the congruence class of the product of all the even numbers between 1 and p:

$$2 \cdot 4 \cdot 6 \cdot 8 \cdot \ldots \cdot (p-5) \cdot (p-3) \cdot (p-1)$$

Notice there are $\frac{p-1}{2}$ factors.

② Factor a 2 from each factor:

$$\begin{aligned} &[2\cdot 1]\cdot[2\cdot 2]\cdot[2\cdot 3]\cdot \ldots \cdot\left[2\cdot \tfrac{p-5}{2}\right]\cdot\left[2\cdot\tfrac{p-3}{2}\right]\cdot\left[2\cdot\tfrac{p-1}{2}\right] \\ &= 2^{\frac{p-1}{2}} \cdot \left(1\cdot 2\cdot 3 \cdot \ldots \cdot \tfrac{p-5}{2}\cdot\tfrac{p-3}{2}\cdot\tfrac{p-1}{2}\right) \\ &= 2^{\frac{p-1}{2}} \cdot \left(\tfrac{p-1}{2}\right)! \end{aligned}$$

③ For each number in our original product, replace that number with a congruent number (mod p) in the range $\left[-\frac{(p-1)}{2}, \frac{p-1}{2}\right]$

Now multiply these "new" values together, and notice this product is $(-1)^k \cdot \left(\frac{p-1}{2}\right)!$ for some $k \in \mathbb{N}$

④ Notice that steps ② and ③ together tell us

$$2^{\frac{p-1}{2}} \cdot \left(\tfrac{p-1}{2}\right)! \equiv (-1)^k \cdot \left(\tfrac{p-1}{2}\right)! \pmod{p}$$

$$\Rightarrow 2^{\frac{p-1}{2}} \equiv (-1)^k \pmod{p}$$

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

Let's explain step ③ in more detail. The factors in our original product were

$$2, 4, 6, 8, \ldots, p-5, p-3, p-1$$

The number $\frac{p-1}{2}$ is roughly in the middle of this list — note $\frac{p-1}{2}$ could be even or odd. We cut our list into two halves: one consists of values $\leq \frac{p-1}{2}$, and one consists of values $> \frac{p-1}{2}$.

If $\frac{p-1}{2}$ is even, then the first half of our list is

$$2, 4, 6, \ldots, \frac{p-1}{2}$$

and the second half is

$$\frac{p-1}{2}+2, \frac{p-1}{2}+4, \ldots, \frac{p-1}{2}+\frac{p-1}{2}$$

If $\frac{p-1}{2}$ is ~~ev~~ odd, then the first half is

$$2, 4, 6, \ldots, \frac{p-1}{2}-1$$

and the second half is

$$\frac{p-1}{2}+1, \frac{p-1}{2}+3, \frac{p-1}{2}+5, \ldots, \frac{p-1}{2}+\frac{p-1}{2}-2, \frac{p-1}{2}+\frac{p-1}{2}$$

We then replace each entry in the second list by a congruent number by subtracting p from each element of the list.

Notice the entries in the second list, after subtracting p are exactly the negative versions of the odd numbers in $[1, \frac{p-1}{2}]$. Hence multiplying everything together gives $(-1)^k(\frac{p-1}{2})!$ where k is the number of entries in the 2^{nd} half of the list.

For example, say $p = 31$. The even number in $[1, 31]$ are

$$2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30$$

We cut the list into two halves depending on the numbers being ≤ 15 or > 15

$$2, 4, 6, 8, 10, 12, 14$$
$$16, 18, 20, 22, 24, 26, 28, 30$$

Subtract 31 from each number in the second list

$$-15, -13, -11, -9, -7, -5, -3, -1$$

Now multiply everything together

$$(-1) \cdot 2 \cdot (-3) \cdot 4 \cdot (-5) \cdot 6 \cdot (-7) \cdot 8 \cdot (-9) \cdot 10 \cdot (-11) \cdot 12 \cdot (-13) \cdot 14 \cdot (-15)$$
$$= (-1)^8 15!$$

We know this is congruent to $2^{15} \cdot 15!$,

$$2^{15} \cdot 15! \equiv (-1)^8 \cdot 15! \pmod{31}$$
$$\Rightarrow 2^{15} \equiv 1 \pmod{31}$$
$$\Rightarrow \left(\frac{2}{31}\right) = 1$$

So 2 is a QR mod 31.

Thm (Quadratic Reciprocity, part 2)

Let $p>2$ be prime. Then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p\equiv 1 \pmod 8 \text{ or } p\equiv 7 \pmod 8 \\ -1 & \text{if } p\equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \end{cases}$$

Pf

Case 1 $p\equiv 1 \pmod 8$

Note $p = 8k+1$, so $\frac{p-1}{2} = 4k$. The first half of the list described above is

$$2, 4, 6, \ldots, 4k$$

and the second half is

$$4k+2, 4k+4, 4k+6, \ldots, 8k$$

We need to determine how many items are in the second list. Each item in the 2nd list has the form $4k+2n$. We start at $n=1$ and go up to when $4k+2n=8k$, meaning $2n=4k \Rightarrow n=2k$. Hence there are $2k$ elements of the second list, so

$$2^{\frac{p-1}{2}} \cdot \left(\tfrac{p-1}{2}\right)! \equiv (-1)^{2k}\left(\tfrac{p-1}{2}\right)! \pmod p$$
$$\Rightarrow 2^{\frac{p-1}{2}} \equiv 1 \pmod p$$
$$\Rightarrow \left(\frac{2}{p}\right) = 1$$

Case 2 $p \equiv 7 \pmod 8$

$p = 8k+7$, and $\frac{p-1}{2} = 4k+3$. The first half of our list is

$$2, 4, 6, \ldots, 4k+2$$

the second half of the list is

$$4k+4,\ 4k+6,\ 4k+8,\ \ldots,\ 8k+6.$$

Each element of this list is of the form

$$4k+2+2n$$

where n ranges from 1 up to when $4k+2+2n=8k+6$,

$$4k+2+2n = 8k+6$$
$$\Rightarrow 2n = 4k+4$$
$$\Rightarrow n = 2k+2$$

Thus

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

so 2 is a QR mod p for $p \equiv 7 \pmod 8$

<u>Case 3</u> $p \equiv 3 \pmod 8$

$p = 8k+3$, so ~~p~~ $\frac{p-1}{2} = \frac{8k+2}{2} = 4k+1$.

The values in $2,4,6,\ldots,p-1$ which stay the same are thus $2,4,6,\ldots,4k$, and the values which will be replaced with a congruent negative number are

$$4k+2,\ 4k+4,\ 4k+6,\ldots,\ 8k+2$$

These numbers have the form

$$4k+2n$$

for n from 1 until $4k+2n=8k+2$, which means $n=2k+1$. Hence

$$2^{\frac{p-1}{2}} \equiv (-1)^{2k+1} \pmod{p}$$

and so $\left(\frac{2}{p}\right)=-1$.

<u>Case 4</u> $p \equiv 5 \pmod{8}$

$p=8k+5$, so $\frac{p-1}{2} \equiv 4k+2$.

The first half of our list of numbers, which remains unchanged, is

$$2, 4, 6, \ldots, 4k+2$$

The second half is

$$4k+4, 4k+6, 4k+8, \ldots, 8k+4.$$

These again have the form $4k+2n+2$ where n ranges from 1 until $4k+2n+2=8k+4$, meaning $n=2k+1$, and so $\left(\frac{2}{p}\right) \equiv -1$.

We're now ready to start working our way to the general version of the law of quadratic reciprocity. Again, our ultimate goal is to determine if a given value a is a quadratic residue modulo a prime $p>2$. In terms of the Legendre symbols, this means we need to know if $\left(\frac{a}{p}\right) = \pm 1$. Because of the fundamental theorem of arithmetic and the multiplicative law of Legendre symbols — i.e., $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$ — it suffices to determine $\left(\frac{q}{p}\right)$ when q is a prime.

Quadratic reciprocity will give us an algorithm for expressing $\left(\frac{q}{p}\right)$ in terms of "simpler" Legendre symbols.

<u>Thm</u> (Quadratic Reciprocity, version 3)
Let p, q be odd primes, $p \neq q$. Then

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4 \end{cases} \quad \square$$

Before proving this, we show how quadratic reciprocity can be used to calculate Legendre symbols:

Question

Is 17,408 a quadratic residue modulo 67?

$$\left(\frac{17,408}{67}\right) = \left(\frac{17\cdot 1,024}{67}\right) = \left(\frac{17}{67}\right)\cdot\left(\frac{1,024}{67}\right)$$
$$= \left(\frac{17}{67}\right)\cdot 1$$
$$= \left(\frac{67}{17}\right)$$
$$= \left(\frac{16}{17}\right)$$
$$= 1$$

Lemma

The law of quadratic reciprocity (pt. 3) above is equivalent to the following:

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

Pf.

- Suppose the law of quadratic reciprocity is true.
  - Case 1 Either of p or q is congruent to 1 modulo 4.
    Suppose, WLOG, $p \equiv 1 \pmod 4$. So $p = 4k+1$ for some k. Hence $\frac{p-1}{2} = 2k$, so $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = 1$ since we raise -1 to an even power. Note too that by the law of quadratic reciprocity,
    $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)\cdot\left(\frac{p}{q}\right) = (\pm 1)^2 = 1$. Hence
    $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

- Case 2   Both p and q are congruent to 3 modulo 4. So $p = 4k+3$ and $q = 4l+3$. Thus $\frac{p-1}{2} = 2k+1$, $\frac{q-1}{2} = 2l+1$. So $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ because -1 is raised to an odd number.

By quad. reciprocity, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, so

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

$$= -1\cdot(\pm 1)^2$$

$$= -1$$

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

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

By the above this means $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ if either p or q is congruent to 1 modulo 4, and $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$ otherwise. $\square$

So to prove the law of quadratic reciprocity we'll prove $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$, which we'll do by first proving three preliminary lemmas.

In the following, p is an odd prime and $H = \frac{p-1}{2}$.

Lemma

Let a be an integer which is not a multiple of p. Consider the set of congruence classes

$$S = \{\bar{a}, \overline{2a}, \overline{3a}, \dots, \overline{Ha}\}$$
$$T = \{\bar{r}_1, \bar{r}_2, \bar{r}_3, \dots, \bar{r}_H\}$$

where $\bar{r}_i$ is a number congruent to $\overline{ai}$ in $-H \le r_i \le H$. Then $S = T$ equals the set

$$\mathcal{U} = \{\bar{v}_1, \overline{2v_2}, \overline{3v_3}, \dots, \overline{Hv_H}\}$$

where each $v_i = \pm 1$. (That is, there is some choice of $v_1, \dots, v_H$ such that $T = S$ may be written in this way.)

Pf

We first show $\#T = H$ - i.e., there are no "duplicates" among $\bar{r}_1, \dots, \bar{r}_H$. Note for some $q_i \in \mathbb{Z}$,

$$ai = pq_i + r_i, \qquad -H \le r_i \le H$$

If r_i and r_j we're the same, or negatives of one another, then $r_i = er_j$ where $e = \pm 1$. This gives

$$\begin{aligned} ai - eaj &= pq_i + r_i - e(pq_j + r_j) \\ &= pq_i - epq_j + r_i - er_j \\ &= pq_i - epq_j \\ &= p(q_i - eq_j) \end{aligned}$$

So $p \mid a(i-ej)$. But $p \nmid a$, so $p \mid i-ej$.

But $|i-ej| < p-1$:

$$\begin{aligned} |i-ej| \leq |i| + |ej| &= |i| + |e||j) \\ &= |i| + |j| \\ &= i + j \\ &\leq H + H \\ &= 2H \\ &= p-1 \end{aligned}$$

Thus, for p to divide $i-ej$, we must have $i-ej=0$, so $i=ej$ which implies $i=j$ as $e=\pm 1$ and $i,j>0$.

Hence each element of T (equiv. S) is a distinct congruence class. As each r_i is in $[-H,H]$, it follows we may choose $v_1, v_2, \dots, v_H \in \{\pm 1\}$ to make

$S = \mathcal{U} = T.$ □

This lemma tells us that if we replace each number in the list

$$a, 2a, 3a, \ldots, Ha$$

with a congruent number in $[-H, H]$, our list has the form

$$\pm 1, \pm 2, \pm 3, \ldots, \pm H$$

with the absolute values of these being precisely $1, 2, \ldots, H$, and no two values are congruent. Let $\mu(a,p)$ denote the number of negatives in this list.

$$\mu(a,p) = \#\{ai \mid 1 \le i \le H, \text{ and } ai \text{ is congruent to a number } -H, -(H-1), \ldots, -1 \text{ modulo } p\}$$

<u>Lemma</u> (Gauss' Criterion)
Let p be an odd prime and a a number which is not a multiple of p. Then

$$\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}$$

Pf/ Note

$$a\cdot 2a\cdot 3a\cdot\ldots\cdot Ha = a^{H}\cdot H!$$

But by the earlier lemma,

$$a\cdot 2a\cdot 3a\cdot\ldots\cdot Ha \equiv v_1 2v_2\cdot\ldots\cdot Hv_H \pmod{p}$$

$$\equiv (v_1\cdots v_H)\cdot H! \pmod{p}$$

$$\equiv (-1)^{\mu(a,p)}\cdot H! \pmod{p}$$

Thus

$$a^{H} \equiv (-1)^{\mu(a,p)} \pmod{p}$$

But Euler's criterion tells us

$$\left(\frac{a}{p}\right) \equiv a^{H} \pmod{p}$$

Hence

$$\left(\frac{a}{p}\right) \equiv (-1)^{\mu(a,p)} \pmod{p}.$$

As $\left(\frac{a}{p}\right)$ and $(-1)^{\mu(a,p)}$ are both ±1, and $p>2$, this means $\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}$ □

Lemma

Suppose a is an odd integer, $p \nmid a$. Then

$$\sum_{k=1}^{H} \left\lfloor \frac{ka}{p} \right\rfloor \equiv \mu(a,p) \pmod 2)$$

This doesn't tell us how to calculate $\mu(a,p)$ per se, but it <u>does</u> tell us how to calculate $(-1)^{\mu(a,p)}$.

Pf

We again let r_k between $-H$ and H denote the congruence class of ak:

$$ak = pq_k + r_k$$

$$\Longrightarrow \frac{a \cdot k}{p} = q_k + \frac{r_k}{p}$$

Notice $-\frac{1}{2} < \frac{r_k}{p} < \frac{1}{2}$. Thus

$$\left\lfloor \frac{ka}{p} \right\rfloor = \begin{cases} q_k & \text{if } r_k > 0 \\ q_k - 1 & \text{if } r_k < 0 \end{cases}$$

If we add all of these together we thus pick up all the q_k and some -1's. We pick up a -1 each time $r_k < 0$ — i.e., each time we have a congruence class in $[-H, 0)$. Thus

$$\sum_{k=1}^{H}\left\lfloor \frac{ka}{p}\right\rfloor = \sum_{k=1}^{H} q_k - \mu(a,p)$$

Our next goal is to show $\sum_{k=1}^{H} q_k$ is even. Note

$$ak = pq_k + r_k$$
$$\Rightarrow k \equiv q_k + r_k \pmod 2$$

as a and p are odd. Hence

$$\sum_{k=1}^{H} k \equiv \sum_{k=1}^{H} q_k + \sum_{k=1}^{H} r_k \pmod 2$$

But

$$\sum_{k=1}^{H} r_k \equiv 1+2+\dots+H \pmod 2$$

But this is exactly the ~~right~~ left-hand side of the equation above—

$$\sum_{k=1}^{H} k \equiv \sum_{k=1}^{H} r_k \pmod 2$$

So

$$\sum_{k=1}^{H} q_k \equiv 0 \pmod 2.$$

So

$$\begin{aligned}\sum_{k=1}^{H}\left\lfloor \frac{ka}{p}\right\rfloor &\equiv -\mu(a,p) \pmod 2\\ &\equiv \mu(a,p) \pmod 2\end{aligned}$$

$\square$

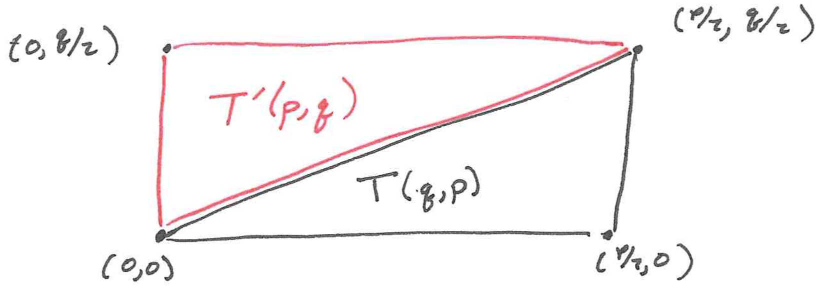
We are now finally in position to prove the law of quadratic reciprocity:

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

where $p \neq q$ are odd primes.

<u>Pf of the law of quadratic reciprocity</u>

Let $H = \frac{p-1}{2}$ and $J = \frac{q-1}{2}$. Now let $T(q,p)$ be the triangle in the xy-plane with vertices $(0,0)$, $(\frac{q}{2}, \frac{q}{2})$, $(\frac{q}{2}, 0)$. Let $T'(p,q)$ be the triangle with vertices $(0,0)$, $(\frac{q}{2}, \frac{q}{2})$, $(0, \frac{q}{2})$.



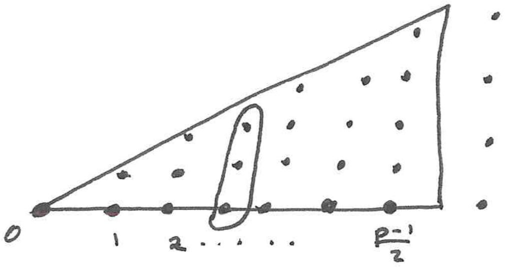
Now we count the number of integer pairs in the interior of these triangles (excluding the boundaries $x=0$ and $y=0$). The slope of the line separating the triangles is

$$\frac{p/2}{q/2} = \frac{p}{q}$$

In $T(q,p)$ the integer points live below this line. For $x=k$ there are

$\left\lfloor \frac{kq}{p} \right\rfloor$ points:

$$(k,1),\ (k,2),\ (k,3),\ \ldots,\ \left(k, \left\lfloor \frac{kq}{p} \right\rfloor\right)$$



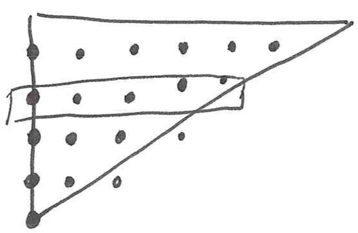
Hence the number of integer points in $T(q,p)$ is

$$\sum_{k=1}^{H} \left\lfloor \frac{kq}{p} \right\rfloor \cancel{= \mu(q,p)}$$

Note modulo 2 this is $\mu(q,p)$.

Similarly the number of points in $T'(p,q)$ is

$$\sum_{k=1}^{J} \left\lfloor \frac{kp}{q} \right\rfloor$$



And modulo 2 this is $\mu(p,q)$.

However, the number of points inside the rectangle formed by these triangles is

$$\left\lfloor \frac{p}{2} \right\rfloor \left\lfloor \frac{q}{2} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

So

$$\mu(p,q) + \mu(q,p) \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod{2}.$$

But by Gauss' criterion,

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

$$= (-1)^{\mu(p,q) + \mu(q,p)}$$

$$= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \qquad \square$$

An extension of the Legendre symbol to non-prime denominators is the Jacobi symbol, defined as follows: if $b = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ is the prime factorization of b, then the Jacobi symbol of a modulo b is, w/ b odd,

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_n}\right)^{\alpha_n}$$

where Legendre symbols appear on the right.

<u>Basic properties</u>

- If p is an odd prime, the Jacobi symbol and the Legendre symbol are the same
- $\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right)$
- $\left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{c}\right)$

Unfortunately, the Jacobi symbol is not as helpful for determining quadratic residues. Consider

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)\cdot(-1) = 1$$

However 2 is <u>not</u> a quadratic residue modulo 15! (Why?)

The Jacobi symbol satisfies a law of quadratic reciprocity, just as the Legendre symbol does.

Thm (Quadratic Reciprocity for Jacobi symbols)
Let a, b be positive odd integers. Then

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

$$\left(\frac{2}{b}\right) = \begin{cases} 1 & \text{if } b \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } b \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$$

$$\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right) & \text{if } a \equiv 1 \text{ or } b \equiv 1 \pmod 4 \\ -\left(\frac{b}{a}\right) & \text{if } a \equiv 3 \equiv b \pmod 4 \end{cases}$$

Pf

Exercise - mimic the proof of quad. recip. for Legendre symbols.