Quadratic reciprocity

1 Introduction

We now begin our next important topic, quadratic reciprocity. We have already answered the following question:

**Question 1:** Given an odd prime $p$, and an integer $a$ with $(a,p) = 1$, when does the equation $x^2 \equiv a \pmod{p}$ have a solution?

Our answer was to consider $a^{(p-1)/2}$ modulo $p$. If this is 1, then $a$ is a square, and if this is $-1$, then $a$ is not a square.

The question that motivates us now is as follows:

**Question 2:** Given an integer $a$, for which primes $p$ does the equation $x^2 \equiv a \pmod{p}$ have a solution?

So, we are now fixing $a$, and letting $p$ vary. This is a much harder question! In Question 1, when $p$ is fixed, there are only finitely many $a$ to consider. In Question 2, when $a$ is fixed, there are infinitely many $p$ to consider. It is not at all obvious whether Question 2 even has a reasonable answer. In fact, a reasonable person might first guess that if $a$ is fixed, the $p$ for which $a$ is a square modulo $p$ vary wildly with no discernible pattern or rule.

Before we dig into this, we introduce a little notation for quadratic residue, the so-called Legendre symbol. Suppose $p$ is an odd prime. One defines

$$\left(\frac{a}{p}\right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic reside modulo } p \\
-1 & \text{if } a \text{ is a non-quadratic reside modulo } p \\
0 & \text{if } p | a.
\end{cases}$$

We already know that if $(a,p) = 1$, then $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. Regarding the Legendre symbol, we have the following simple lemma.

**Lemma 1.** Suppose $p$ is an odd prime. Then

- If $a \equiv b \pmod{p}$, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
- $\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
- If $(a,p) = 1$, then $\left(\frac{a^2}{p}\right) = 1$ and $\left(\frac{a^{2k}}{p}\right) = \left(\frac{b}{p}\right)$.

2 Special cases

Before we state quadratic reciprocity, which will help us evaluate $\left(\frac{a}{p}\right)$ for $a$ fixed and $p$ varying, we are going to work out some (increasingly) involved special cases.

We have already proved the following result:
Lemma 2. Suppose $p$ is an odd prime. Then
\[
\left( \frac{-1}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{4} \\
-1 & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
\]

Let’s see if we can work out if there is a simple rule to calculate $\left( \frac{-3}{p} \right)$. (Of course, I chose this example because we can easily work it out now.)

Lemma 3. Suppose $p > 3$ is prime. Then $\left( \frac{-3}{p} \right)$ is 1 if $p \equiv 1 \pmod{3}$ and $-1$ if $p \equiv 2 \pmod{3}$. In other words, the equation $y^2 \equiv -3 \pmod{p}$ has a solution if and only if $p$ is equivalent to 1 modulo 3.

Proof. Suppose first that $p \equiv 1 \pmod{3}$, and take $g$ with $ord_p(g) = p - 1$. Set $x \equiv g^{(p-1)/3}$. Then $x^3 - 1 \equiv 0 \pmod{p}$. But $x^3 - 1 = (x - 1)(x^2 + x + 1)$, so $x^2 + x + 1 \equiv 0 \pmod{p}$. Multiplying by 4 gives $4x^2 + 4x + 4 \equiv 0 \pmod{p}$, or $(2x + 1)^2 \equiv -3 \pmod{p}$. Thus we may take $y \equiv 2x + 1$.

Conversely, suppose there is a residue class $y$ with $y^2 \equiv -3 \pmod{p}$. Let $x = 2^{-1}(y - 1)$. Then
\[
4(x^2 + x + 1) \equiv (2x)^2 + 2(2x) + 4 \equiv (y - 1)^2 + 2(y - 1) + 4 \equiv y^2 + 3 \equiv 0 \pmod{p}.
\]

Thus $x^2 + x + 1 \equiv 0 \pmod{p}$, so multiplying by $x - 1$ gives $x^3 - 1 \equiv 0$. If $x \equiv 1$, then we could not have $x^2 + x + 1 \equiv 0$, as $p > 3$. Thus $ord_p(x) = 3$, so $3|(p - 1)$ as desired.

We next consider the much trickier case of evaluating $\left( \frac{2}{p} \right)$. We begin with a warm up.

Lemma 4. Suppose $p \equiv 1 \pmod{8}$. Then $\left( \frac{2}{p} \right) = 1$.

Proof. The idea of the proof is as follows: consider the complex number $y_C = \frac{1}{\sqrt{2}}(1 + i)$. This number satisfies $y_C^8 = 1$. Moreover, $y_C^{-1} = \frac{1}{\sqrt{2}}(1 - i)$ so $y_C + y_C^{-1} = \frac{2}{\sqrt{2}} = \sqrt{2}$ and therefore $(y_C + y_C^{-1})^2 = 2$.

We will mimic the above calculations modulo $p$ instead of in the complex numbers. Specifically, let as usual $g$ be a generator, so that $ord_p(g) = p - 1$, and set $y = g^{(p-1)/8}$ (using that $p \equiv 1 \pmod{8}$), so that $ord_p(y) = 8$. Take $x \equiv y + y^{-1} \pmod{p}$. We will check that $x^2 \equiv 2 \pmod{p}$.

To do this, first note that $(y^4 - 1)(y^4 + 1) \equiv y^8 - 1 \equiv 0 \pmod{p}$. Because $y$ does not have order 4, we obtain $y^4 + 1 \equiv 0$. Multiplying by $y^2$ gives $y^2 + (y^{-1})^2 \equiv 0$. Consequently
\[
x^2 \equiv (y + y^{-1})^2 \equiv y^2 + 2 + y^{-2} \equiv 2
\]
as required.

We now evaluate $\left( \frac{2}{p} \right)$ completely.

Proposition 5. Suppose $p$ is an odd prime. Then
\[
\left( \frac{2}{p} \right) = (-1)^{\frac{p^2 - 1}{8}} = \begin{cases} 
1 & \text{if } p \equiv \pm 1 \pmod{8} \\
-1 & \text{if } p \equiv \pm 3 \pmod{8}.
\end{cases}
\]
Proof. Set \( s = (p - 1)/2 \). We’d like to calculate \( 2^s \pmod{p} \), explicitly determining whether this is +1 or −1 modulo \( p \) in terms of whatever \( p \) is modulo 8. In the course of the proof, we will use the following simple fact:

\[
(2) \cdot (4) \cdot (6) \cdots (2p - 4) \cdot (2s) = 2^s s!.
\]

(1)

We will consider two cases: \( p \equiv 1 \pmod{4} \), so that \( s \) is even, and \( p \equiv 3 \pmod{4} \), so that \( s \) is odd. In the first case, we define \( s_0 \) via \( s = 2s_0 \), so that \( s_0 = \frac{p - 1}{4} \). In the second case, we define \( s_0 \) via \( s = 2s_0 + 1 \), so that \( s_0 = \frac{p - 3}{4} \).

The idea of the proof is to calculate the product (1) in another way. In case \( p \equiv 1 \pmod{4} \), one obtains

\[
2 \cdot 4 \cdots (2s) \equiv 2 \cdot 4 \cdot (2s_0) \cdot (-2s_0 + 1)(-2s_0 + 3) \cdots (-5)(-3)(-1)
\equiv (2)(4) \cdots (2s_0)(-1)^{s_0}(1)(3) \cdots (2s_0 - 1)
\equiv (-1)^{s_0} s!.
\]

Therefore we obtain \( 2^s s! \equiv (-1)^{s_0} s! \), so \( 2^s \equiv (-1)^{s_0} (-1)^{(p-1)/4} \). This proves the proposition in the case that \( p \) is 1 or 5 modulo 8.

The second case is nearly identical. One obtains

\[
2 \cdot 4 \cdots (2s) \equiv 2 \cdot 4 \cdot (2s_0) \cdot (-2s_0 - 1)(-2s_0 + 1) \cdots (-5)(-3)(-1)
\equiv (2)(4) \cdots (2s_0)(-1)^{s_0+1}(1)(3) \cdots (2s_0 + 1)
\equiv (-1)^{s_0+1} s!.
\]

Thus \( 2^s s! \equiv (-1)^{s_0+1} s! \) so that \( 2^s \equiv (-1)^{s_0+1} \pmod{p} \). This proves the proposition in case \( p \equiv 3, 7 \pmod{8} \). \( \square \)

3 Quadratic reciprocity

We now come to the statement of quadratic reciprocity.

**Theorem 6** (Quadratic Reciprocity, version I). Suppose the integer \( a \) is fixed. For primes \( p \) with \( (a, p) = 1 \), the value \( \left( \frac{a}{p} \right) \) only depends on \( p \pmod{4|a|} \). That is, if \( p \equiv p' \pmod{4|a|} \) are prime numbers relatively prime to \( a \), then \( \left( \frac{a}{p} \right) = \left( \frac{a}{p'} \right) \).

This theorem follows from the following more precise result together with Proposition 5. Here is what is usually called quadratic reciprocity.

**Theorem 7** (Quadratic Reciprocity, version II). Suppose \( p, q \) are distinct odd primes. Then

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

Some equivalent formulations are: With \( p, q \) odd primes,

1. \( \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left( \frac{p}{q} \right) \) (this is good for computing)
2. \( \left( \frac{q}{p} \right) = \left( \frac{p^*}{q} \right) \) where \( p^* = (-1)^{\frac{p-1}{2}} p \) (this is a more conceptual statement, once you learn more number theory)
3.1 Examples

1. \((\frac{13}{101}) = (\frac{101}{13}) = (\frac{10}{13}) = (-1)(\frac{5}{13}) = (-1)(\frac{2}{13}) = (-1)(\frac{3}{13}) = 1.\) Thus 13 is a square modulo 101.

2. \((\frac{19}{47}) = (\frac{47}{19}) = (\frac{−1}{19}).\) Thus 19 is a quadratic non-residue modulo 19.

3. For which primes \(p\) is 15 a square?

\[
(\frac{15}{p}) = \left(\frac{3}{p}\right) \left(\frac{5}{p}\right) = (-1)^{(p-1)/2} \left(\frac{p}{3}\right) \left(\frac{p}{5}\right).
\]

Now \((-1)^{(p-1)/2}\) is +1 if \(p\) is 1 mod 4 and \(-1\) if \(p\) is 3 modulo 4; \((\frac{p}{3})\) is 1 if \(p\) is 1 modulo 3 and \(-1\) if \(p\) is 2 mod 3; \((\frac{p}{5})\) is 1 if \(p\) is 1, 4 mod 5 and \(-1\) if \(p\) is 2, 3 mod 5. These facts allow us to say for which \(p\) is 15 a square. For example, if \(p\) is 1 mod 4, 2 modulo 3 and 3 modulo 5, then \((\frac{15}{p}) = 1.\) Or, for example, if \(p\) is 3 modulo 4, 1 modulo 3 and 3 modulo 5, then \((\frac{15}{p}) = 1.

Let’s now prove Theorem 6

Proof of Theorem 6. We can write \(a = (a')^2(-1)^u q_1 q_2 \cdots q_r\) for an integer \(a',\ u = 0\ or\ 1,\) and \(q_1, q_2, \ldots, q_j\) distinct primes. Then

\[
(\frac{a}{p}) = (\frac{-1}{p})^u \left(\frac{q_1}{p}\right) \cdots \left(\frac{q_r}{p}\right)
\]

and similarly

\[
(\frac{a}{p'}) = (\frac{-1}{p'})^u \left(\frac{q_1}{p'}\right) \cdots \left(\frac{q_r}{p'}\right).
\]

We claim that the Legendre symbols in each product are equal term-by-term. There are three cases:

1. \((\frac{-1}{p}) = (\frac{-1}{p'}).\) Indeed, because \(p \equiv p' \pmod{4a},\ p \equiv p' \pmod{4},\) and thus \((-1)^{(p-1)/2} = (-1)^{(p'-1)/2}.

2. \((\frac{2}{p}) = (\frac{2}{p'})\) if \(2|a.\) We only need to be concerned with the prime 2 if 2 divides \(a.\) It if does, then \(8|4a\) and thus \(p \equiv p' \pmod{8}.\) Consequently, \((\frac{2}{p}) = (\frac{2}{p'}).\)

3. If \(q\) is an odd prime dividing \(a,\) then \((\frac{q}{p}) = (\frac{q}{p'}).\) Indeed, by quadratic reciprocity, \((\frac{2}{q}) = (-1)^{(q-1)/2} \left(\frac{2}{q}\right).\) But if \(p \equiv p' \pmod{4a},\) then \(p \equiv p' \pmod{4}\) so \((-1)^{(p-1)(q-1)/4} = (-1)^{(p'-1)(q-1)/4},\) and \(p \equiv p' \pmod{q},\) so \((\frac{q}{p}) = (\frac{q}{p'}).\)

The theorem follows.
4 Proof of quadratic reciprocity

We will now sketch one proof of quadratic reciprocity (there are many, many different proofs). We will use the binomial theorem; see section 1.4 in the book if you are not already familiar with this. As a consequence of the binomial theorem, one obtains

**Lemma 8.** Suppose $q$ is a prime number. Then $(x+y)^q \equiv x^q + y^q$ modulo $q$. That is, the difference $(x+y)^q - (x^q + y^q)$ is $q$ times an integer polynomial in $x$ and $y$.

**Proof.** By the binomial theorem, one has

$$(x+y)^q = x^q + y^q + \sum_{k=1}^{q-1} \binom{q}{k} x^{q-k} y^k.$$

But $\binom{q}{k} = \frac{q!}{k!(q-k)!}$. If $1 \leq k \leq q-1$, then the denominator is relatively prime to $q$. But the ratio $\binom{q}{k}$ is an integer, and the numerator is divisible by $q$, so $\binom{q}{k}$ is divisible by $q$. The lemma follows. \qed

By iterating, it follows that

$$(x_1 + x_2 + \cdots + x_r)^q \equiv x_1^q + x_2^q + \cdots + x_r^q \pmod{q} \quad (2)$$

We will sketch the proof of quadratic reciprocity by manipulating some special complex numbers. Specifically, let $\zeta_p = e^{2\pi i/p}$. Then, $\zeta_p$ is a primitive $p$th-root of unity, in the sense that $\zeta_p^p = 1$ and $\zeta_p = 1$ implies $p | r$. The special complex number we will consider is a sum of $p$th-roots of unity, as follows:

$$\tau := \sum_{a \mod p} \left( \frac{a}{p} \right) \zeta_p^a.$$

Here the sum is over nonzero residue classes modulo $p$. Technically, one can write

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

However, if $a \equiv a' \mod p$, then $\left( \frac{a}{p} \right) = \left( \frac{a'}{p} \right)$ and $\zeta_p^a = \zeta_p^{a'}$ so the terms only depend on the residue class $a$ modulo $p$, not the specific integers chosen. That is why we write that the sum is over $a \mod p$, as opposed to from $a = 1$ to $p-1$.

This number $\tau$ satisfies the following very special property:

**Theorem 9.** $\tau^2 = (-1)^{(p-1)/2}p$.

We will not prove this theorem, but will content ourselves with proving the following weaker statement: $|\tau|^2 = p$. To do this, we require the following lemma.

**Lemma 10.** Suppose $r$ is an integer. Then

$$\sum_{b=0}^{p-1} \zeta_p^{rb} = \begin{cases} p & \text{if } p \mid r \\ 0 & \text{if } p \nmid r. \end{cases}$$
Proof. Clearly, if \( p \mid r \), then each term in the sum is 1. As there are \( p \) terms, one gets \( p \), as desired. So, we consider the second case. Let \( S \) denote the sum in question. Multiplying \( S \) by \( \zeta_p^r \) preserves \( S \), as \( \zeta_p^r \zeta_p^p = 1 \). Thus \( \zeta_p^r S = S \). Because \( p \nmid r, \zeta_p^r \neq 1 \) and so \( S = 0 \).

Let’s now evaluate \(|\tau|^2|\).

**Theorem 11.** With notations as above, \(|\tau|^2 = p\).

**Proof.** We have that the complex conjugate \( \tau^* = \sum_{b \mod p} \left(\frac{b}{p}\right) \zeta_p^{-b} \). Thus

\[
|\tau|^2 = \tau \tau^* = \sum_{a \mod p, b \mod p} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \zeta_p^{-ab} = \sum_{a \mod p, b \mod p} \left(\frac{ab}{p}\right) \zeta_p^{-ab} = \sum_{a \mod p, b \mod p} \left(\frac{a}{p}\right) (\zeta_p^{-1})^b.
\]

In the second to last line, we have made the variable change \( a \mapsto ab \). Thus

\[
|\tau|^2 = \sum_{a \mod p} \left(\frac{a}{p}\right) \left(\sum_{b=1}^{p-1} (\zeta_p^{-1})^b\right) = \left(\frac{1}{p}\right) \sum_{b=1}^{p-1} 1 + \sum_{a=2}^{p-1} \left(\frac{a}{p}\right) \left(\sum_{b=1}^{p-1} (\zeta_p^{-1})^b\right) = (p-1) + \sum_{a=2}^{p-1} \left(\frac{a}{p}\right) (-1).
\]

Here we used Lemma [10] to obtain

\[
\sum_{b=1}^{p-1} (\zeta_p^{-1})^b = -1 + \sum_{b=0}^{p-1} (\zeta_p^{-1})^b = -1.
\]

But now

\[
\sum_{a=2}^{p-1} \left(\frac{a}{p}\right) = -1 + \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = -1
\]

because half of the residue classes modulo \( p \) are squares and half are non-squares. Putting everything together, we get \(|\tau|^2 = (p-1) + (-1)(-1) = p\).

Before finally proving quadratic reciprocity, we need a couple lemmas. Define

\[
\mathbb{Z}[\zeta_p] = \{a_0 + a_1 \zeta_p + \cdots + a_{p-1} \zeta_p^{p-1} : a_0, a_1, \ldots, a_{p-1} \in \mathbb{Z}\}.
\]
Lemma 12. If \( x, y \in \mathbb{Z}[\zeta_p] \) then so are \( x + y \), \( -y \) and \( xy \).

Proof. That \( x + y \) and \( -y \) are in \( \mathbb{Z}[\zeta_p] \) is immediate. To see that \( xy \) is in \( \mathbb{Z}[\zeta_p] \), note that \( xy \) is a sum of integer multiples of \( \zeta_j \zeta_k^p = \zeta_{j+k}^p \) for integers \( j, k \) between 0 and \( p - 1 \). But \( \zeta_{j+k}^p = \zeta_r^p \) for an integer \( r \) with \( 0 \leq r \leq p - 1 \). The lemma follows. \( \square \)

If \( q \) is a prime and \( x, y \in \mathbb{Z} [\zeta_p] \), we write \( x \equiv y \pmod{q \mathbb{Z}[\zeta_p]} \) if \( x - y = qz \) for some element \( z \in \mathbb{Z} [\zeta_p] \).

Lemma 13. Suppose \( q \neq p \) is an odd prime. Then

1. \( \left( \frac{q}{p} \right) \tau = \sum_{a \mod p} \left( \frac{aq}{p} \right) \zeta_{p}^{aq} \)
2. \( \tau^q \equiv \left( \frac{q}{p} \right) \tau \pmod{q \mathbb{Z}[\zeta_p]} \).

Proof. For the first part, we have

\[
\left( \frac{q}{p} \right) \tau = \sum_{a \mod p} \left( \frac{aq}{p} \right) \zeta_{p}^{aq} \]

For the second equality, we have made the variable change \( a \mapsto aq \), which just reorders the sum.

For the second statement of the lemma, we have

\[
\tau^q = \left( \sum_{a \mod p} \left( \frac{aq}{p} \right) \zeta_{p}^{aq} \right)^q = \sum_{a \mod p} \left( \frac{aq}{p} \right) \zeta_{p}^{aq} = \sum_{a \mod p} \left( \frac{a}{p} \right) \zeta_{p}^{aq} = \left( \frac{q}{p} \right) \tau \pmod{q \mathbb{Z}[\zeta_p]}.
\]

Here we have used \( \left( \frac{aq}{p} \right) \zeta_{p}^{aq} = \left( \frac{a}{p} \right) \zeta_{p}^{aq} \) to get from the first line to the second, and part (1) of the lemma for the final equality. \( \square \)

We now come to our sketch of the proof of quadratic reciprocity.

Proof of QR. Let \( p, q \) be our distinct odd primes. We have

\[
\left( \frac{q}{p} \right) \tau \equiv \tau^q = \tau (\tau^2)^{\frac{q-1}{2}} = \tau (-1)^{(p-1)/2} p^{\frac{q-1}{2}} = \tau (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} p^{\frac{q-1}{2}} \pmod{q \mathbb{Z}[\zeta_p]}.
\]

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

\[
\left( \frac{q}{p} \right) \tau \equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \tau \left( \frac{p}{q} \right) \pmod{q \mathbb{Z}[\zeta_p]}.
\]
Set \( p^* = (-1)^{(p-1)/2} \), so that \( \tau^2 = p^* \). Multiplying by \( \tau \) we obtain

\[
\left( \frac{q}{p} \right) p^* \equiv (-1)^{(p-1)(q-1)/4} \left( \frac{p}{q} \right) p^* \pmod{\mathbb{Z}[[\zeta_p]]}. \tag{3}
\]

We will not prove it, but it follows from (3) that the two sides are equivalent modulo \( q \), i.e., the two integers in (3) differ by \( qz \) where \( z \in \mathbb{Z} \) and not just \( z \in \mathbb{Z}[[\zeta_p]] \). Consequently, \( \left( \frac{q}{p} \right) \equiv (-1)^{(p-1)(q-1)/4} \left( \frac{p}{q} \right) \pmod{q} \). Because each side of this equivalence is \( \pm 1 \), that they are equivalent modulo \( q \) implies that they are in fact equal. Thus

\[
\left( \frac{q}{p} \right) = (-1)^{(p-1)(q-1)/4} \left( \frac{p}{q} \right),
\]

which is quadratic reciprocity. \( \square \)