By the end of this section you will be able to
- understand the application of law of quadratic reciprocity
- prove the law of quadratic reciprocity

D1 Appreciation of the Law of Quadratic Reciprocity
We stated the law of quadratic reciprocity in the last section:

The Law of Quadratic Reciprocity (7.16).
Let \( p \) and \( q \) be distinct odd primes. Then

\[
\left( \frac{p}{q} \right) \times \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}
\]

Why is this a useful rule?
Well in the last section we established a rule for testing the residues \(-1\) and \(2\) by looking at a given prime and seeing how it was related to modulo \(4\) and \(8\) respectively. What about if a residue is not equal to \(-1\) and \(2\)?

Say we wanted to find the Legendre symbol \( \left( \frac{10}{p} \right) \) where \( p > 5 \). We know \( 10 = 2 \times 5 \) so we have

\[
\left( \frac{10}{p} \right) = \left( \frac{2}{p} \right) \times \left( \frac{5}{p} \right)
\]

For evaluating \( \left( \frac{2}{p} \right) \) we can use (7.15) from the last section:

\[
\left( \frac{2}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv \pm1 \pmod{8} \\
-1 & \text{if } p \equiv \pm3 \pmod{8}
\end{cases}
\]

But how do we find \( \left( \frac{5}{p} \right) \)?
Note that \( 5 \) and \( p \) are distinct odd primes so we can use the above law of quadratic reciprocity (7.16).

In general if we want to find if \( a \) is a quadratic residue of an odd prime \( p \) then we decompose \( a \) into its prime decomposition and then use the law of quadratic reciprocity or the Corollary (7.17) given in the last section.

For example if \( a = q_1 \times q_2 \times \cdots \times q_m \) where \( q \)'s are primes then the Legendre symbol

\[
\left( \frac{a}{p} \right) = \left( \frac{q_1 q_2 \times \cdots \times q_m}{p} \right) = \left( \frac{q_1}{p} \right) \times \left( \frac{q_2}{p} \right) \times \cdots \times \left( \frac{q_m}{p} \right)
\]

This means that we can use the law of quadratic reciprocity or its corollary to find the Legendre symbol \( \left( \frac{a}{p} \right) \) which tells us whether \( a \) is a quadratic residue of modulo \( p \).

How does the Law of Quadratic Reciprocity help?
Consider the following example:
Chapter 7: Quadratic Residues

Example 17

Determine \( (-1)^{\frac{p-1}{2}} \left( \frac{q-1}{2} \right) \) for

(a) \( p \equiv q \equiv 1 \pmod{4} \) 

(b) \( p \equiv q \equiv 3 \pmod{4} \)

(c) \( p \equiv 1 \pmod{4} \), \( q \equiv 3 \pmod{4} \)

(d) \( p \equiv 3 \pmod{4} \), \( q \equiv 1 \pmod{4} \)

Solution

(a) We are given that \( p \equiv q \equiv 1 \pmod{4} \) so there are positive integers \( k \) and \( m \) such that

\[
p = 4k + 1 \quad \text{and} \quad q = 4m + 1
\]

Substituting these \( p = 4k + 1 \) and \( q = 4m + 1 \) into the index \( \left( \frac{p-1}{2} \right) \times \left( \frac{q-1}{2} \right) \) gives

\[
\left( \frac{p-1}{2} \right) \times \left( \frac{q-1}{2} \right) = \left( \frac{4k+1-1}{2} \right) \times \left( \frac{4m+1-1}{2} \right) = 2k \times 2m = 4km \quad \text{[even number]}
\]

Hence \( (-1)^{\frac{p-1}{2}} \left( \frac{q-1}{2} \right) = (-1)^{2km} = 1 \) because we have an even index.

(b) Similarly for \( p \equiv q \equiv 3 \pmod{4} \) we have positive integers \( k \) and \( m \) such that

\[
p = 4k + 3 \quad \text{and} \quad q = 4m + 3
\]

Substituting these \( p = 4k + 3 \) and \( q = 4m + 3 \) into the index \( \left( \frac{p-1}{2} \right) \times \left( \frac{q-1}{2} \right) \) gives

\[
\left( \frac{p-1}{2} \right) \times \left( \frac{q-1}{2} \right) = \left( \frac{4k+3-1}{2} \right) \times \left( \frac{4m+3-1}{2} \right) = (2k+1) \times (2m+1) = 4km + 2k + 2m + 1 \quad \text{[odd number]}
\]

Hence \( (-1)^{\frac{p-1}{2}} \left( \frac{q-1}{2} \right) = (-1)^{4km+2k+2m+1} = -1 \) because we have an odd index.

(c) and (d) See Exercise 7(d).

You will see the solutions to parts (c) and (d) are 1.

From these results of Example 17 what can we conclude about \( \left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2}} \left( \frac{q-1}{2} \right) \)?

Apart from when both \( p \equiv q \equiv 3 \pmod{4} \) we have

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

What does this mean?

It means we must have \( \left( \frac{p}{q} \right) = 1 \) or \( \left( \frac{p}{q} \right) = \left( \frac{q}{p} \right) = -1 \). This \( \left( \frac{p}{q} \right) = \left( \frac{q}{p} \right) = 1 \) implies that \( p \) is a quadratic residue modulo \( q \) and \( q \) is a quadratic residue modulo \( p \). The other result \( \left( \frac{p}{q} \right) = \left( \frac{q}{p} \right) = -1 \) implies that \( p \) is a quadratic non-residue modulo \( q \) and \( q \) is a quadratic non-residue modulo \( p \). Both are quadratic residues or both are quadratic non-residues.

However if \( p \equiv q \equiv 3 \pmod{4} \) then
\[
\left( \frac{p}{q} \right) \times \left( \frac{q}{p} \right) = (-1)^{\left\lfloor \frac{p-1}{2} \right\rfloor \left\lfloor \frac{q-1}{2} \right\rfloor} = -1
\]

**What does this imply?**

\[
\left( \frac{p}{q} \right) = 1 \text{ and } \left( \frac{q}{p} \right) = -1 \text{ or } \left( \frac{p}{q} \right) = -1 \text{ and } \left( \frac{q}{p} \right) = 1
\]

The Legendre symbols in this case are different, that is \( p \) is a quadratic residue of \( q \) but \( q \) is a quadratic non-residue of \( p \) or vice versa.

**D2 Eisenstein’s Lemma**

The proof of the Law of Quadratic Reciprocity given towards the end of this section is the one given by Eisenstein.

Originally Eisenstein was from a Jewish family but even before Eisenstein was born the family had converted to Christianity.

Eisenstein had five siblings, none of them survived childhood. As a young child he took a great interest in mathematics and music. He excelled in mathematics at school and when he was just 17 years old he attended lectures at the University of Berlin.

Writing in his autobiography Eisenstein stated why he loved mathematics – ‘This way of deducing and discovering new truths from old ones ... had an irresistible fascination with me.’

Eisenstein met Gauss at the University of Göttingen in 1844 and Gauss was impressed by Eisenstein’s proof of the Law of Quadratic Reciprocity.

Eisenstein died at the young age of 29 of tuberculosis.

**Example 18**

Determine \( \sum_{k=1}^{(q-1)/2} \left[ \frac{k \times p}{q} \right] + \sum_{k=1}^{(p-1)/2} \left[ \frac{k \times q}{p} \right] \) for the primes \( p = 11 \) and \( q = 13 \). Also find

\[
\left( \frac{p-1}{2} \right) \times \left( \frac{q-1}{2} \right)
\]

**What do you notice about your results?**

**Solution**

Evaluating the first term in the sigma notation by substituting \( p = 11 \) and \( q = 13 \) gives

\[
\sum_{k=1}^{(q-1)/2} \left[ \frac{k \times p}{q} \right] = \sum_{k=1}^{11} \left[ \frac{k \times 11}{13} \right] = \sum_{k=1}^{6} \left[ \frac{k \times 11}{13} \right] = \left[ \frac{1 \times 11}{13} \right] + \left[ \frac{2 \times 11}{13} \right] + \left[ \frac{3 \times 11}{13} \right] + \left[ \frac{4 \times 11}{13} \right] + \left[ \frac{5 \times 11}{13} \right] + \left[ \frac{6 \times 11}{13} \right]
\]

\[
= \left[ \frac{11}{13} \right] + \left[ \frac{22}{13} \right] + \left[ \frac{33}{13} \right] + \left[ \frac{44}{13} \right] + \left[ \frac{55}{13} \right] + \left[ \frac{66}{13} \right] = 0 + 1 + 2 + 3 + 4 + 5 = 15
\]

[Remember \( \left[ \frac{a}{b} \right] \) is the floor function.]
Similarly evaluating the second term in the given sigma notation:
\[
\sum_{k=1}^{(p-1)/2} \left[ \frac{k \times q}{p} \right] = \sum_{k=1}^{(q-1)/2} \left[ \frac{k \times p}{q} \right] = \frac{1 \times 13}{11} + \frac{2 \times 13}{11} + \frac{3 \times 13}{11} + \frac{4 \times 13}{11} + \frac{5 \times 13}{11} = \frac{13}{11} + \frac{26}{11} + \frac{39}{11} + \frac{52}{11} + \frac{65}{11} = 1 + 2 + 3 + 4 + 5 = 15
\]

Adding these two results together gives
\[
\sum_{k=1}^{(p-1)/2} \left[ \frac{k \times p}{q} \right] + \sum_{k=1}^{(q-1)/2} \left[ \frac{k \times q}{p} \right] = 15 + 15 = 30
\]

Working out \( \left( \frac{p-1}{2} \right) \times \left( \frac{q-1}{2} \right) \) with \( p = 11 \) and \( q = 13 \) yields
\[
\left( \frac{11-1}{2} \right) \times \left( \frac{13-1}{2} \right) = 5 \times 6 = 30
\]

In this case we have
\[
\sum_{k=1}^{(p-1)/2} \left[ \frac{k \times p}{q} \right] + \sum_{k=1}^{(q-1)/2} \left[ \frac{k \times q}{p} \right] = \left( \frac{p-1}{2} \right) \times \left( \frac{q-1}{2} \right).
\]

We can illustrate this example geometrically by drawing a line \( y = \frac{q}{p} \times x \) and counting the number of integer (lattice) points to the left and right of this line:

![Figure 12](image)

By *lattice point* we mean a point whose both \( x \) and \( y \) coordinates are integers.

We can count the number of lattice points above the line \( y = \frac{13}{11} \times x \) by counting each of the points to the left of the diagonal \( y = \frac{13}{11} \times x \) as shown in Fig.12. This is the sum:
Similarly the number of lattice points below the diagonal \( y = \frac{x}{11} \) are given by the calculation
\[
\sum_{i=1}^{5} \left\lfloor \frac{13k}{11} \right\rfloor = 1 + 2 + 3 + 4 + 5 = 15
\]

As you can see from Fig.12 that the number of lattice points inside the rectangle between 0 and \( p/2 = 11/2 \) and 0 and \( q/2 = 13/2 \) is
\[
\left( \frac{p-1}{2} \right) \times \left( \frac{q-1}{2} \right) = \left( \frac{11-1}{2} \right) \times \left( \frac{13-1}{2} \right) = 5 \times 6
\]

Since \( p = 11 \) and \( q = 13 \) are distinct primes, the straight line \( y = \frac{13}{11} x \) does not lie on any of the lattice points between \( x = 0 \) and \( p/2 = 11/2 \) and \( y = 0 \) and \( q/2 = 13/2 \).

This result from the above example \( \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor + \sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor = \left( \frac{p-1}{2} \right) \times \left( \frac{q-1}{2} \right) \) is not true for these distinct primes but is true for all distinct odd primes \( p \) and \( q \).

This is Eisenstein's Lemma.
This floor function \( \left\lfloor \frac{kp}{q} \right\rfloor \) gives the number of lattice points on the horizontal line \( y = k \) which lies in the triangle ABC as shown above. We want to find the total number of lattice points in this triangle ABC. How?

We find the number of lattice points along each of the horizontal lines from \( y = 1 \) to \( y = \frac{q-1}{2} \).

Each horizontal line \( y = k \) has \( \left\lfloor \frac{kp}{q} \right\rfloor \) lattice points in the triangle ABC and we have \( y = 1, \cdots, y = \frac{q-1}{2} \) horizontal lines so we sum \( \left\lfloor \frac{kp}{q} \right\rfloor \) from \( k = 1 \) to \( k = \frac{q-1}{2} \):

\[
\sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor
\]

The sum \( \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor \) gives us the total number of lattice points in the upper triangle ABC shown in Fig. 14 below:

![Figure 14](image)

Arguing along similar lines we need to find the number of lattice points below the line \( y = \frac{q}{p}x \), that is in the lower triangle ACD as shown in Figure 15:

![Figure 15](image)
The floor function $\left\lfloor \frac{kq}{p} \right\rfloor$ gives the number of lattice points on the vertical line $x = k$ which lie in the lower triangle ACD.

The number of lattice points on each vertical line $x = k$ is $\left\lfloor \frac{kq}{p} \right\rfloor$. We sum the number of lattice points on each of the lines from $x = 1$ to $x = \frac{p-1}{2}$ which is given by $\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor$.

Hence the total number of lattice points in the lower triangle ACD is $\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor$.

The total number of lattice points in the rectangle ABCD is given by adding the lattice points in each triangle, that is

$$\quad \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor = \text{Number of lattice points in triangle ABC},$$

$$\quad \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor = \text{Number of lattice points in triangle ACD}.$$

Clearly the number of lattice points inside the rectangle ABCD shown in the above diagram is $(\frac{p-1}{2}) \times (\frac{q-1}{2})$. Hence we have our result:

$$\quad \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor = \left( \frac{p-1}{2} \right) \times \left( \frac{q-1}{2} \right)$$

This completes our proof.

We use this lemma to prove the Law of Quadratic Reciprocity. Before we provide the proof we look at a numerical example as well as stating the remaining lemma.

Example 19

Let $p = 23$ and $a = 3$. Show that

$$\quad \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor \equiv g \pmod{2}$$

where $g$ is the number of negative residues as defined in Gauss’s Lemma (7.14).

Solution

We are given that $p = 23$, $a = 3$ and $k = 1, 2, 3, \ldots, \frac{p-1}{2} = \frac{23-1}{2} = 11$.

Evaluating the summation $\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor = \sum_{k=1}^{11} \left\lfloor \frac{3k}{23} \right\rfloor$ gives

$$\sum_{k=1}^{11} \left\lfloor \frac{ka}{p} \right\rfloor = \left\lfloor \frac{3}{23} \right\rfloor + \left\lfloor \frac{6}{23} \right\rfloor + \left\lfloor \frac{9}{23} \right\rfloor + \left\lfloor \frac{12}{23} \right\rfloor + \left\lfloor \frac{15}{23} \right\rfloor + \left\lfloor \frac{18}{23} \right\rfloor + \left\lfloor \frac{21}{23} \right\rfloor + \left\lfloor \frac{24}{23} \right\rfloor + \left\lfloor \frac{27}{23} \right\rfloor + \left\lfloor \frac{30}{23} \right\rfloor + \left\lfloor \frac{33}{23} \right\rfloor$$

$$= 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 1 + 1 + 1 + 1 = 4$$

Writing the elements $ka \pmod{23}$ in the set $S$ we have;
Chapter 7: Quadratic Residues

There are 4 negative residues

\[ \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33\} \]

Since there are 4 negative residues modulo 23 in the above set \( S \) so \( g = 4 \). Hence we have

\[ \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor \equiv 4 \equiv g \pmod{2} \]

This is no coincidence but is generally true so long as \( a \) is odd.

Lemma (7.20).
Let \( p \) be an odd prime and \( a \) also be odd such that \( p \nmid a \). Let \( g \) be the number of negative residues as defined in Gauss’s Lemma (7.14). We have

\[ \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor \equiv g \pmod{2} \]

Proof.
See Exercise 7(d).

Note: Lemma (7.20) can be understood as follows, \( g \pmod{2} \) is either 1 (in the case that \( g \) is odd) or 0 (in the case that \( g \) is even). From Gauss’s lemma we know that the Legendre symbol \( \left( \frac{a}{p} \right) \) is equal to \((-1)^g\) where \( g \) was the number of negative residues. Well, the actual value of \( g \) is not too important, but what is important is whether \( g \) is odd or even. After all;

\[ (-1)^2 = (-1)^{20} = (-1)^{100} \]

D3 Proof of the Law of Quadratic Reciprocity

The Law of Quadratic Reciprocity (7.16).
Let \( p \) and \( q \) be distinct odd primes. Then

\[ \left( \frac{p}{q} \right) \times \left( \frac{q}{p} \right) = (-1)^{\left\lfloor \frac{p-1}{2} \right\rfloor \left\lfloor \frac{q-1}{2} \right\rfloor} \]

Proof.
Consider the least positive residues modulo \( p \) which are the product of \( q \) and the first \( \frac{p-1}{2} \) least positive residues:

\[ S = \left\{ q, 2q, 3q, \ldots, \left( \frac{p-1}{2} \right) q \right\} \]

By the previous lemma (7.20) with \( a = q \) we have

\[ \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor \equiv g \pmod{2} \quad (\dagger) \]

where \( g \) is as defined in Gauss’s Lemma (7.14).
Applying the lemma (7.20) again to the set containing the product $p$ and the first $\frac{q-1}{2}$ least positive residues:

$$T = \left\{ p, \ 2p, \ 3p, \ \ldots, \ \left(\frac{q-1}{2}\right)p \right\}.$$ 

With $a = p$ we have

$$\sum_{k=1}^{\left(\frac{q-1}{2}\right)} \left\lfloor \frac{kp}{q} \right\rfloor = h \mod 2 \quad (\dagger\dagger)$$

where $h$ is same representation as $g$ was in Gauss’s Lemma (7.14).

By applying Gauss’s Lemma (7.14):

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

To $(p/q)$ and $(q/p)$ we have

$$\left(\frac{p}{q}\right) \times \left(\frac{q}{p}\right) = (-1)^g \times (-1)^b = (-1)^{g+b} \quad [\text{By using the rules of indices}]$$

By $(\dagger)$ and $(\dagger\dagger)$ we have

$$\left(\frac{p}{q}\right) \times \left(\frac{q}{p}\right) = (-1)^{g+b} = (-1)$$

By Eisenstein’s Lemma (7.19):

$$\sum_{k=1}^{\left(\frac{q-1}{2}\right)} \left\lfloor \frac{k \times p}{q} \right\rfloor + \sum_{k=1}^{\left(\frac{q-1}{2}\right)} \left\lfloor \frac{k \times q}{p} \right\rfloor = \left(\frac{p-1}{2}\right) \times \left(\frac{q-1}{2}\right)$$

By substituting this into the last line of the above calculation yields

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

This is our required result.

This Law of Quadratic Reciprocity is a very powerful result as you may have noticed from the last section. A more useful result follows from this, which is:

**Corollary (7.17).** Let $p$ and $q$ be distinct odd primes then

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

**Proof.**

See Exercise 7(d).

We have used this corollary to see if a given integer is a quadratic residue of an odd prime $p$ in the last section. We apply this again in the example below.
Example 20
Determine whether the congruence \( x^2 \equiv 35 \pmod{541} \) is solvable (541 is prime).

Solution
We need to find the Legendre symbol \( \left( \frac{35}{541} \right) \). Since \( 35 = 5 \times 7 \) so we have

\[
\left( \frac{35}{541} \right) = \left( \frac{5}{541} \right) \times \left( \frac{7}{541} \right) \quad (*)
\]

Both 5 and 7 are odd primes so we can use the above corollary:

\[
\left( \frac{p}{q} \right) = \begin{cases} 
(q/p) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\
-(q/p) & \text{if both } p \equiv 3 \pmod{4} \text{ and } q \equiv 3 \pmod{4}
\end{cases}
\]

Since \( 5 \equiv 1 \pmod{4} \) so using this on the first term on the right hand side of (*) gives

\[
\left( \frac{5}{541} \right) = \left( \frac{541}{5} \right) = \left( \frac{1}{5} \right) = 1 \quad \text{[Because } 541 \equiv 1 \pmod{5} \text{]}
\]

Examining the second term on the right hand side of (*). We have \( 7 \equiv 3 \pmod{4} \) but \( 541 \equiv 1 \pmod{4} \) so using the above corollary we have

\[
\left( \frac{7}{541} \right) = \left( \frac{541}{7} \right) = \left( \frac{2}{7} \right) \quad \text{[Because } 541 \equiv 2 \pmod{7} \text{]}
\]

We have already established a test for the residue 2 in the last section, Proposition (7.15):

\[
\left( \frac{2}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv \pm 1 \pmod{8} \\
-1 & \text{if } p \equiv \pm 3 \pmod{8}
\end{cases}
\]

Since \( 7 \equiv -1 \pmod{8} \) so using this result we have \( \left( \frac{2}{7} \right) = 1 \).

Multiplying these two Legendre symbols \( \left( \frac{5}{541} \right) = 1 \) and \( \left( \frac{2}{7} \right) = 1 \) of (*) together we have

\[
\left( \frac{35}{541} \right) = \left( \frac{5}{541} \right) \times \left( \frac{7}{541} \right) = 1 \times 1 = 1
\]

Hence \( x^2 \equiv 35 \pmod{541} \) is solvable. (We can find the square root of 35 modulo 541.)

Summary
In this section we have proven the Law of Quadratic Reciprocity

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

and have seen how powerful this result is.