

# The Law of Quadratic Reciprocity

## Reading

- Section 11.3
- Section 11.4

## Practice Problems

**11.3** 1-10

**11.4** 1-10, 13, 14

## Notes

### Law of Quadratic Reciprocity

The Law of Quadratic reciprocity provides us a relation between the Legendre Symbols  $\left(\frac{p}{q}\right)$  and  $\left(\frac{q}{p}\right)$ . It offers us a way to quickly determine one from the other.

#### Law of Quadratic Reciprocity

Let  $p, q$  be odd prime numbers with  $p \neq q$ . Then:

1. If at least one of  $p, q$  is equal to 1 mod 4, then  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ .
2. If both  $p$  and  $q$  are equal to 3 mod 4, then  $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ .

Before looking at the proof, let us see how we can use this in a simple example. Say we want to see if 3 is a quadratic residue modulo 47. They are both primes. Since both 3 and 47 are equal to 3 modulo 4, we are in case 2, so we would have:

$$\left(\frac{3}{47}\right) = -\left(\frac{47}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$$

The last step is by direct inspection, as 2 is not a square modulo 3. So we conclude that 3 is in fact a quadratic residue modulo 47. In fact with some inspection we can see that  $12^2 = 144 = 3 \pmod{47}$ .

As another example, consider  $p = 127$  and  $q = 157$ . We want to determine if 127 is a quadratic residue modulo 157. Since  $157 = 1 \pmod{4}$ , we have, we are in the first case, so:

$$\left(\frac{127}{157}\right) = \left(\frac{157}{127}\right) = \left(\frac{30}{127}\right) = \left(\frac{2}{127}\right) \left(\frac{3}{127}\right) \left(\frac{5}{127}\right)$$

We now have 3 things to compute, but they will all be easier:

- $\left(\frac{2}{127}\right)$ . We will learn how to deal with this case later on. For now, suffice to say that 2 is in fact a square modulo 127, namely  $16^2 = 256 = 2 \pmod{127}$ .
- $\left(\frac{3}{127}\right)$ . We will have to use quadratic reciprocity again, and both 3 and 127 are  $3 \pmod{4}$ , so we would have:

$$\left(\frac{3}{127}\right) = -\left(\frac{127}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

- $\left(\frac{5}{127}\right)$ . Again we start with quadratic reciprocity, and we have (since  $5 = 1 \pmod{4}$ ):

$$\left(\frac{5}{127}\right) = \left(\frac{127}{5}\right) = \left(\frac{2}{5}\right) = -1$$

The last step is because the only squares modulo 5 are 1 and 4.

Now we put it all together:

$$\left(\frac{127}{157}\right) = \left(\frac{2}{127}\right) \left(\frac{3}{127}\right) \left(\frac{5}{127}\right) = 1 \times -1 \times -1 = 1$$

So 127 is a quadratic residue modulo 157. In fact,  $21^2 = 441 = 127 \pmod{157}$ .

## Restatement of Law of Quadratic Reciprocity

We start with a restatement:

### Law of Quadratic Reciprocity (restatement)

Let  $p, q$  be odd primes,  $p \neq q$ . Then:

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

We start by proving that this restatement implies the law of quadratic reciprocity:

- The right-hand-side is 1 if and only if the exponent is even, which happens if and only if at least one of  $\frac{p-1}{2}$  or  $\frac{q-1}{2}$  is even, which is equivalent to at least one of  $p = 1 \pmod{4}$ ,  $q = 1 \pmod{4}$ .
- The left-hand-side is 1 if and only if the two symbols have the same sign, i.e. if and only if  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ .

It is this restatement that we will prove in the following sections.

## Gauss's Lemma

Gauss's lemma is a natural followup to Euler's identity. Let us review that identity:

$$\left(\frac{a}{p}\right) = \bar{a}^{\frac{p-1}{2}} \bmod p$$

The right-hand-side suggests an analogy with Fermat's theorem. In that proof, we obtained the power  $a^{p-1}$  by observing the effect that multiplying by  $a$  had on all the reduced residues. We will do something similar here.

We start with a definition:

We separate the reduced residues modulo  $p$  in two groups:

- $1, 2, \dots, \frac{p-1}{2}$  we will call **positive residues**. The remaining ones, which we can write as  $-\frac{p-1}{2}, -\frac{p-1}{2} + 1, \dots, -1$ , we will call **negative residues**. They are just the negatives of the positive residues.

Multiplying the positive residues by  $\bar{a}$  have a specific behavior: It results in a reordering of the positive residues, with possibly some of them replaced by their negative residues.

If  $p > 2$  is prime and  $\bar{a}$  is a reduced residue, consider the set:

$$\left\{ a \cdot 1, a \cdot 2, \dots, a \cdot \frac{p-1}{2} \right\}$$

The resulting numbers are a reordering of  $\{1, 2, \dots, \frac{p-1}{2}\}$ , with possibly some signs introduced.

To prove this, the only thing needed is the following:

- If  $ax = b$  and  $ay = -b$ , then  $x = a^{-1}b = -y$ .
- Since the  $x$ 's we consider are only the positive residues, this can't happen.
- In other words, the values we get from computing  $ax$  can never include a positive residue as well as the corresponding negative residue.
- So up to the question of the sign, we will see every positive residue exactly once.

This was a preamble to Gauss's Lemma:

## Gauss's Lemma

Let  $p > 2$  be prime, and  $\bar{a}$  be a reduced residue. Let  $g$  be the number of negative residues appearing in the list:

$$\left\{ a \cdot 1, a \cdot 2, \dots, a \cdot \frac{p-1}{2} \right\}$$

Then

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

Let us prove Gauss's lemma:

- Per our previous discussion, we have:

$$(a \cdot 1)(a \cdot 3) \cdots (a \cdot \frac{p-1}{2}) = (-1)^g 1 \cdot 2 \cdots \frac{p-1}{2}$$

- We can cancel out the common terms, and get:

$$\bar{a}^{\frac{p-1}{2}} = (-1)^g$$

- Euler's identity already tells us how to do the next step:

$$\left( \frac{a}{p} \right) = \bar{a}^{\frac{p-1}{2}} = (-1)^g$$

Let us do an illustration:

We'll work modulo  $p = 13$ . The positive residues are then the numbers  $1, 2, \dots, 6$ .

We consider  $\bar{a} = 3$ . We will multiply all the positive residues with it:

$$3 \cdot 1 = 3$$

$$3 \cdot 2 = 6$$

$$3 \cdot 3 = 9 = -4$$

$$3 \cdot 4 = 12 = -1$$

$$3 \cdot 5 = 15 = 2$$

$$3 \cdot 6 = 18 = 5$$

So notice that up to the signs we just permuted the numbers 1 through 6. And we got 2 signs, so  $g = 2$ .

Therefore  $\left( \frac{3}{13} \right) = (-1)^2 = 1$  and 3 is a quadratic residue. In particular  $4^2 = 16 = 3 \pmod{13}$ .

Let's try another number,  $a = 5$  which will turn out to be a quadratic nonresidue. We would have:

$$5 \cdot 1 = 5$$

$$5 \cdot 2 = 10 = -3$$

$$5 \cdot 3 = 15 = 2$$

$$5 \cdot 4 = 20 = -6$$

$$5 \cdot 5 = 25 = -1$$

$$5 \cdot 6 = 30 = 4$$

Notice once again how the numbers 1 through 6 got permuted. This time we got 3 negative signs, so  $g = 3$  and  $\left(\frac{5}{13}\right) = (-1)^3 = -1$ , so 5 is a quadratic nonresidue.

## The quadratic character of 2

We will use Gauss's lemma in our explorations on quadratic reciprocity, starting with determining when 2 is a quadratic residue.

### Quadratic Character of 2

Let  $p > 2$  be prime. Then:

1. If  $p \equiv \pm 1 \pmod{8}$ , then  $\left(\frac{2}{p}\right) = 1$ .
2. If  $p \equiv \pm 3 \pmod{8}$ , then  $\left(\frac{2}{p}\right) = -1$ .
3. We have:

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

We proceed with the proof:

We will use Gauss's lemma. In order to do that, we need to understand how many of the products

$$\left\{ 2 \cdot 1, 2 \cdot 2, \dots, 2 \cdot \frac{p-1}{2} \right\}$$

are negative. Note that the last of these is exactly,  $p-1$  so the values never "roll over to the positives", they are already reduced.

- The product  $2k$  is a positive residue exactly when  $2k \leq \frac{p-1}{2}$ , or in other words when  $k \leq \frac{p-1}{4}$ .
- Therefore the number of positive residues in the products is equal to  $\lfloor \frac{p-1}{4} \rfloor$ , the largest integer less than or equal to  $\frac{p-1}{4}$ .
- So the number of negative residues equals the rest:

$$g = \frac{p-1}{2} - \lfloor \frac{p-1}{4} \rfloor$$

- All that remains is to perform this computation for the various cases of  $p$  that we have to deal with:
  - If  $p = 1 \pmod 8$ , then:
    - \*  $\frac{p-1}{2}$  is **even**.
    - \*  $\lfloor \frac{p-1}{4} \rfloor = \frac{p-1}{4}$  and is **even**.
    - \*  $g = \frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4}$  is **even**.
  - If  $p = 3 \pmod 8$ , then:
    - \*  $\frac{p-1}{2}$  is **odd**.
    - \*  $\lfloor \frac{p-1}{4} \rfloor = \frac{p-1}{4} - \frac{1}{2} = \frac{p-3}{4}$  and is **even**.
    - \*  $g = \frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4}$  is **odd**.
  - If  $p = -3 = 5 \pmod 8$ , then:
    - \*  $\frac{p-1}{2}$  is **even**.
    - \*  $\lfloor \frac{p-1}{4} \rfloor = \frac{p-1}{4}$  and is **odd**.
    - \*  $g = \frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4}$  is **odd**.
  - If  $p = -1 = 7 \pmod 8$ , then:
    - \*  $\frac{p-1}{2}$  is **odd**.
    - \*  $\lfloor \frac{p-1}{4} \rfloor = \frac{p-1}{4} - \frac{1}{2} = \frac{p-3}{4}$  and is **odd**.
    - \*  $g = \frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4}$  is **even**.

As an illustration, recall that earlier we needed to compute  $\left(\frac{2}{127}\right)$ . Since  $127 = -1 \pmod 8$ , we see that  $\left(\frac{2}{127}\right) = 1$  and that 2 is a quadratic residue.