# Chapter 6

# Quadratic Reciprocity

## 6.1 Residue Class Rings

We have already seen that the unit group of $\mathbb{Z}$ is simply $\mathbb{Z}^\times = \{-1, +1\}$, a group of order 2. Let us now determine the unit groups of the rings of residue classes $\mathbb{Z}/m\mathbb{Z}$. Observe that a residue class $[u]_m$ modulo $m$ is a unit if there exists an integer $v$ such that $[uv]_m = [1]_m$, in other words: if $uv \equiv 1 \bmod m$ for some $v \in \mathbb{Z}$.

Now we claim

**Theorem 6.1.** *We have* $(\mathbb{Z}/m\mathbb{Z})^\times = \{a \bmod m : \gcd(a, m) = 1\}$.

*Proof.* It is now that the Bezout representation begins to show its full power. If $\gcd(a, m) = 1$, then there exist integers $x, y \in \mathbb{Z}$ such that $ax + my = 1$. Reducing this equation modulo $m$ gives $ax \equiv 1 \bmod m$, in other words: the residue class $a \bmod m$ is a unit! Not only that: the extended Euclidean algorithm gives us a method to compute the inverse elements.

To prove the converse, assume that $a \bmod m$ is a unit. Then $ac \equiv 1 \bmod m$ for some $c \in \mathbb{Z}$, so $ac = km + 1$ for some $k \in \mathbb{Z}$. But then $ac - km = 1$ shows that $\gcd(a, m) = 1$. □

If $m = p$ is a prime, the unit groups are particularly simple: we have $\gcd(a, p) = 1$ if and only if $p \nmid a$, hence $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \ldots, p-1\} = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$. But if every element $\neq 0$ of a ring has an inverse, then that ring is a field, and we have given a second proof of the following

**Corollary 6.2.** *If $p$ is a prime, then the residue class ring $\mathbb{Z}/p\mathbb{Z}$ is a field.*

The field $\mathbb{Z}/p\mathbb{Z}$ is called a finite field because it has finitely many elements. As we have seen, there are finite fields with $p$ elements for every prime $p$. Later we will see that there exist finite fields with $m > 1$ elements if and only if $m$ is a prime power.

The fact that $\mathbb{Z}/p\mathbb{Z}$ is a field means that expressions like $\frac{1}{7} \bmod 11$ make sense. To compute such 'fractions', you can choose one of the following two methods:

1. Change the numerator mod 11 until the division becomes possible:

$$\frac{1}{7} \equiv \frac{12}{7} \equiv \frac{23}{7} \equiv \frac{34}{7} \equiv \frac{45}{7} \equiv \frac{56}{7} = 8 \bmod 11,$$

   and in fact $7 \cdot 8 = 56 \equiv 1 \bmod 11$. This method only works well if $p$ is small.

2. Apply the Euclidean algorithm to the pair $(7, 11)$, and compute a Bezout representation; you will find that $1 = 2 \cdot 11 - 3 \cdot 7$, and reducing mod 11 gives $1 \equiv (-3) \cdot 7 \bmod 11$, hence the multiplicative inverse of 7 mod 11 is $-3 \equiv 8 \bmod 11$.

## 6.2 Fermat's Little Theorem

**Theorem 6.3** (Fermat's Little Theorem)**.** *If $p$ is a prime and $a$ an integer not divisible by $p$, then $a^{p-1} \equiv 1 \bmod p$.*

The following proof is due to Leibniz[1] and probably the oldest proof known for Fermat's Little Theorem. It uses binomial coefficients: these are the entries in Pascal's triangle, and they occur in the binomial theorem

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + \ldots + \binom{n}{n-1} ab^{n-1} + b^n.$$

We will need two properties of $\binom{n}{k}$: first we use the formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ (which was how we defined them in Chapter 3), and then we claim

**Lemma 6.4.** *If $p$ is a prime, then the numbers $\binom{p}{k}$, $k = 1, 2, \ldots, p-1$, are all divisible by $p$.*

For example, the fifth row of Pascal's triangle is 1 5 10 10 5 1. The claim is not true if $p$ is not a prime: the sixth row is 1 6 15 20 15 6 1, and the numbers 15 and 20 are not divisible by 6.

*Proof.* From $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ we see that the numerator is divisible by $p$ while the denominator is not divisible by $p$ unless $k = 0$ or $k = p$. Thus we conclude that $p \mid \binom{p}{k}$ for $0 < k < p$. □

Now we can give an induction proof of Fermat's Little Theorem:

[1] Gottfried Wilhelm von Leibniz, 1646 (Leipzig) – 1716 (Hannover).

*Proof.* We prove the equivalent (!) statement $a^p \equiv a \bmod p$ for all $a \in \mathbb{Z}$ via induction on $a$. The claim is clearly trivial for $a = 1$; assume it has been proved for some $a$; then

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \ldots + \binom{p}{p-1} a + 1.$$

Since the binomial coefficients are all $\equiv 0 \bmod p$ by the lemma, we find

$$(a+1)^p \equiv a^p + 1 \bmod p,$$

and by the induction assumption, $a^p \equiv a \bmod p$, so we get $(a+1)^p \equiv a+1 \bmod p$, and the induction step is established. □

There is another proof of Fermat's little theorem that works for any finite group. To see what's going on, consider $(\mathbb{Z}/5\mathbb{Z})^\times = \{[1], [2], [3], [4]\}$, where $[r]$ denotes the residue class $r$ mod 5. If we multiply each of these classes by 3, we get

$$\begin{aligned} [1] \cdot [3] &= [3], \\ [2] \cdot [3] &= [1], \\ [3] \cdot [3] &= [4], \\ [4] \cdot [3] &= [2]; \end{aligned}$$

thus multiplying all prime residue classes mod 5 by 3 yields the same classes again, though in a different order. If we multiply these four equations together, we get $[1][2][3][4] \cdot [3]^4 = [3][1][4][2] = [1][2][3][4]$, hence $[3]^4 = [1]$, or, in other words, $3^4 \equiv 1 \bmod 5$. This can be done in general:

*Second Proof of Thm. 6.3.* Write $(\mathbb{Z}/p\mathbb{Z})^\times = \{[1], [2], \ldots, [p-1]\}$; let $a$ be an integer not divisible by $p$. If we multiply each residue class with $[a]$, we get the $p-1$ classes $[a]$, $[2a]$, …, $[(p-1)a]$:

$$\begin{aligned} [1] \cdot [a] &= [a] \\ [2] \cdot [a] &= [2a] \\ &\vdots \\ [p-1] \cdot [a] &= [(p-1)a] \end{aligned}$$

If we can show that the classes on the right hand side are all different, then they must be a permutation of the classes $[1], \ldots, [p-1]$ that we started with. Taking this for granted, the products $[a] \cdot [2a] \cdots [(p-1)a] = [(p-1)!][a^{p-1}]$ and $[1] \cdot [2] \cdots [p-1] = [(p-1)!]$ must be equal (after all, the factors are just rearranged). But $(p-1)!$ is coprime to $p$, so we may cancel this factor, and get $[a^{p-1}] = [1]$, i.e., $a^{p-1} \equiv 1 \bmod p$.

It remains to show that the classes $[a]$, $[2a]$, …, $[(p-1)a]$ are all different. Assume therefore that $[ra] = [sa]$ for integers $1 \le r, s \le p-1$; we have to show

that $r = s$. But $[ra] = [sa]$ means that $[(r-s)a] = [0]$, i.e. that $p \mid (r-s)a$. Since $p \nmid a$ by assumption, the fact that $p$ is prime implies $p \mid (r-s)$. But $r - s$ is an integer strictly between $-p$ and $p$, and the only such integer is 0: thus $r = s$ as claimed. □

One of the ideas behind this proof can be formalized somewhat: First, multiplication by an integer $a$ not divisible by $p$ gives a map $\pi_a : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$; thus $\phi_a[r] = [ar]$. We claim that it is injective. This means that if $\phi_a([r]) = \phi_a([s])$, then $[r] = [s]$. In fact, assume that $\phi_a([r]) = \phi_a([s])$; then $[ar] = [as]$, and since $p \nmid a$, we can cancel the factor $a$ and get $[r] = [s]$.

Now it is clear that injective maps between finite sets of the same cardinality (i.e., with the same number of elements) are necessarily bijective. This proves again that the residue classes $[1 \cdot a]$, $[2 \cdot a]$, ..., $[(p-1) \cdot a]$ are just the classes $[1]$, $[2]$, ..., $[p-1]$ in some different order.

## 6.3 Quadratic Residues

Let $b$ be an integer; an integer $a$ coprime to $b$ is called a quadratic residue modulo $b$ if $a \equiv x^2 \bmod b$ for some integer $x$, and a quadratic nonresidue modulo $b$ otherwise. The quadratic residues modulo 7 are 1, $2 \equiv 3^2$ and 4, whereas 2, 5 and 6 are quadratic nonresidues modulo 7. We have already proved that $-1$ is a quadratic residue modulo $p$ for primes $p \equiv 1 \bmod 4$, and a quadratic nonresidue for primes $p \equiv 3 \bmod 4$.

**Lemma 6.5.** *There are exactly $\frac{p-1}{2}$ quadratic residues modulo an odd prime $p$, namely the squares of the integers $1, 2, \ldots, \frac{p-1}{2}$.*

*Proof.* Clearly the residue classes $1^2, 2^2, \ldots, k^2 \bmod p$, where $p = 2k+1$, are quadratic residues modulo $p$. We claim that they are pairwise distinct. In fact, assume that $i^2 \equiv j^2 \bmod p$ for $1 \le i, j, \le k$. Then $p \mid (i^2 - j^2) = (i-j)(i+j)$. Since $2 \le i+j \le p-1$ we have $p \nmid (i+j)$; since $p$ is prime, this implies $p \mid (i-j)$. Now $-k < i - j < k$, and since the only integer in this interval that is divisible by $p$ is 0, we conclude that $i = j$.

Actually what we have shown is that the function $f(x) = x^2$ is injective as a function of $[1, k] \longrightarrow \mathbb{Z}/p\mathbb{Z}$. In particular, there are at least $k$ quadratic residues. Actually, there aren't any others: if $a \equiv x^2 \bmod p$, then we can reduce $x \bmod p$ in such a way that $-k \le x \le k$, and replacing $x$ by $-x$ if necessary we see that $a \equiv x^2 \bmod p$ for some $x \in [1, k]$. □

Since there are $p-1$ nonzero residue classes modulo $p$ and $\frac{p-1}{2}$ of them are squares, this implies that there exist exactly $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ quadratic nonresidues modulo $p$. These can be represented as follows:

**Lemma 6.6.** *Let $p$ be an odd prime and $n$ some quadratic nonresidue. Then the $k = \frac{p-1}{2}$ quadratic nonresidues are given by $n \cdot 1^2, n \cdot 2^2, \ldots, n \cdot k^2$.*

*Proof.* None of these numbers is a quadratic residue: in fact, $n \cdot r^2 \equiv s^2 \bmod p$ implies that $n \equiv (sr^{-1})^2 \bmod p$ is a square, contradicting our assumption.

Moreover, these numbers are pairwise distinct: $n \cdot r^2 \equiv n \cdot s^2 \bmod p$ implies $r^2 \equiv s^2 \bmod p$, which by the proof of the preceding lemma is only possible if $r = s$.

Since there exist exactly $k$ quadratic nonresidues, the list above must be complete. □

Let us also introduce the following notation: we write

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

The symbol $(\frac{a}{p})$ is called the quadratic Legendre symbol. Here are its most basic properties:

**Proposition 6.7.** *Let $p$ be an odd prime; then*

1. *$a \equiv b \bmod p$ implies $(\frac{a}{p}) = (\frac{b}{p})$;*
2. *the Legendre symbol is multiplicative: $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$ for $a, b \in \mathbb{Z}$ coprime to $p$.*

*Proof.* The first property is clear: If $a \equiv x^2 \bmod p$ and $a \equiv b \bmod p$, then $b \equiv x^2 \bmod p$ and vice versa.

As for the second claim, there are several cases.

1. $(\frac{a}{p}) = (\frac{b}{p}) = +1$: then $a \equiv r^2 \bmod p$ and $b \equiv s^2 \bmod p$, hence $ab \equiv (rs)^2 \bmod p$ and therefore $(\frac{ab}{p}) = 1$.
2. $(\frac{a}{p}) = +1$, $(\frac{b}{p}) = -1$: then $a \equiv r^2 \bmod p$ and $b \equiv n \cdot s^2 \bmod p$, hence $ab \equiv n \cdot (rs)^2 \bmod p$ and therefore $(\frac{ab}{p}) = -1$.
3. $(\frac{a}{p}) = -1$, $(\frac{b}{p}) = +1$: same as above.
4. $(\frac{a}{p}) = (\frac{b}{p}) = -1$: then $a \equiv nr^2 \bmod p$ and $b \equiv ns^2 \bmod p$, hence $ab \equiv (nrs)^2 \bmod p$ and therefore $(\frac{ab}{p}) = 1$.

□

How can we tell whether a given integer is a quadratic residue or not? The following result does not seem to be very useful at first:

**Proposition 6.8** (Euler's Criterion)**.** *We have*

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

*Proof.* The fact that $a^{(p-1)/2} \equiv 1 \bmod p$ if $a$ is a quadratic residue follows trivially from Fermat's Little Theorem. Assume therefore that $(a/p) = -1$. Then every nonzero residue class can be written uniquely as $r^2$ or $ar^2$ for some $1 \leq r \leq \frac{p-1}{2}$. Thus

$$(p-1)! \equiv \prod_r (ar^2)(r^2) \equiv a^{\frac{p-1}{2}} \prod_r [r(p-r)]^2 = a^{\frac{p-1}{2}} [(p-1)!]^2 \bmod p.$$

Since $(p-1)! \equiv -1 \bmod p$ by Wilson's theorem, the claim follows. □

We now give a second proof of the multiplicativity of the numerator of the Legendre symbol using Euler's criterion:

**Proposition 6.9.** *For integers $a, b$ coprime to $p$ we have*

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

*Proof.* If $(\frac{a}{p}) = +1$ or $(\frac{b}{p}) = +1$, this actually follows easily from the definitions. If, however, $(\frac{a}{p}) = (\frac{b}{p}) = -1$, then we have to work harder. The following proof covers all cases: we have $(\frac{a}{p}) \equiv a^{(p-1)/2} \bmod p$, $(\frac{b}{p}) \equiv b^{(p-1)/2} \bmod p$, and $(\frac{ab}{p}) \equiv (ab)^{(p-1)/2} \bmod p$. This implies $(\frac{a}{p})(\frac{b}{p}) \equiv (\frac{ab}{p}) \bmod p$, hence $p$ divides the difference $(\frac{a}{p})(\frac{b}{p}) - (\frac{ab}{p})$. But the absolute value of this difference is $\leq 2$, and since the only number in this interval that is divisible by $p$ is 0, the difference must be 0. □

Another corollary is the quadratic character of $-1$:

**Proposition 6.10.** *For odd primes $p$ we have*

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

This is called the first supplementary law of quadratic reciprocity. The proof is easy: by Euler's criterion, we have $(\frac{-1}{p}) \equiv (-1)^{(p-1)/2} \bmod p$. Thus $(\frac{-1}{p}) - (-1)^{(p-1)/2}$ is an integer between $-2$ and $+2$ that is divisible by $p$: this implies equality $(\frac{-1}{p}) = (-1)^{(p-1)/2}$.

This simple result allows us to prove that there are infinitely many primes of the form $4n+1$. We first formulate a little

**Lemma 6.11.** *If $p > 0$ is an odd prime divisor of an integer of the form $n^2+1$, then $p \equiv 1 \bmod 4$.*

*Proof.* From $p \mid n^2+1$ we deduce that $n^2 \equiv -1 \bmod p$. Thus $-1$ is a quadratic residue modulo $p$, hence $p \equiv 1 \bmod 4$. □

**Corollary 6.12.** *There are infinitely many primes of the form $4n+1$.*

*Proof.* Assume there are only finitely many primes of the form $4n+1$, say $p_1 = 5$, $p_2$, …, $p_n$. Then $N = 4p_1^2 \cdots p_n^2 + 1$ is of the form $4n+1$ and greater than all the primes $p_k$ of this form, hence $N$ must be composite. Now $N$ is odd, hence so is any prime divisor $p$ of $N$, and since any such $p$ is of the form $4n+1$ by Prop. 6.10, we conclude that $p = p_k$ for some index $k$. But then $p_k \mid N$ and $p_k \mid N - 1 = 4p_1^2 \cdots p_n^2$, and we get the contradiction that $p_k \mid (N - (N-1)) = 1$. □

Now let us study the behaviour of the prime 2:

| $p$ | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|
| $(2/p)$ | $-1$ | $-1$ | $+1$ | $-1$ | $-1$ | $+1$ | $-1$ | $+1$ | $-1$ | $+1$ |
| $\sqrt{2}$ | $-$ | $-$ | $\pm 3$ | $-$ | $-$ | $\pm 6$ | $-$ | $\pm 5$ | $-$ | $\pm 8$ |

Thus 2 is a quadratic residue modulo 7, 17, 23, and 31; among the primes in this table, these are exactly the primes of the form $p \equiv \pm 1 \bmod 8$. Thus we conjecture:

**Proposition 6.13.** *The prime 2 is a quadratic residue modulo an odd prime $p$ if and only if $p \equiv \pm 1 \bmod 8$. In other words: we have $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$.*

The fact that the second claim is equivalent to the first is easy to check: Basically, the proof boils down to the following table:

| $a \bmod 8$ | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| $\frac{1}{8}(a^2-1) \bmod 2$ | 0 | 1 | 1 | 0 |

We will prove this conjecture below. Can you use it to prove that there are infinitely many primes of the form $p \equiv \pm 1 \bmod 8$?

## 6.4 Gauss's Lemma

The main ingredient of the elementary proofs of the quadratic reciprocity law is a lemma that Gauss invented for his third proof. Recall how we proved Fermat's Little Theorem: we took a complete set of nonzero residue classes $\{1, 2, \ldots, p-1\}$, multiplied everything by $a$, and pulled out the factor $a^{p-1}$. For quadratic reciprocity, Euler's criterion suggests that we would like to pull out a factor $a^{(p-1)/2}$. That's what made Gauss introduce a halfsystem modulo $p$: this is any set $A = \{a_1, \ldots, a_m\}$ of representatives for residue classes modulo $p = 2m+1$ with the following properties:
a) the $a_j$ are distinct modulo $p$, that is: if $a_i \equiv a_j \bmod p$, then $i = j$;
b) every integer is either congruent modulo $p$ to $a_i$ or to $-a_i$ for some $1 \le i \le \frac{p-1}{2}$.

In other words: a halfsystem $A$ is any set of integers such $A \cup -A$ is a complete set of nonzero residue classes modulo $p$. A typical halfsystem modulo $p$ is the set $A = \{1, 2, \ldots, \frac{p-1}{2}\}$.

Now consider the prime $p = 13$, choose $A = \{1, 2, 3, 4, 5, 6\}$, and look at $a = 2$. Proceeding as in the proof of Fermat's Little Theorem, we multiply everything in sight by 2 and find

$$\begin{aligned} 2 \cdot 1 &\equiv +2 \bmod 13, \\ 2 \cdot 2 &\equiv +4 \bmod 13, \\ 2 \cdot 3 &\equiv +6 \bmod 13, \\ 2 \cdot 4 &\equiv -5 \bmod 13, \\ 2 \cdot 5 &\equiv -3 \bmod 13, \\ 2 \cdot 6 &\equiv -1 \bmod 13. \end{aligned}$$

Thus three products still lie in $A$, while three others lie in $-A$. Thus there is an odd number of sign changes, and 2 is a quadratic nonresidue.

What about $a = 3$? Here we find

$$\begin{aligned} 3 \cdot 1 &\equiv +3 \bmod 13, \\ 3 \cdot 2 &\equiv +6 \bmod 13, \\ 3 \cdot 3 &\equiv -4 \bmod 13, \\ 3 \cdot 4 &\equiv -1 \bmod 13, \\ 3 \cdot 5 &\equiv +2 \bmod 13, \\ 3 \cdot 6 &\equiv +5 \bmod 13. \end{aligned}$$

Here the number of sign changes is even (there are two), and 3 is a quadratic residue modulo 13.

Gauss realized that this is not an accident:

**Lemma 6.14** (Gauss's Lemma)**.** *Let $p = 2n + 1$ be an odd prime, put $A = \{a_1, \ldots, a_n\}$, and let $a$ be an integer not divisible by $p$. Write*

$$a_i a \equiv (-1)^{s(i)} a_{t(i)} \bmod p \tag{6.1}$$

*for every $a_i \in A$, where $s(i) \in \{0, 1\}$ and $t(i) \in \{1, 2, \ldots, n\}$. Then*

$$a^n \equiv \prod_{i=1}^{n} (-1)^{s(i)} \bmod p.$$

Thus $a$ is a quadratic residue or nonresidue modulo $p$ according as the number of sign changes is even or odd. The proof is quite simple:

*Proof.* Observe that the $a_{t(i)}$ in (6.1) run through $A$ if the $a_i$ do, that is: the $a_{t(i)}$ are just the $a_i$ in a different order. In fact, if we had $a_i a \equiv (-1)^{s(i)} a_{t(i)} \bmod p$ and $a_k a \equiv (-1)^{s(k)} a_{t(k)} \bmod p$ with $a_{t(i)} = a_{t(k)}$, then dividing the first

congruence by the second gives $a_i/a_k \equiv (-1)^{s(i)-s(k)} \bmod p$, that is, we have $a_i \equiv \pm a_k \bmod p$ for some choice of sign. But this implies $a_i = a_k$ since $1 \leq a_i, a_k \leq \frac{p-1}{2}$.

Now we apply the usual trick: if two sets of integers coincide, then the product over all elements must be the same. In our case, this means that $\prod_{i=1}^n a_i a \equiv \prod_{i=1}^n (-1)^{s(i)} a_{t(i)} \bmod p$. The left hand side equals $(a_1 a) \cdot (a_2 a) \cdots (a_n a) = a^n \prod_{i=1}^n a_i$, whereas the right hand side is $\prod_{i=1}^n (-1)^{s(i)} \cdot \prod_{i=1}^n a_{t(i)}$. But we have $\prod_{i=1}^n a_{t(i)} = \prod_{i=1}^n a_i$ by the preceding paragraph. Thus we find $a^n \prod_{i=1}^n a_i \equiv \prod_{i=1}^n (-1)^{s(i)} \prod_{i=1}^n a_i$, and since the product over the $a_i$ is coprime to $p$, it may be canceled; this proves the claim. □

Let's apply this to give a proof for our conjecture that $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$. We have to count the number of sign changes when we multiply the "half system" $A = \{1, 2, \ldots, \frac{p-1}{2}\}$ by 2.

1. Assume first that $p = 4k+1$, i.e. $\frac{p-1}{2} = 2k$.

$$\begin{aligned} [1] \cdot [2] &= [2] \\ [2] \cdot [2] &= [4] \\ \ldots &= \ldots \\ [k] \cdot [2] &= [2k] \\ [k+1] \cdot [2] &= [2k+2] = -[2k-1] \\ \ldots &= \ldots \\ [2k] \cdot [2] &= [4k] = -[1] \end{aligned}$$

Here $2a \leq 2k$ for $a < k$, that is for $a = 1, 2, \ldots, k$, so there are no sign changes at all for these $a$. If $k < a \leq 2k$, however, then $2k < 2a \leq p-1$, hence $1 \leq p - 2a < p - 2k = 2k + 1$, which implies that there are sign changes for each $a$ in this interval. Since there are exactly $k$ such $a$, Gauss's Lemma says that $(\frac{2}{p}) = (-1)^k$; we only have to check that $k \equiv \frac{p^2-1}{8} \bmod 2$. But this follows from $\frac{p^2-1}{8} = \frac{1}{8}(p-1)(p+1) = \frac{1}{8} \cdot 4k(4k+2) = k(2k+1)$.

2. Now assume that $p = 4k-1$; then there are no sign changes whenever $1 \leq a \leq k-1$, and there are exactly $k$ sign changes for $k \leq a < 2k$, so again we have $(\frac{2}{p}) = (-1)^k$. But now $\frac{p^2-1}{8} = \frac{1}{8}(p-1)(p+1) = (2k-1)k$ shows that $k \equiv \frac{p^2-1}{8} \bmod 2$, and we have proved

**Proposition 6.15.** *The prime 2 is a quadratic residue of the odd prime $p$ if and only if $p = 8k \pm 1$; in other words: $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$.*

As a corollary, consider the Mersenne numbers $M_q$, where $q$ is odd and $p = 2q+1$ is prime. If $q \equiv 3 \bmod 4$, then $p \equiv 7 \bmod 8$, hence $(2/p) = 1$. By Euler's criterion, this means that $2^q = 2^{(p-1)/2} \equiv 1 \bmod p$, and this in turn shows that $p \mid M_q$.

**Corollary 6.16.** *If $p = 2q+1 \equiv 7 \bmod 8$ is prime, then $p \mid M_q$, the $q$-th Mersenne number.*

In particular, $23 \mid M_{11}$ and $83 \mid M_{41}$. Thus some Mersenne numbers can easily be seen to be composite. There are similar (but more complicated) rules for $p \mid M_q$ when $p = 4q + 1$; in this case, we have to study $2^{(p-1)/4} \bmod p$, which leads us to quartic reciprocity. There is a quartic reciprocity law, but this cannot be formulated in $\mathbb{Z}$: Gauss showed in 1832 that one has to enlarge $\mathbb{Z}$ to the ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$ for doing that.

## 6.5 The Quadratic Reciprocity Law

The quadratic reciprocity law connects the quadratic residue character of two distinct primes $p$ and $q$; at first, it seems completely unlikely that whether $p$ is a square modulo $q$ should have something to do with whether $q$ is a square modulo $p$. Yet we have

**Theorem 6.17** (The Quadratic Reciprocity Law)**.** *For two odd positive primes $p$ and $q$ we have*

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

(As a matter of fact, the reciprocity law also holds in this form if one of $p$ or $q$ is negative; it does not hold if $p$ and $q$ are both negative.)

Thus if $p \equiv 1 \bmod 4$ or $q \equiv 1 \bmod 4$, then $p$ is a quadratic residue modulo $q$ if and only if $q$ is a quadratic residue modulo $p$; and if $p \equiv q \equiv 3 \bmod 4$, then $p$ is a quadratic residue modulo $q$ if and only if $q$ is a quadratic nonresidue modulo $p$.

For example, we have $(\frac{5}{13}) = -1$ and $(\frac{13}{5}) = -1$; on the other hand, $(\frac{3}{7}) = -1$ and $(\frac{7}{3}) = +1$.

Euler first stated a theorem equivalent to the quadratic reciprocity law in 1744; in modern terminology, Euler observed that the quadratic residue character of $p$ modulo primes of the form $4pn \pm s$ with $0 < s < 4p$ and $(s, 2p) = 1$ does not depend on $n$). Using Legendre's notation, we can write this in the following form:

**Theorem 6.18.** *Let $a$ be a nonzero squarefree positive integer; if $p$ and $q$ are odd primes coprime to $4a$, then*

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

*whenever $p \equiv q \bmod 4a$.*

This is easily seen to be equivalent to the more familiar version of quadratic reciprocity: assume that Euler's version holds and consider the case $p \equiv q \bmod 4$; we may assume that $p > q$ and then put $a = (p - q)/4 > 0$. Then $(\frac{p}{q}) = (\frac{p-q}{q}) = (\frac{a}{q})$ as well as $(\frac{q}{p}) = (\frac{-1}{p})(\frac{p-q}{q}) = (\frac{-1}{p})(\frac{a}{p})$. By assumption we have $(\frac{a}{p}) = (\frac{a}{q})$ since $p \equiv q \bmod 4a$, hence $(\frac{p}{q})(\frac{q}{p}) = (\frac{-1}{p})$, which is the quadratic reciprocity law if $p \equiv q \bmod 4$.

If $p \equiv -q \bmod 4$, we put $a = (p+q)/4$ instead, and the same reasoning as above (this time we have $(\frac{a}{p}) = (\frac{a}{-q})$ because $p \equiv -q \bmod 4a$, and of course $(\frac{a}{-q}) = (\frac{a}{q})$ since $a \equiv x^2 \bmod q$ if and only if $a \equiv x^2 \bmod -q$) implies that $(\frac{p}{q}) = (\frac{q}{p})$.

Now assume that Thm. 6.17 holds and let $p$, $q$ be primes with $p \equiv q \bmod 4a$ for some odd positive integer $a$. Then

$$\begin{aligned}\Big(\frac{a}{p}\Big)\Big(\frac{a}{q}\Big) &= (-1)^{\frac{a-1}{2}\frac{p-1}{2}}(-1)^{\frac{a-1}{2}\frac{q-1}{2}}\Big(\frac{p}{a}\Big)\Big(\frac{q}{a}\Big)\\ &= (-1)^{\frac{a-1}{2}(\frac{p-1}{2}+\frac{q-1}{2}} = 1;\end{aligned}$$

here we have used the following facts:

1. $q \equiv p \bmod a$ implies $(\frac{p}{a})(\frac{q}{a}) = (\frac{p}{a})(\frac{p}{a}) = 1$;
2. $\frac{p-1}{2} + \frac{q-1}{2} \equiv 0 \bmod 2$ since $p \equiv q \bmod 4$.

*Proof of Theorem 6.18.* First observe that the quantity $\mu$ in Gauss's Lemma equals the number of all $r$ in the half system $H_p = \{1, 2, \ldots, \frac{p-1}{2}\}$ modulo $p$ such that the fractional part of $ar$ is $> \frac{p}{2}$; denoting the fractional part of a real number $x$ by $\{x\} = x - \lfloor x \rfloor$, we see that $\mu$ is the cardinality of the set

$$P(a) = \Big\{r \in H_p : \Big\{\frac{ar}{p}\Big\} > \frac{1}{2}\Big\}.$$

We can write $P(a)$ as the disjoint union of sets $P_s(a)$, where $P_s(a)$ consists of all the $r$ in the halfsystem modulo $p$ satsifying $\frac{s}{2a}p < r < \frac{s+1}{2a}p$ and $\{\frac{ar}{p}\} > \frac{1}{2}$. The inequality $\frac{s}{2a}p < r < \frac{s+1}{2a}p$ is equivalent to $\frac{s}{2} < \frac{ar}{p} < \frac{s+1}{2}$, and this shows that the sets $P_s(a)$ with $s$ even are empty, and that the condition $\{\frac{ar}{p}\} > \frac{1}{2}$ is automatically satisfied if $s$ is odd. Thus we may put

$$P_s(a) = \Big\{r \in \mathbb{Z} : \frac{s}{2a}p < r < \frac{s+1}{2a}p\Big\}$$

and have

$$\mu = \sum_{0 \le s < a,\ 2 \nmid s} \#P_s(a).$$

Similarly, we have $(\frac{a}{q}) = (-1)^\nu$, where

$$\nu = \sum_{0 \le s < a,\ 2 \nmid s} \#Q_s(a)$$

and

$$Q_s(a) = \Big\{r \in \mathbb{Z} : \frac{s}{2a}q < r < \frac{s+1}{2a}q\Big\}.$$

Now assume that $p - q = 4at$ for some $t \in \mathbb{N}$. Then

$$\begin{aligned} P_s(a) &= \Big\{ r \in \mathbb{Z} : \frac{s}{2a} p < r < \frac{s+1}{2a} p \Big\} \\ &= \Big\{ r \in \mathbb{Z} : \frac{s}{2a}(q + 4at) < r < \frac{s+1}{2a}(q + 4qt) \Big\} \\ &= \Big\{ r \in \mathbb{Z} : \frac{s}{2a} q + 2st < r < \frac{s+1}{2a} q + 2st + 2t) \Big\} \\ &= \Big\{ r' \in \mathbb{Z} : \frac{s}{2a} q < r' < \frac{s+1}{2a} q + 2t) \Big\}, \end{aligned}$$

where $r' = r - 2st$. The last line shows that $\# P_s(a) = \# Q_s(a) + 2t$. Thus $\mu + \nu$ is an even number, and this proves that $(\frac{a}{p}) = (\frac{a}{q})$. □

## 6.6 The Jacobi Symbol

The Legendre symbol $(\frac{a}{p})$ can be generalized to composite values of $p$: if $b = p_1 \cdots p_r$ is a product of odd primes, then we put

$$\Big(\frac{a}{b}\Big) = \Big(\frac{a}{p_1}\Big) \cdots \Big(\frac{a}{p_r}\Big).$$

Thus $(\frac{2}{15}) = (\frac{2}{3})(\frac{2}{5}) = (-1)(-1) = +1$. Note, however, that 2 is not a quadratic residue modulo 15. In fact, we only have

**Proposition 6.19.** *If $(\frac{a}{b}) = -1$, then $a$ is a quadratic nonresidue modulo $b$.*

*Proof.* If $(\frac{a}{b}) = -1$ and $b = \prod p$, then $\prod (\frac{a}{p}) = -1$, and this implies that $(fracap) = -1$ for at least one prime dividing $b$. Now $a \equiv x^2 \bmod b$ implies $a \equiv x^2 \bmod p$, hence $a$ is a quadratic nonresidue modulo $b$. □

We also can generalize the first supplementary law:

**Proposition 6.20.** *We have*

$$\Big(\frac{-1}{a}\Big) = (-1)^{\frac{a-1}{2}}$$

*for all odd integers $a > 0$.*

*Proof.* Write $n = p_1 \cdots p_r$; then

$$\Big(\frac{-1}{n}\Big) = \Big(\frac{-1}{p_1}\Big) \cdots \Big(\frac{-1}{p_r}\Big) = (-1)^{\frac{p_1-1}{2} + \ldots + \frac{p_r-1}{2}}.$$

Thus it remains to show that

$$\frac{n-1}{2} \equiv \frac{p_1 - 1}{2} + \ldots + \frac{p_r - 1}{2} \bmod 2. \tag{6.2}$$

This is done by induction. We start with the observation that $(a-1)(b-1) \equiv 0 \bmod 4$ for odd integers $a, b$, hence $ab-1 \equiv (a-1)+(b-1) \bmod 4$, and dividing by 2 gives

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \bmod 2.$$

Now use induction. □

Now let us treat the reciprocity law similarly.

**Theorem 6.21** (Reciprocity Law for Jacobi Symbols)**.** *If $m$ and $n$ are coprime positive odd integers, then*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) \;=\; (-1)^{\frac{m-1}{2}\,\frac{n-1}{2}}.$$

*Moreover, we have the supplementary laws*

$$\left(\frac{-1}{n}\right) \;=\; (-1)^{\frac{n-1}{2}}, \quad \left(\frac{2}{n}\right) \;=\; (-1)^{\frac{n^2-1}{8}}.$$

*Proof.* Write $m = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$; then

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{(p_i-1)(q_j-1)/4},$$

and our claim will follow if we can prove that

$$\frac{m-1}{2}\frac{n-1}{2} \equiv \sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\frac{q_j-1}{2} \bmod 4.$$

But this follows by multiplying the two congruences you get by applying (6.2) to $m$ and $n$.

Finally, consider the second supplementary law. Similar to the above, everything boils down to showing

$$\frac{n^2-1}{8} \equiv \frac{p_1^2-1}{8} + \ldots + \frac{p_r^2-1}{8} \bmod 2.$$

Now clearly $16 \mid (a^2-1)(b^2-1)$ (as a matter of fact, even this product is even divisible by 64), hence

$$(ab)^2 - 1 \equiv a^2 - 1 + b^2 - 1 \bmod 16.$$

Now induction does the rest. □

# Exercises

6.1 Use Gauss's Lemma to prove that $(\frac{-2}{p}) = +1$ or $-1$ according as $p \equiv 1, 3 \bmod 8$ or $p \equiv 5, 7 \bmod 8$.

6.2 Show that there are infinitely many primes $p \equiv 1 \bmod 3$.

6.3 All primes dividing a number of the form $n^2 + 1$ are congruent to 1 mod 4.

6.4 Show that all odd prime divisors of $9998 = 1000^2 - 2$ satisfy $p \equiv \pm 1 \bmod 8$

6.5 Show that $y^2 = x^3 + 7$ has no integer solutions.

Hints: (This proof is due to V.A. Lebesgue)

1. Show that $x$ is odd.
2. Write the equation as $y^2 + 1 = x^3 + 8$ and factor the right hand side.
3. Show that the quadratic factor is divisible by some prime $p \equiv 3 \bmod 4$
4. Look at the left hand side.

6.6 Generalize the preceding exercise to an infinite family of diophantine equations $y^2 = x^3 + c$.

6.7 (This is a conjecture by Euler) Prove that if $p \equiv 1 \bmod 4$ is prime and $a = \frac{p-1}{4} - n - n^2$, then $(q/p) = +1$ for every $q \mid a$.

6.8 (Euler) If $p \equiv 1 \bmod 4$ is prime, then $\frac{p-1}{4} - n(n+1)$ is a quadratic residue modulo $p$ for every integer $n$.

6.9 (Euler) If $q \equiv 3 \bmod 4$ is prime, then $\frac{q+1}{4} + n(n+1)$ is a quadratic residue modulo $q$ for every integer $n$.

6.10 (Bork) If $q$ and $p = q + 4$ are prime, then $(p/q) = 1$.

6.11 (Bickmore) Since $S_p = 2^{2p} + 1$ is the sum of two squares, so is each of its factors. Verify that, for $p = 2m + 1$, $S_p = A_p B_p$ for $A_p = 2^p - 2^{m+1} + 1$ and $B_p = 2^p + 2^{m+1} + 1$, and write $A_p$ and $B_p$ as a sum of two squares. Use the quadratic reciprocity law to prove that $5 \mid A_p \iff (2/p) = -1$ and $5 \mid B_p \iff (2/p) = +1$.

6.12 Show that $2^{340} \equiv 1 \bmod 341$ (Hint: $341 \cdot 3 = 1023$). Also show that 341 is not prime.