2

Congruences

This chapter introduces the basic properties of congruences modulo n, along with the related notion of residue classes modulo n. Other items discussed include the Chinese remainder theorem, Euler's phi function, Euler's theorem, Fermat's little theorem, quadratic residues, and finally, summations over divisors.

2.1 Equivalence relations

Before discussing congruences, we review the definition and basic properties of equivalence relations.

Let S be a set. A binary relation $\sim$ on S is called an **equivalence relation** if it is

reflexive: $a \sim a$ for all $a \in S$,

symmetric: $a \sim b$ implies $b \sim a$ for all $a, b \in S$, and

transitive: $a \sim b$ and $b \sim c$ implies $a \sim c$ for all $a, b, c \in S$.

If $\sim$ is an equivalence relation on S, then for $a \in S$ one defines its **equivalence class** as the set $\{x \in S : x \sim a\}$.

Theorem 2.1. *Let $\sim$ be an equivalence relation on a set S, and for $a \in S$, let $[a]$ denote its equivalence class. Then for all $a, b \in S$, we have:*

(i) $a \in [a]$*;*

(ii) $a \in [b]$ *implies* $[a] = [b]$.

Proof. (i) follows immediately from reflexivity. For (ii), suppose $a \in [b]$, so that $a \sim b$ by definition. We want to show that $[a] = [b]$. To this end, consider any

$x \in S$. We have

$$\begin{aligned} x \in [a] &\implies x \sim a \text{ (by definition)} \\ &\implies x \sim b \text{ (by transitivity, and since } x \sim a \text{ and } a \sim b) \\ &\implies x \in [b]. \end{aligned}$$

Thus, $[a] \subseteq [b]$. By symmetry, we also have $b \sim a$, and reversing the roles of a and b in the above argument, we see that $[b] \subseteq [a]$. □

This theorem implies that each equivalence class is non-empty, and that each element of S belongs to a unique equivalence class; in other words, the distinct equivalence classes form a *partition* of S (see Preliminaries). A member of an equivalence class is called a **representative** of the class.

EXERCISE 2.1. Consider the relations $=$, $\leq$, and $<$ on the set $\mathbb{R}$. Which of these are equivalence relations? Explain your answers.

EXERCISE 2.2. Let $S := (\mathbb{R} \times \mathbb{R}) \setminus \{(0,0)\}$. For $(x, y), (x', y') \in S$, let us say $(x, y) \sim (x', y')$ if there exists a real number $\lambda > 0$ such that $(x, y) = (\lambda x', \lambda y')$. Show that $\sim$ is an equivalence relation; moreover, show that each equivalence class contains a unique representative that lies on the unit circle (i.e., the set of points (x, y) such that $x^2 + y^2 = 1$).

2.2 Definitions and basic properties of congruences

Let n be a positive integer. For integers a and b, we say that a **is congruent to** b **modulo** n if $n \mid (a - b)$, and we write $a \equiv b \pmod{n}$. If $n \nmid (a - b)$, then we write $a \not\equiv b \pmod{n}$. Equivalently, $a \equiv b \pmod{n}$ if and only if $a = b + ny$ for some $y \in \mathbb{Z}$. The relation $a \equiv b \pmod{n}$ is called a **congruence relation**, or simply, a **congruence**. The number n appearing in such congruences is called the **modulus** of the congruence. This usage of the "mod" notation as part of a congruence is not to be confused with the "mod" operation introduced in §1.1.

If we view the modulus n as fixed, then the following theorem says that the binary relation "$\cdot \equiv \cdot \pmod{n}$" is an equivalence relation on the set $\mathbb{Z}$.

Theorem 2.2. *Let n be a positive integer. For all $a, b, c \in \mathbb{Z}$, we have:*

(i) $a \equiv a \pmod{n}$*;*

(ii) $a \equiv b \pmod{n}$ *implies* $b \equiv a \pmod{n}$*;*

(iii) $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$ *implies* $a \equiv c \pmod{n}$*.*

Proof. For (i), observe that n divides $0 = a - a$. For (ii), observe that if n divides

$a - b$, then it also divides $-(a - b) = b - a$. For (iii), observe that if n divides $a - b$ and $b - c$, then it also divides $(a - b) + (b - c) = a - c$. □

Another key property of congruences is that they are "compatible" with integer addition and multiplication, in the following sense:

Theorem 2.3. *Let $a, a', b, b', n \in \mathbb{Z}$ with $n > 0$. If*

$$a \equiv a' \pmod{n} \ \textit{ and } \ b \equiv b' \pmod{n},$$

then

$$a + b \equiv a' + b' \pmod{n} \ \textit{ and } \ a \cdot b \equiv a' \cdot b' \pmod{n}.$$

Proof. Suppose that $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. This means that there exist integers x and y such that $a = a' + nx$ and $b = b' + ny$. Therefore,

$$a + b = a' + b' + n(x + y),$$

which proves the first congruence of the theorem, and

$$ab = (a' + nx)(b' + ny) = a'b' + n(a'y + b'x + nxy),$$

which proves the second congruence. □

Theorems 2.2 and 2.3 allow one to work with congruence relations modulo n much as one would with ordinary equalities: one can add to, subtract from, or multiply both sides of a congruence modulo n by the same integer; also, if b is congruent to a modulo n, one may substitute b for a in any simple arithmetic expression (involving addition, subtraction, and multiplication) appearing in a congruence modulo n.

Now suppose a is an arbitrary, fixed integer, and consider the set of integers z that satisfy the congruence $z \equiv a \pmod{n}$. Since z satisfies this congruence if and only if $z = a + ny$ for some $y \in \mathbb{Z}$, we may apply Theorems 1.4 and 1.5 (with a as given, and $b := n$) to deduce that every interval of n consecutive integers contains exactly one such z. This simple fact is of such fundamental importance that it deserves to be stated as a theorem:

Theorem 2.4. *Let $a, n \in \mathbb{Z}$ with $n > 0$. Then there exists a unique integer z such that $z \equiv a \pmod{n}$ and $0 \le z < n$, namely, $z := a \bmod n$. More generally, for every $x \in \mathbb{R}$, there exists a unique integer $z \in [x, x + n)$ such that $z \equiv a \pmod{n}$.*

Example 2.1. Let us find the set of solutions z to the congruence

$$3z + 4 \equiv 6 \pmod{7}. \tag{2.1}$$

Suppose that z is a solution to (2.1). Subtracting 4 from both sides of (2.1), we obtain

$$3z \equiv 2 \pmod{7}. \tag{2.2}$$

Next, we would like to divide both sides of this congruence by 3, to get z by itself on the left-hand side. We cannot do this directly, but since $5 \cdot 3 \equiv 1 \pmod{7}$, we can achieve the same effect by multiplying both sides of (2.2) by 5. If we do this, and then replace $5 \cdot 3$ by 1, and $5 \cdot 2$ by 3, we obtain

$$z \equiv 3 \pmod{7}.$$

Thus, if z is a solution to (2.1), we must have $z \equiv 3 \pmod{7}$; conversely, one can verify that if $z \equiv 3 \pmod{7}$, then (2.1) holds. We conclude that the integers z that are solutions to (2.1) are precisely those integers that are congruent to 3 modulo 7, which we can list as follows:

$$\ldots, -18, -11, -4, 3, 10, 17, 24, \ldots \quad \Box$$

In the next section, we shall give a systematic treatment of the problem of solving linear congruences, such as the one appearing in the previous example.

Exercise 2.3. Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Show that $a \equiv b \pmod{n}$ if and only if $(a \bmod n) = (b \bmod n)$.

Exercise 2.4. Let $a, b, n \in \mathbb{Z}$ with $n > 0$ and $a \equiv b \pmod{n}$. Also, let $c_0, c_1, \ldots, c_k \in \mathbb{Z}$. Show that

$$c_0 + c_1 a + \cdots + c_k a^k \equiv c_0 + c_1 b + \cdots + c_k b^k \pmod{n}.$$

Exercise 2.5. Let $a, b, n, n' \in \mathbb{Z}$ with $n > 0$, $n' > 0$, and $n' \mid n$. Show that if $a \equiv b \pmod{n}$, then $a \equiv b \pmod{n'}$.

Exercise 2.6. Let $a, b, n, n' \in \mathbb{Z}$ with $n > 0$, $n' > 0$, and $\gcd(n, n') = 1$. Show that if $a \equiv b \pmod{n}$ and $a \equiv b \pmod{n'}$, then $a \equiv b \pmod{nn'}$.

Exercise 2.7. Let $a, b, n \in \mathbb{Z}$ with $n > 0$ and $a \equiv b \pmod{n}$. Show that $\gcd(a, n) = \gcd(b, n)$.

Exercise 2.8. Let a be a positive integer whose base-10 representation is $a = (a_{k-1} \cdots a_1 a_0)_{10}$. Let b be the sum of the decimal digits of a; that is, let $b := a_0 + a_1 + \cdots + a_{k-1}$. Show that $a \equiv b \pmod{9}$. From this, justify the usual "rules of thumb" for determining divisibility by 9 and 3: a is divisible by 9 (respectively, 3) if and only if the sum of the decimal digits of a is divisible by 9 (respectively, 3).

EXERCISE 2.9. Let e be a positive integer. For $a \in \{0, \dots, 2^e - 1\}$, let $\tilde{a}$ denote the integer obtained by inverting the bits in the e-bit, binary representation of a (note that $\tilde{a} \in \{0, \dots, 2^e - 1\}$). Show that $\tilde{a} + 1 \equiv -a \pmod{2^e}$. This justifies the usual rule for computing negatives in 2's complement arithmetic (which is really just arithmetic modulo 2^e).

EXERCISE 2.10. Show that the equation $7y^3 + 2 = z^3$ has no solutions $y, z \in \mathbb{Z}$.

EXERCISE 2.11. Show that there are 14 distinct, possible, yearly (Gregorian) calendars, and show that all 14 calendars actually occur.

2.3 Solving linear congruences

In this section, we consider the general problem of solving linear congruences. More precisely, for a given positive integer n, and arbitrary integers a and b, we wish to determine the set of integers z that satisfy the congruence

$$az \equiv b \pmod{n}. \tag{2.3}$$

Observe that if (2.3) has a solution z, and if $z \equiv z' \pmod{n}$, then z' is also a solution to (2.3). However, (2.3) may or may not have a solution, and if it does, such solutions may or may not be uniquely determined modulo n. The following theorem precisely characterizes the set of solutions of (2.3); basically, it says that (2.3) has a solution if and only if $d := \gcd(a, n)$ divides b, in which case the solution is uniquely determined modulo n/d.

Theorem 2.5. *Let $a, n \in \mathbb{Z}$ with $n > 0$, and let $d := \gcd(a, n)$.*

(i) For every $b \in \mathbb{Z}$, the congruence $az \equiv b \pmod{n}$ has a solution $z \in \mathbb{Z}$ if and only if $d \mid b$.

(ii) For every $z \in \mathbb{Z}$, we have $az \equiv 0 \pmod{n}$ if and only if $z \equiv 0 \pmod{n/d}$.

(iii) For all $z, z' \in \mathbb{Z}$, we have $az \equiv az' \pmod{n}$ if and only if $z \equiv z' \pmod{n/d}$.

Proof. For (i), let $b \in \mathbb{Z}$ be given. Then we have

$$\begin{aligned} & az \equiv b \pmod{n} \ \text{ for some } z \in \mathbb{Z} \\ \iff\ & az = b + ny \ \text{ for some } z, y \in \mathbb{Z} \text{ (by definition of congruence)} \\ \iff\ & az - ny = b \ \text{ for some } z, y \in \mathbb{Z} \\ \iff\ & d \mid b \ \text{ (by Theorem 1.8).} \end{aligned}$$

For (ii), we have

$$n \mid az \iff n/d \mid (a/d)z \iff n/d \mid z.$$

All of these implications follow rather trivially from the definition of divisibility, except that for the implication $n/d \mid (a/d)z \implies n/d \mid z$, we use Theorem 1.9 and the fact that $\gcd(a/d, n/d) = 1$.

For (iii), we have

$$\begin{aligned} az \equiv az' \pmod{n} &\iff a(z - z') \equiv 0 \pmod{n} \\ &\iff z - z' \equiv 0 \pmod{n/d} \quad \text{(by part (ii))} \\ &\iff z \equiv z' \pmod{n/d}. \quad \square \end{aligned}$$

We can restate Theorem 2.5 in more concrete terms as follows. Let $a, n \in \mathbb{Z}$ with $n > 0$, and let $d := \gcd(a, n)$. Let $I_n := \{0, \ldots, n - 1\}$ and consider the "multiplication by a" map

$$\begin{aligned} \tau_a :\ \ & I_n \to I_n \\ & z \mapsto az \bmod n. \end{aligned}$$

The image of τ_a consists of the n/d integers

$$i \cdot d \ \ (i = 0, \ldots, n/d - 1).$$

Moreover, every element b in the image of τ_a has precisely d pre-images

$$z_0 + j \cdot (n/d) \ \ (j = 0, \ldots, d - 1),$$

where $z_0 \in \{0, \ldots, n/d - 1\}$. In particular, τ_a is a bijection if and only if a and n are relatively prime.

Example 2.2. The following table illustrates what Theorem 2.5 says for $n = 15$ and $a = 1, 2, 3, 4, 5, 6$.

z	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$2z$ mod 15	0	2	4	6	8	10	12	14	1	3	5	7	9	11	13
$3z$ mod 15	0	3	6	9	12	0	3	6	9	12	0	3	6	9	12
$4z$ mod 15	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11
$5z$ mod 15	0	5	10	0	5	10	0	5	10	0	5	10	0	5	10
$6z$ mod 15	0	6	12	3	9	0	6	12	3	9	0	6	12	3	9

In the second row, we are looking at the values $2z$ mod 15, and we see that this row is just a permutation of the first row. So for every b, there exists a unique z such that $2z \equiv b \pmod{15}$. This is implied by the fact that $\gcd(2, 15) = 1$.

In the third row, the only numbers hit are the multiples of 3, which follows from the fact that $\gcd(3, 15) = 3$. Also note that the pattern in this row repeats every five columns; that is, $3z \equiv 3z' \pmod{15}$ if and only if $z \equiv z' \pmod{5}$.

In the fourth row, we again see a permutation of the first row, which follows from the fact that $\gcd(4, 15) = 1$.

In the fifth row, the only numbers hit are the multiples of 5, which follows from the fact that $\gcd(5, 15) = 5$. Also note that the pattern in this row repeats every three columns; that is, $5z \equiv 5z' \pmod{15}$ if and only if $z \equiv z' \pmod 3$.

In the sixth row, since $\gcd(6, 15) = 3$, we see a permutation of the third row. The pattern repeats after five columns, although the pattern is a permutation of the pattern in the third row. □

We develop some further consequences of Theorem 2.5.

A cancellation law. Let $a, n \in \mathbb{Z}$ with $n > 0$. Part (iii) of Theorem 2.5 gives us a **cancellation law** for congruences:

if $\gcd(a, n) = 1$ and $az \equiv az' \pmod n$, then $z \equiv z' \pmod n$.

More generally, if $d := \gcd(a, n)$, then we can cancel a from both sides of a congruence modulo n, as long as we replace the modulus by n/d.

Example 2.3. Observe that

$$5 \cdot 2 \equiv 5 \cdot (-4) \pmod 6. \tag{2.4}$$

Part (iii) of Theorem 2.5 tells us that since $\gcd(5, 6) = 1$, we may cancel the common factor of 5 from both sides of (2.4), obtaining $2 \equiv -4 \pmod 6$, which one can also verify directly.

Next observe that

$$15 \cdot 5 \equiv 15 \cdot 3 \pmod 6. \tag{2.5}$$

We cannot simply cancel the common factor of 15 from both sides of (2.5); indeed, $5 \not\equiv 3 \pmod 6$. However, $\gcd(15, 6) = 3$, and as part (iii) of Theorem 2.5 guarantees, we do indeed have $5 \equiv 3 \pmod 2$. □

Modular inverses. Again, let $a, n \in \mathbb{Z}$ with $n > 0$. We say that $z \in \mathbb{Z}$ is a **multiplicative inverse of** a **modulo** n if $az \equiv 1 \pmod n$. Part (i) of Theorem 2.5 says that a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$. Moreover, part (iii) of Theorem 2.5 says that the multiplicative inverse of a, if it exists, is uniquely determined modulo n; that is, if z and z' are multiplicative inverses of a modulo n, then $z \equiv z' \pmod n$. Note that if z is a multiplicative inverse of a modulo n, then a is a multiplicative inverse of z modulo n. Also note that if $a \equiv a' \pmod n$, then z is a multiplicative inverse of a modulo n if and only if z is a multiplicative inverse of a' modulo n.

Now suppose that $a, b, n \in \mathbb{Z}$ with $n > 0$, $a \neq 0$, and $\gcd(a, n) = 1$. Theorem 2.5 says that there exists a unique integer z satisfying

$$az \equiv b \pmod n \text{ and } 0 \leq z < n.$$

Setting $s := b/a \in \mathbb{Q}$, we may generalize the "mod" operation, defining $s \bmod n$ to be this value z. As the reader may easily verify, this definition of $s \bmod n$ does not depend on the particular choice of fraction used to represent the rational number s. With this notation, we can simply write $a^{-1} \bmod n$ to denote the unique multiplicative inverse of a modulo n that lies in the interval $0, \ldots, n-1$.

Example 2.4. Looking back at the table in Example 2.2, we see that

$$2^{-1} \bmod 15 = 8 \text{ and } 4^{-1} \bmod 15 = 4,$$

and that neither 3, 5, nor 6 have modular inverses modulo 15. □

Example 2.5. Let $a, b, n \in \mathbb{Z}$ with $n > 0$. We can describe the set of solutions $z \in \mathbb{Z}$ to the congruence $az \equiv b \pmod{n}$ very succinctly in terms of modular inverses.

If $\gcd(a, n) = 1$, then setting $t := a^{-1} \bmod n$, and $z_0 := tb \bmod n$, we see that z_0 is the unique solution to the congruence $az \equiv b \pmod{n}$ that lies in the interval $\{0, \ldots, n-1\}$.

More generally, if $d := \gcd(a, n)$, then the congruence $az \equiv b \pmod{n}$ has a solution if and only if $d \mid b$. So suppose that $d \mid b$. In this case, if we set $a' := a/d$, $b' := b/d$, and $n' := n/d$, then for each $z \in \mathbb{Z}$, we have $az \equiv b \pmod{n}$ if and only if $a'z \equiv b' \pmod{n'}$. Moreover, $\gcd(a', n') = 1$, and therefore, if we set $t := (a')^{-1} \bmod n'$ and $z_0 := tb' \bmod n'$, then the solutions to the congruence $az \equiv b \pmod{n}$ that lie in the interval $\{0, \ldots, n-1\}$ are the d integers $z_0, z_0 + n', \ldots, z_0 + (d-1)n'$. □

EXERCISE 2.12. Let $a_1, \ldots, a_k, b, n$ be integers with $n > 0$. Show that the congruence

$$a_1 z_1 + \cdots + a_k z_k \equiv b \pmod{n}$$

has a solution $z_1, \ldots, z_k \in \mathbb{Z}$ if and only if $d \mid b$, where $d := \gcd(a_1, \ldots, a_k, n)$.

EXERCISE 2.13. Let p be a prime, and let a, b, c, e be integers, such that $e > 0$, $a \not\equiv 0 \pmod{p^{e+1}}$, and $0 \leq c < p^e$. Define N to be the number of integers $z \in \{0, \ldots, p^{2e} - 1\}$ such that

$$\left\lfloor \left((az + b) \bmod p^{2e} \right) / p^e \right\rfloor = c.$$

Show that $N = p^e$.

2.4 The Chinese remainder theorem

Next, we consider systems of linear congruences with respect to moduli that are relatively prime in pairs. The result we state here is known as the Chinese remainder theorem, and is extremely useful in a number of contexts.

Theorem 2.6 (Chinese remainder theorem). *Let $\{n_i\}_{i=1}^k$ be a pairwise relatively prime family of positive integers, and let $a_1, \ldots, a_k$ be arbitrary integers. Then there exists a solution $a \in \mathbb{Z}$ to the system of congruences*

$$a \equiv a_i \pmod{n_i} \ \ (i = 1, \ldots, k).$$

Moreover, any $a' \in \mathbb{Z}$ is a solution to this system of congruences if and only if $a \equiv a' \pmod{n}$, where $n := \prod_{i=1}^k n_i$.

Proof. To prove the existence of a solution a to the system of congruences, we first show how to construct integers $e_1, \ldots, e_k$ such that for $i, j = 1, \ldots, k$, we have

$$e_j \equiv \begin{cases} 1 \pmod{n_i} & \text{if } j = i, \\ 0 \pmod{n_i} & \text{if } j \neq i. \end{cases} \tag{2.6}$$

If we do this, then setting

$$a := \sum_{i=1}^k a_i e_i,$$

one sees that for $j = 1, \ldots, k$, we have

$$a \equiv \sum_{i=1}^k a_i e_i \equiv a_j \pmod{n_j},$$

since all the terms in this sum are zero modulo n_j, except for the term $i = j$, which is congruent to a_j modulo n_j.

To construct $e_1, \ldots, e_k$ satisfying (2.6), let $n := \prod_{i=1}^k n_i$ as in the statement of the theorem, and for $i = 1, \ldots, k$, let $n_i^* := n/n_i$; that is, n_i^* is the product of all the moduli n_j with $j \neq i$. From the fact that $\{n_i\}_{i=1}^k$ is pairwise relatively prime, it follows that for $i = 1, \ldots, k$, we have $\gcd(n_i, n_i^*) = 1$, and so we may define $t_i := (n_i^*)^{-1} \bmod n_i$ and $e_i := n_i^* t_i$. One sees that $e_i \equiv 1 \pmod{n_i}$, while for $j \neq i$, we have $n_i \mid n_j^*$, and so $e_j \equiv 0 \pmod{n_i}$. Thus, (2.6) is satisfied.

That proves the existence of a solution a to the given system of congruences. If $a \equiv a' \pmod{n}$, then since $n_i \mid n$ for $i = 1, \ldots, k$, we see that $a' \equiv a \equiv a_i \pmod{n_i}$ for $i = 1, \ldots, k$, and so a' also solves the system of congruences.

Finally, if a' is a solution to the given system of congruences, then $a \equiv a_i \equiv a' \pmod{n_i}$ for $i = 1, \ldots, k$. Thus, $n_i \mid (a - a')$ for $i = 1, \ldots, k$. Since $\{n_i\}_{i=1}^k$ is pairwise relatively prime, this implies $n \mid (a - a')$, or equivalently, $a \equiv a' \pmod{n}$. □

We can restate Theorem 2.6 in more concrete terms, as follows. For each positive integer m, let I_m denote $\{0, \ldots, m-1\}$. Suppose $\{n_i\}_{i=1}^k$ is a pairwise relatively prime family of positive integers, and set $n := n_1 \cdots n_k$. Then the map

$$\begin{aligned} \tau : \quad I_n &\to I_{n_1} \times \cdots \times I_{n_k} \\ a &\mapsto (a \bmod n_1, \ldots, a \bmod n_k) \end{aligned}$$

is a bijection.

Example 2.6. The following table illustrates what Theorem 2.6 says for $n_1 = 3$ and $n_2 = 5$.

a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
a mod 3	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
a mod 5	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4

We see that as a ranges from 0 to 14, the pairs $(a \bmod 3, a \bmod 5)$ range over all pairs (a_1, a_2) with $a_1 \in \{0, 1, 2\}$ and $a_2 \in \{0, \ldots, 4\}$, with every pair being hit exactly once. □

EXERCISE 2.14. Compute the values e_1, e_2, e_3 in the proof of Theorem 2.6 in the case where $k = 3$, $n_1 = 3$, $n_2 = 5$, and $n_3 = 7$. Also, find an integer a such that $a \equiv 1 \pmod{3}$, $a \equiv -1 \pmod{5}$, and $a \equiv 5 \pmod{7}$.

EXERCISE 2.15. If you want to show that you are a real nerd, here is an age-guessing game you might play at a party. You ask a fellow party-goer to divide his age by each of the numbers 3, 4, and 5, and tell you the remainders. Show how to use this information to determine his age.

EXERCISE 2.16. Let $\{n_i\}_{i=1}^k$ be a pairwise relatively prime family of positive integers. Let $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$ be integers, and set $d_i := \gcd(a_i, n_i)$ for $i = 1, \ldots, k$. Show that there exists an integer z such that $a_i z \equiv b_i \pmod{n_i}$ for $i = 1, \ldots, k$ if and only if $d_i \mid b_i$ for $i = 1, \ldots, k$.

EXERCISE 2.17. For each prime p, let $\nu_p(\cdot)$ be defined as in §1.3. Let $p_1, \ldots, p_r$ be distinct primes, $a_1, \ldots, a_r$ be arbitrary integers, and $e_1, \ldots, e_r$ be arbitrary non-negative integers. Show that there exists an integer a such that $\nu_{p_i}(a - a_i) = e_i$ for $i = 1, \ldots, r$.

EXERCISE 2.18. Suppose n_1 and n_2 are positive integers, and let $d := \gcd(n_1, n_2)$. Let a_1 and a_2 be arbitrary integers. Show that there exists an integer a such that $a \equiv a_1 \pmod{n_1}$ and $a \equiv a_2 \pmod{n_2}$ if and only if $a_1 \equiv a_2 \pmod{d}$.

2.5 Residue classes

As we already observed in Theorem 2.2, for any fixed positive integer n, the binary relation "$\cdot \equiv \cdot \pmod{n}$" is an equivalence relation on the set $\mathbb{Z}$. As such, this relation partitions the set $\mathbb{Z}$ into equivalence classes. We denote the equivalence class containing the integer a by $[a]_n$, and when n is clear from context, we simply write $[a]$. By definition, we have

$$z \in [a] \iff z \equiv a \pmod{n} \iff z = a + ny \text{ for some } y \in \mathbb{Z},$$

and hence

$$[a] = a + n\mathbb{Z} := \{a + ny : y \in \mathbb{Z}\}.$$

Historically, these equivalence classes are called **residue classes modulo** n, and we shall adopt this terminology here as well. Note that a given residue class modulo n has many different "names"; for example, the residue class $[n-1]$ is the same as the residue class $[-1]$. Any member of a residue class is called a **representative** of that class.

We define $\mathbb{Z}_n$ to be the set of residue classes modulo n. The following is simply a restatement of Theorem 2.4:

Theorem 2.7. *Let n be a positive integer. Then $\mathbb{Z}_n$ consists of the n distinct residue classes $[0], [1], \ldots, [n-1]$. Moreover, for every $x \in \mathbb{R}$, each residue class modulo n contains a unique representative in the interval $[x, x+n)$.*

When working with residue classes modulo n, one often has in mind a particular set of representatives. Typically, one works with the set of representatives $\{0, 1, \ldots, n-1\}$. However, sometimes it is convenient to work with another set of representatives, such as the representatives in the interval $[-n/2, n/2)$. In this case, if n is odd, we can list the elements of $\mathbb{Z}_n$ as

$$[-(n-1)/2], \ldots, [-1], [0], [1], \ldots, [(n-1)/2],$$

and when n is even, we can list the elements of $\mathbb{Z}_n$ as

$$[-n/2], \ldots, [-1], [0], [1], \ldots, [n/2-1].$$

We can "equip" $\mathbb{Z}_n$ with binary operations defining addition and multiplication in a natural way as follows: for $a, b \in \mathbb{Z}$, we define

$$[a] + [b] := [a+b],$$
$$[a] \cdot [b] := [a \cdot b].$$

Of course, one has to check that this definition is unambiguous, in the sense that the sum or product of two residue classes should not depend on which particular representatives of the classes are chosen in the above definitions. More precisely, one must check that if $[a] = [a']$ and $[b] = [b']$, then $[a + b] = [a' + b']$ and $[a \cdot b] = [a' \cdot b']$. However, this property follows immediately from Theorem 2.3.

Observe that for all $a, b, c \in \mathbb{Z}$, we have

$$[a] + [b] = [c] \iff a + b \equiv c \pmod{n},$$

and

$$[a] \cdot [b] = [c] \iff a \cdot b \equiv c \pmod{n},$$

Example 2.7. Consider the residue classes modulo 6. These are as follows:

$$\begin{aligned}
[0] &= \{\ldots, -12, -6, 0, 6, 12, \ldots\} \\
[1] &= \{\ldots, -11, -5, 1, 7, 13, \ldots\} \\
[2] &= \{\ldots, -10, -4, 2, 8, 14, \ldots\} \\
[3] &= \{\ldots, -9, -3, 3, 9, 15, \ldots\} \\
[4] &= \{\ldots, -8, -2, 4, 10, 16, \ldots\} \\
[5] &= \{\ldots, -7, -1, 5, 11, 17, \ldots\}\ .
\end{aligned}$$

Let us write down the addition and multiplication tables for $\mathbb{Z}_6$. The addition table looks like this:

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4] .

The multiplication table looks like this:

·	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1] .

Instead of using representatives in the interval $[0, 6)$, we could just as well use representatives from another interval, such as $[-3, 3)$. Then, instead of naming the residue classes [0], [1], [2], [3], [4], [5], we would name them [−3], [−2], [−1], [0], [1], [2]. Observe that [−3] = [3], [−2] = [4], and [−1] = [5]. □

These addition and multiplication operations on $\mathbb{Z}_n$ yield a very natural algebraic structure. For example, addition and multiplication are commutative and associative; that is, for all $\alpha, \beta, \gamma \in \mathbb{Z}_n$, we have

$$\alpha + \beta = \beta + \alpha, \ \ (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma),$$
$$\alpha\beta = \beta\alpha, \ \ (\alpha\beta)\gamma = \alpha(\beta\gamma).$$

Note that we have adopted here the usual convention of writing $\alpha\beta$ in place of $\alpha \cdot \beta$. Furthermore, multiplication distributes over addition; that is, for all $\alpha, \beta, \gamma \in \mathbb{Z}_n$, we have

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma.$$

All of these properties follow from the definitions, and the corresponding properties for $\mathbb{Z}$; for example, the fact that addition in $\mathbb{Z}_n$ is commutative may be seen as follows: if $\alpha = [a]$ and $\beta = [b]$, then

$$\alpha + \beta = [a] + [b] = [a + b] = [b + a] = [b] + [a] = \beta + \alpha.$$

Because addition and multiplication in $\mathbb{Z}_n$ are associative, for $\alpha_1, \dots, \alpha_k \in \mathbb{Z}_n$, we may write the sum $\alpha_1 + \cdots + \alpha_k$ and the product $\alpha_1 \cdots \alpha_k$ without any parentheses, and there is no ambiguity; moreover, since both addition and multiplication are commutative, we may rearrange the terms in such sums and products without changing their values.

The residue class $[0]$ acts as an **additive identity**; that is, for all $\alpha \in \mathbb{Z}_n$, we have $\alpha + [0] = \alpha$; indeed, if $\alpha = [a]$, then $a + 0 \equiv a \pmod{n}$. Moreover, $[0]$ is the only element of $\mathbb{Z}_n$ that acts as an additive identity; indeed, if $a + z \equiv a \pmod{n}$ holds for all integers a, then it holds in particular for $a = 0$, which implies $z \equiv 0 \pmod{n}$. The residue class $[0]$ also has the property that $\alpha \cdot [0] = [0]$ for all $\alpha \in \mathbb{Z}_n$.

Every $\alpha \in \mathbb{Z}_n$ has an **additive inverse**, that is, an element $\beta \in \mathbb{Z}_n$ such that $\alpha + \beta = [0]$; indeed, if $\alpha = [a]$, then clearly $\beta := [-a]$ does the job, since $a + (-a) \equiv 0 \pmod{n}$. Moreover, α has a unique additive inverse; indeed, if $a + z \equiv 0 \pmod{n}$, then subtracting a from both sides of this congruence yields $z \equiv -a \pmod{n}$. We naturally denote the additive inverse of α by $-\alpha$. Observe that the additive inverse of $-\alpha$ is α; that is $-(-\alpha) = \alpha$. Also, we have the identities

$$-(\alpha + \beta) = (-\alpha) + (-\beta), \ (-\alpha)\beta = -(\alpha\beta) = \alpha(-\beta), \ (-\alpha)(-\beta) = \alpha\beta.$$

For $\alpha, \beta \in \mathbb{Z}_n$, we naturally write $\alpha - \beta$ for $\alpha + (-\beta)$.

The residue class $[1]$ acts as a **multiplicative identity**; that is, for all $\alpha \in \mathbb{Z}_n$, we have $\alpha \cdot [1] = \alpha$; indeed, if $\alpha = [a]$, then $a \cdot 1 \equiv a \pmod{n}$. Moreover, $[1]$ is the only element of $\mathbb{Z}_n$ that acts as a multiplicative identity; indeed, if $a \cdot z \equiv a \pmod{n}$ holds for all integers a, then in particular, it holds for $a = 1$, which implies $z \equiv 1 \pmod{n}$.

For $\alpha \in \mathbb{Z}_n$, we call $\beta \in \mathbb{Z}_n$ a **multiplicative inverse** of α if $\alpha\beta = [1]$. Not all $\alpha \in \mathbb{Z}_n$ have multiplicative inverses. If $\alpha = [a]$ and $\beta = [b]$, then β is a multiplicative inverse of α if and only if $ab \equiv 1 \pmod{n}$. Theorem 2.5 implies that α has a multiplicative inverse if and only if $\gcd(a, n) = 1$, and that if it exists, it is unique. When it exists, we denote the multiplicative inverse of α by α^{-1}.

We define $\mathbb{Z}_n^*$ to be the set of elements of $\mathbb{Z}_n$ that have a multiplicative inverse. By the above discussion, we have

$$\mathbb{Z}_n^* = \{[a] : a = 0, \ldots, n-1, \ \gcd(a, n) = 1\}.$$

If n is prime, then $\gcd(a, n) = 1$ for $a = 1, \ldots, n-1$, and we see that $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{[0]\}$. If n is composite, then $\mathbb{Z}_n^* \subsetneq \mathbb{Z}_n \setminus \{[0]\}$; for example, if $d \mid n$ with $1 < d < n$, we see that $[d]$ is not zero, nor does it belong to $\mathbb{Z}_n^*$. Observe that if $\alpha, \beta \in \mathbb{Z}_n^*$, then so are α^{-1} and $\alpha\beta$; indeed,

$$(\alpha^{-1})^{-1} = \alpha \ \text{ and } \ (\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}.$$

For $\alpha \in \mathbb{Z}_n$ and $\beta \in \mathbb{Z}_n^*$, we naturally write α/β for $\alpha\beta^{-1}$.

Suppose α, β, γ are elements of $\mathbb{Z}_n$ that satisfy the equation

$$\alpha\beta = \alpha\gamma.$$

If $\alpha \in \mathbb{Z}_n^*$, we may multiply both sides of this equation by α^{-1} to infer that

$$\beta = \gamma.$$

This is the **cancellation law** for $\mathbb{Z}_n$. We stress the requirement that $\alpha \in \mathbb{Z}_n^*$, and not just $\alpha \neq [0]$. Indeed, consider any $\alpha \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$. Then we have $\alpha = [a]$ with $d := \gcd(a, n) > 1$. Setting $\beta := [n/d]$ and $\gamma := [0]$, we see that

$$\alpha\beta = \alpha\gamma \ \text{ and } \ \beta \neq \gamma.$$

Example 2.8. We list the elements of $\mathbb{Z}_{15}^*$, and for each $\alpha \in \mathbb{Z}_{15}^*$, we also give α^{-1}:

α	[1]	[2]	[4]	[7]	[8]	[11]	[13]	[14]
α^{-1}	[1]	[8]	[4]	[13]	[2]	[11]	[7]	[14]

. □

For $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}_n$, we may naturally write their sum as $\sum_{i=1}^k \alpha_i$. By convention, this sum is $[0]$ when $k = 0$. It is easy to see that $-\sum_{i=1}^k \alpha_i = \sum_{i=1}^k (-\alpha_i)$; that is, the additive inverse of the sum is the sum of the additive inverses. In the special case where all the α_i's have the same value α, we define $k \cdot \alpha := \sum_{i=1}^k \alpha$; thus, $0 \cdot \alpha = [0]$, $1 \cdot \alpha = \alpha$, $2 \cdot \alpha = \alpha + \alpha$, $3 \cdot \alpha = \alpha + \alpha + \alpha$, and so on. The additive inverse of $k \cdot \alpha$ is $k \cdot (-\alpha)$, which we may also write as $(-k) \cdot \alpha$; thus, $(-1) \cdot \alpha = -\alpha$, $(-2) \cdot \alpha = (-\alpha) + (-\alpha) = -(\alpha + \alpha)$, and so on. Therefore, the notation $k \cdot \alpha$, or more simply, $k\alpha$, is defined for all integers k. Note that for all integers k and a, we have $k[a] = [ka] = [k][a]$.

For all $\alpha, \beta \in \mathbb{Z}_n$ and $k, \ell \in \mathbb{Z}$, we have the identities:

$$k(\ell\alpha) = (k\ell)\alpha = \ell(k\alpha),\ (k+\ell)\alpha = k\alpha + \ell\alpha,\ k(\alpha+\beta) = k\alpha + k\beta,$$
$$(k\alpha)\beta = k(\alpha\beta) = \alpha(k\beta).$$

Analogously, for $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}_n$, we may write their product as $\prod_{i=1}^{k} \alpha_i$. By convention, this product is $[1]$ when $k = 0$. It is easy to see that if all of the α_i's belong to $\mathbb{Z}_n^*$, then so does their product, and in particular, $(\prod_{i=1}^{k} \alpha_i)^{-1} = \prod_{i=1}^{k} \alpha_i^{-1}$; that is, the multiplicative inverse of the product is the product of the multiplicative inverses. In the special case where all the α_i's have the same value α, we define $\alpha^k := \prod_{i=1}^{k} \alpha$; thus, $\alpha^0 = [1]$, $\alpha^1 = \alpha$, $\alpha^2 = \alpha\alpha$, $\alpha^3 = \alpha\alpha\alpha$, and so on. If $\alpha \in \mathbb{Z}_n^*$, then the multiplicative inverse of α^k is $(\alpha^{-1})^k$, which we may also write as α^{-k}; for example, $\alpha^{-2} = \alpha^{-1}\alpha^{-1} = (\alpha\alpha)^{-1}$. Therefore, when $\alpha \in \mathbb{Z}_n^*$, the notation α^k is defined for all integers k.

For all $\alpha, \beta \in \mathbb{Z}_n$ and all *non-negative* integers k and ℓ, we have the identities:

$$(\alpha^\ell)^k = \alpha^{k\ell} = (\alpha^k)^\ell,\ \alpha^{k+\ell} = \alpha^k\alpha^\ell,\ (\alpha\beta)^k = \alpha^k\beta^k. \tag{2.7}$$

If $\alpha, \beta \in \mathbb{Z}_n^*$, the identities in (2.7) hold for all $k, \ell \in \mathbb{Z}$.

For all $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_\ell \in \mathbb{Z}_n$, the distributive property implies that

$$(\alpha_1 + \cdots + \alpha_k)(\beta_1 + \cdots + \beta_\ell) = \sum_{\substack{1 \le i \le k \\ 1 \le j \le \ell}} \alpha_i\beta_j.$$

One last notational convention. As already mentioned, when the modulus n is clear from context, we usually write $[a]$ instead of $[a]_n$. Although we want to maintain a clear distinction between integers and their residue classes, occasionally even the notation $[a]$ is not only redundant, but distracting; in such situations, we may simply write a instead of $[a]$. For example, for every $\alpha \in \mathbb{Z}_n$, we have the identity $(\alpha + [1]_n)(\alpha - [1]_n) = \alpha^2 - [1]_n$, which we may write more simply as $(\alpha + [1])(\alpha - [1]) = \alpha^2 - [1]$, or even more simply, and hopefully more clearly, as $(\alpha + 1)(\alpha - 1) = \alpha^2 - 1$. Here, the only reasonable interpretation of the symbol "1" is $[1]$, and so there can be no confusion.

In summary, algebraic expressions involving residue classes may be manipulated in much the same way as expressions involving ordinary numbers. Extra complications arise only because when n is composite, some non-zero elements of $\mathbb{Z}_n$ do not have multiplicative inverses, and the usual cancellation law does not apply for such elements.

In general, one has a choice between working with congruences modulo n, or with the algebraic structure $\mathbb{Z}_n$; ultimately, the choice is one of taste and convenience, and it depends on what one prefers to treat as "first class objects": integers and congruence relations, or elements of $\mathbb{Z}_n$.

An alternative, and somewhat more concrete, approach to constructing $\mathbb{Z}_n$ is to directly define it as the set of n “symbols” $[0], [1], \dots, [n-1]$, with addition and multiplication defined as

$$[a] + [b] := [(a + b) \bmod n], \quad [a] \cdot [b] := [(a \cdot b) \bmod n],$$

for $a, b \in \{0, \dots, n-1\}$. Such a definition is equivalent to the one we have given here. One should keep this alternative characterization of $\mathbb{Z}_n$ in mind; however, we prefer the characterization in terms of residue classes, as it is mathematically more elegant, and is usually more convenient to work with.

We close this section with a reinterpretation of the Chinese remainder theorem (Theorem 2.6) in terms of residue classes.

Theorem 2.8 (Chinese remainder map). *Let $\{n_i\}_{i=1}^k$ be a pairwise relatively prime family of positive integers, and let $n := \prod_{i=1}^k n_i$. Define the map*

$$\begin{aligned} \theta : \quad \mathbb{Z}_n &\to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \\ [a]_n &\mapsto ([a]_{n_1}, \dots, [a]_{n_k}). \end{aligned}$$

(i) The definition of θ is unambiguous.

(ii) θ is bijective.

(iii) For all $\alpha, \beta \in \mathbb{Z}_n$, if $\theta(\alpha) = (\alpha_1, \dots, \alpha_k)$ and $\theta(\beta) = (\beta_1, \dots, \beta_k)$, then:

- *(a) $\theta(\alpha + \beta) = (\alpha_1 + \beta_1, \dots, \alpha_k + \beta_k)$;*
- *(b) $\theta(-\alpha) = (-\alpha_1, \dots, -\alpha_k)$;*
- *(c) $\theta(\alpha\beta) = (\alpha_1\beta_1, \dots, \alpha_k\beta_k)$;*
- *(d) $\alpha \in \mathbb{Z}_n^*$ if and only if $\alpha_i \in \mathbb{Z}_{n_i}^*$ for $i = 1, \dots, k$, in which case $\theta(\alpha^{-1}) = (\alpha_1^{-1}, \dots, \alpha_k^{-1})$.*

Proof. For (i), note that $a \equiv a' \pmod{n}$ implies $a \equiv a' \pmod{n_i}$ for $i = 1, \dots, k$, and so the definition of θ is unambiguous (it does not depend on the choice of a).

(ii) follows directly from the statement of the Chinese remainder theorem.

For (iii), let $\alpha = [a]_n$ and $\beta = [b]_n$, so that for $i = 1, \dots, k$, we have $\alpha_i = [a]_{n_i}$ and $\beta_i = [b]_{n_i}$. Then we have

$$\begin{aligned} \theta(\alpha + \beta) &= \theta([a + b]_n) = ([a + b]_{n_1}, \dots, [a + b]_{n_k}) = (\alpha_1 + \beta_1, \dots, \alpha_k + \beta_k), \\ \theta(-\alpha) &= \theta([-a]_n) = ([-a]_{n_1}, \dots, [-a]_{n_k}) = (-\alpha_1, \dots, -\alpha_k), \text{ and} \\ \theta(\alpha\beta) &= \theta([ab]_n) = ([ab]_{n_1}, \dots, [ab]_{n_k}) = (\alpha_1\beta_1, \dots, \alpha_k\beta_k). \end{aligned}$$

That proves parts (a), (b), and (c). For part (d), we have

$$\begin{aligned} \alpha \in \mathbb{Z}_n^* &\iff \gcd(a, n) = 1 \\ &\iff \gcd(a, n_i) = 1 \ \text{ for } i = 1, \ldots, k \\ &\iff \alpha_i \in \mathbb{Z}_{n_i}^* \ \text{ for } i = 1, \ldots, k. \end{aligned}$$

Moreover, if $\alpha \in \mathbb{Z}_n^*$ and $\beta = \alpha^{-1}$, then

$$(\alpha_1\beta_1, \ldots, \alpha_k\beta_k) = \theta(\alpha\beta) = \theta([1]_n) = ([1]_{n_1}, \ldots, [1]_{n_k}),$$

and so for $i = 1, \ldots, k$, we have $\alpha_i\beta_i = [1]_{n_i}$, which is to say $\beta_i = \alpha_i^{-1}$. □

Theorem 2.8 is very powerful conceptually, and is an indispensable tool in many situations. It says that if we want to understand what happens when we add or multiply $\alpha, \beta \in \mathbb{Z}_n$, it suffices to understand what happens when we add or multiply their "components" $\alpha_i, \beta_i \in \mathbb{Z}_{n_i}$. Typically, we choose $n_1, \ldots, n_k$ to be primes or prime powers, which usually simplifies the analysis. We shall see many applications of this idea throughout the text.

Exercise 2.19. Let $\theta : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ be as in Theorem 2.8, and suppose that $\theta(\alpha) = (\alpha_1, \ldots, \alpha_k)$. Show that for every non-negative integer m, we have $\theta(\alpha^m) = (\alpha_1^m, \ldots, \alpha_k^m)$. Moreover, if $\alpha \in \mathbb{Z}_n^*$, show that this identity holds for all integers m.

Exercise 2.20. Let p be an odd prime. Show that $\sum_{\beta \in \mathbb{Z}_p^*} \beta^{-1} = \sum_{\beta \in \mathbb{Z}_p^*} \beta = 0$.

Exercise 2.21. Let p be an odd prime. Show that the numerator of $\sum_{i=1}^{p-1} 1/i$ is divisible by p.

Exercise 2.22. Suppose n is square-free (see Exercise 1.15), and let $\alpha, \beta, \gamma \in \mathbb{Z}_n$. Show that $\alpha^2\beta = \alpha^2\gamma$ implies $\alpha\beta = \alpha\gamma$.

2.6 Euler's phi function

Euler's phi function (also called **Euler's totient function**) is defined for all positive integers n as

$$\varphi(n) := |\mathbb{Z}_n^*|.$$

Equivalently, $\varphi(n)$ is equal to the number of integers between 0 and $n - 1$ that are relatively prime to n. For example, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, and $\varphi(4) = 2$.

Using the Chinese remainder theorem, more specifically Theorem 2.8, it is easy to get a nice formula for $\varphi(n)$ in terms of the prime factorization of n, as we establish in the following sequence of theorems.

Theorem 2.9. *Let $\{n_i\}_{i=1}^k$ be a pairwise relatively prime family of positive integers, and let $n := \prod_{i=1}^k n_i$. Then*

$$\varphi(n) = \prod_{i=1}^{k} \varphi(n_i).$$

Proof. Consider the map $\theta : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ in Theorem 2.8. By parts (ii) and (iii.d) of that theorem, restricting θ to $\mathbb{Z}_n^*$ yields a one-to-one correspondence between $\mathbb{Z}_n^*$ and $\mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$. The theorem now follows immediately. □

We already know that $\varphi(p) = p - 1$ for every prime p, since the integers $1, \ldots, p - 1$ are not divisible by p, and hence are relatively prime to p. The next theorem generalizes this, giving us a formula for Euler's phi function at prime powers.

Theorem 2.10. *Let p be a prime and e be a positive integer. Then*

$$\varphi(p^e) = p^{e-1}(p - 1).$$

Proof. The multiples of p among $0, 1, \ldots, p^e - 1$ are

$$0 \cdot p, 1 \cdot p, \ldots, (p^{e-1} - 1) \cdot p,$$

of which there are precisely p^{e-1}. Thus, $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p - 1)$. □

If $n = p_1^{e_1} \cdots p_r^{e_r}$ is the factorization of n into primes, then the family of prime powers $\{p_i^{e_i}\}_{i=1}^r$ is pairwise relatively prime, and so Theorem 2.9 implies $\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r})$. Combining this with Theorem 2.10, we have:

Theorem 2.11. *If $n = p_1^{e_1} \cdots p_r^{e_r}$ is the factorization of n into primes, then*

$$\varphi(n) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1) = n \prod_{i=1}^{r} (1 - 1/p_i).$$

EXERCISE 2.23. Show that $\varphi(nm) = \gcd(n, m) \cdot \varphi(\operatorname{lcm}(n, m))$.

EXERCISE 2.24. Show that if n is divisible by r distinct odd primes, then $2^r \mid \varphi(n)$.

EXERCISE 2.25. Define $\varphi_2(n)$ to be the number of integers $a \in \{0, \ldots, n-1\}$ such that $\gcd(a, n) = \gcd(a + 1, n) = 1$. Show that if $n = p_1^{e_1} \cdots p_r^{e_r}$ is the factorization of n into primes, then $\varphi_2(n) = n \prod_{i=1}^r (1 - 2/p_i)$.

2.7 Euler's theorem and Fermat's little theorem

Let n be a positive integer, and let $\alpha \in \mathbb{Z}_n^*$.

Consider the sequence of powers of α:

$$1 = \alpha^0, \alpha^1, \alpha^2, \ldots.$$

Since each such power is an element of $\mathbb{Z}_n^*$, and since $\mathbb{Z}_n^*$ is a finite set, this sequence of powers must start to repeat at some point; that is, there must be a positive integer k such that $\alpha^k = \alpha^i$ for some $i = 0, \ldots, k-1$. Let us assume that k is chosen to be the smallest such positive integer. This value k is called the **multiplicative order of** α.

We claim that $\alpha^k = 1$. To see this, suppose by way of contradiction that $\alpha^k = \alpha^i$, for some $i = 1, \ldots, k-1$; we could then cancel α from both sides of the equation $\alpha^k = \alpha^i$, obtaining $\alpha^{k-1} = \alpha^{i-1}$, which would contradict the minimality of k.

Thus, we can characterize the multiplicative order of α as the smallest positive integer k such that

$$\alpha^k = 1.$$

If $\alpha = [a]$ with $a \in \mathbb{Z}$ (and $\gcd(a, n) = 1$, since $\alpha \in \mathbb{Z}_n^*$), then k is also called the **multiplicative order of** a **modulo** n, and can be characterized as the smallest positive integer k such that

$$a^k \equiv 1 \pmod{n}.$$

From the above discussion, we see that the first k powers of α, that is, $\alpha^0, \alpha^1, \ldots, \alpha^{k-1}$, are distinct. Moreover, other powers of α simply repeat this pattern. The following is an immediate consequence of this observation.

Theorem 2.12. *Let n be a positive integer, and let α be an element of $\mathbb{Z}_n^*$ of multiplicative order k. Then for every $i \in \mathbb{Z}$, we have $\alpha^i = 1$ if and only if k divides i. More generally, for all $i, j \in \mathbb{Z}$, we have $\alpha^i = \alpha^j$ if and only if $i \equiv j \pmod{k}$.*

Example 2.9. Let $n = 7$. For each value $a = 1, \ldots, 6$, we can compute successive powers of a modulo n to find its multiplicative order modulo n.

i	1	2	3	4	5	6
1^i mod 7	1	1	1	1	1	1
2^i mod 7	2	4	1	2	4	1
3^i mod 7	3	2	6	4	5	1
4^i mod 7	4	2	1	4	2	1
5^i mod 7	5	4	6	2	3	1
6^i mod 7	6	1	6	1	6	1

So we conclude that modulo 7: 1 has order 1; 6 has order 2; 2 and 4 have order 3; and 3 and 5 have order 6. □

Theorem 2.13 (Euler's theorem). *Let n be a positive integer and $\alpha \in \mathbb{Z}_n^*$. Then $\alpha^{\varphi(n)} = 1$. In particular, the multiplicative order of α divides $\varphi(n)$.*

Proof. Since $\alpha \in \mathbb{Z}_n^*$, for every $\beta \in \mathbb{Z}_n^*$ we have $\alpha\beta \in \mathbb{Z}_n^*$, and so we may define the "multiplication by α" map

$$\begin{aligned} \tau_\alpha : \quad \mathbb{Z}_n^* &\to \mathbb{Z}_n^* \\ \beta &\mapsto \alpha\beta. \end{aligned}$$

It is easy to see that τ_α is a bijection:

Injectivity: If $\alpha\beta = \alpha\beta'$, then cancel α to obtain $\beta = \beta'$.

Surjectivity: For every $\gamma \in \mathbb{Z}_n^*$, $\alpha^{-1}\gamma$ is a pre-image of γ under τ_α.

Thus, as β ranges over the set $\mathbb{Z}_n^*$, so does $\alpha\beta$, and we have

$$\prod_{\beta \in \mathbb{Z}_n^*} \beta = \prod_{\beta \in \mathbb{Z}_n^*} (\alpha\beta) = \alpha^{\varphi(n)} \Big(\prod_{\beta \in \mathbb{Z}_n^*} \beta \Big). \tag{2.8}$$

Canceling the common factor $\prod_{\beta \in \mathbb{Z}_n^*} \beta \in \mathbb{Z}_n^*$ from the left- and right-hand side of (2.8), we obtain

$$1 = \alpha^{\varphi(n)}.$$

That proves the first statement of the theorem. The second follows immediately from Theorem 2.12. □

As a consequence of this, we obtain:

Theorem 2.14 (Fermat's little theorem). *For every prime p, and every $\alpha \in \mathbb{Z}_p$, we have $\alpha^p = \alpha$.*

Proof. If $\alpha = 0$, the statement is obviously true. Otherwise, $\alpha \in \mathbb{Z}_p^*$, and by Theorem 2.13 we have $\alpha^{p-1} = 1$. Multiplying this equation by α yields $\alpha^p = \alpha$. □

In the language of congruences, Fermat's little theorem says that for every prime p and every integer a, we have

$$a^p \equiv a \pmod{p}.$$

For a given positive integer n, we say that $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$ is a **primitive root modulo** n if the multiplicative order of a modulo n is equal to $\varphi(n)$. If this is the case, then for $\alpha := [a] \in \mathbb{Z}_n^*$, the powers α^i range over all elements of $\mathbb{Z}_n^*$ as i ranges over the interval $0, \ldots, \varphi(n) - 1$. Not all positive integers have primitive roots—we will see in §7.5 that the only positive integers n for which there exists a primitive root modulo n are

$$n = 1, 2, 4, p^e, 2p^e,$$

where p is an odd prime and e is a positive integer.

The following theorem is sometimes useful in determining the multiplicative order of an element in $\mathbb{Z}_n^*$.

Theorem 2.15. *Suppose $\alpha \in \mathbb{Z}_n^*$ has multiplicative order k. Then for every $m \in \mathbb{Z}$, the multiplicative order of α^m is $k/\gcd(m,k)$.*

Proof. Applying Theorem 2.12 to α^m, we see that the multiplicative order of α^m is the smallest positive integer ℓ such that $\alpha^{m\ell} = 1$. But we have

$$\begin{aligned} \alpha^{m\ell} = 1 &\iff m\ell \equiv 0 \pmod{k} \quad \text{(applying Theorem 2.12 to } \alpha\text{)} \\ &\iff \ell \equiv 0 \pmod{k/\gcd(m,k)} \quad \text{(by part (ii) of Theorem 2.5).} \quad \square \end{aligned}$$

EXERCISE 2.26. Find all elements of $\mathbb{Z}_{19}^*$ of multiplicative order 18.

EXERCISE 2.27. Let $n \in \mathbb{Z}$ with $n > 1$. Show that n is prime if and only if $\alpha^{n-1} = 1$ for every non-zero $\alpha \in \mathbb{Z}_n$.

EXERCISE 2.28. Let $n = pq$, where p and q are distinct primes. Show that if $m := \operatorname{lcm}(p-1, q-1)$, then $\alpha^m = 1$ for all $\alpha \in \mathbb{Z}_n^*$.

EXERCISE 2.29. Let p be any prime other than 2 or 5. Show that p divides infinitely many of the numbers 9, 99, 999, etc.

EXERCISE 2.30. Let n be an integer greater than 1. Show that n does not divide $2^n - 1$.

EXERCISE 2.31. Prove the following generalization of Fermat's little theorem: for every positive integer n, and every $\alpha \in \mathbb{Z}_n$, we have $\alpha^n = \alpha^{n-\varphi(n)}$.

EXERCISE 2.32. This exercise develops an alternative proof of Fermat's little theorem.

(a) Using Exercise 1.14, show that for all primes p and integers a, we have $(a+1)^p \equiv a^p + 1 \pmod{p}$.

(b) Now derive Fermat's little theorem from part (a).

2.8 Quadratic residues

In §2.3, we studied linear congruences. It is natural to study congruences of higher degree as well. In this section, we study a special case of this more general problem, namely, congruences of the form $z^2 \equiv a \pmod{n}$. The theory we develop here nicely illustrates many of the ideas we have discussed earlier, and has a number of interesting applications as well.

We begin with some general, preliminary definitions and general observations about powers in $\mathbb{Z}_n^*$. For each integer m, we define

$$(\mathbb{Z}_n^*)^m := \{\beta^m : \beta \in \mathbb{Z}_n^*\},$$

the set of mth powers in $\mathbb{Z}_n^*$. The set $(\mathbb{Z}_n^*)^m$ is non-empty, as it obviously contains $[1]$.

Theorem 2.16. *Let n be a positive integer, let $\alpha, \beta \in \mathbb{Z}_n^*$, and let m be any integer.*

(i) If $\alpha \in (\mathbb{Z}_n^*)^m$, then $\alpha^{-1} \in (\mathbb{Z}_n^*)^m$.

(ii) If $\alpha \in (\mathbb{Z}_n^*)^m$ and $\beta \in (\mathbb{Z}_n^*)^m$, then $\alpha\beta \in (\mathbb{Z}_n^*)^m$.

(iii) If $\alpha \in (\mathbb{Z}_n^*)^m$ and $\beta \notin (\mathbb{Z}_n^*)^m$, then $\alpha\beta \notin (\mathbb{Z}_n^*)^m$.

Proof. For (i), if $\alpha = \gamma^m$, then $\alpha^{-1} = (\gamma^{-1})^m$.

For (ii), if $\alpha = \gamma^m$ and $\beta = \delta^m$, then $\alpha\beta = (\gamma\delta)^m$.

For (iii), suppose that $\alpha \in (\mathbb{Z}_n^*)^m$, $\beta \notin (\mathbb{Z}_n^*)^m$, and $\alpha\beta \in (\mathbb{Z}_n^*)^m$. Then by (i), $\alpha^{-1} \in (\mathbb{Z}_n^*)^m$, and by (ii), $\beta = \alpha^{-1}(\alpha\beta) \in (\mathbb{Z}_n^*)^m$, a contradiction. □

Theorem 2.17. *Let n be a positive integer. For each $\alpha \in \mathbb{Z}_n^*$, and all $\ell, m \in \mathbb{Z}$ with $\gcd(\ell, m) = 1$, if $\alpha^\ell \in (\mathbb{Z}_n^*)^m$, then $\alpha \in (\mathbb{Z}_n^*)^m$.*

Proof. Suppose $\alpha^\ell = \beta^m \in (\mathbb{Z}_n^*)^m$. Since $\gcd(\ell, m) = 1$, there exist integers s and t such that $\ell s + mt = 1$. We then have

$$\alpha = \alpha^{\ell s + mt} = \alpha^{\ell s}\alpha^{mt} = \beta^{ms}\alpha^{mt} = (\beta^s\alpha^t)^m \in (\mathbb{Z}_n^*)^m. \ \square$$

We now focus on the squares in $\mathbb{Z}_n^*$, rather than general powers. An integer a is called a **quadratic residue modulo** n if $\gcd(a, n) = 1$ and $a \equiv b^2 \pmod{n}$ for some integer b; in this case, we say that b is a **square root of** a **modulo** n. In terms of residue classes, a is a quadratic residue modulo n if and only if $[a] \in (\mathbb{Z}_n^*)^2$.

To avoid some annoying technicalities, from now on, we shall consider only the case where n is odd.

2.8.1 Quadratic residues modulo p

We first study quadratic residues modulo an odd prime p, and we begin by determining the square roots of 1 modulo p.

Theorem 2.18. *Let p be an odd prime and $\beta \in \mathbb{Z}_p$. Then $\beta^2 = 1$ if and only if $\beta = \pm 1$.*

Proof. Clearly, if $\beta = \pm 1$, then $\beta^2 = 1$. Conversely, suppose that $\beta^2 = 1$. Write $\beta = [b]$, where $b \in \mathbb{Z}$. Then we have $b^2 \equiv 1 \pmod{p}$, which means that

$$p \mid (b^2 - 1) = (b - 1)(b + 1),$$

and since p is prime, we must have $p \mid (b-1)$ or $p \mid (b+1)$. This implies $b \equiv \pm 1 \pmod{p}$, or equivalently, $\beta = \pm 1$. □

This theorem says that modulo p, the only square roots of 1 are 1 and -1, which obviously belong to distinct residue classes (since $p > 2$). From this seemingly trivial fact, a number of quite interesting and useful results may be derived.

Theorem 2.19. *Let p be an odd prime and $\gamma, \beta \in \mathbb{Z}_p^*$. Then $\gamma^2 = \beta^2$ if and only if $\gamma = \pm\beta$.*

Proof. This follows from the previous theorem:

$$\gamma^2 = \beta^2 \iff (\gamma/\beta)^2 = 1 \iff \gamma/\beta = \pm 1 \iff \gamma = \pm\beta. \quad \square$$

This theorem says that if $\alpha = \beta^2$ for some $\beta \in \mathbb{Z}_p^*$, then α has precisely two square roots: β and $-\beta$.

Theorem 2.20. *Let p be an odd prime. Then $|(\mathbb{Z}_p^*)^2| = (p-1)/2$.*

Proof. By the previous theorem, the "squaring map" $\sigma : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ that sends β to β^2 is a two-to-one map: every element in the image of σ has precisely two pre-images. As a general principle, if we have a function $f : A \to B$, where A is a finite set and every element in $f(A)$ has exactly d pre-images, then $|f(A)| = |A|/d$. Applying this general principle to our setting, we see that the image of σ is half the size of $\mathbb{Z}_p^*$. □

Thus, for every odd prime p, exactly half the elements of $\mathbb{Z}_p^*$ are squares, and half are non-squares. If we choose our representatives for the residue classes modulo p from the interval $[-p/2, p/2)$, we may list the elements of $\mathbb{Z}_p$ as

$$[-(p-1)/2], \ldots, [-1], [0], [1], \ldots, [(p-1)/2].$$

We then see that $\mathbb{Z}_p^*$ consists of the residue classes

$$[\pm 1], \ldots, [\pm(p-1)/2],$$

and so $(\mathbb{Z}_p^*)^2$ consists of the residue classes

$$[1]^2, \ldots, [(p-1)/2]^2,$$

which must be distinct, since we know that $|(\mathbb{Z}_p^*)^2| = (p-1)/2$.

Example 2.10. Let $p = 7$. We can list the elements of $\mathbb{Z}_p^*$ as

$$[\pm 1], [\pm 2], [\pm 3].$$

Squaring these, we see that

$$(\mathbb{Z}_p^*)^2 = \{[1]^2, [2]^2, [3]^2\} = \{[1], [4], [2]\}. \quad \square$$

We next derive an extremely important characterization of quadratic residues.

Theorem 2.21 (Euler's criterion). *Let p be an odd prime and $\alpha \in \mathbb{Z}_p^*$.*

(i) $\alpha^{(p-1)/2} = \pm 1$.

(ii) If $\alpha \in (\mathbb{Z}_p^*)^2$ then $\alpha^{(p-1)/2} = 1$.

(iii) If $\alpha \notin (\mathbb{Z}_p^*)^2$ then $\alpha^{(p-1)/2} = -1$.

Proof. For (i), let $\gamma = \alpha^{(p-1)/2}$. By Euler's theorem (Theorem 2.13), we have

$$\gamma^2 = \alpha^{p-1} = 1,$$

and hence by Theorem 2.18, we have $\gamma = \pm 1$.

For (ii), suppose that $\alpha = \beta^2$. Then again by Euler's theorem, we have

$$\alpha^{(p-1)/2} = (\beta^2)^{(p-1)/2} = \beta^{p-1} = 1.$$

For (iii), let $\alpha \in \mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$. We study the product

$$\varepsilon := \prod_{\beta \in \mathbb{Z}_p^*} \beta.$$

We shall show that, on the one hand, $\varepsilon = \alpha^{(p-1)/2}$, while on the other hand, $\varepsilon = -1$.

To show that $\varepsilon = \alpha^{(p-1)/2}$, we group elements of $\mathbb{Z}_p^*$ into pairs of distinct elements whose product is α. More precisely, let $\mathcal{P} := \{S \subseteq \mathbb{Z}_p^* : |S| = 2\}$, and define $C := \{\, \{\kappa, \lambda\} \in \mathcal{P} : \kappa\lambda = \alpha\}$. Note that for every $\kappa \in \mathbb{Z}_p^*$, there is a unique $\lambda \in \mathbb{Z}_p^*$ such that $\kappa\lambda = \alpha$, namely, $\lambda := \alpha/\kappa$; moreover, $\kappa \neq \lambda$, since otherwise, we would have $\kappa^2 = \alpha$, contradicting the assumption that $\alpha \notin (\mathbb{Z}_p^*)^2$. Thus, every element of $\mathbb{Z}_p^*$ belongs to exactly one pair in C; in other words, the elements of C form a partition of $\mathbb{Z}_p^*$. It follows that

$$\varepsilon = \prod_{\{\kappa,\lambda\} \in C} (\kappa \cdot \lambda) = \prod_{\{\kappa,\lambda\} \in C} \alpha = \alpha^{(p-1)/2}.$$

To show that $\varepsilon = -1$, we group elements of $\mathbb{Z}_p^*$ into pairs of distinct elements whose product is $[1]$. Define $\mathcal{D} := \{\, \{\kappa, \lambda\} \in \mathcal{P} : \kappa\lambda = 1\}$. For every $\kappa \in \mathbb{Z}_p^*$, there exists a unique $\lambda \in \mathbb{Z}_p^*$ such that $\kappa\lambda = 1$, namely, $\lambda := \kappa^{-1}$; moreover, $\kappa = \lambda$ if and only if $\kappa^2 = 1$, and by Theorem 2.18, this happens if and only if $\kappa = \pm 1$. Thus, every element of $\mathbb{Z}_p^*$ except for $[\pm 1]$ belongs to exactly one pair in $\mathcal{D}$; in other words, the elements of $\mathcal{D}$ form a partition of $\mathbb{Z}_p^* \setminus \{[\pm 1]\}$. It follows that

$$\varepsilon = [1] \cdot [-1] \cdot \prod_{\{\kappa,\lambda\} \in \mathcal{D}} (\kappa \cdot \lambda) = [-1] \cdot \prod_{\{\kappa,\lambda\} \in \mathcal{D}} [1] = -1. \quad \square$$

Thus, Euler's criterion says that for every $\alpha \in \mathbb{Z}_p^*$, we have $\alpha^{(p-1)/2} = \pm 1$ and

$$\alpha \in (\mathbb{Z}_p^*)^2 \iff \alpha^{(p-1)/2} = 1.$$

In the course of proving Euler's criterion, we proved the following result, which we state here for completeness:

Theorem 2.22 (Wilson's theorem). *Let p be an odd prime. Then $\prod_{\beta \in \mathbb{Z}_p^*} \beta = -1$.*

In the language of congruences, Wilson's theorem may be stated as follows:

$$(p-1)! \equiv -1 \pmod{p}.$$

We also derive the following simple consequence of Theorem 2.21:

Theorem 2.23. *Let p be an odd prime and $\alpha, \beta \in \mathbb{Z}_p^*$. If $\alpha \notin (\mathbb{Z}_p^*)^2$ and $\beta \notin (\mathbb{Z}_p^*)^2$, then $\alpha\beta \in (\mathbb{Z}_p^*)^2$.*

Proof. Suppose $\alpha \notin (\mathbb{Z}_p^*)^2$ and $\beta \notin (\mathbb{Z}_p^*)^2$. Then by Euler's criterion, we have

$$\alpha^{(p-1)/2} = -1 \text{ and } \beta^{(p-1)/2} = -1.$$

Therefore,

$$(\alpha\beta)^{(p-1)/2} = \alpha^{(p-1)/2} \cdot \beta^{(p-1)/2} = [-1] \cdot [-1] = 1,$$

which again by Euler's criterion implies that $\alpha\beta \in (\mathbb{Z}_p^*)^2$. □

This theorem, together with parts (ii) and (iii) of Theorem 2.16, gives us the following simple rules regarding squares in $\mathbb{Z}_p^*$:

square	×	square	=	square,
square	×	non-square	=	non-square,
non-square	×	non-square	=	square.

2.8.2 Quadratic residues modulo p^e

We next study quadratic residues modulo p^e, where p is an odd prime. The key is to establish the analog of Theorem 2.18:

Theorem 2.24. *Let p be an odd prime, e be a positive integer, and $\beta \in \mathbb{Z}_{p^e}$. Then $\beta^2 = 1$ if and only if $\beta = \pm 1$.*

Proof. Clearly, if $\beta = \pm 1$, then $\beta^2 = 1$. Conversely, suppose that $\beta^2 = 1$. Write $\beta = [b]$, where $b \in \mathbb{Z}$. Then we have $b^2 \equiv 1 \pmod{p^e}$, which means that

$$p^e \mid (b^2 - 1) = (b-1)(b+1).$$

In particular, $p \mid (b-1)(b+1)$, and so $p \mid (b-1)$ or $p \mid (b+1)$. Moreover, p cannot divide both $b-1$ and $b+1$, as otherwise, it would divide their difference $(b+1)-(b-1)=2$, which is impossible (because p is odd). It follows that $p^e \mid (b-1)$ or $p^e \mid (b+1)$, which means $\beta = \pm 1$. □

Theorems 2.19–2.23 generalize immediately from $\mathbb{Z}_p^*$ to $\mathbb{Z}_{p^e}^*$: we really used nothing in the proofs of these theorems other than the fact that ±1 are the only square roots of 1 modulo p. As such, we state the analogs of these theorems for $\mathbb{Z}_{p^e}^*$ without proof.

Theorem 2.25. *Let p be an odd prime, e be a positive integer, and $\gamma, \beta \in \mathbb{Z}_{p^e}^*$. Then $\gamma^2 = \beta^2$ if and only if $\gamma = \pm\beta$.*

Theorem 2.26. *Let p be an odd prime and e be a positive integer. Then we have $|(\mathbb{Z}_{p^e}^*)^2| = \varphi(p^e)/2$.*

Theorem 2.27. *Let p be an odd prime, e be a positive integer, and $\alpha \in \mathbb{Z}_{p^e}^*$.*

(i) $\alpha^{\varphi(p^e)/2} = \pm 1$.

(ii) If $\alpha \in (\mathbb{Z}_{p^e}^*)^2$ *then* $\alpha^{\varphi(p^e)/2} = 1$.

(iii) If $\alpha \notin (\mathbb{Z}_{p^e}^*)^2$ *then* $\alpha^{\varphi(p^e)/2} = -1$.

Theorem 2.28. *Let p be an odd prime and e be a positive integer. Then we have $\prod_{\beta \in \mathbb{Z}_{p^e}^*} \beta = -1$.*

Theorem 2.29. *Let p be an odd prime, e be a positive integer, and $\alpha, \beta \in \mathbb{Z}_{p^e}^*$. If $\alpha \notin (\mathbb{Z}_{p^e}^*)^2$ and $\beta \notin (\mathbb{Z}_{p^e}^*)^2$, then $\alpha\beta \in (\mathbb{Z}_{p^e}^*)^2$.*

It turns out that an integer is a quadratic residue modulo p^e if and only if it is a quadratic residue modulo p.

Theorem 2.30. *Let p be an odd prime, e be a positive integer, and a be any integer. Then a is a quadratic residue modulo p^e if and only if a is a quadratic residue modulo p.*

Proof. Suppose that a is a quadratic residue modulo p^e. Then a is not divisible by p and $a \equiv b^2 \pmod{p^e}$ for some integer b. It follows that $a \equiv b^2 \pmod{p}$, and so a is a quadratic residue modulo p.

Suppose that a is not a quadratic residue modulo p^e. If a is divisible by p, then by definition a is not a quadratic residue modulo p. So suppose a is not divisible by p. By Theorem 2.27, we have

$$a^{p^{e-1}(p-1)/2} \equiv -1 \pmod{p^e}.$$

This congruence holds modulo p as well, and by Fermat's little theorem (applied

$e - 1$ times),

$$a \equiv a^p \equiv a^{p^2} \equiv \cdots \equiv a^{p^{e-1}} \pmod{p},$$

and so

$$-1 \equiv a^{p^{e-1}(p-1)/2} \equiv a^{(p-1)/2} \pmod{p}.$$

Theorem 2.21 therefore implies that a is not a quadratic residue modulo p. □

2.8.3 Quadratic residues modulo *n*

We now study quadratic residues modulo n, where n is an arbitrary, odd integer, with $n > 1$. Let

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

be the prime factorization of n. Our main tools here are the Chinese remainder map

$$\theta : \mathbb{Z}_n \to \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}},$$

introduced in Theorem 2.8, together with the results developed so far for quadratic residues modulo odd prime powers.

Let $\alpha \in \mathbb{Z}_n^*$ with $\theta(\alpha) = (\alpha_1, \ldots, \alpha_r)$.

- On the one hand, suppose $\alpha = \beta^2$ for some $\beta \in \mathbb{Z}_n^*$. If $\theta(\beta) = (\beta_1, \ldots, \beta_r)$, we have

  $$(\alpha_1, \ldots, \alpha_r) = \theta(\alpha) = \theta(\beta^2) = (\beta_1^2, \ldots, \beta_r^2),$$

  where we have used part (iii.c) of Theorem 2.8. It follows that $\alpha_i = \beta_i^2$ for each i.
- On the other hand, suppose that for each i, $\alpha_i = \beta_i^2$ for some $\beta_i \in \mathbb{Z}_{p_i{}^{e_i}}^*$. Then setting $\beta := \theta^{-1}(\beta_1, \ldots, \beta_r)$, we have

  $$\theta(\beta^2) = (\beta_1^2, \ldots, \beta_r^2) = (\alpha_1, \ldots, \alpha_r) = \theta(\alpha),$$

  where we have again used part (iii.c) of Theorem 2.8, along with the fact that θ is bijective (to define β). Thus, $\theta(\alpha) = \theta(\beta^2)$, and again since θ is bijective, it follows that $\alpha = \beta^2$.

We have shown that

$$\alpha \in (\mathbb{Z}_n^*)^2 \iff \alpha_i \in \left(\mathbb{Z}_{p_i^{e_i}}^*\right)^2 \text{ for } i = 1, \ldots, r.$$

In particular, restricting θ to $(\mathbb{Z}_n^*)^2$ yields a one-to-one correspondence between $(\mathbb{Z}_n^*)^2$ and

$$\left(\mathbb{Z}_{p_1^{e_1}}^*\right)^2 \times \cdots \times \left(\mathbb{Z}_{p_r{}^{e_r}}^*\right)^2,$$

and therefore, by Theorem 2.26 (and Theorem 2.9), we have

$$|(\mathbb{Z}_n^*)^2| = \prod_{i=1}^{r} (\varphi(p_i^{e_i})/2) = \varphi(n)/2^r.$$

Now suppose that $\alpha = \beta^2$, with $\beta \in \mathbb{Z}_n^*$ and $\theta(\beta) = (\beta_1, \ldots, \beta_r)$. Consider an arbitrary element $\gamma \in \mathbb{Z}_n^*$, with $\theta(\gamma) = (\gamma_1, \ldots, \gamma_r)$. Then we have

$$\begin{aligned} \gamma^2 = \beta^2 &\iff \theta(\gamma^2) = \theta(\beta^2) \\ &\iff (\gamma_1^2, \ldots, \gamma_r^2) = (\beta_1^2, \ldots, \beta_r^2) \\ &\iff (\gamma_1, \ldots, \gamma_r) = (\pm\beta_1, \ldots, \pm\beta_r) \text{ (by Theorem 2.25).} \end{aligned}$$

Therefore, α has precisely 2^r square roots, namely, $\theta^{-1}(\pm\beta_1, \ldots, \pm\beta_r)$.

2.8.4 Square roots of -1 modulo p

Using Euler's criterion, we can easily characterize those primes modulo which -1 is a quadratic residue. This turns out to have a number of nice applications.

Consider an odd prime p. The following theorem says that the question of whether -1 is a quadratic residue modulo p is decided by the residue class of p modulo 4. Since p is odd, either $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.

Theorem 2.31. *Let p be an odd prime. Then -1 is a quadratic residue modulo p if and only $p \equiv 1 \pmod 4$.*

Proof. By Euler's criterion, -1 is a quadratic residue modulo p if and only if $(-1)^{(p-1)/2} \equiv 1 \pmod p$. If $p \equiv 1 \pmod 4$, then $(p-1)/2$ is even, and so $(-1)^{(p-1)/2} = 1$. If $p \equiv 3 \pmod 4$, then $(p-1)/2$ is odd, and so $(-1)^{(p-1)/2} = -1$. □

In fact, when $p \equiv 1 \pmod 4$, any non-square in $\mathbb{Z}_p^*$ yields a square root of -1 modulo p, as follows:

Theorem 2.32. *Let p be a prime with $p \equiv 1 \pmod 4$, $\gamma \in \mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$, and $\beta := \gamma^{(p-1)/4}$. Then $\beta^2 = -1$.*

Proof. This is a simple calculation, based on Euler's criterion:

$$\beta^2 = \gamma^{(p-1)/2} = -1. \quad \square$$

The fact that -1 is a quadratic residue modulo primes $p \equiv 1 \pmod 4$ can be used to prove Fermat's theorem that such primes may be written as the sum of two squares. To do this, we first need the following technical lemma:

Theorem 2.33 (Thue's lemma). *Let $n, b, r^*, t^* \in \mathbb{Z}$, with $0 < r^* \leq n < r^*t^*$. Then there exist $r, t \in \mathbb{Z}$ with*

$$r \equiv bt \pmod{n}, \quad |r| < r^*, \quad \textit{and} \quad 0 < |t| < t^*.$$

Proof. For $i = 0, \ldots, r^*-1$ and $j = 0, \ldots, t^*-1$, we define the number $v_{ij} := i-bj$. Since we have defined r^*t^* numbers, and $r^*t^* > n$, two of these numbers must lie in the same residue class modulo n; that is, for some $(i_1, j_1) \neq (i_2, j_2)$, we have $v_{i_1j_1} \equiv v_{i_2j_2} \pmod{n}$. Setting $r := i_1-i_2$ and $t := j_1-j_2$, this implies $r \equiv bt \pmod{n}$, $|r| < r^*$, $|t| < t^*$, and that either $r \neq 0$ or $t \neq 0$. It only remains to show that $t \neq 0$. Suppose to the contrary that $t = 0$. This would imply that $r \equiv 0 \pmod{n}$ and $r \neq 0$, which is to say that r is a non-zero multiple of n; however, this is impossible, since $|r| < r^* \leq n$. □

Theorem 2.34 (Fermat's two squares theorem). *Let p be an odd prime. Then $p = r^2 + t^2$ for some $r, t \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod{4}$.*

Proof. One direction is easy. Suppose $p \equiv 3 \pmod{4}$. It is easy to see that the square of every integer is congruent to either 0 or 1 modulo 4; therefore, the sum of two squares is congruent to either 0, 1, or 2 modulo 4, and so can not be congruent to p modulo 4 (let alone equal to p).

For the other direction, suppose $p \equiv 1 \pmod{4}$. We know that -1 is a quadratic residue modulo p, so let b be an integer such that $b^2 \equiv -1 \pmod{p}$. Now apply Theorem 2.33 with $n := p$, b as just defined, and $r^* := t^* := \lfloor\sqrt{p}\rfloor + 1$. Evidently, $\lfloor\sqrt{p}\rfloor + 1 > \sqrt{p}$, and hence $r^*t^* > p$. Also, since p is prime, $\sqrt{p}$ is not an integer, and so $\lfloor\sqrt{p}\rfloor < \sqrt{p} < p$; in particular, $r^* = \lfloor\sqrt{p}\rfloor + 1 \leq p$. Thus, the hypotheses of that theorem are satisfied, and therefore, there exist integers r and t such that

$$r \equiv bt \pmod{p}, \quad |r| \leq \lfloor\sqrt{p}\rfloor < \sqrt{p}, \quad \text{and} \quad 0 < |t| \leq \lfloor\sqrt{p}\rfloor < \sqrt{p}.$$

It follows that

$$r^2 \equiv b^2t^2 \equiv -t^2 \pmod{p}.$$

Thus, $r^2 + t^2$ is a multiple of p and $0 < r^2 + t^2 < 2p$. The only possibility is that $r^2 + t^2 = p$. □

The fact that -1 is a quadratic residue modulo an odd prime p only if $p \equiv 1 \pmod{4}$ can be used so show there are infinitely many such primes.

Theorem 2.35. *There are infinitely many primes $p \equiv 1 \pmod{4}$.*

Proof. Suppose there were only finitely many such primes, $p_1, \ldots, p_k$. Set $M := \prod_{i=1}^{k} p_i$ and $N := 4M^2 + 1$. Let p be any prime dividing N. Evidently, p is not among the p_i's, since if it were, it would divide both N and $4M^2$, and so also $N - 4M^2 = 1$. Also, p is clearly odd, since N is odd. Moreover, $(2M)^2 \equiv -1 \pmod{p}$; therefore, -1 is a quadratic residue modulo p, and so $p \equiv 1 \pmod{4}$, contradicting the assumption that $p_1, \ldots, p_k$ are the only such primes. □

For completeness, we also state the following fact:

Theorem 2.36. *There are infinitely many primes* $p \equiv 3 \pmod{4}$.

Proof. Suppose there were only finitely many such primes, $p_1, \ldots, p_k$. Set $M := \prod_{i=1}^{k} p_i$ and $N := 4M - 1$. Since $N \equiv 3 \pmod{4}$, there must be some prime $p \equiv 3 \pmod{4}$ dividing N (if all primes dividing N were congruent to 1 modulo 4, then so too would be their product N). Evidently, p is not among the p_i's, since if it were, it would divide both N and $4M$, and so also $4M - N = 1$. This contradicts the assumption that $p_1, \ldots, p_k$ are the only primes congruent to 3 modulo 4. □

EXERCISE 2.33. Let $n, m \in \mathbb{Z}$, where $n > 0$, and let $d := \gcd(m, \varphi(n))$. Show that:

(a) if $d = 1$, then $(\mathbb{Z}_n^*)^m = (\mathbb{Z}_n^*)$;

(b) if $\alpha \in (\mathbb{Z}_n^*)^m$, then $\alpha^{\varphi(n)/d} = 1$.

EXERCISE 2.34. Calculate the sets C and $\mathcal{D}$ in the proof of Theorem 2.21 in the case $p = 11$ and $\alpha = -1$.

EXERCISE 2.35. Calculate the square roots of 1 modulo 4, 8, and 16.

EXERCISE 2.36. Let $n \in \mathbb{Z}$ with $n > 1$. Show that n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

EXERCISE 2.37. Let p be a prime with $p \equiv 1 \pmod{4}$, and $b := ((p-1)/2)!$. Show that $b^2 \equiv -1 \pmod{p}$.

EXERCISE 2.38. Let $n := pq$, where p and q are distinct, odd primes. Show that there exist $\alpha, \beta \in \mathbb{Z}_n^*$ such that $\alpha \notin (\mathbb{Z}_n^*)^2$, $\beta \notin (\mathbb{Z}_n^*)^2$, and $\alpha\beta \notin (\mathbb{Z}_n^*)^2$.

EXERCISE 2.39. Let n be an odd positive integer, and let a be any integer. Show that a is a quadratic residue modulo n if and only if a is a quadratic residue modulo p for each prime $p \mid n$.

EXERCISE 2.40. Show that if p is an odd prime, with $p \equiv 3 \pmod{4}$, then $(\mathbb{Z}_p^*)^4 = (\mathbb{Z}_p^*)^2$. More generally, show that if n is an odd positive integer, where $p \equiv 3 \pmod{4}$ for each prime $p \mid n$, then $(\mathbb{Z}_n^*)^4 = (\mathbb{Z}_n^*)^2$.

EXERCISE 2.41. Let p be an odd prime, and let $e \in \mathbb{Z}$ with $e > 1$. Let a be an integer of the form $a = p^f b$, where $0 \leq f < e$ and $p \nmid b$. Consider the integer solutions z to the congruence $z^2 \equiv a \pmod{p^e}$. Show that a solution exists if and only if f is even and b is a quadratic residue modulo p, in which case there are exactly $2p^f$ distinct solutions modulo p^e.

EXERCISE 2.42. Suppose p is an odd prime, and that $r^2+t^2 = p$ for some integers r, t. Show that if x, y are integers such that $x^2+y^2 = p$, then (x, y) must be $(\pm r, \pm t)$ or $(\pm t, \pm r)$.

EXERCISE 2.43. Show that if both u and v are the sum of two squares of integers, then so is their product uv.

EXERCISE 2.44. Suppose $r^2 + t^2 \equiv 0 \pmod{n}$, where n is a positive integer, and suppose p is an odd prime dividing n. Show that:

(a) if p divides neither r nor t, then $p \equiv 1 \pmod{4}$;

(b) if p divides one of r or t, then it divides the other, and moreover, p^2 divides n, and $(r/p)^2 + (t/p)^2 \equiv 0 \pmod{n/p^2}$.

EXERCISE 2.45. Let n be a positive integer, and write $n = ab^2$ where a and b are positive integers, and a is square-free (see Exercise 1.15). Show that n is the sum of two squares of integers if and only if no prime $p \equiv 3 \pmod{4}$ divides a. Hint: use the previous two exercises.

2.9 Summations over divisors

We close this chapter with a brief treatment of summations over divisors. To this end, we introduce some terminology and notation. By an **arithmetic function**, we simply mean a function from the positive integers into the reals (actually, one usually considers complex-valued functions as well, but we shall not do so here). Let f and g be arithmetic functions. The **Dirichlet product** of f and g, denoted $f \star g$, is the arithmetic function whose value at n is defined by the formula

$$(f \star g)(n) := \sum_{d \mid n} f(d) g(n/d),$$

the sum being over all positive divisors d of n. Another, more symmetric, way to write this is

$$(f \star g)(n) = \sum_{n = d_1 d_2} f(d_1) g(d_2),$$

the sum being over all pairs (d_1, d_2) of positive integers with $d_1 d_2 = n$.

The Dirichlet product is clearly commutative (i.e., $f \star g = g \star f$), and is associative as well, which one can see by checking that

$$(f \star (g \star h))(n) = \sum_{n=d_1 d_2 d_3} f(d_1)g(d_2)h(d_3) = ((f \star g) \star h)(n),$$

the sum being over all triples (d_1, d_2, d_3) of positive integers with $d_1 d_2 d_3 = n$.

We now introduce three special arithmetic functions: I, $\mathit{1}$, and μ. The functions I and $\mathit{1}$ are defined as follows:

$$I(n) := \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{if } n > 1; \end{cases} \qquad \mathit{1}(n) := 1.$$

The **Möbius function** μ is defined as follows: if $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n, then

$$\mu(n) := \begin{cases} 0 & \text{if } e_i > 1 \text{ for some } i = 1, \ldots, r; \\ (-1)^r & \text{otherwise.} \end{cases}$$

In other words, $\mu(n) = 0$ if n is not square-free (see Exercise 1.15); otherwise, $\mu(n)$ is $(-1)^r$ where r is the number of distinct primes dividing n. Here are some examples:

$$\mu(1) = 1,\ \mu(2) = -1,\ \mu(3) = -1,\ \mu(4) = 0,\ \mu(5) = -1,\ \mu(6) = 1.$$

It is easy to see from the definitions that for every arithmetic function f, we have

$$I \star f = f \ \text{ and } \ (\mathit{1} \star f)(n) = \sum_{d \mid n} f(d).$$

Thus, I acts as a multiplicative identity with respect to the Dirichlet product, while "$\mathit{1} \star$" acts as a "summation over divisors" operator.

An arithmetic function f is called **multiplicative** if $f(1) = 1$ and for all positive integers n, m with $\gcd(n, m) = 1$, we have $f(nm) = f(n)f(m)$.

The reader may easily verify that I, $\mathit{1}$, and μ are multiplicative functions. Theorem 2.9 says that Euler's function φ is multiplicative. The reader may also verify the following:

Theorem 2.37. *If f is a multiplicative arithmetic function, and if $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n, then $f(n) = f(p_1^{e_1}) \cdots f(p_r^{e_r})$.*

Proof. Exercise. □

A key property of the Möbius function is the following:

Theorem 2.38. *Let f be a multiplicative arithmetic function. If $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n, then*

$$\sum_{d \mid n} \mu(d) f(d) = (1 - f(p_1)) \cdots (1 - f(p_r)). \tag{2.9}$$

Proof. The only non-zero terms appearing in the sum on the left-hand side of (2.9) are those corresponding to divisors d of the form $p_{i_1} \cdots p_{i_\ell}$, where $p_{i_1}, \ldots, p_{i_\ell}$ are distinct; the value contributed to the sum by such a term is $(-1)^\ell f(p_{i_1} \cdots p_{i_\ell}) = (-1)^\ell f(p_{i_1}) \cdots f(p_{i_\ell})$. These are the same as the terms in the expansion of the product on the right-hand side of (2.9). □

If we set $f := 1$ in the previous theorem, then we see that

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{if } n > 1. \end{cases}$$

Translating this into the language of Dirichlet products, we have

$$1 \star \mu = I.$$

Thus, with respect to the Dirichlet product, the functions 1 and μ are multiplicative inverses of one another. Based on this, we may easily derive the following:

Theorem 2.39 (Möbius inversion formula). *Let f and F be arithmetic functions. Then $F = 1 \star f$ if and only if $f = \mu \star F$.*

Proof. If $F = 1 \star f$, then

$$\mu \star F = \mu \star (1 \star f) = (\mu \star 1) \star f = I \star f = f,$$

and conversely, if $f = \mu \star F$, then

$$1 \star f = 1 \star (\mu \star F) = (1 \star \mu) \star F = I \star F = F. \quad \square$$

The Möbius inversion formula says this:

$$\begin{aligned} & F(n) = \sum_{d \mid n} f(d) \ \text{ for all positive integers } n \\ \iff \quad & f(n) = \sum_{d \mid n} \mu(d) F(n/d) \ \text{ for all positive integers } n. \end{aligned}$$

The Möbius inversion formula is a useful tool. As an application, we use it to obtain a simple proof of the following fact:

Theorem 2.40. *For every positive integer n, we have $\sum_{d \mid n} \varphi(d) = n$.*

Proof. Let us define the arithmetic functions $N(n) := n$ and $M(n) := 1/n$. Our goal is to show that $N = \mathit{1} \star \varphi$, and by Möbius inversion, it suffices to show that $\mu \star N = \varphi$. If $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n, we have

$$\begin{aligned}(\mu \star N)(n) &= \sum_{d \mid n} \mu(d)(n/d) = n \sum_{d \mid n} \mu(d)/d \\ &= n \prod_{i=1}^{r} (1 - 1/p_i) \ \ \text{(applying Theorem 2.38 with } f := M) \\ &= \varphi(n) \ \ \text{(by Theorem 2.11).} \quad \square\end{aligned}$$

EXERCISE 2.46. In our definition of a multiplicative function f, we made the requirement that $f(1) = 1$. Show that if we dropped this requirement, the only other function that would satisfy the definition would be the zero function (i.e., the function that is everywhere zero).

EXERCISE 2.47. Let f be a polynomial with integer coefficients, and for each positive integer n, define $\omega_f(n)$ to be the number of integers $x \in \{0, \ldots, n-1\}$ such that $f(x) \equiv 0 \pmod{n}$. Show that ω_f is multiplicative.

EXERCISE 2.48. Show that if f and g are multiplicative, then so is $f \star g$. Hint: use Exercise 1.18.

EXERCISE 2.49. Let $\tau(n)$ be the number of positive divisors of n. Show that:

(a) τ is a multiplicative function;

(b) $\tau(n) = \prod_{i=1}^{r} (e_i + 1)$, where $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n;

(c) $\sum_{d \mid n} \mu(d)\tau(n/d) = 1$;

(d) $\sum_{d \mid n} \mu(d)\tau(d) = (-1)^r$, where $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n.

EXERCISE 2.50. Define $\sigma(n) := \sum_{d \mid n} d$. Show that:

(a) σ is a multiplicative function;

(b) $\sigma(n) = \prod_{i=1}^{r} (p_i^{e_i+1} - 1)/(p_i - 1)$, where $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n;

(c) $\sum_{d \mid n} \mu(d)\sigma(n/d) = n$;

(d) $\sum_{d \mid n} \mu(d)\sigma(d) = (-1)^r p_1 \cdots p_r$, where $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n.

EXERCISE 2.51. The **Mangoldt function** $\Lambda(n)$ is defined for all positive integers n as follows: $\Lambda(n) := \log p$, if $n = p^k$ for some prime p and positive integer k, and $\Lambda(n) := 0$, otherwise. Show that $\sum_{d \mid n} \Lambda(d) = \log n$, and from this, deduce that $\Lambda(n) = -\sum_{d \mid n} \mu(d) \log d$.

EXERCISE 2.52. Show that if f is multiplicative, and if $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n, then $\sum_{d \mid n} \mu(d)^2 f(d) = (1 + f(p_1)) \cdots (1 + f(p_r))$.

EXERCISE 2.53. Show that n is square-free if and only if $\sum_{d \mid n} \mu(d)^2 \varphi(d) = n$.

EXERCISE 2.54. Show that for every arithmetic function f with $f(1) \neq 0$, there is a unique arithmetic function g, called the **Dirichlet inverse** of f, such that $f \star g = I$. Also, show that if $f(1) = 0$, then f has no Dirichlet inverse.

EXERCISE 2.55. Show that if f is a multiplicative function, then so is its Dirichlet inverse (as defined in the previous exercise).

EXERCISE 2.56. This exercise develops an alternative proof of Theorem 2.40 that does not depend on Theorem 2.11. Let n be a positive integer. Define

$$F_n := \{i/n \in \mathbb{Q} : i = 0, \ldots, n-1\}.$$

Also, for each positive integer d, define

$$G_d := \{a/d \in \mathbb{Q} : a \in \mathbb{Z},\ \gcd(a, d) = 1\}.$$

(a) Show that for each $x \in F_n$, there exists a unique positive divisor d of n such that $x \in G_d$.

(b) Show that for each positive divisor d of n, we have

$$F_n \cap G_d = \{a/d : a = 0, \ldots, d-1,\ \gcd(a, d) = 1\}.$$

(c) Using (a) and (b), show that $\sum_{d \mid n} \varphi(d) = n$.

EXERCISE 2.57. Using Möbius inversion, directly derive Theorem 2.11 from Theorem 2.40.