2

Congruences

This chapter introduces the basic properties of congruences modulo n, along with the related notion of congruence classes modulo n. Other items discussed include the Chinese remainder theorem, Euler's phi function, arithmetic functions and Möbius inversion, and Fermat's little theorem.

2.1 Definitions and basic properties

For positive integer n, and for $a, b \in \mathbb{Z}$, 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 $a \not\equiv b \pmod{n}$. 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.

A simple observation is that $a \equiv b \pmod{n}$ if and only if there exists an integer c such that $a = b + cn$. From this, and Theorem 1.4, the following is immediate:

Theorem 2.1. *Let n be a positive integer. For every integer a, there exists a unique integer b such that $a \equiv b \pmod{n}$ and $0 \leq b < n$, namely, $b := a \bmod n$.*

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 $(a - b) + (b - c) = a - c$. □

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

Theorem 2.3. *For all positive integers n, and all $a, a', b, b' \in \mathbb{Z}$, if $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then*

$$a + b \equiv a' + b' \pmod{n}$$

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 c and d such that $a' = a + cn$ and $b' = b + dn$. Therefore,

$$a' + b' = a + b + (c + d)n,$$

which proves the first congruence of the theorem, and

$$a'b' = (a + cn)(b + dn) = ab + (ad + bc + cdn)n,$$

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 x is congruent to y modulo n, one may substitute y for x in any simple arithmetic expression (more precisely, any polynomial in x with integer coefficients) appearing in a congruence modulo n.

***Example* 2.1.** Observe that

$$3 \cdot 5 \equiv 1 \pmod{7}. \tag{2.1}$$

Using this fact, let us find the set of solutions z to the congruence

$$3z + 4 \equiv 6 \pmod{7}. \tag{2.2}$$

Suppose that z is a solution to (2.2). Subtracting 4 from both sides of (2.2), we see that

$$3z \equiv 2 \pmod{7}. \tag{2.3}$$

Now, multiplying both sides of (2.3) by 5, and using (2.1), we obtain

$$z \equiv 1 \cdot z \equiv (3 \cdot 5) \cdot z \equiv 2 \cdot 5 \equiv 3 \pmod{7}.$$

Thus, if z is a solution to (2.2), we must have $z \equiv 3 \pmod 7$; conversely, one can verify that if $z \equiv 3 \pmod 7$, then (2.2) holds. We conclude that the integers z that are solutions to (2.2) are precisely those integers that are congruent to 3 modulo 7, which we can list as follows:

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

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 2.1. Let $x, y, n \in \mathbb{Z}$ with $n > 0$ and $x \equiv y \pmod n$. Also, let $a_0, a_1, \ldots, a_k$ be integers. Show that

$$a_0 + a_1 x + \cdots + a_k x^k \equiv a_0 + a_1 y + \cdots + a_k y^k \pmod n.$$

EXERCISE 2.2. Let $a, b, n, n' \in \mathbb{Z}$ with $n > 0$ and $n' \mid n$. Show that if $a \equiv b \pmod n$, then $a \equiv b \pmod{n'}$.

EXERCISE 2.3. 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 2.4. Let $a, b, n \in \mathbb{Z}$ such that $n > 0$ and $a \equiv b \pmod n$. Show that $\gcd(a, n) = \gcd(b, n)$.

EXERCISE 2.5. Prove that for any prime p and integer x, if $x^2 \equiv 1 \pmod p$ then $x \equiv 1 \pmod p$ or $x \equiv -1 \pmod p$.

EXERCISE 2.6. 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 2.7. Show that there are 14 distinct, possible, yearly (Gregorian) calendars, and show that all 14 calendars actually occur.

2.2 Solving linear congruences

For a positive integer n, and $a \in \mathbb{Z}$, we say that $a' \in \mathbb{Z}$ is a **multiplicative inverse of a modulo n** if $aa' \equiv 1 \pmod n$.

Theorem 2.4. *Let $a, n \in \mathbb{Z}$ with $n > 0$. Then a has a multiplicative inverse modulo n if and only if a and n are relatively prime.*

Proof. This follows immediately from Theorem 1.6: a and n are relatively prime if and only if there exist $s, t \in \mathbb{Z}$ such that $as + nt = 1$, if and only if there exists $s \in \mathbb{Z}$ such that $as \equiv 1 \pmod{n}$. □

Note that the existence of a multiplicative inverse of a modulo n depends only on the value of a modulo n; that is, if $b \equiv a \pmod{n}$, then a has an inverse if and only if b does. Indeed, by Theorem 2.3, if $b \equiv a \pmod{n}$, then for any integer a', $aa' \equiv 1 \pmod{n}$ if and only if $ba' \equiv 1 \pmod{n}$. (This fact is also implied by Theorem 2.4 together with Exercise 2.4.)

We now prove a simple "cancellation law" for congruences:

Theorem 2.5. *Let $a, n, z, z' \in \mathbb{Z}$ with $n > 0$. If a is relatively prime to n, then $az \equiv az' \pmod{n}$ if and only if $z \equiv z' \pmod{n}$. More generally, if $d := \gcd(a, n)$, then $az \equiv az' \pmod{n}$ if and only if $z \equiv z' \pmod{n/d}$.*

Proof. For the first statement, assume that $\gcd(a, n) = 1$, and let a' be a multiplicative inverse of a modulo n. Then, $az \equiv az' \pmod{n}$ implies $a'az \equiv a'az' \pmod{n}$, which implies $z \equiv z' \pmod{n}$, since $a'a \equiv 1 \pmod{n}$. Conversely, if $z \equiv z' \pmod{n}$, then trivially $az \equiv az' \pmod{n}$. That proves the first statement.

For the second statement, let $d = \gcd(a, n)$. Simply from the definition of congruences, one sees that in general, $az \equiv az' \pmod{n}$ holds if and only if $(a/d)z \equiv (a/d)z' \pmod{n/d}$. Moreover, since a/d and n/d are relatively prime (see Exercise 1.9), the first statement of the theorem implies that $(a/d)z \equiv (a/d)z' \pmod{n/d}$ holds if and only if $z \equiv z' \pmod{n/d}$. That proves the second statement. □

Theorem 2.5 implies that multiplicative inverses modulo n are uniquely determined modulo n; indeed, if a is relatively prime to n, and if $aa' \equiv 1 \equiv aa'' \pmod{n}$, then we may cancel a from the left- and right-hand sides of this congruence, obtaining $a' \equiv a'' \pmod{n}$.

***Example* 2.2.** Observe that

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

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

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

We cannot simply cancel the common factor of 3 from both sides of (2.5);

indeed, $5 \not\equiv 3 \pmod 6$. However, $\gcd(3, 6) = 3$, and as Theorem 2.5 guarantees, we do indeed have $5 \equiv 3 \pmod 2$. □

Next, we consider the problem of determining the solutions z to congruences of the form $az + c \equiv b \pmod n$, for given integers a, b, c, n. Since we may both add and subtract c from both sides of a congruence modulo n, it is clear that z is a solution to the above congruence if and only if $az \equiv b - c \pmod n$. Therefore, it suffices to consider the problem of determining the solutions z to congruences of the form $az \equiv b \pmod n$, for given integers a, b, n.

Theorem 2.6. *Let $a, b, n \in \mathbb{Z}$ with $n > 0$. If a is relatively prime to n, then the congruence $az \equiv b \pmod n$ has a solution z; moreover, any integer z' is a solution if and only if $z \equiv z' \pmod n$.*

Proof. The integer $z := ba'$, where a' is a multiplicative inverse of a modulo n, is clearly a solution. For any integer z', we have $az' \equiv b \pmod n$ if and only if $az' \equiv az \pmod n$, which by Theorem 2.5 holds if and only if $z \equiv z' \pmod n$. □

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

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

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 $0, \ldots, n - 1$.

Theorem 2.6 may be generalized as follows:

Theorem 2.7. *Let $a, b, n \in \mathbb{Z}$ with $n > 0$, and let $d := \gcd(a, n)$. If $d \mid b$, then the congruence $az \equiv b \pmod n$ has a solution z, and any integer z' is also a solution if and only if $z \equiv z' \pmod{n/d}$. If $d \nmid b$, then the congruence $az \equiv b \pmod n$ has no solution z.*

Proof. For the first statement, suppose that $d \mid b$. In this case, by Theorem 2.5, we have $az \equiv b \pmod n$ if and only if $(a/d)z \equiv (b/d) \pmod{n/d}$, and so the statement follows immediately from Theorem 2.6, and the fact that a/d and n/d are relatively prime.

For the second statement, we show that if $az \equiv b \pmod n$ for some

integer z, then d must divide b. To this end, assume that $az \equiv b \pmod{n}$ for some integer z. Then since $d \mid n$, we have $az \equiv b \pmod{d}$. However, $az \equiv 0 \pmod{d}$, since $d \mid a$, and hence $b \equiv 0 \pmod{d}$; that is, $d \mid b$. □

***Example* 2.3.** The following table illustrates what the above theorem 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
$2z \bmod 15$	0	2	4	6	8	10	12	14	1	3	5	7	9	11	13
$3z \bmod 15$	0	3	6	9	12	0	3	6	9	12	0	3	6	9	12
$4z \bmod 15$	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11
$5z \bmod 15$	0	5	10	0	5	10	0	5	10	0	5	10	0	5	10
$6z \bmod 15$	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 $2z \bmod 15$, 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 $2z \equiv b \pmod{15}$. We could have inferred this fact from the theorem, since $\gcd(2, 15) = 1$.

In the third row, the only numbers hit are the multiples of 3, which follows from the theorem and the fact that $\gcd(3, 15) = 3$. Also note that the pattern in this row repeats every five columns; that is also implied by the theorem; 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 theorem and the fact that $\gcd(4, 15) = 1$.

In the fifth row, the only numbers hit are the multiples of 5, which follows from the theorem and the fact that $\gcd(5, 15) = 5$. Also note that the pattern in this row repeats every three columns; that is also implied by the theorem; 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. □

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 2.8 (Chinese remainder theorem). *Let $n_1, \ldots, n_k$ be pairwise relatively prime, positive integers, and let $a_1, \ldots, a_k$ be arbitrary integers. Then there exists an integer z such that*

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

Moreover, any other integer z' is also a solution of these congruences if and only if $z \equiv z' \pmod{n}$, where $n := \prod_{i=1}^{k} n_i$.

Proof. Let $n := \prod_{i=1}^{k} n_i$, as in the statement of the theorem. Let us also define

$$n_i' := n/n_i \quad (i = 1, \ldots, k).$$

From the fact that $n_1, \ldots, n_k$ are pairwise relatively prime, it is clear that $\gcd(n_i, n_i') = 1$ for $i = 1, \ldots, k$. Therefore, let

$$m_i := (n_i')^{-1} \bmod n_i \quad \text{and} \quad w_i := n_i' m_i \quad (i = 1, \ldots, k).$$

By construction, one sees that for $i = 1, \ldots, k$, we have

$$w_i \equiv 1 \pmod{n_i}$$

and

$$w_i \equiv 0 \pmod{n_j} \quad \text{for } j = 1, \ldots, k \text{ with } j \neq i.$$

That is to say, for $i, j = 1, \ldots, k$, we have $w_i \equiv \delta_{ij} \pmod{n_j}$, where

$$\delta_{ij} := \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Now define

$$z := \sum_{i=1}^{k} w_i a_i.$$

One then sees that

$$z \equiv \sum_{i=1}^{k} w_i a_i \equiv \sum_{i=1}^{k} \delta_{ij} a_i \equiv a_j \pmod{n_j} \quad \text{for } j = 1, \ldots, k.$$

Therefore, this z solves the given system of congruences.

Moreover, if $z' \equiv z \pmod{n}$, then since $n_i \mid n$ for $i = 1, \ldots, k$, we see that $z' \equiv z \equiv a_i \pmod{n_i}$ for $i = 1, \ldots, k$, and so z' also solves the system of congruences.

Finally, if z' solves the system of congruences, then $z' \equiv z \pmod{n_i}$ for $i = 1, \ldots, k$. That is, $n_i \mid (z' - z)$ for $i = 1, \ldots, k$. Since $n_1, \ldots, n_k$ are pairwise relatively prime, this implies that $n \mid (z' - z)$, or equivalently, $z' \equiv z \pmod{n}$. □

***Example* 2.4.** The following table illustrates what the above theorem says for $n_1 = 3$ and $n_2 = 5$.

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

We see that as z ranges from 0 to 14, the pairs $(z \bmod 3, z \bmod 5)$ 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 2.8. Let $a_1, \ldots, a_k, n, b$ be integers with $n > 0$, and let $d := \gcd(a_1, \ldots, a_k, n)$. Show that the congruence

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

has a solution $z_1, \ldots, z_k$ if and only if $d \mid b$.

EXERCISE 2.9. Find an integer z such that $z \equiv -1 \pmod{100}$, $z \equiv 1 \pmod{33}$, and $z \equiv 2 \pmod{7}$.

EXERCISE 2.10. If you want to show that you are a real nerd, here is an age-guessing game you might play at a party. First, prepare 2 cards as follows:

$$\begin{array}{cccccccc} 1 & 4 & 7 & 10 & \cdots & 94 & 97 \\ 2 & 5 & 8 & 11 & \cdots & 95 & 98 \end{array}$$

and 4 cards as follows:

$$\begin{array}{cccccccc} 1 & 6 & 11 & 16 & \cdots & 91 & 96 \\ 2 & 7 & 12 & 17 & \cdots & 92 & 97 \\ 3 & 8 & 13 & 18 & \cdots & 93 & 98 \\ 4 & 9 & 14 & 19 & \cdots & 94 & 99 \end{array}$$

At the party, ask a person to tell you if their age is odd or even, and then ask them to tell you on which of the six cards their age appears. Show how to use this information (and a little common sense) to determine their age.

2.3 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 $[a]_n$, or when n is clear from context, we may simply write $[a]$. Historically, these equivalence classes are called **residue classes modulo** n, and we shall adopt this terminology here as well.

It is easy to see from the definitions that

$$[a]_n = a + n\mathbb{Z} := \{a + nz : z \in \mathbb{Z}\}.$$

Note that a given residue class modulo n has many different "names"; for example, the residue class $[1]_n$ is the same as the residue class $[1 + n]_n$. For any integer a in a residue class, we call a a **representative** of that class.

The following is simply a restatement of Theorem 2.1:

Theorem 2.9. *For a positive integer n, there are precisely n distinct residue classes modulo n, namely, $[a]_n$ for $a = 0, \ldots, n - 1$.*

Fix a positive integer n. Let us define $\mathbb{Z}_n$ as the set of residue classes modulo n. 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

$$[a]_n + [b]_n := [a + b]_n,$$

and we define

$$[a]_n \cdot [b]_n := [a \cdot b]_n.$$

Of course, one has to check 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 $[a]_n = [a']_n$ and $[b]_n = [b']_n$, then $[a \text{ op } b]_n = [a' \text{ op } b']_n$, for op $\in \{+, \cdot\}$. However, this property follows immediately from Theorem 2.3.

It is also convenient to define a negation operation on $\mathbb{Z}_n$, defining

$$-[a]_n := [-1]_n \cdot [a]_n = [-a]_n.$$

Having defined addition and negation operations on $\mathbb{Z}_n$, we naturally define a subtraction operation on $\mathbb{Z}_n$ as follows: for $a, b \in \mathbb{Z}$,

$$[a]_n - [b]_n := [a]_n + (-[b]_n) = [a - b]_n.$$

***Example* 2.5.** 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:

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[2]$	$[0]$	$[2]$	$[4]$	$[0]$	$[2]$	$[4]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$	$[3]$
$[4]$	$[0]$	$[4]$	$[2]$	$[0]$	$[4]$	$[2]$
$[5]$	$[0]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

□

These operations on $\mathbb{Z}_n$ yield a very natural algebraic structure whose salient properties are as follows:

Theorem 2.10. *Let n be a positive integer, and consider the set $\mathbb{Z}_n$ of residue classes modulo n with addition and multiplication of residue classes as defined above. For all $\alpha, \beta, \gamma \in \mathbb{Z}_n$, we have*

(i) $\alpha + \beta = \beta + \alpha$ *(addition is commutative),*

(ii) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ *(addition is associative),*

(iii) $\alpha + [0]_n = \alpha$ *(existence of additive identity),*

(iv) $\alpha - \alpha = [0]_n$ *(existence of additive inverses),*

(v) $\alpha \cdot \beta = \beta \cdot \alpha$ *(multiplication is commutative),*

(vi) $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$ *(multiplication is associative),*

(vii) $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$ *(multiplication distributes over addition)*

(viii) $\alpha \cdot [1]_n = \alpha$ *(existence of multiplicative identity).*

Proof. All of these properties follow easily from the corresponding properties for the integers, together with the definitions of addition, subtraction, and multiplication of residue classes. For example, for (i), we have

$$[a]_n + [b]_n = [a + b]_n = [b + a]_n = [b]_n + [a]_n,$$

where the first and third equalities follow from the definition of addition of residue classes, and the second equality follows from the commutativity property of integer addition. The reader may verify the other properties using similar arguments. □

An algebraic structure satisfying the conditions in the above theorem is known more generally as a "commutative ring with unity," a notion that we will discuss in Chapter 9.

Note that while all elements of $\mathbb{Z}_n$ have an additive inverses, not all elements of $\mathbb{Z}_n$ have a multiplicative inverse. Indeed, for $a \in \mathbb{Z}$, the residue class $[a]_n \in \mathbb{Z}_n$ has a multiplicative inverse in $\mathbb{Z}_n$ if and only if a has a multiplicative inverse modulo n, which by Theorem 2.4, holds if and only if $\gcd(a, n) = 1$. Since multiplicative inverses modulo n are uniquely determined modulo n (see discussion following Theorem 2.5), it follows that if $\alpha \in \mathbb{Z}_n$ has a multiplicative inverse in $\mathbb{Z}_n$, then this inverse is unique, and we may denote it by α^{-1}.

One denotes by $\mathbb{Z}_n^*$ the set of all residue classes that have a multiplicative inverse. It is easy to see that $\mathbb{Z}_n^*$ is closed under multiplication; indeed, if $\alpha, \beta \in \mathbb{Z}_n^*$, then $(\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}$. Also, note that for $\alpha \in \mathbb{Z}_n^*$ and $\beta, \beta' \in \mathbb{Z}_n$, if $\alpha\beta = \alpha\beta'$, we may effectively cancel α from both sides of this equation, obtaining $\beta = \beta'$—this is just a restatement of the first part of Theorem 2.5 in the language of residue classes.

For $\alpha \in \mathbb{Z}_n$ and positive integer k, the expression α^k denotes the product $\alpha \cdot \alpha \cdot \cdots \cdot \alpha$, where there are k terms in the product. One may extend this definition to $k = 0$, defining α^0 to be the multiplicative identity $[1]_n$. If α has a multiplicative inverse, then it is easy to see that for any integer $k \geq 0$, α^k has a multiplicative inverse as well, namely, $(\alpha^{-1})^k$, which we may naturally write as α^{-k}.

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 defining $\mathbb{Z}_n$ is to simply define it to consist of the n "symbols" $\overline{0}, \overline{1}, \ldots, \overline{n-1}$, with addition and multiplication defined as

$$\overline{a} + \overline{b} := \overline{(a + b) \bmod n}, \quad \overline{a} \cdot \overline{b} := \overline{(a \cdot b) \bmod n},$$

for $a, b = 0, \ldots, n-1$. Such a definition is equivalent to the one we have given here, with the symbol $\overline{a}$ corresponding to the residue class $[a]_n$. 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.

EXERCISE 2.11. Show that for any positive integer n, and any integer k, the residue classes $[k+a]_n$, for $a = 0, \ldots, n-1$, are distinct and therefore include all residue classes modulo n.

EXERCISE 2.12. Verify the following statements for $\mathbb{Z}_n$:

(a) There is only one element of $\mathbb{Z}_n$ that acts as an additive identity; that is, if $\alpha \in \mathbb{Z}_n$ satisfies $\alpha + \beta = \beta$ for all $\beta \in \mathbb{Z}_n$, then $\alpha = [0]_n$.

(b) Additive inverses in $\mathbb{Z}_n$ are unique; that is, for all $\alpha \in \mathbb{Z}_n$, if $\alpha + \beta = [0]_n$, then $\beta = -\alpha$.

(c) If $\alpha \in \mathbb{Z}_n^*$ and $\gamma, \delta \in \mathbb{Z}_n$, then there exists a unique $\beta \in \mathbb{Z}_n$ such that $\alpha\beta + \gamma = \delta$.

EXERCISE 2.13. Verify the usual "rules of exponent arithmetic" for $\mathbb{Z}_n$. That is, show that for $\alpha \in \mathbb{Z}_n$, and non-negative integers k_1, k_2, we have

$$(\alpha^{k_1})^{k_2} = \alpha^{k_1 k_2} \quad \text{and} \quad \alpha^{k_1}\alpha^{k_2} = \alpha^{k_1 + k_2}.$$

Moreover, show that if $\alpha \in \mathbb{Z}_n^*$, then these identities hold for all integers k_1, k_2.

2.4 Euler's phi function

Euler's phi function $\phi(n)$ is defined for positive integer n as the number of elements of $\mathbb{Z}_n^*$. Equivalently, $\phi(n)$ is equal to the number of integers between 0 and $n-1$ that are relatively prime to n. For example, $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, and $\phi(4) = 2$.

A fact that is sometimes useful is the following:

Theorem 2.11. *For any positive integer n, we have*

$$\sum_{d \mid n} \phi(d) = n,$$

where the sum is over all positive divisors d of n.

Proof. Consider the list of n rational numbers $0/n, 1/n, \ldots, (n-1)/n$. For any divisor d of n and for any integer a with $0 \leq a < d$ and $\gcd(a, d) = 1$, the fraction a/d appears in the list exactly once, and moreover, every number in the sequence, when expressed as a fraction in lowest terms, is of this form. □

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

Theorem 2.12. *For positive integers n, m with $\gcd(n, m) = 1$, we have*

$$\phi(nm) = \phi(n)\phi(m).$$

Proof. Consider the map

$$\begin{aligned} \rho : \quad \mathbb{Z}_{nm} &\to \mathbb{Z}_n \times \mathbb{Z}_m \\ [a]_{nm} &\mapsto ([a]_n, [a]_m). \end{aligned}$$

First, note that the definition of ρ is unambiguous, since $a \equiv a' \pmod{nm}$ implies $a \equiv a' \pmod{n}$ and $a \equiv a' \pmod{m}$. Second, according to the Chinese remainder theorem, the map ρ is one-to-one and onto. Moreover, it is easy to see that $\gcd(a, nm) = 1$ if and only if $\gcd(a, n) = 1$ and $\gcd(a, m) = 1$ (verify). Therefore, the map ρ carries $\mathbb{Z}_{nm}^*$ injectively onto $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$. In particular, $|\mathbb{Z}_{nm}^*| = |\mathbb{Z}_n^* \times \mathbb{Z}_m^*|$. □

Theorem 2.13. *For a prime p and a positive integer e, we have $\phi(p^e) = p^{e-1}(p-1)$.*

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, $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$. □

As an immediate consequence of the above two theorems, we have:

Theorem 2.14. *If $n = p_1^{e_1} \cdots p_r^{e_r}$ is the factorization of n into primes, then*

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

Exercise 2.14. Show that $\phi(nm) = \gcd(n, m) \cdot \phi(\mathrm{lcm}(n, m))$.

2.5 Fermat's little theorem

Let n be a positive integer, and let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Consider the sequence of powers of $\alpha := [a]_n \in \mathbb{Z}_n^*$:

$$[1]_n = \alpha^0, \alpha^1, \alpha^2, \ldots.$$

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. We claim that $i = 0$, or equivalently, $\alpha^k = [1]_n$. To see this, suppose by way of contradiction that $\alpha^k = \alpha^i$, for some $i = 1, \ldots, k-1$. Then we can cancel α from both sides of the equation $\alpha^k = \alpha^i$, obtaining $\alpha^{k-1} = \alpha^{i-1}$, and this contradicts the minimality of k.

From the above discussion, we see that the first k powers of α, that is, $[1]_n = \alpha^0, \alpha^1, \ldots, \alpha^{k-1}$, are distinct, and subsequent powers of α simply repeat this pattern. More generally, we may consider both positive and negative powers of α—it is easy to see (verify) that for all $i, j \in \mathbb{Z}$, we have $\alpha^i = \alpha^j$ if and only if $i \equiv j \pmod{k}$. In particular, we see that for any integer i, we have $\alpha^i = [1]_n$ if and only if k divides i.

This value k is called the **multiplicative order of** α or the **multiplicative order of** a **modulo** n. It can be characterized as the smallest positive integer k such that

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

***Example* 2.6.** 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
$1^i \bmod 7$	1	1	1	1	1	1
$2^i \bmod 7$	2	4	1	2	4	1
$3^i \bmod 7$	3	2	6	4	5	1
$4^i \bmod 7$	4	2	1	4	2	1
$5^i \bmod 7$	5	4	6	2	3	1
$6^i \bmod 7$	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 2.15 (Euler's Theorem). *For any positive integer n, and any integer a relatively prime to n, we have $a^{\phi(n)} \equiv 1 \pmod{n}$. In particular, the multiplicative order of a modulo n divides $\phi(n)$.*

Proof. Let $\alpha := [a]_n \in \mathbb{Z}_n^*$. Consider the map $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ that sends $\beta \in \mathbb{Z}_n^*$ to $\alpha\beta$. Observe that f is injective, since if $\alpha\beta = \alpha\beta'$, we may cancel α from both sides of this equation, obtaining $\beta = \beta'$. Since f maps $\mathbb{Z}_n^*$ injectively into itself, and since $\mathbb{Z}_n^*$ is a finite set, it must be the case that f is surjective

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

$$\prod_{\beta \in \mathbb{Z}_n^*} \beta = \prod_{\beta \in \mathbb{Z}_n^*} (\alpha\beta) = \alpha^{\phi(n)} \Big(\prod_{\beta \in \mathbb{Z}_n^*} \beta \Big). \tag{2.6}$$

Canceling the common factor $\prod_{\beta \in \mathbb{Z}_n^*} \beta \in \mathbb{Z}_n^*$ from the left- and right-hand side of (2.6), we obtain

$$\alpha^{\phi(n)} = [1]_n.$$

That proves the first statement of the theorem. The second follows from the observation made above that $\alpha^i = [1]_n$ if and only if the multiplicative order of α divides i. □

As a consequence of this, we obtain:

Theorem 2.16 (Fermat's little theorem). *For any prime p, and any integer $a \not\equiv 0 \pmod{p}$, we have $a^{p-1} \equiv 1 \pmod{p}$. Moreover, for any integer a, we have $a^p \equiv a \pmod{p}$.*

Proof. The first statement follows from Theorem 2.15, and the fact that $\phi(p) = p - 1$. The second statement is clearly true if $a \equiv 0 \pmod{p}$, and if $a \not\equiv 0 \pmod{p}$, we simply multiply both sides of the congruence $a^{p-1} \equiv 1 \pmod{p}$ by a. □

For a 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 $\phi(n)$. If this is the case, then for $\alpha := [a]_n$, the powers α^i range over all elements of $\mathbb{Z}_n^*$ as i ranges over the interval $0, \ldots, \phi(n) - 1$. Not all positive integers have primitive roots — we will see in §10.2 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.

Exercise 2.15. Find an integer whose multiplicative order modulo 101 is 100.

Exercise 2.16. Suppose $\alpha \in \mathbb{Z}_n^*$ has multiplicative order k. Show that for any $m \in \mathbb{Z}$, the multiplicative order of α^m is $k/\gcd(m, k)$.

Exercise 2.17. Suppose $\alpha \in \mathbb{Z}_n^*$ has multiplicative order k, $\beta \in \mathbb{Z}_n^*$ has multiplicative order ℓ, and $\gcd(k, \ell) = 1$. Show that $\alpha\beta$ has multiplicative order $k\ell$. Hint: use the previous exercise.

EXERCISE 2.18. Prove that for any prime p, we have

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

Hint: using the result of Exercise 2.5, we know that the only elements of $\mathbb{Z}_p^*$ that act as their own multiplicative inverse are $[\pm 1]_n$; rearrange the terms in the product $\prod_{\beta \in \mathbb{Z}_p^*} \beta$ so that except for $[\pm 1]_n$, the terms are arranged in pairs, where each pair consists of some $\beta \in \mathbb{Z}_p^*$ and its multiplicative inverse.

2.6 Arithmetic functions and Möbius inversion

A function, such as Euler's function ϕ, from the positive integers into the reals is sometimes called an **arithmetic function** (actually, one usually considers complex-valued functions as well, but we shall not do so here). 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 $f(nm) = f(n)f(m)$. Theorem 2.12 simply says that ϕ is multiplicative.

In this section, we develop some of the theory of arithmetic functions that is pertinent to number theory; however, the results in this section will play only a very minor role in the remainder of the text.

We begin with a simple observation, which the reader may easily verify:

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

Next, we define a binary operation on arithmetic functions that has a number of interesting properties and applications. 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

$$(f \star (g \star h))(n) = \sum_{n=d_1d_2d_3} f(d_1)g(d_2)h(d_3) = ((f \star g) \star h)(n),$$

the sum being over all triples (d_1, d_2, d_3) of positive integers with $d_1d_2d_3 = n$.

We now introduce three special arithmetic functions: I, J, and μ. The function $I(n)$ is defined to be 1 when $n = 1$ and 0 when $n > 1$. The function $J(n)$ is defined to be 1 for all n.

The **Möbius function** μ is defined for positive integers n as follows:

$$\mu(n) := \begin{cases} 0 & \text{if } n \text{ is divisible by a square other than 1;} \\ (-1)^r & \text{if } n \text{ is the product of } r \geq 0 \text{ distinct primes.} \end{cases}$$

Thus, if $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n, then $\mu(n) = 0$ if $e_i > 1$ for some i, and otherwise, $\mu(n) = (-1)^r$. 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 (verify) that for any arithmetic function f, we have

$$I \star f = f \quad \text{and} \quad (J \star f)(n) = \sum_{d|n} f(d).$$

Also, the functions I, J, and μ are multiplicative (verify). A useful property of the Möbius function is the following:

Theorem 2.17. *For any multiplicative function f, if $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n, we have*

$$\sum_{d|n} \mu(d)f(d) = (1 - f(p_1)) \cdots (1 - f(p_r)). \tag{2.7}$$

In case $r = 0$ (i.e., $n = 1$), the product on the right-hand side of (2.7) is interpreted (as usual) as 1.

Proof. The non-zero terms in the sum on the left-hand side of (2.7) 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 (2.7). □

For example, suppose $f(d) = 1/d$ in the above theorem, and let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of n. Then we obtain:

$$\sum_{d|n} \mu(d)/d = (1 - 1/p_1) \cdots (1 - 1/p_r). \tag{2.8}$$

As another example, suppose $f = J$. Then we obtain

$$(\mu \star J)(n) = \sum_{d|n} \mu(d) = \prod_{i=1}^{r} (1-1),$$

which is 1 if $n = 1$, and is zero if $n > 1$. Thus, we have

$$\mu \star J = I. \tag{2.9}$$

Theorem 2.18 (Möbius inversion formula). *Let f and F be arithmetic functions. Then we have $F = J \star f$ if and only if $f = \mu \star F$.*

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

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

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

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

The Möbius inversion formula says this:

$$F(n) = \sum_{d|n} f(d) \quad \text{for all positive integers } n$$

if and only if

$$f(n) = \sum_{d|n} \mu(d) F(n/d) \quad \text{for all positive integers } n.$$

As an application of the Möbius inversion formula, we can get a different proof of Theorem 2.14, based on Theorem 2.11. Let $F(n) := n$ and $f(n) := \phi(n)$. Theorem 2.11 says that $F = J \star f$. Applying Möbius inversion to this yields $f = \mu \star F$, and using (2.8), we obtain

$$\begin{aligned} \phi(n) &= \sum_{d|n} \mu(d) n/d = n \sum_{d|n} \mu(d)/d \\ &= n(1 - 1/p_1) \cdots (1 - 1/p_r). \end{aligned}$$

Of course, one could turn the above argument around, using Möbius inversion and (2.8) to derive Theorem 2.11 from Theorem 2.14.

Exercise 2.19. 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 2.20. Let f be a polynomial with integer coefficients, and for positive integer n define $\omega_f(n)$ to be the number of integers $z \in \{0, \ldots, n-1\}$ such that $f(z) \equiv 0 \pmod{n}$. Show that ω_f is multiplicative.

EXERCISE 2.21. Show that if f and g are multiplicative, then so is $f \star g$.

EXERCISE 2.22. Define $\tau(n)$ to be the number of positive divisors of n.

(a) Show that τ is a multiplicative function.

(b) Show that

$$\tau(n) = (e_1 + 1) \cdots (e_r + 1),$$

where $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n.

(c) Show that

$$\sum_{d|n} \mu(d)\tau(n/d) = 1.$$

(d) Show that

$$\sum_{d|n} \mu(d)\tau(d) = (-1)^r,$$

where $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n.

EXERCISE 2.23. Define $\sigma(n) := \sum_{d|n} d$.

(a) Show that σ is a multiplicative function.

(b) Show that

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{e_i+1} - 1}{p_i - 1},$$

where $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n.

(c) Show that

$$\sum_{d|n} \mu(d)\sigma(n/d) = n.$$

(d) Show that

$$\sum_{d|n} \mu(d)\sigma(d) = (-1)^r p_1 \cdots p_r,$$

where $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n.

EXERCISE 2.24. The **Mangoldt function** $\Lambda(n)$ is defined for all positive integers n by

$$\Lambda(n) := \begin{cases} \log p & \text{if } n = p^k, \text{ where } p \text{ is prime and } k \text{ is a positive integer;} \\ 0 & \text{otherwise.} \end{cases}$$

(a) Show that

$$\sum_{d|n} \Lambda(d) = \log n.$$

(b) Using part (a), show that

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d.$$

EXERCISE 2.25. 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

$$\sum_{d|n} (\mu(d))^2 f(d) = (1 + f(p_1)) \cdots (1 + f(p_r)).$$

EXERCISE 2.26. Show that n is square-free (see Exercise 1.13) if and only if $\sum_{d|n} (\mu(d))^2 \phi(d) = n$.

EXERCISE 2.27. Show that for any 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 2.28. Show that if f is a multiplicative function, then so is its Dirichlet inverse (as defined in the previous exercise).