**Queen's University**
**School of Computing**

**CISC 203: Discrete Structures II**
**Number Theory**
**Fall 2025**

This module covers the following topics:

- Dividing
- Greatest Common Divisor
- Modular Arithmetic
- The Chinese Remainder Theorem

Coverage of these topics can also be found in Sections 4.1 (Divisibility and Modular Arithmetic), 4.3 (Primes and Greatest Common Divisors), and 4.4 (Solving Congruences).

# 1 Division

**Definition 1** ($a \mid b$)**.** Let $a, b \in \mathbb{Z}$ and $a \neq 0$. If $b = ak$ for some integer $k$ (i.e., if $b$ is a multiple of $a$), we say that $a$ divides $b$, and denote this as $a \mid b$.

**Theorem 2** (Division)**.** *Let $a, b \in \mathbb{Z}$ with $b > 0$. There exist exactly one pair of integers $q$ and $r$ such that $a = qb + r$ and $0 \leq r < b$.*

*Proof.* Omitted. See Theorem 2 in §4.1.3: The Division Algorithm (p. 257) of the textbook. □

We call $d$ the **divisor**, $a$ the **dividend**, $q$ the **quotient**, and $r$ the **remainder**. The remainder of $a$ divided by $b$ is the smallest natural number that can be formed by subtracting multiples of $b$ from $a$.

**Definition 3** (div and mod)**.** Let $a, b \in \mathbb{Z}$ with $b > 0$. We define the operations div and mod by

$$a \text{ div } b = q$$

and

$$a \bmod b = r,$$

where $q$ and $r$ are the unique pair of numbers (by Theorem 2) where $a = qb + r$ and $0 \leq r < b$.

The quotient may be negative, but the remainder is always positive. For example, $-37 \text{ div } 5 = -8$ and $-37 \bmod 5 = 3$.

A different (but related) notation, which we distinguish using parentheses, denotes the equivalence relation of congruence modulo $n$.

**Definition 4** (Congruence modulo $n$)**.** Let $n$ be a positive integer and $x$ and $y$ be any two integers. If $n|(x - y)$, we say that $x$ and $y$ are congruent modulo $n$. This is denoted $x \equiv y \mod n$.

The set of all integers congruant to an integer $a$ modulo $m$ is called the **congruence class** of $a$ modulo $m$.

**Example 5.** $53 \equiv 23 \pmod{10}$ means that $53 - 23 = 30$ is a multiple of 10. However, $53 \bmod 10 = 3$ means that the remainder of $53 \text{ div } 10$ is 3.

**Theorem 6.** *Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Then,*

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

*if and only if*

$$a \bmod n = b \bmod n.$$

*Proof.* Omitted. See Theorem 3 in §4.1.4: Modular Arithmetic (p. 258) of the textbook. □

**Example 7.** $9 \equiv 17 \pmod 4$ is a true statement, so we also have $9 \bmod 4 = 1$ and $17 \bmod 4 = 1$.

## 2 Greatest Common Divisor

**Definition 8** (Common divisor)**.** Let $a, b \in \mathbb{Z}$. If an integer $d$ divides both $a$ and $b$, we say that $d$ is a **common divisor** of $a$ and $b$.

**Example 9.** The common divisors of 18 and 12 are $\pm 1$, $\pm 2$, $\pm 3$, and $\pm 6$.

The common divisors of 25 and 50 are $\pm 1$, $\pm 5$, and $\pm 25$.

**Definition 10** (Greatest common divisor)**.** Let $a, b \in \mathbb{Z}$. We say that an integer $d$ is the **greatest common divisor** of $a$ and $b$, provided that

1. $d$ is a common divisor of $a$ and $b$ and
2. if $e \mid a$ and $e \mid b$, then $e \leq d$.

The greatest common divisor of $a$ and $b$ is denoted $\gcd(a, b)$. By definition, it is always positive.

Note that the greatest common divisor is unique.

**Example 11.** The greatest common divisor of 18 and 12 is 6.

The greatest common divisor of 25 and 50 is 25.

The most naive way to calculate $\gcd(a, b)$ is to

1. Find all the divisors of $a$ (i.e., note down each $j$ where $j \mid a$ for $1 \leq j \leq a$).
2. Find all the divisors of $b$ (i.e., note down each $k$ where $k \mid b$ for $1 \leq k \leq b$).
3. Choose the largest number that is both a divisor of $a$ and a divisor of $b$.

However, this is very inefficient for large values of $a$ and $b$.

**Theorem 12** (The Fundamental Theorem of Arithmetic)**.** *Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes, where the prime factors are written in order of nondecreasing size.*

*Proof.* Omitted. See Theorem 1 in §4.3.2: Primes (p. 276) of the textbook. □

**Example 13.** The prime factorizations of 20, 23, 621, and 256 are given by

$$\begin{aligned}
r_0 &= 20 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 5, \\
r_1 &= 23 = 23, \\
r_2 &= 288 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^5 \cdot 3^2, \\
r_3 &= 621 = 3 \cdot 3 \cdot 3 \cdot 23 = 3^3 \cdot 23.
\end{aligned}$$

We can find the greatest common divisor of two numbers by taking the product of all common prime factors. So, $\gcd(r_0, r_2) = 2^2 = 4$ and $\gcd(r_2, r_3) = 3^2 = 9$. Since $r_0$ does not have any common prime factors with $r_3$, we have $\gcd(r_0, r_3) = 1$. We can also find the least common multiple of two numbers using this method (see p. 286 of the textbook).

However, the above method is also inefficient. In fact, for large numbers that are often used in public-key cryptography, factoring is not even computationally feasible. We will see a much more efficient method, called the Euclidean Algorithm.

**Definition 14** (Relatively prime)**.** Let $a$ and $b$ be integers. We call $a$ and $b$ **relatively prime** provided that $\gcd(a, b) = 1$.

**Example 15.** We observe from Example 13 that 20 and 621 are relatively prime, since $\gcd(20, 621) = 1$.

## 2.1 Euclidean Algorithm

**Lemma 16.** *Let $a = bq + r$, where $a, b, q, r \in \mathbb{Z}$. Then,* $\gcd(a, b) = \gcd(b, r)$.

*Proof.* Omitted. See Lemma 1 in §4.3.7: The Euclidean Algorithm (p. 286) of the textbook. □

The Lemma above forms the basis for the Euclidean algorithm, which finds $\gcd(a, b)$, where $a$ and $b$ are positive integers, as follows:

1. Let $c = a \bmod b$.
2. If $c = 0$, then the answer is $b$.
3. Otherwise (i.e., if $c \neq 0$), the answer is $\gcd(b, c)$.

Note that the algorithm is **recursive**.

**Example 17.** To find $\gcd(360, 84)$ using the Euclidean Algorithm:

$$\begin{aligned} 360 \bmod 84 &= 24 \\ 84 \bmod 24 &= 12 \\ 24 \bmod 12 &= 0. \end{aligned}$$

So, $\gcd(360, 84) = 12$.

**Example 18.** To find $\gcd(796, 26)$ using the Euclidean Algorithm:

$$\begin{aligned} 796 \bmod 26 &= 16 \\ 26 \bmod 16 &= 10 \\ 16 \bmod 10 &= 6 \\ 10 \bmod 6 &= 4 \\ 6 \bmod 4 &= 2 \\ 4 \bmod 2 &= 0. \end{aligned}$$

So, $\gcd(796, 26) = 2$.

**Theorem 19.** *Let $a$ and $b$ be integers, at least one of them not 0. The greatest common divisor $d$ of $a$ and $b$ can be written as*

$$d = ax + by$$

*for some integers $x$ and $y$; and $d$ is the smallest positive integer that can be written in this form.*

*Proof.* Omitted. See Theorem 6 in §4.3.8: gcds as Linear Combinations (p. 289) of the textbook. ☐

Given two integers $a$ and $b$, with $b > 0$, we can use the Euclidean Algorithm to find $x$ and $y$ such that $ax + by = \gcd(a, b)$. However, we will need to write our steps a bit differently.

Recall from Theorem 2 that for any integers $a$ and $b$ with $b > 0$, if we divide $a$ by $b$ we obtain $r = a \bmod b$ (the remainder) and $q = a \text{ div } b$ (the quotient), and we can write $a = bq + r$.

Note that in the first step of the Euclidean Algorithm, we only kept track of the remainder ($a \bmod b$), but now we will also keep track of the quotient ($a \text{ div } b$), and will write each line in the form $a = bq + r$.

**Example 20.** Using the Euclidean Algorithm, we find the integers $x$ and $y$ such that $360x + 84y = \gcd(360, 84)$, as follows.

$$\begin{aligned} 360 &= 84 \cdot 4 + 24 \\ 84 &= 24 \cdot 3 + 12 \\ 24 &= 12 \cdot 2 + 0 \end{aligned}$$

We see above (highlighted in blue) that $\gcd(360, 84) = 12$ (which we already found in Example 17).

Now, let us rearrange each of the lines above (except for the last one, which we don't need) so that the remainders are on the left-hand side of the equals sign, and everything else is on the right-hand side, with the quotients enclosed in round parentheses and highlighted in red.

$$\begin{aligned} 24 &= 360 + 84(-4) \\ 12 &= 84 + 24(-3) \end{aligned}$$

Notice that the first equation above contains 360 and the second equation contains 84, and we want an equation in the form $360x + 84y$. Working backwards, replace 24 (highlighted in green) in the second equation with the first equation, as follows:

$$\begin{aligned} 12 &= 84 + 24(-3) \\ &= 84 + [360 + 84(-4)](-3) \\ &= 360(-3) + 84(13) \end{aligned}$$

Note that when collecting terms, we work with the quotients and keep all the other numbers as they are.

So, for $x = -3$ and $y = 13$, we have $360x + 84y = \gcd(360, 84) = 12$.

**Example 21.** Using the Euclidean Algorithm, we find the integers $x$ and $y$ such that $1205x + 37y = \gcd(1205, 37)$.

To find $\gcd(1205, 37)$ using the Euclidean Algorithm:

$$\begin{aligned} 1205 &= 37 \cdot 32 + 21 \\ 37 &= 21 \cdot 1 + 16 \\ 21 &= 16 \cdot 1 + 5 \\ 16 &= 5 \cdot 3 + 1 \\ 5 &= 1 \cdot 5 + 0 \end{aligned}$$

We see above (highlighted in blue) that $\gcd(1205, 37) = 1$.

Now, we rearrange the equations (except for the last one) again as in the previous example:

$$\begin{aligned} 21 &= 1205 + 37(-32) \\ 16 &= 37 + 21(-1) \\ 5 &= 21 + 16(-1) \\ 1 &= 16 + 5(-3) \end{aligned}$$

Working backwards, take the last equation and substitute the value 5 with the previous equation:

$$\begin{aligned} 1 &= 16 + 5(-3) \\ &= 16 + [21 + 16(-1)](-3) \\ &= 16(4) + 21(-3) \end{aligned}$$

Now, replace the value 16 with the previous equation:

$$\begin{aligned} 1 &= 16(4) + 21(-3) \\ &= [37 + 21(-1)](4) + 21(-3) \\ &= 37(4) + 21(-7) \end{aligned}$$

Now, replace the value 21 with the previous equation:

$$\begin{aligned} 1 &= 37(4) + 21(-7) \\ &= 37(4) + [1205 + 37(-32)](-7) \\ &= 37(228) + 1205(-7) \end{aligned}$$

So, for $x = 228$ and $y = -7$, we have $1205x + 37y = \gcd(1205, 37) = 1$.

Notice in the example above that there exists no integer greater than 1 that divides both 1205 and 37. So, 1205 and 37 are **relatively prime**.

## 2.2 Extended Euclidean Algorithm

In the previous example we expressed $\gcd(a, b)$ in the form $ax+by$ by first executing the Euclidean Algorithm and then working backwards to perform substitutions to obtain the integers $x$ and $y$. The Extended Euclidean Algorithm can obtain $x$ and $y$ with a single forward pass of the algorithm.

Observe from Example 20 that each step $j$ of the algorithm (starting from $j = 0$) performs the computation $r_j = r_{j+1} \cdot q_{j+1} + r_{j+2}$. Thus, we can represent the steps of the algorithm in tabular form as follows:

| $j$ | $r_j$ | $r_{j+1}$ | $q_{j+1}$ | $r_{j+2}$ |
|---|---|---|---|---|
| 0 | 360 | 84 | 4 | 24 |
| 1 | 84 | 24 | 3 | 12 |
| 2 | 24 | 12 | 2 | 0 |

(1)

The Extended Euclidean Algorithm keeps track of two additional values $s_j = s_{j-2} - q_{j-1}s_{j-1}$ and $t_j = t_{j-2} - q_{j-1}t_{j-1}$, with the initial values fixed to $s_0 = 1, s_1 = 0, t_0 = 0$, and $t_1 = 1$. After reaching the final step $j$ of the Euclidean Algorithm, we must compute one final iteration of $s_{j+1}$ and $t_{j+1}$. The result is as follows:

| $j$ | $r_j$ | $r_{j+1}$ | $q_{j+1}$ | $r_{j+2}$ | $s_j$ | $t_j$ |
|---|---|---|---|---|---|---|
| 0 | 360 | 84 | 4 | 24 | 1 | 0 |
| 1 | 84 | 24 | 3 | 12 | 0 | 1 |
| 2 | 24 | 12 | 2 | 0 | $1-(4)(0)=1$ | $0-(4)(1)=-4$ |
| 3 | | | | | $0-(3)(1)=-3$ | $1-(3)(-4)=13$ |

(2)

Now, we take $x = s_3$ and $y = t_3$, which yields $\gcd(360, 84) = 12 = (-3)360 + (13)84$.

# 3 Modular Arithmetic

We are accustomed to performing arithmetic on infinite sets of numbers, like $\mathbb{Z}$ or $\mathbb{R}$. But sometimes we need to perform arithmetic on a finite set, and we need it to make sense and be consistent (as far as possible) with normal arithmetic. In this unit we will discuss versions of addition, multiplication, subtraction and division for finite sets of numbers.

We will focus on the sets defined by $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$ where $n \geq 2$.

$\mathbb{Z}_n$ is just the set of remainders we can get when we divide integers by $n$. We call this number system "the integers mod $n$".

One of the important features we want to build into our mathematical operations for finite sets is **closure**: the property that when we apply an operation to two elements of the set, the result is also an element of the set.

## 3.1 Modular Addition and Multiplication

We will use the symbols $\oplus, \otimes, \ominus$, and $\oslash$ to represent addition mod $n$, multiplication mod $n$, subtraction mod $n$, and division mod $n$, respectively.

**Definition 22** (Modular addition and modular multiplication)**.** Let $n$ be a positive integer and $a, b \in \mathbb{Z}_n$. We define

$$a \oplus b = (a + b) \bmod n \quad \text{and}$$
$$a \otimes b = (ab) \bmod n.$$

Note that because we end each calculation with mod $n$ we are guaranteed that our results will be in $\mathbb{Z}_n$, so we will have closure.

**Example 23.** Let $n = 7$. We have the following:

$$3 \oplus 6 = (3 + 6) \bmod 7 = 9 \bmod 7 = 2$$

$$3 \otimes 6 = (3 \cdot 6) \bmod 7 = 18 \bmod 7 = 4$$

Let $n = 8$. We have the following:

$$3 \oplus 6 = (3 + 6) \bmod 8 = 9 \bmod 8 = 1$$

$$3 \otimes 6 = (3 \cdot 6) \bmod 8 = 18 \bmod 8 = 2$$

Note that the symbols $\oplus$ and $\otimes$ depend on the context. If we are working in $\mathbb{Z}_{10}$, then $5 \oplus 5 = 0$. But if we are working in $\mathbb{Z}_9$, $5 \oplus 5 = 1$.

**Proposition 24** (Properties of modular addition and modular multiplication)**.** *Let $n$ be an integer with $n \geq 2$. The operations $\oplus$ and $\otimes$ have the following properties:*

- *Commutativity: For all $a, b \in \mathbb{Z}_n$, we have $a \oplus b = b \oplus a$ and $a \otimes b = b \otimes a$.*
- *Associativity: For all $a, b, c \in \mathbb{Z}_n$, we have $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ and $a \otimes (b \otimes c) = (a \otimes b) \otimes c$.*
- *Distributivity: For all $a, b, c \in \mathbb{Z}_n$, we have $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$.*
- *Identity element 0, for addition: For all $a \in \mathbb{Z}_n$, $a \oplus 0 = a$.*
- *Identity element 1, for multiplication: For all $a \in \mathbb{Z}_n$, $a \otimes 1 = a$.*

*Note that 0 is not an identity element for multiplication, since $a \otimes 0 = 0$.*

Let us prove the commutative property for $\oplus$:

$$a \oplus b = (a + b) \bmod n = (b + a) \bmod n = b \oplus a.$$

The proof that $\otimes$ is commutative is just as easy. The key step for proving the associative property for $\oplus$ and $\otimes$ is to write $a \oplus b = a + b + kn$ or $a \otimes b = ab + ln$, where $k$ and $l$ are integers.

## 3.2 Modular Subtraction

In ordinary arithmetic, when we write $a - b = x$, we understand that this is equivalent to writing $a = b + x$.

Similarly, to find the value of $x$ in the equation $a \ominus b = x$, we say that $x$ is the element of $\mathbb{Z}_n$ such that $a = b \oplus x$. This definition relies on the fact that there is exactly one $x \in \mathbb{Z}_n$ such that $a = b \oplus x$.[1]

**Definition 25** (Modular subtraction)**.** Let $n$ be a positive integer and $a, b \in \mathbb{Z}_n$. We define $a \ominus b$ to be the unique $x \in \mathbb{Z}_n$ such that $a = b \oplus x$.

Alternatively, we could have defined $a \ominus b$ to be $(a - b) \bmod n$. We prove below that this would have given the same result.

**Proposition 26** (Modular subtraction)**.** *Let $n$ be a positive integer and $a, b \in \mathbb{Z}_n$. Then, $a \ominus b = (a - b) \bmod n$.*

*Proof.* First, we need to show that $[(a - b) \bmod n] \in \mathbb{Z}_n$. This is obvious from the definition of mod.

Next, we show that if $x = (a - b) \bmod n$, then $a = b \oplus x$. So, we take $b \oplus x$ and substitute $x = (a - b) \bmod n = a - b + kn$. Then,

$$\begin{aligned} b \oplus x &= (b + (a - b + kn)) \bmod n \\ &= (a + kn) \bmod n \\ &= a. \end{aligned}$$

□

**Example 27.** We will compute $2 \ominus 3$ in two ways: Using Definition 25 and Proposition 26.

First, let's look at the addition table below, which shows all the values of $a \oplus b$ for $\mathbb{Z}_5$.

| | | b | | | | |
|---|---|---|---|---|---|---|
| | $\oplus$ | 0 | 1 | 2 | 3 | 4 |
| | 0 | 0 | 1 | 2 | 3 | 4 |
| | 1 | 1 | 2 | 3 | 4 | 0 |
| a | 2 | 2 | 3 | 4 | 0 | 1 |
| | 3 | 3 | 4 | 0 | 1 | 2 |
| | 4 | 4 | 0 | 1 | 2 | 3 |

[1] Proving this is left as an exercise for the reader. Hint: Suppose for the sake of contradiction that there are two solutions, i.e., $a = b \oplus x$ and $a = b \oplus y$ with $x \neq y$.

So, by Definition 25, to find $x = 2 \ominus 3$, we must find the value $x$ that satisfies $3 \oplus x = 2$. So, in the table above, we look at the row for $a = 3$ and step through each value until we find the column where the value is 2. We see that this happens when $x = 4$.

By Proposition 26, we can compute $2 \ominus 3$ as

$$\begin{aligned} 2 \ominus 3 &= (2 - 3) \bmod 5 \\ &= -1 \bmod 5 \\ &= 4. \end{aligned}$$

So, we found the same answer using both methods.

**Exercise**

Working in $\mathbb{Z}_5$, find $3 \ominus 2$ and $1 \ominus 2$ using both Definition 25 and Proposition 26.

## 3.3 Modular Division

Modular division is significantly different from the other three modular operations.

When working with the rational numbers $\mathbb{Q}$, when we write $x = a \div b$ we understand that $x = a \cdot b^{-1}$, where $b^{-1}$ is $\frac{1}{b}$ and is referred to as the **reciprocal** (or inverse) of $b$. Note that $b = 0$ has no reciprocal, and for all other $b \in \mathbb{Q}$ we have have $b \cdot b^{-1} = 1$.

Similarly, it seems reasonable that for modular division in $\mathbb{Z}_n$ we should let $b^{-1}$ be the element that satisfies $b \otimes b^{-1} = 1$. However, it turns out that for many of the sets $\mathbb{Z}_n$, there are elements (besides 0) that have no reciprocal. For example, consider the multiplication table below, which shows all the values of $a \otimes b$ for $\mathbb{Z}_{10}$.

| | | b | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | $\otimes$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | 2 | 0 | 2 | 4 | 6 | 8 | 0 | 2 | 4 | 6 | 8 |
| | 3 | 0 | 3 | 6 | 9 | 2 | 5 | 8 | 1 | 4 | 7 |
| | 4 | 0 | 4 | 8 | 2 | 6 | 0 | 4 | 8 | 2 | 6 |
| a | 5 | 0 | 5 | 0 | 5 | 0 | 5 | 0 | 5 | 0 | 5 |
| | 6 | 0 | 6 | 2 | 8 | 4 | 0 | 6 | 2 | 8 | 4 |
| | 7 | 0 | 7 | 4 | 1 | 8 | 5 | 2 | 9 | 6 | 3 |
| | 8 | 0 | 8 | 6 | 4 | 2 | 0 | 8 | 6 | 4 | 2 |
| | 9 | 0 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

In the table above, to find the reciprocal of an element $a$ in $\mathbb{Z}_{10}$, locate the element $b$ for which $a \otimes b = 1$. All such occurrences in the table are highlighted. Note that:

- 0 does not have a reciprocal (as expected).
- The element 1 is its own reciprocal.
- The reciprocal of 3 is 7, and the reciprocal of 7 is 3. That is because if $b = a^{-1}$, it must be the case that $a = b^{-1}$.
- The element 9 is its own reciprocal.
- The elements 2, 4, 5, 6, and 8 do not have reciprocals.
- All elements that do have a reciprocal each have exactly one unique reciprocal. This is proved in Proposition 37.10 (p. 270) of the textbook.

More formally, we define the modular reciprocal as follows.

**Definition 28** (Modular reciprocal)**.** Let $n$ be a positive integer and let $a \in \mathbb{Z}_n$. A reciprocal of $a$ is an element $b \in \mathbb{Z}_n$ such that $a \otimes b = 1$. An element of $\mathbb{Z}_n$ that has a reciprocal is called **invertible**.

Note also from the multiplication table that an element $a \in \mathbb{Z}_n$ is only invertible if the greatest common divisor of $a$ and $n$ is 1, i.e., if $a$ and $n$ are relatively prime.

**Theorem 29** (Invertible elements of $\mathbb{Z}_n$)**.** *Let $n$ be a positive integer and let $a \in \mathbb{Z}_n$. Then $a$ is invertible if and only if $a$ and $n$ are relatively prime.*

*Proof.* Omitted. See proof of Theorem 37.14 on p. 271 of the textbook. □

You may be wondering, then, if it is possible to pick an $n$ such that every element of $\mathbb{Z}_n$ (except for 0) is invertible. We prove below that this is the case if and only if $n$ is prime.

**Proposition 30.** *Every element of $\mathbb{Z}_n$ except 0 is invertible if and only if $n$ is prime.*

*Proof.* If $n$ is prime and $a \in \{1, 2, \ldots, n-1\}$, then the greatest common divisor of $n$ and $a$ is 1. So, by Theorem 29, $a^{-1}$ exists for all $a \in \{1, 2, \ldots, n-1\}$.

If $a^{-1}$ exists for all $a \in \{1, 2, \ldots, n-1\}$, then by Theorem 29 the greatest common divisor of $a$ and $n$ is 1 for all $a \in \{1, 2, \ldots, n-1\}$. So, $n$ is prime. □

To illustrate, we can observe in the multiplication table for $\mathbb{Z}_7$ below that every $a \in \mathbb{Z}_7$ is invertible.

b

| | ⊗ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|---|
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| | 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| a | 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| | 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| | 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| | 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

We can now define modular division as follows.

**Definition 31** (Modular division)**.** Let $n$ be a positive integer and let $b$ be an invertible element of $\mathbb{Z}_n$. Let $a \in \mathbb{Z}_n$ be arbitrary. Then $a \oslash b$ is defined to be $a \otimes b^{-1}$.

**Example 32.** In $\mathbb{Z}_{10}$, calculate $8 \oslash 3$. Note that $3^{-1} = 7$, so

$$8 \oslash 3 = 8 \otimes 7 = 6.$$

**Example 33.** In $\mathbb{Z}_{10}$, calculate $8 \oslash 2$. Note that 2 is not invertible in $\mathbb{Z}_{10}$, so $8 \oslash 2$ is undefined.

**Exercise**

In $\mathbb{Z}_{10}$, calculate $2 \oslash 7$ using the multiplication table for $\mathbb{Z}_{10}$ (check your answer using Example 37.13 on p. 271 of the textbook).

In the following example, we see how to calculate the reciprocal without the help of a multiplication table as we used above. The Euclidean Algorithm will play a crucial role.

**Example 34.** In $\mathbb{Z}_{1205}$, find $37^{-1}$.

First, we verify that 1205 and 37 are relatively prime. We did this already in Example 21, using the Euclidean Algorithm. Using our steps from Example 21, we write $\gcd(1205, 37) = 1$ in the form $1205x + 37y$:

$$\gcd(1205, 37) = 1 = 37(228) + 1205(-7)$$

Now, we rewrite the above equation by applying mod1205 on both sides of the equation:

$$\begin{aligned}
1 \bmod 1205 &= [37(228) + 1205(-7)] \bmod 1205 \\
&= 37(228) \bmod 1205 + 1205(-7) \bmod 1205 \\
&= 37(228) \bmod 1205
\end{aligned}$$

So, we have $37 \otimes 228 = 1$ in $\mathbb{Z}_{1205}$ (by Definition 22). Thus, we have $37^{-1} = 228$ in $\mathbb{Z}_{1205}$ (by Definition 28).

**Example 35.** In $\mathbb{Z}_{1205}$, find $100 \oslash 37$.

First, we need to check if 37 has a reciprocal. From Example 34 above, we know that $37^{-1} = 228$. So, we can write

$$\begin{aligned}
100 \oslash 37 &= 100 \otimes 37^{-1} \\
&= 100 \otimes 228 \\
&= 100 \cdot 228 \bmod 1205 \\
&= 1110
\end{aligned}$$

So, $100 \oslash 37 = 1110$ in $\mathbb{Z}_{1205}$.

Now, let us solve an equation that uses modular arithmetic.

**Example 36.** Given the equation $5x \equiv 7 \pmod{19}$, find $x$.

First, we rewrite the equation by applying Proposition 6:

$$5x \bmod 19 = 7 \bmod 19$$

So, we have $5 \otimes x = 7$ in $\mathbb{Z}_{19}$ (by Definition 22). Then, $x = 7 \otimes 5^{-1}$.

We can find that $5^{-1} = 4$ (for small values, we can use a "trick" by working backwards and noticing that $5 \otimes 4 = 5 \cdot 4 = 20 \bmod 19 = 1$), so we have $x = 7 \otimes 4 = 28 \bmod 19 = 9$.

# 4 Chinese Remainder Theorem

Suppose we have a box of bananas. We know that:

- If we distribute the bananas among five monkeys, we would have one banana remaining.
- If we distribute the bananas among seven monkeys, we would have two bananas remaining.
- There are less than 35 bananas in the box.

How can we determine the number of bananas that are in the box? To do so, we can write the following equations, where $x$ denotes the number of bananas in the box:

$$\begin{aligned}
&x = 1 + 5k, \text{ for a non-negative integer } k\text{; and} \\
&x = 2 + 7l, \text{ for a non-negative integer } l.
\end{aligned}$$

In other words, we have

$$\begin{aligned} x &\equiv 1 \pmod 5 \text{ and} \\ x &\equiv 2 \pmod 7. \end{aligned}$$

We need to find $x$. So, let us substitute the first equation into the second equation as follows:

$$\begin{aligned} 1 + 5k &\equiv 2 \pmod 7 \\ 5k &\equiv 1 \pmod 7 \\ k &\equiv 5^{-1} \pmod 7 \\ k &\equiv 3 \pmod 7, \end{aligned}$$

which means that $k = 3 + 7t$ for some non-negative integer $t$. Now, we substitute our equation for $k$ into the first equation, $x = 1 + 5k$:

$$\begin{aligned} x &= 1 + 5k \\ &= 1 + 5(3 + 7t) \\ &= 1 + 15 + 35t \\ &= 16 + 35t \end{aligned}$$

Notice that for all $t > 0$, we have $x > 35$. But we know that we have less than 35 bananas in the box. So, we know that $t = 0$ and thus $x = 16$, meaning that we have 16 bananas in the box.

**Exercise**

If we knew that there are between 35 and 70 bananas in the box, how many would there be? Hint: You can just use the last equation that we arrived at above.

**Exercise**

Notice that we substituted the first equation into the second equation to find our answer. Now, as an exercise, substitute the second equation into the first equation and see that you obtain the same answer.

This leads us to the Chinese Remainder Theorem, which simply states that given a pair of equations as we had above, there will always be a solution for $x$ as long as the moduli are relatively prime.

**Theorem 37** (Chinese Remainder Theorem)**.** *Let $a, b, m, n$ be integers with $m$ and $n$ positive and relatively prime. There is a unique integer $x_0$ with $0 \leq x_0 < mn$ that solves the pair of equations*

$$\begin{aligned} x &\equiv a \pmod m \textit{ and} \\ x &\equiv b \pmod n. \end{aligned}$$

*Furthermore, every solution to these equations differs from $x_0$ by a multiple of $mn$.*

*Proof.* Omitted. See Theorem 2 in §4.4.3: The Chinese Remainder Theorem (p. 292) of the textbook. □

**Exercise**

Solve the pair of congruences

$$\begin{aligned} x &\equiv 1 \pmod 7 \text{ and} \\ x &\equiv 4 \pmod{11}. \end{aligned}$$

There is also a more generalized version of the Chinese Remainder Theorem, as follows.

**Theorem 38** (Chinese Remainder Theorem (Generalized))**.** *Let $n_1, n_2, \ldots, n_m$ be positive and pairwise relatively prime integers. Let $a_1, a_2, \ldots, a_m$ be integers. There is an integer $x_0$ that satisfies the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_m \pmod{n_m}. \end{aligned}$$

*Furthermore, every solution to these equations differs from $x_0$ by a multiple of $n_1 n_2 \cdots n_m$.*

*Proof.* Omitted. □

Note that when we had a pair of congruences and we wanted to solve for $x$, we substituted the first equation into the second equation. But if we had three or more congruences and needed to solve for $x$, we would have substituted the first equation into the second equation, and then the second equation into the third equation, until we reached the last equation.

**Example 39.** Solve the system of congruences

$$\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 2 \pmod{7} \\ x &\equiv 3 \pmod{6} \end{aligned}$$

Note that at the start of this section we already found that $x = 16 + 35t$ when solving for the first two congruences. Now, we substitute that result into the third congruence as follows.

$$16 + 35t \equiv 3 \pmod{6},$$

from which we obtain

$$35t \equiv -13 \equiv 5 \pmod{6},$$

Since $35t \equiv 5 \pmod{6}$, we have

$$5t \equiv 5 \pmod{6}.$$

So,

$$\begin{aligned} t &\equiv 5 \cdot 5^{-1} \pmod{6} \\ &\equiv 1 \pmod{6}. \end{aligned}$$

So, we have $t = 1 + 6s$ for some non-negative integer $s$. Now, we substitute $t = 1 + 6s$ into $x = 16 + 35t$:

$$\begin{aligned} x &= 16 + 35t \\ &= 16 + 35(1 + 6s) \\ &= 16 + 35 + 210s \\ &= 51 + 210s \end{aligned}$$

Note that $x$ is a solution to the three congruences for any value of $s$, so we have infinitely many solutions. Also note that the term $210s$ tells us that we only have one solution less than 210, and that each solution to the equation differs from the next by a multiple of 210, and $210 = 5 \cdot 7 \cdot 6$, which is the product of the moduli.

**Exercise**

Solve the following system of three congruences

$$\begin{aligned} x &\equiv 3 \pmod{9} \\ x &\equiv 4 \pmod{10} \\ x &\equiv 2 \pmod{11} \end{aligned}$$