# Learning Number Theory

To my wife, Sally, and our children,

Courtney, Rebecca, and Benjamin,

whose support made this book possible

David A. Smith

# Learning Number Theory

## With Python

First Edition

Direct Knowledge

Cover photo attribution: *Pillars of Creation (NIRCam and MIRI Composite Image)* courtesy of NASA, ESA, CSA, STScI. Published on November 30, 2022. For more information visit: https://webbtelescope.org

ISBN: 978-1-951290-02-3

Typeset with LaTeX and written in the United States of America.

David A. Smith
B.S. Mathematics, M.S. Mathematics
https://directknowledge.com

Direct Knowledge

# Preface

## Writing Philosophy

Writing effectively and with intention requires more than just a penchant for words; it necessitates an innate assurance that allows one to express unique ideas, reasoned perspectives, and engaging arguments. Establishing technical proficiency in syntax, grammar rules, and punctuation is also essential – standards I practice diligently. To learn the specifics of my writing practices visit https://directknowledge.com/writing

## Acknowledgements

I cannot adequately express my gratitude for all of those who dedicated their efforts to bring this book into its finished state. Their generous aid is greatly admired, and I extend them many thanks.

David A. Smith \ Fort Worth, Texas

# Table of contents

# Chapter 1

# Peano's Axioms

**Peano's Axioms** $\mathbb{N}$ is a set with the following properties.

- $\mathbb{N}$ has a distinguished element which we call **1**.
- There exists a distinguished set map $s : \mathbb{N} \to \mathbb{N}$.
- The mapping $s$ is injective.
- There does not exists an element $n \in \mathbb{N}$ such that $s(n) = 1$.
- If $S$ is a subset of $\mathbb{N}$ with the properties: $1 \in S$ and if $n \in S$, then $s(n) \in S$, then $S = \mathbb{N}$.

We call such a set $\mathbb{N}$ to be the set of natural numbers and elements of this set to be natural numbers.

**Theorem 1.1.** *If $n \in \mathbb{N}$ and $n \neq 1$, then there exists a unique $m \in \mathbb{N}$ such that $s(m) = n$.*

*Proof.* Consider the subset

$$S = \{n \in \mathbb{N} \mid n = 1 \text{ or } n = s(m), \text{ for some } m \in \mathbb{N}\}. \tag{1.1}$$

By definition, $1 \in S$. If $n \in S$, clearly $s(n) \in S$, again by definition of $S$. Thus by induction, we see that $S = \mathbb{N}$. Further injectivity of $s$ implies uniqueness as claimed.

□

## 1.1 Addition

By **??**, the following definition of addition is well-defined.

**Definition 1.1.** Let *addition* be the operation $+ : X \times X \to X$ recursively defined on $y$ by

$$x + y := \begin{cases} x & \text{if } y = 0 \\ s(x+z) & \text{if } y \in s(X) \text{ and } y = s(z) \end{cases} \tag{1.2}$$

Notice $0 + 0 = 0$ and that $x + 0 = x$, for all $x \in X$.

**Lemma 1.1.** *For all $x \in X$, $x + 1 = s(x)$.*

*Proof.* Let $x \in X$. Immediately, $x + 1 = x + s(0) = s(x + 0) = s(x)$.

□

**Lemma 1.2.** *For all $x \in X$, $0 + x = x$.*

*Proof.* We use induction on $x$. First, $0+1 = 0+s(0) = s(0+0) = s(0) = 1$. Assume that $0 + y = y$. We must show that $0 + s(y) = s(y)$. We have $0 + s(y) = s(0 + y) = s(y)$. Therefore, $0 + x = x$, for all $x \in X$.

□

**Lemma 1.3.** *For all $x, y \in X$, $s(x + y) = s(x) + y$.*

*Proof.* Let $x \in X$. We use induction on $y$. First, $s(x+0) = s(x) = s(x)+0$. Let $z \in X$ and assume that $s(x + z) = s(x) + z$. We must show that $s(x+s(z)) = s(x)+s(z)$. We have $s(x+s(z)) = s(s(x+z)) = s(s(x)+z) = s(x) + s(z)$. Therefore, $s(x + y) = s(x) + y$, for all $x, y \in X$.

□

**Lemma 1.4.** *For all $x, y \in X$, $x + y = y + x$.*

*Proof.* Let $x \in X$. We use induction on $y$. The case $y = 0$ follows from 1.2. Let $z \in X$ and assume that $x + z = z + x$. We must show that $x + s(z) = s(z) + x$. We have $x + s(z) = s(x + z) = s(z + x) = s(z) + x$, where the last equality follows by 1.3. Therefore, $x + y = y + x$, for all $x, y \in X$.

□

**Lemma 1.5.** *For all $x, y, z \in X$, $(x + y) + z = x + (y + z)$.*

*Proof.* Let $x, y \in X$. We use induction on $z$. First, $(x + y) + 0 = x + y = x+(y+0)$. Let $w \in X$ and assume $(x+y)+w = x+(y+w)$, we must show $s(w)$ has the same property. In fact, $(x + y) + s(w) = s((x + y) + w) = s(x + (y + w)) = x + s(y + w) = x + (y + s(w))$ as we needed. Therefore, $(x + y) + z = x + (y + z)$, for all $x, y, z \in X$.

□

**Lemma 1.6.** *For all $x, y, z \in X$,*

$$x + y = z + y \implies x = z. \tag{1.3}$$

*Proof.* Let $x, z \in X$. We use induction on $y$. If $y = 0$, then (1.3) holds. Let $w \in X$ and assume that (1.3) holds for $w$.
We must show that $x + s(w) = z + (w)$ implies $x = z$. Notice $x + s(w) = z + s(w)$ is equivalent to $s(x + w) = s(z + w)$. Since $s$ is injective, this implies $x + w = z + w$ as needed.

□

## 1.2 Multiplication

By **??**, the following definition of multiplication is well-defined.

**Definition 1.2.** We define *multiplication* $x \cdot y$, recursively on $y$, by

$$x \cdot 0 = 0, \qquad x \cdot s(y) = x \cdot y + x. \tag{1.4}$$

**Lemma 1.7.** *For all $x \in X$, $x \cdot 1 = x$.*

*Proof.* Let $x \in X$. Immediately, $x \cdot 1 = x \cdot s(0) = x \cdot 0 + x = 0 + x = x$.

□

**Lemma 1.8.** *For all $y \in X$, $0 \cdot y = 0$.*

*Proof.* We use induction on $y$. First, $0 \cdot 0 = 0$. Let $z \in X$ and assume $0 \cdot z = 0$. We must show that $0 \cdot s(z) = 0$. We have $0 \cdot s(z) = 0 \cdot z + 0 = 0 + 0 = 0$. Therefore, $0 \cdot y = 0$, for all $y \in X$.

□

**Lemma 1.9.** *For all $x, y \in X$, $s(x) \cdot y = x \cdot y + y$.*

*Proof.* Let $x \in X$. We use induction on $y$. First, $s(x) \cdot 0 = 0 = 0 + 0 = x \cdot 0 + 0$. Let $z \in X$ and assume $s(x) \cdot z = x \cdot z + z$. We must show that $s(x) \cdot s(z) = x \cdot s(z) + s(z)$. We have $s(x) \cdot s(z) = s(x) \cdot z + s(x) = x \cdot z + z + (x + 1) = x \cdot z + x + (z + 1) = x \cdot s(z) + s(z)$. Therefore, $s(x) \cdot y = x \cdot y + y$, for all $x, y \in X$.

□

**Lemma 1.10.** *For all $x, y \in X$, $x \cdot y = y \cdot x$.*

*Proof.* Let $x \in X$. We use induction on $y$. First, $x \cdot 0 = 0 = 0 \cdot x$. Let $z \in X$ and assume $x \cdot z = z \cdot x$. We must show that $x \cdot s(z) = s(z) \cdot x$. We have $x \cdot s(z) = x \cdot z + x = z \cdot x + x = s(z) \cdot x$. Therefore, $x \cdot y = y \cdot x$, for all $x, y \in X$.

□

**Lemma 1.11.** *For all $x, y, z \in X$, $(x + y) \cdot z = x \cdot z + y \cdot z$.*

*Proof.* Let $x, y \in X$. We use induction on $z$. Clearly, $(x+y) \cdot 0 = x \cdot 0 + y \cdot 0$. Let $w \in X$ and assume $(x + y) \cdot w = x \cdot w + y \cdot w$. We must show that $(x + y) \cdot s(w) = x \cdot s(w) + y \cdot s(w)$. We have

$$\begin{aligned}(x + y) \cdot s(w) &= (x + y) \cdot w + (x + y) = x \cdot w + y \cdot w + (x + y) \\ &= (x \cdot w + x) + (y \cdot w + y) = x \cdot s(w) + y \cdot s(w)\end{aligned}$$

which follow by the commutative and associative laws for addition. Therefore, $(x + y) \cdot z = x \cdot z + y \cdot z$, for all $x, y, z \in X$.

□

**Lemma 1.12.** *For all $x, y, z \in X$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.*

*Proof.* Let $x, y \in X$. We use induction on $z$. Clearly, $(x \cdot y) \cdot 0 = x \cdot (y \cdot 0)$. Let $w \in X$ and assume $(x \cdot y) \cdot w = x \cdot (y \cdot w)$. We must show that $(x \cdot y) \cdot s(w) = x \cdot (y \cdot s(w))$. We have

$$\begin{aligned}(x \cdot y) \cdot s(w) &= (x \cdot y) \cdot w + (x \cdot y) = x \cdot (y \cdot w) + (x \cdot y) \\ &= x \cdot (y \cdot w + y) = x \cdot (y \cdot s(w))\end{aligned}$$

which follow from the commutative law of multiplication and the distributive law. Therefore, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, for all $x, y, z \in X$.

□

**Lemma 1.13.** *For all $x, y \in X$,*

$$x > y \text{ if and only if } x = y + u \text{ for some } 0 \neq u \in X. \tag{1.5}$$

*Proof.* We use induction on $y$. The case for $y = 0$ is clear. Let $z \in X$. Assume 1.5 holds for $z$, for all $x \in X$. We will prove that

$$t > s(z) \Leftrightarrow t = s(z) + v \text{ for some } 0 \neq v \in X.$$

Assume $t > s(z)$. Then $t > s(z) > z$ and so by hypothesis, there exists $0 \neq v \in X$ such that $t = z + v$. Since $s$ is onto, let $v = s(u)$. Then $t = z + v = z + s(u) = s(z + u) = s(z) + u$. If $u = 0$, then $t = s(z)$ contrary to hypothesis.

To prove conversely, assume $t = s(z) + v$ for some nonzero element $v$. If $t = s(z)$, then $v = 0$ contrary to hypothesis. Suppose $t < s(z)$. Case: $t > z$. Then $z < t < s(z)$ which can not happen. Case: $t = z$. Then $z = s(z) + v$ and so $s(z) = z + 1 = s(z) + v + 1$. Hence $0 = v + 1 = v + s(0) = s(v + 0) = s(v)$ which implies $v = 1$ since $s$ is injective. Hence $0 = 1 + 1$, this absurdity implies that this case can not happen. Case: $t > z$. Then $s(z) + v < z$ and so $x = z + v < s(z + v) = s(z) + v < z$. By induction hypothesis $x > z$. Therefore, this case cannot happen either. All cases considered, it now follows that $t > s(z)$. Whence, 1.5 holds for all $x, y \in X$.

□

**Lemma 1.14.** *For all $w, x, y, z \in X$, if $w < x$ and $y < z$, then $w + y < x + z$.*

*Proof.* Assume $w < x$ and $y < z$. Then there exists nonzero $s$ and $t$ such that $x = w + s$ and $z = y + t$. Then $x + z = w + y + (s + t)$ and so by 1.13, $w + y < x + z$.

□

**Lemma 1.15.** *For all $x, y, z \in X$,*

$$x \cdot y = x \cdot z, x \neq 0 \implies y = z. \tag{1.6}$$

*Proof.* Assume $x \cdot y = x \cdot z$. If $y < z$ then there exists $w > 0$ such that $z = y + w$. Then $x \cdot y = x \cdot z = x \cdot (y + w) = x \cdot y + x \cdot w$. By 1.6, we have $x \cdot w = 0$. Since $x \neq 0$ and $w \neq 0$, let $x = s(u)$ and $w = s(t)$. Then $x \cdot w = x \cdot s(t) = x \cdot t + s(u) = s(x \cdot t + u) \neq 0$. Hence, we find that $y < z$ cannot happen. Similarly, the case for $y > z$ cannot happen, and thus $y = z$.

□

**Lemma 1.16.** *For all $x, y, z \in X$, if $x < y$ and $0 < z$, then $xz < yz$.*

*Proof.* Assume $x < y$ and $0 < z$. Then there exist nonzero $s$ such that $y = x + s$. Then $yz = (x + s)z = xz + sz$ If $sz = 0$, then $yz = xz$. By 1.15, we have $y = x$, contrary to hypothesis. Therefore, $sx \neq 0$ and so we have $xz < yz$.

□

## 1.3 Mathematical Induction

Now it's time to take a closer look at the principle of mathematical induction and see how it works. Then we'll explore some examples so that you can get a better understanding of this important principle.

Mathematical induction is a principle that allows us to prove a theorem by assuming that the theorem is true for a certain value of a variable and then demonstrating that the theorem holds for all larger values of the variable. This principle is incredibly important in mathematics and can be used to solve problems both big and small.

But, mathematical induction is challenging, especially for beginners. That's why I made this article and video series so you can become skilled. So let's start learning about mathematical induction.

The idea behind mathematical induction (or just **induction**) is simple: we prove that the statement holds for the first element in a well-ordered set (this is called the **base case**), and then we prove that if the statement holds for any given element in the set, it must also hold for the next element in the set (this is called the **inductive step**). By showing these two steps, the base case and the inductive step, it follows by mathematical induction that the statement holds for all elements in the set.

This process can be used to prove statements involving natural numbers, integers, rational numbers, and real numbers; and is basically used throughout mathematics.

The most basic form of mathematical induction is called **natural induction**. This type of induction can be used to prove statements involving the natural numbers

$$\mathbb{N} = \{0, 1, 2, 3, ...\}.$$

To use natural induction, we first need to prove the statement for the first natural number, which is 0. This is called the base case.

On the other hand, we also use mathematical induction to prove statements involving the positive integers

$$\mathbb{Z}^+ = \{1, 2, 3, ...\}.$$

In using this method, the base case is at 1. Now whichever of these two methods you wish to use, the next step is the same.

Next, we assume that the statement is true for some number $n$. This is called the **induction hypothesis**. Finally, we must prove that the statement is also true for the next number, $n + 1$. This is called the induction step. If we can successfully complete these two steps (base case) and inductive step), then we have written a mathematical proof based on the principle of mathematical induction. For more on mathematical induction see (Davenport 2008, 6–8).

Does this sound confusing yet? Well, we have just begun. So let's go into more detail.

What is mathematical induction and why is it useful in proofs? Mathematical induction is a method of mathematical proof that is used to establish a given statement for all natural numbers. In other words, it allows us to prove statements about infinitely many objects (such as natural numbers) by proving them for just one object, and then using that result to prove the statement for the next object, and so on. Here is the full statement of mathematical induction (Burton 2006, 2–6):

**Mathematical Induction**. If $P$ **is a subset** of the natural numbers with the following properties:

1. $0 \in P$, and
2. for all $k \in \mathbb{N}$, $k \in P$ implies $k + 1 \in P$,

then $P$ is **the set** of natural numbers.

Notice that this statement is an implication, containing two substatements, the second of which is an implication.

To use mathematical induction to prove a statement, we first need to prove two things:

1. The statement is true for the first natural number.
2. If the statement is true for some natural number $k$, then it is also true for $k + 1$.

If both of these things can be proven, then the statement is true for all natural numbers. Notice that the second statement is where the difficulty lies, mostly because it is an implication. More on this in a moment.

Here are three examples where a proof by mathematical induction can be used.

1. Proof that $1 + 2 + 3 + ... + n = n(n + 1)/2$ for all natural numbers $n$. (see **dasmith2021_2?**)
2. Proof that every natural number greater than 1 is either a prime number or can be written as a product of prime numbers. (see Rosen 2005, 108 – 110)
3. Proof that the Fibonacci sequence $F(n)$ satisfies the formula

   $$F(n + 1)F(n - 1) - F(n)^2 = (-1)^n$$

   for all natural numbers $n$. (see **asmith2022Fib?**)

We will begin proving statements using mathematical induction after mentioning a few applications, in the next lecture.

One of the most important applications of mathematical induction is in combinatorics, where it is used to prove statements about counting objects (such as the number of ways to choose $k$ objects from a set of $n$). To be clear though, mathematical induction is used throughout sciences, engineering, and humanities, i.e. (see William 2016).

1. In computer science, mathematical induction is used to design algorithms that work for all inputs of a certain size or larger.
2. In physics and engineering, mathematical induction is used to derive formulas for the sum of infinitely many terms in a series.
3. In mathematics, induction is used to prove statements about sets of numbers, such as integers or real numbers.
4. In economics, induction is used to study optimal behavior in situations where agents have incomplete information.
5. Induction is also used in philosophy, for example, to justify the belief that the future will be like the past.
6. In linguistics, mathematical induction is used to study the structure of language.
7. In biology, mathematical induction is used to study the behavior of populations over time.

This list is just a few applications, to be clear, mathematical induction is ubiquitous.

Now in order to understand mathematical induction we need to work out some examples. Lots of examples and exercises.

Mathematical induction (induction) is important because it allows us to prove statements that are true for all natural numbers. This means that we can use induction to prove statements about infinite sets, which is something difficult to do. To be clear, mathematical induction provides a rigorous method of proving mathematical statements involving infinite sets of numbers.

Mathematical induction is the following statement:

> If $P$ is a subset of the natural numbers with the properties:
>
> - $0 \in P$, and
> - for all $k \in \mathbb{N}$, $k \in P$ implies $k + 1 \in P$,
>
> then $P$ is the set of the natural numbers.

The advantage of mathematical induction is that it gives us a procedure to change the **is a subset** in the hypothesis to **is the set** in the conclusion. Before understanding the foundations of mathematical induction (later in this series), let's work through some examples and see how it works.

We will now look at some examples of how to use mathematical induction.

**Example 1.1.** Prove that for all natural numbers $n$,

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}. \tag{1.7}$$

*Solution.* Let $P$ be the set of natural numbers for which (1.7) is true. Since $0 = 0 = 0(1)/2$ we see that $0 \in P$. Assume $k \in P$. Then we find,

$$\sum_{i=0}^{k+1} i = \sum_{i=0}^{k} i + (k+1) \tag{1.8}$$

$$= \frac{k(k+1)}{2} + (k+1) \tag{1.9}$$

$$= \frac{(k+1)(k+2)}{2} \tag{1.10}$$

which shows $k + 1 \in P$. By mathematical induction $P = \mathbb{N}$ as desired. □

Notice that the **induction hypothesis** is used in moving from steps (1.8) to (1.9).

In the next example, I leave out the reference to the set $P$. Also notice that I start the base case at 1 and use the set of positive integers.

**Example 1.2.** Prove that

$$\sum_{i=1}^{n} i^2 = \frac{n(2n+1)(n+1)}{6} \tag{1.11}$$

for all positive integers $n$.

*Solution.* For $n = 1$,

$$1 = \sum_{i=1}^{1} i^2 = \frac{1(2+1)(1+1)}{6} = 1 \tag{1.12}$$

and so the base case holds. Assume that (1.11) is true for some positive integer $k$, we need to show that

$$\sum_{i=1}^{k+1} i^2 = \frac{(k+1)(2k+2)(k+2)}{6} \tag{1.13}$$

holds. We have

$$\sum_{i=1}^{k+1} i^2 = (k+1)^2 + \sum_{i=1}^{k} i^2 \tag{1.14}$$

$$= (k+1)^2 + \frac{k(2k+1)(k+1)}{6} \tag{1.15}$$

$$= \frac{(k+1)(2k+2)(k+2)}{6}. \tag{1.16}$$

Therefore, by mathematical induction (1.11) holds for all positive integers $n$. □

The next example also demonstrates how to use mathematical induction.

Notice in this example, that we define a set of numbers with the intent of showing that this subset of natural numbers is in fact the entire set of natural numbers. We do this in two steps. First, we verify the base case. For the second step, using an induction hypothesis, we verify the needed implication. The final statement is simply the conclusion that this subset of natural numbers $P$ is in fact the entire set of natural numbers.

**Example 1.3.** Prove that, for all natural numbers $n$, $2^n > n$.

*Solution.* Let $P$ be the set of all natural numbers for which $2^n > n$ is true. Since $2^0 = 1 > 0$ is true, $0 \in P$. Assume $k \in P$ and $k > 0$. Then $2^k > k$ is true and since

$$
\begin{aligned}
2^{k+1} &= 2^k \cdot 2 && (1.17)\\
&> k \cdot 2 && (1.18)\\
&= k + k && (1.19)\\
&> k + 1 && (1.20)
\end{aligned}
$$

it follows $k+1 \in P$. Thus, for all $k \in P$, $k \in P$ implies $k+1 \in P$ is true and so by mathematical induction $P = \mathbb{N}$ as desired. □

**And there we have it our first three examples. We will have several more examples to come.**

But first you should checkout the well-ordering principle.

## 1.4 The Well-Ordering Principle

The **well-ordering principle** (also called the **well-ordering axiom**) for the natural numbers is important because it provides a way to order the natural numbers. This ordering can be used to prove mathematical statements about the natural numbers. For example, the well-ordering principle can be used to show that every natural number has a unique successor. This fact can then be used to prove that there are no infinite descending sequences of natural numbers.

One answer is to simply use the order in which they are defined, so that $0 < 1 < 2 < 3 < 4$ and so on. However, we are looking for an ordering in the sense of being antisymmetric and transitive.

**Definition 1.3.** The relation $\leq$ defined on $\mathbb{N}$ by, for all $m, n \in \mathbb{N}$,

$$m \leq n \iff \exists p \in \mathbb{N} : \, m + p = n. \tag{1.21}$$

We call $\leq$ an ordering because it is **reflexive**, **antisymmetric**, and **transitive**.

Let's see why. If $m \in \mathbb{N}$, then $m + 0 = m$ and so $m \leq m$ by definition of $\leq$. In other words $p = 0$ and so $\leq$ is reflexive.

Notice the ordering is antisymmetric also. To see this suppose that $m \leq n$ and $n \leq m$. Then there exists $p_1$ and $p_2$ such that $m + p_1 = n$ and $n + p_2 = m$. From this we see that $m = n$ because

$$m + p_1 = (n + p_2) + p_1 \tag{1.22}$$

$$= n + (p_1 + p_2) \tag{1.23}$$

$$= n \tag{1.24}$$

which yields that $p_1 = p_2 = 0$.

Finally to show that $\leq$ is transitive just assume that $r \leq s$ and $s \leq t$ where $r, s, t$ are natural numbers. Then there exists $p_1$ and $p_2$ such that $r + p_1 = s$ and $s + p_2 = t$. From this we see that

$$r + (p_1 + p_2) = (r + p_1) + p_2 \tag{1.25}$$

$$= s + p_2 \tag{1.26}$$

$$= t \tag{1.27}$$

which yields that $r \leq t$.

The well-ordering principle is the simple claim that:

> every nonempty set of positive integers has a least element.

This sometimes overlooked and obvious statement will be proven to be logically equivalent to mathematical induction, in a later tutorial. To be clear, though, it can not be proven using the familiar properties satisfied by the integers under addition and multiplication.

For now, let's consider some examples.

**Example 1.4.** Find the smallest element in each subset of $\mathbb{N}$.

1. $A =$
   $n \in \mathbb{N} \mid n$ is prime
2. $B =$
   $n \in \mathbb{N} \mid\ n$ is a multiple of 7
3. $C =$
   $n \in \mathbb{N} \mid\ n = 110 - 7m$ for some $m \in \mathbb{Z}$
4. $D =$
   $n \in \mathbb{N} \mid\ n = 12s + 18t$ for some $s, t \in \mathbb{Z}$

*Solution.* The smallest prime is 2. The smallest positive multiple of 7 is 7. As $m$ takes on the values $1, 2, 3, ...$, then values of $n$ form the sequence

$$93, 76, 59, \ldots, 8, -9, ...$$

Hence the smallest element of $C$ is 8. Notice that $12s + 18t = 6(2s + 3t)$ and so elements of $D$ are multiples of 6. In fact, $6 = (12)(-1) + 18(1)$ and so 6 is in $D$. Since 6 is the smallest positive multiple of 6, we see that 6 is the least element of $D$. □

In other words, no matter how a subset of natural numbers is defined, as long as it is nonempty, the Well-Ordering Principle guarantees us, that it must have a least element.

On the one hand, the Well-Ordering Principle seems like an obvious statement, and on the other hand, the Principal of Mathematical Induction is an incredibly useful method of proof. In a later article we'll be proving this theorem here.

**Theorem 1.2.** *The following statements are equivalent.*

1. ***(Well-Ordering Axiom)*** *Every nonempty set of positive integers has a least element.*
2. ***(Mathematical Induction)*** *If $P$ is a subset of the positive integers with the following properties: 1) $0 \in P$, and 2) for all $k \in \mathbb{N}$, $k \in P$ implies $k + 1 \in P$, then $P$ is the set of positive integers.*

Notice in the proof of the following theorem, that the well-ordering principle is used.

**Theorem 1.3.** *If $a$ and $b$ are positive integers, then there exists a positive integer $n$ such that $na \geq b$.*

*Proof.* Assume for a contradiction that $a$ and $b$ do not satisfy the statement; that is, assume there exists positive integers $a$ and $b$ such that $na < b$ for every positive integer $n$. Consider the set,

$$S = \{b - na \,|\, n \text{ is a positive integer}\}$$

which consists only of positive integers. By the well-ordering principle, $S$ possess a least element, say $b - ma$ for some positive integer $m$. However, $b - (m + 1)a$ is in $S$ and $b - (m + 1)a$ is less than $b - ma$ by

$$b - (m + 1)a = (b - ma) - a < b - ma.$$

Therefore, for positive integers $a$ and $b$ there must exist a positive integer $n$ such that $na \geq b$. □

□

**Remark**. Can the reader prove that the Archimedean Property implies the Well-Ordering Principle?

Later, we will use the Well-Ordering Principle to prove the Division Algorithm and the Fundamental Theorem of Arithmetic. Before, we get to these theorems though, let's practice using mathematical induction.

When proving a statement by mathematical induction, you should look for a pattern in the statement that can be used to create a base case and an inductive case. The base case is the simplest version of the statement, and the inductive case is a more complicated version of the statement that builds on the base case. You can then use mathematical induction to justify that the statement holds true for all cases.

In our first example, we are proving that

$$\sum_{i=1}^{n}(2i-1)=n^2$$

for all positive integers $n$. For example, notice that

$$\sum_{i=1}^{1}(2i-1)=1=1^2$$

so the base case holds for $n=1$ (i.e. the first positive integer). However, to demonstrate that sometimes a change in the index is desired, we show how to accomplish this.

**Example 1.5.** Prove that for all natural numbers $n$,

$$\sum_{i=0}^{n}(2i+1)=(n+1)^2. \tag{1.28}$$

*Solution.* Let $P$ be the set of natural numbers for which (Equation 1.28) is true, that is

$$P=\left\{n\in\mathbb{N}\mid\sum_{i=0}^{n}(2i+1)=(n+1)^2\right\}.$$

The basis step is easily verified by

$$\sum_{i=0}^{0}(2i+1)=1=1^2$$

and so we see $0 \in P$. For an induction hypothesis, assume $k \in P$. Then

$$\sum_{i=0}^{k}(2i+1) = (k+1)^2$$

is true and thus,

$$\begin{aligned}
\sum_{i=0}^{k+1}(2i+1) &= \sum_{i=0}^{k}(2i+1) + (2(k+1)+1) && (1.29)\\
&= (k+1)^2 + 2k + 3 && (1.30)\\
&= (k+2)^2 && (1.31)
\end{aligned}$$

which shows $k+1 \in P$. By mathematical induction, $P = \mathbb{N}$ as desired. □

In our next example, we work with an alternating sum.

**Example 1.6.** Prove that for all positive integers $n$,

$$\sum_{i=1}^{n}(-1)^i\, i = \frac{(-1)^n(2n+1)-1}{4} \tag{1.32}$$

*Solution.* Let $P$ be the set of positive integers for which (Equation 1.32) is true. The basis step is easily verified by

$$\sum_{i=1}^{1}(-1)^i\, i = -1 = \frac{(-1)^1(2(1)+1)-1}{4}$$

and so we see $1 \in P$. For an induction hypothesis, assume $k \in P$. Then

$$\sum_{i=1}^{k}(-1)^i\, i = \frac{(-1)^k(2k+1)-1}{4}$$

is true and thus,

$$\begin{aligned}
\sum_{i=1}^{k+1}(-1)^i\, i &= \sum_{i=1}^{k}(-1)^i\, i + (-1)^{k+1}(k+1) && (1.33)\\
&= \frac{(-1)^k(2k+1)-1}{4} + (-1)^{k+1}(k+1) && (1.34)\\
&= \frac{(-1)^{k+1}(2(k+1)+1)-1}{4} && (1.35)
\end{aligned}$$

which shows $k+1 \in P$. By mathematical induction $P = \mathbb{Z}^+$ as desired. □

In this next example, we work with an inequality, showing that exponential growth is greater than linear growth.

**Example 1.7.** Prove that for all positive integers $n$, $3^n > 3n - 1$.

*Solution.* If $n = 1$, then $3^1 = 3 > 2 = 3(1) - 1$ so the base case holds. Let $k$ be a positive integer and assume that $3^k > 3k - 1$. Then

$$3^{k+1} = 3^k \cdot 3 > (3k-1) \cdot 3 \geq 3k + 2 = 3(k+1) - 1.$$

So the result follows by mathematical induction. □

Now let's generalize the previous example.

**Example 1.8.** Let $x$ be any real number greater than $-1$. Use mathematical induction to prove that

$$(1+x)^n \geq 1 + nx \tag{1.36}$$

for all positive integers $n$.

*Solution.* If $n = 1$, then $(1+x)^1 \geq 1 + (1)x$ and so the base case holds. Let $k$ be a positive integer and assume that $(1+x)^k \geq 1 + kx$. Then

$$\begin{align}
(1+x)^{k+1} &= (1+x)^k(1+x) \tag{1.37}\\
&\geq (1+kx)(1+x) \tag{1.38}\\
&= 1 + x + kx + kx^2 \tag{1.39}\\
&= 1 + (k+1)x + kx^2 \tag{1.40}\\
&\geq 1 + (k+1)x \tag{1.41}
\end{align}$$

because $x^2 \geq 0$ and $k \geq 0$. So the result follows by mathematical induction. □

In our fifth example, we have a sum of the reciprocals of squares involved with an inequality. These types of inequalities can be very useful in other subjects such as analysis.

**Example 1.9.** Prove that for all integers $n \geq 1$,

$$\sum_{i=1}^{n} \frac{1}{i^2} \leq 2 - \frac{1}{n}. \tag{1.42}$$

*Solution.* If $n = 1$, then $\sum_{i=1}^{1} \frac{1}{1^2} = 1 \leq 2 - \frac{1}{1}$ and so the base case holds. Let $k$ be a positive integer and assume that $\sum_{i=1}^{k} \frac{1}{i^2} \leq 2 - \frac{1}{k}$. Then

$$\begin{aligned} \sum_{i=1}^{k+1} \frac{1}{i^2} &= \sum_{i=1}^{k} \frac{1}{i^2} + \frac{1}{(k+1)^2} && (1.43) \\ &\leq 2 - \frac{1}{k} + \frac{1}{(k+1)^2} && (1.44) \\ &\leq 2 - \frac{1}{k+1} && (1.45) \end{aligned}$$

So the result follows by mathematical induction. □

Now that we've seen some examples, let's go for a deeper understanding of mathematical induction.

Now we will demonstrate the usefulness of mathematical induction by providing rigorous proofs for the summation formulas for finite sums of arithmetic and geometric progressions.

Arithmetic progressions are found all around us in nature and in everyday life. The temperature on a day might rise steadily from morning until evening, for instance. Or the population of a town might grow gradually over time. The study of arithmetic progressions has many practical applications. Businesses use them to forecast future sales, for example. And mathematicians use them to solve problems in physics and other areas of mathematics.

**Definition 1.4.** A sequence of the form $a, a + d, a + 2d, \ldots, a + nd, \ldots$ where $a, d \in \mathbb{R}$ is called an **arithmetic progression.**

For example, if $a = 0$ and $d = 1$, then the sequence is $0, 1, 2, 3, 4, \ldots$, in other words the natural numbers. Or let's say, $a = 1/2$ and $d = -2$, then the sequence is $1/2, -3/2, -7/2, -11/2, -15/2$, and so on.

In the following example, we prove a wonderful formula for the sum of the terms in arithmetic progression.

**Example 1.10.** Let $a, d \in \mathbb{R}$. Prove that for every positive integer $n$, that

$$a + (a + d) + \cdots + (a + nd) = \frac{(n+1)(2a + nd)}{2}. \qquad (1.46)$$

*Solution.* Let $P$ be the set of positive integers for which (1.46) holds. Since

$$a + (a + d) = [(1 + 1)(2a + d)]/2,$$

we see that $1 \in P$. Assume $k \in P$. We find

$$\begin{aligned} a + (a + d) + \cdots + (a + kd) + (a + (k + 1)d) && (1.47)\\ = \frac{(k + 1)(2a + kd)}{2} + (a + (k + 1)d) && (1.48)\\ = \frac{(k + 1)(2a + kd) + 2(a + (k + 1)d)}{2} && (1.49)\\ = \frac{(k + 2)(2a + (k + 1)d)}{2} && (1.50) \end{aligned}$$

Therefore, $k + 1 \in P$ and thus (1.46) holds for $n \geq 1$, by mathematical induction. □

A geometric progression is a sequence of numbers in which each term after the first is found by multiplying the previous term by a fixed number, called the **common ratio**. In other words, each number in the sequence is determined by multiplying the previous number by a (fixed) certain amount. Let's now explore geometric progressions.

**Definition 1.5.** Recall a sequence of the form $a, ar, ar^2, \ldots, ar^n, \ldots$ where $a, r \in \mathbb{R}$ and $r \geq 1$ is called a **geometric progression.**

For example, if $a = 1$ and $r = 2$, the sequence is $1, 2, 4, 8, 16, 32, \ldots$. Or let's say, $a = 1/2$ and $r = -2$, then the sequence is $1/2, -1, 2, -4, 8, \cdots$ and so on.

**Example 1.11.** Let $a, r \in \mathbb{R}$ and suppose $r \geq 1$. Prove that, for each positive integer $n$, that

$$a + ar + \cdots + ar^n = a\left(\frac{r^{n+1} - 1}{r - 1}\right). \qquad (1.51)$$

*Solution.* Let $P$ be the set of positive integers for which (1.51) holds. Since $a + ar = a(r^2 - 1)/(r - 1)$, we see that $1 \in P$. Assume $k \in P$. We find

$$\begin{aligned}
&a + ar + ar^2 + \cdots + ar^k + ar^{k+1} \\
&\quad = a\left(\frac{r^{k+1}-1}{r-1}\right) + ar^{k+1} \\
&\quad = \frac{ar^{k+1} - a + (r-1)ar^{k+1}}{r-1} \\
&\quad = a\left(\frac{r^{k+2}-1}{r-1}\right).
\end{aligned}$$

Therefore, $k+1 \in P$ and thus (1.51) holds for $n \geq 1$, by mathematical induction. □

The **mathematical induction principle** is analogous to an infinite string of equally spaced dominos set up in a single line arranged so that if one falls down then so does the next one. Imagine you knock down the first domino, and then after some time has passed you check back and the dominos are still falling. Would you believe that this will continue indefinitely?

The method of proof of using the principle of mathematical induction is frequently useful in the theory of numbers. Familiarity with this type of argument is essential to subsequent work.

In any proof by induction, we must not forget to show that 0 is in $P$. Even if we show that the truth of $k$ in $P$ implies that $k+1$ is in $P$, if 0 is not in $P$, then we cannot conclude that $P$ is the set of natural numbers. For example, let $P$ be the set of all natural numbers that satisfy:

$$n + (n+1) = 2n. \tag{1.52}$$

Suppose $k$ satisfies, (Equation 1.52). Using this we have

$$\begin{aligned}
(k+1) + (k+2) &= k + (k+1) + 2 \\
&= 2k + 2 \\
&= 2(k+1)
\end{aligned}$$

and thus $k+1$ also satisfies (Equation 1.52). So, if 1 satisfies (Equation 1.52) then, it would follow that (Equation 1.52) is true for all natural numbers $n$. However, 0 does not satisfy (Equation 1.52). In fact, obviously, (Equation 1.52) is false for all natural numbers $n$. We conclude that the basis step is a **necessary** part of any proof by mathematical induction.

The assumption that the statement is true for some number $n = k$ will often be referred to as the induction hypothesis. Sometimes the role that 1 plays in the principle of mathematical induction will be replaced by some other integer, say $a$, in such instances mathematical induction establishes the statement for all integers $n \geq a$.

The method of mathematical induction has its limitations in that it consists of testing a known (or conjectured) formula. All that the induction process enables us to do is to show that any special case can be proved on the assumption that all the preceding cases have been verified.

## 1.5 The Mathematical Induction Equivalence

In the hypothesis of mathematical induction, the statement $0 \in P$ is called the **base case**. Mathematical induction can be thought of as a collection of principles, for example, the base case may start at 0, or 1, or 2, etc. instead of 0. In each of these scenarios, the goal is to prove a collection of statements is true, for all $n$ greater than some initial value which must be verified (base case).

Now that we have established that a base case is required when using mathematical induction. It is now natural to ask: does the base case need to start at the first natural number 0. We have seen previous examples where that base case starts at 1 when proving a statement holds for all positive integers. So let's make this formal.

Let $a$ be a natural number. Consider the set defined by

$$\mathbb{N}_a = \{k \in \mathbb{N} : k \geq a\}.$$

In other words,

$$\mathbb{N}_a = \{a, a+1, a+2, a+3, ...\}.$$

Using this set notation we can formalize variations of mathematical induction as follows.

**Mathematical Induction** is the following statement:

> Let $a$ be a natural number. If $P$ is **a subset** of $\mathbb{N}_a$ with the properties:
>
> 1. $a \in P$, and
> 2. for all $k \in \mathbb{N}_a$, $k \in P$ implies $k+1 \in P$,
>
> then $P$ is **the set** $\mathbb{N}_a$.

Notice that whenever $a = 0$, we have the Principle of Mathematical Induction as stated previously.

For example, while $n! > n$ is not true for \$n=0, 1, 2 \$, it is true for all $n \geq 3$. So our base case is $n = 3$. Let's prove that $n! > n$ for all $n \geq 3$. Since $3! = 1 \cdot 2 \cdot 3 = 6 > 3$ we see that the base case holds. Now assume that for some positive integer $k$ greater than 3, that $k! > k$. Then we see that

$$\begin{aligned}(k+1)! &= k!(k+1)\\ &> k(k+1)\\ &> k+1\end{aligned}$$

Therefore, by mathematical induction, $n! > n$ for all $n \geq 3$.

**Example 1.12.** Prove that $2^{n-1} > n$ for all positive integers $n \geq 3$.

*Solution.* Since $4 = 2^{3-1} = 2^2 = 4 > 3$ the statement is true for $n = 3$. Assume that the result is true for a positive integer $n$, we need to show that $2^{(n+1)-1} > n+1$ holds. Starting from $2^{n-1} > n$ we multiply by 2 to obtain $2^n > 2n$. But $2n = n + n > n + 1$ since $n \geq 3$. Therefore by mathematical induction, $2^{(n+1)-1} > 2n > n+1$ for all positive integers $n \geq 3$ as desired. □

Now let's turn our attention to another variation of mathematical induction called **strong induction**.

The principle of strong (mathematical) induction is also a method of proof and is frequently useful in the theory of numbers. This principle can also be used to prove statements about arays, sequences, and many other structures. Familiarity with this type of argument is essential to subsequent work.

> Strong induction was invented by the mathematician, logician, and philosopher Bertrand Russell.

**Theorem 1.4.** *A set of positive integers that contains the integer 1, and that has the property: for every positive integer $n$, if the set contains $1, 2, \ldots, n$, then it also contains the integer $n+1$; must be the set of all positive integers.*

*Proof.* Let $P$ be the set with the stated properties and let $S$ be the set consisting of all positive integers not in $P$. Assuming that $S$ is nonempty, we can choose $n$ to be the least integer in $S$ by the Well-Ordering Principle.

Since 1 is in $P$ and $n$ is not in $P$, we know that $n > 1$. Further, notice that none of the integers $1, 2, 3, \ldots, n-1$ lies in $S$, so that in fact, they are in $P$. Then by the second property, $n = (n-1) + 1$ is in $P$, which contradicts $n$ is not in $P$. Thus, $S$ is empty and $P$ must be the set of all positive integers. □

□

While the hypothesis is *stronger*, both statements are actually logically equivalent to each other, as the next theorem states.

**Theorem 1.5** (Induction Principles). *The following statements are logically equivalent.*

1. ***(Mathematical Induction)*** *If $P$ is a subset of the natural numbers with the following properties: a) $0 \in P$, and b) for all $k \in \mathbb{N}$, $k \in P$ implies $k+1 \in P$, then $P$ is the set of natural numbers.*
2. ***(Strong Induction)*** *If $P$ is a subset of the natural numbers with the following properties: a) $0 \in P$, and b) for all $k \in \mathbb{N}$, $0, 1, \ldots, k \in P$ implies $k+1 \in P$, then $P$ is the set of natural numbers.*

Which one you choose is often a matter of convenience. Some statements are much easier to work with using one or the other. Can you tell which version is used in the next example?

**Example 1.13.** Let $a$ be a real number. Prove that for all $n \geq 1$,

$$a^n - 1 = (a-1)\left(a^{n-1} + a^{n-2} + a^{n-3} + \ldots + a + 1\right).$$

*Solution.* For $n = 1$, $a - 1 = a - 1$ is obvious. Suppose that the equation is true for $k$ namely,

$$\left(a^k - 1\right) = (a-1)\left(a^{k-1} + a^{k-2} + a^{k-3} + \cdots + a + 1\right).$$

Then for $k+1$ we have

$$\begin{aligned}\left(a^{k+1} - 1\right) &= \left(a^{k+1} - a^k + a^k - 1\right) \\ &= a^k(a-1) + (a-1)\left(a^{k-1} + a^{k-2} + a^{k-3} + \cdots + a + 1\right)\end{aligned}$$

and so

$$\left(a^{k+1} - 1\right) = (a-1)\left(a^k + a^{k-1} + a^{k-2} + a^{k-3} + \cdots + a + 1\right).$$

as desired. □

We can also rely on the strong principle of induction, by considering the formula:

$$a^{n+1} - 1 = (a+1)\left(a^n - 1\right) - a\left(a^{n-1} - 1\right)$$

if desired.

Now in order to understand the difference between strong induction and mathematical induction, we will consider the Lucas numbers. The following example illustrates when strong induction might be the preferred method.

To illustrate the strong form of induction we will discuss the Lucas numbers. Numbers in the sequence $1, 3, 4, 7, 11, 18, ...$ are called **Lucas numbers**. They are defined inductively by, $L_1 = 1$, $L_2 = 3$, and

$$L_n = L_{n-1} + L_{n-2} \quad \text{for all } n \geq 3.$$

The Lucas numbers have a number of interesting mathematical properties, and they can be used to generate a variety of different patterns and sequences. They also show up in a surprising number of real-world applications, from financial markets to computer algorithms.

**Example 1.14.** Prove that for all positive integers $n$,

$$L_n < \left(\frac{7}{4}\right)^n. \tag{1.53}$$

*Solution.* For the basis step notice that

$$L_1 = 1 < \left(\frac{7}{4}\right)^1 = \frac{7}{4}.$$

Now assume (**strong induction hypothesis**) that (Equation 1.53) holds true for $n = 1, ..., k-1$. Then we find,

$$\begin{aligned} L_k = L_{k-1} + L_{k-2} &< \left(\frac{7}{4}\right)^{k-1} + \left(\frac{7}{4}\right)^{k-2} \\ &= \left(\frac{7}{4}\right)^{k-2}\left(\frac{7}{4}+1\right) \\ &= \left(\frac{7}{4}\right)^{k-2}\left(\frac{11}{4}\right) \\ &< \left(\frac{7}{4}\right)^{k-2}\left(\frac{7}{4}\right)^{2} \\ &= \left(\frac{7}{4}\right)^{k}. \end{aligned}$$

Because the inequality is true for $n = k$ whenever it is true for the integers $1, 2, \ldots, k-1$, we conclude, by Strong Induction, that $L_n < (7/4)^n$ for all $n \geq 1$. □

When first studying mathematical induction a student often runs into solving the postage stamp problem.

**Example 1.15.** Show that any amount of postage more than 1-cent can be formed just using 2-cent and 3-cent stamps.

*Solution.* Notice that 2-cent and 3-cent stamps can be formed using 2-cent and 3-cent stamps, so the base case is obvious. Let $k$ be a positive integer with $k \geq 1$. For an induction hypothesis (strong), assume that any amount of postage up to $k$-cents can be formed using 2-cent and 3-cent stamps. Then using $k+1 = k-1+2$, and the fact that 2 is a 2-cent stamp and $k-1$ can be formed using 2-cent and 3-cent stamps, we see that $k+1$ can be formed using 2-cent and 3-cent stamps. Hence by strong induction, any amount can be formed using 2-cent and 3-cent stamps. □

For our next example, let's use a new function. Define a function recursively, for all positive integers $n$ by $f(1) = 1$, $f(2) = 5$ and

$$f(n+1) = f(n) + 2f(n-1).$$

For example, $f(1) = 1$, $f(2) = 5$, $f(3) = 7$, $f(4) = 17$, and so on. We can (exhaustively) search for patterns until we find this gem:

**Example 1.16.** Prove that $f(n) = 2^n + (-1)^n$ for all positive integers $n$.

*Solution.* For $n = 1$ and $n = 2$, we have $f(1) = 1 = 2^1 + (-1)^1$ and $f(2) = 5 = 2^2 + (-1)^2$, so the base case holds. Let $k$ be a positive integer with $k \geq 1$. Assume $f(n) = 2^n + (-1)^n$ holds for $n = 0, \ldots., k$. Then

$$\begin{aligned} f(k+1) &= f(k) + 2f(k-1) && (1.54) \\ &= 2^k + (-1)^k + 2(2^{k-1} + (-1)^{k-1}) && (1.55) \\ &= 2^k + 2^k + (-1)^k + 2((-1)^{k-1}) && (1.56) \\ &= 2^{k+1} + (-1)^{k+1} && (1.57) \end{aligned}$$

Therefore, the result follows by strong induction. □

If you haven't seen these examples on mathematical induction you should work through them before moving on to the Mathematical Induction Equivalence.

In this video, you'll learn the **Mathematical Induction Equivalence**, the equivalence of the well-ordering principle, mathematical induction, and strong induction. You'll see that if the well-ordering principle holds then induction must also hold. Then we'll prove that if induction holds, then strong induction must also hold. Finally, then we prove that if strong induction holds, then the well-ordering principle must also hold. Proving these three statements is the same as proving all three of them are logically equivalent. Effectively, what this means is that if you assume one of them is true, then all three of them must be true.

The Mathematical Induction Equivalence is the statement that all three of these statements:

1. The Well-Ordering Principle
2. The Principle of Mathematical Induction
3. The Strong Form of Induction

are all equivalent to each other.

Now in order to prove the Mathematical Induction Equivalence, let's review what these three statements are.

**Theorem 1.6** (Well-Ordering Principle)**.** *Every nonempty set of natural numbers has a least element.*

**Theorem 1.7** (Mathematical Induction)**.** *If $P$ is a subset of the natural numbers with the following properties: 1) $0 \in P$, and 2) for all $k \in \mathbb{N}$, $k \in P$ implies $k + 1 \in P$, then $P$ is the set of natural numbers.*

**Theorem 1.8** (Strong Induction). *If $P$ is a subset of the natural numbers with the following properties: 1) $0 \in P$, and 2) for all $k \in \mathbb{N}$, $0, 1, ..., k \in P$ implies $k + 1 \in P$, then $P$ is the set of natural numbers.*

Let's use WOP, PMI, and SFI for the abbreviations for these three statements, respectively.

Our goal is to prove the equivalence of these three statements.

Mathematical induction is a technique used to prove that a certain property holds for all natural numbers. The well-ordering principle states that every non-empty set of natural numbers contains a smallest element. We will now prove that the well-ordering principle implies mathematical induction.

**Theorem 1.9.** *$WOP \Rightarrow PMI$*

*Proof.* Let $P$ be a subset of natural numbers with $0 \in P$ and the property, for all natural numbers $k$, $k \in P$ implies $k + 1 \in P$. Assume, for a contradiction, there exists a nonempty set $S$ containing the natural numbers not in $P$. By the Well-Ordering Principle, $S$ has a least natural number, $s$. Since $0 \in P$, $s \neq 0$. Thus there exists a natural number $t$ such that $t + 1 = s$. Notice $t\mathbb{N}ot \in S$ since $t < s$. Thus $t \in P$ and so $s = t + 1 \in P$. This contradiction shows $S$ cannot exist, meaning $P = \mathbb{N}$ as desired. □

□

As a fun exercise for the reader, you should try proving that $PMI \Rightarrow WOP$. After trying that, read on.

In case you've heard of terms like weak induction or strong induction, we will now see they are actually equivalent. The advantage of having different mathematical induction variations though is to have flexibility when writing proofs.

**Theorem 1.10.** *$PMI \Rightarrow SFI$*

*Proof.* Let $S$ be a set of natural numbers with $0 \in S$ and the property, for all natural numbers $k$, $0, 1, 2..., k \in S$ implies $k + 1 \in S$. Let $P$ be the set of natural numbers for which $0, 2, ..., n \in S$ is true. Notice $0 \in P$ since $0 \in S$. Assume $k \in P$. Then $0, 1, 2, ..., k \in S$. Thus $0, 1, 2, 3, ..., k, k+1 \in S$ meaning $k + 1 \in P$. By I, $P = \mathbb{N}$. By definition of $P$, $S = \mathbb{N}$ as desired. □

□

Notice that only $PMI \Rightarrow SFI$ was proven above. The converse statement, namely $SFI \Rightarrow PMI$ is left for the reader.

One of the most important statements in number theory is the well-ordering principle. This principle states that every non-empty set of natural numbers contains a smallest element. In other words, there is no infinite sequence of natural numbers in which each number is smaller than the one before it. The well-ordering principle is often used to prove results by contradiction. This makes it a very powerful tool for mathematical reasoning. Now it's time to show that strong induction implies the well-ordering principle.

**Theorem 1.11.** *$SFI \Rightarrow WOP$*

*Proof.* Assume, for a contradiction, there exists a nonempty set of natural numbers $S$ with no least element. Let $P$ be the set of natural numbers for which $n\mathbb{N}otinS$ is true. Because 0 is the least element of all natural numbers, $0\mathbb{N}otinS$ and so $0 \in P$. Assume $0, 1, ..., k \in P$. If $k+1 \in S$ then $k+1$ is the least element of $S$. However, $S$ has no least element and thus $k+1\mathbb{N}otinS$. Thus, $k+1 \in P$ and so by Strong Induction, $P = \mathbb{N}$. This contradiction shows $S$ can not exist. Therefore, $S = \mathbb{N}$. □

□

Notice that only $SFI \Rightarrow WOP$ was proven above. The converse statement, namely $WOP \Rightarrow SFI$ is left for the reader.

Okay, so we have proven that $WOP \Rightarrow PMI \Rightarrow SFI \Rightarrow WOP$. This means, logically speaking that, $WOP \Leftrightarrow PMI \Leftrightarrow SFI$, and so all three theorems above are proven.

As discussed above, there are several variations of mathematical induction. Now we would like to show that these are equivalent also. Recall we use the notation

$$N_a = \{k \in \mathbb{N} : k \geq a\}$$

where $a$ is a natural number.

**Theorem 1.12** (Mathematical Induction Equivalence**)). *Let $a$ be a fixed natural number. The following statements are logically equivalent.*

1. *Every nonempty set of $\mathbb{N}_a$ has a least element.*
2. *If $a \in P \subseteq \mathbb{N}_a$ and for all $k \in \mathbb{N}_a$, $k \in P$ implies $k+1 \in P$, then $P = \mathbb{N}_a$.*
3. *If $a \in P \subseteq \mathbb{N}_a$ and for all $k \in \mathbb{N}_a$, $a, a+1, \ldots, a+k \in P$ implies $a+k+1 \in P$, then $P = \mathbb{N}_a$.*

*Proof.* (1) $\Rightarrow$ (2): Let $P \subseteq \mathbb{N}_a$ with $a \in P$ and the property, for all natural numbers $k$, $k \in P$ implies $k+1 \in P$. Assume, for a contradiction, there exists a nonempty subset $S$ of $\mathbb{N}_a$ containing the natural numbers not in $P$. By the Well-Ordering Principle, $S$ has a least natural number, $s$. Since $a \in P$, $s \neq a$. Further, since $s \in S \subseteq \mathbb{N}_a$ we know that $s > a$. Thus there exists a natural number $t$ such that $t+1 = a$. Notice $t\mathbb{N}ot \in S$ since $t < s$. Thus $t \in P$ and so $s = t+1 \in P$. This contradiction shows $S$ cannot exist, meaning $P = \mathbb{N}_a$ as desired.

(2) $\Rightarrow$ (3): Let $S$ be a set of natural numbers with $a \in S$ and the property, for all natural numbers $k$, $a, a+1, \dots, a+k \in S$ implies $a+k+1 \in S$. Let $P$ be the set of natural numbers for which $a, a+1, \dots, a+n \in S$ is true. Notice $a \in P$ since $a \in S$. Assume $k \in P$. Then $a, a+1, \dots, a+k \in S$. Thus $a, a+1, \dots, a+k, a+k+1 \in S$ meaning $a+k+1 \in P$. Hence, $P = \mathbb{N}_a$. By definition of $P$, $S = \mathbb{N}_a$ as desired.

(3) $\Rightarrow$ (1): Assume, for a contradiction, there exists a nonempty subset $S$ of $\mathbb{N}_a$ with no least element. Let $P$ be the set of natural numbers for which $n\mathbb{N}otinS$ is true. Because $a$ is the least element of all elements in $\mathbb{N}_a$, $a\mathbb{N}otinS$ and so $a \in P$. Assume $a, a+1, \dots, a+k \in P$. If $a+k+1 \in S$ then $a+k+1$ is the least element of $S$. However, $S$ has no least element and thus $a+k+1\mathbb{N}otinS$. Thus, $a+k+1 \in P$ and so $P = \mathbb{N}_a$. This contradiction shows $S$ can not exist. □

□

There are many other forms of mathematical induction. We are only limited by our imagination. But for now, let's work through more exercises on mathematical induction.

Mathematical induction is one of the most powerful techniques in mathematics. It allows us to prove a statement for a certain set of numbers, and then use that proof to show that the statement is true for all natural numbers. In this section, we will give some exercises on mathematical induction to help you understand the technique better. We will also provide solutions to these exercises so that you can check your work. Let's get started!

**Example 1.17.** Prove that

$$\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

for all positive integers $n$.

*Solution.* For $n = 1$,

$$1 = \sum_{k=1}^{1} k^3 = \left(\frac{1(1+1)}{2}\right)^2 = 1.$$

Assume that the result is true for a positive integer $n$, we need to show that

$$\sum_{k=1}^{n+1} k^3 = \left(\frac{(n+1)(n+2)}{2}\right)^2$$

holds. We have

$$\begin{aligned}\sum_{k=1}^{n+1} k^3 &= (n+1)^3 + \sum_{k=1}^{n} k^3 \\ &= (n+1)^3 + \left(\frac{n(n+1)}{2}\right)^2 \\ &= \left(\frac{(n+1)(n+2)}{2}\right)^2.\end{aligned}$$

Therefore by mathematical induction

$$\sum_{k=1}^{n+1} k^3 = \left(\frac{(n+1)(n+2)}{2}\right)^2$$

holds true for all positive integers $n$. □

**Example 1.18.** Prove that $2 \cdot 6 \cdot 10 \cdot 14 \cdots (4n-2) = \frac{(2n)!}{n!}$ for all positive integers $n$.

*Solution.* For $n = 1$ we have $2 = \frac{2!}{1!} = \frac{2}{1}$ so the base case holds. Assume that

$$2 \cdot 6 \cdot 10 \cdot 14 \cdots (4k-2) = \frac{(2k)!}{k!}$$

for some positive integer $k$. Then

$$
\begin{aligned}
&2 \cdot 6 \cdot 10 \cdot 14 \cdots (4k-2) \cdot (4k+2) \\
&\quad = \frac{(2k)!}{k!} \cdot (4k+2) \\
&\quad = \frac{(2k)!(2)(2k+1)(k+1)}{(k+1)!} \\
&\quad = \frac{1 \cdot 2 \cdots (2k)(2k+1)(2k+2)}{(k+1)!} \\
&\quad = \frac{(2k+2)!}{(k+1)!}
\end{aligned}
$$

$$

as desired. The result follows by mathematical induction. □

## 1.6 The Fibonacci Sequence

Fibonacci numbers have been found to occur in many areas of mathematics, as well as in nature. For example, the proportions of many spiral shells can be expressed as Fibonacci numbers.

> Fibonacci numbers were highlighted by the Italian mathematician Leonardo of Pisa (Fibonacci), who was investigating the growth of rabbit populations. He realized that the Fibonacci sequence could be used to model the way in which rabbits reproduce.

Fibonacci numbers also appear in the DNA molecule and in the arrangement of leaves on a stem. It seems that Fibonacci numbers are ubiquitous in both mathematics and nature!

The **Fibonacci numbers** start with 0 and 1, and then the next Fibonacci number is 1 $(0+1)$, and the next Fibonacci number is 2 $(1+1)$, and so on. As a result, the **Fibonacci sequence** is 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987,...

Fibonacci numbers play an important role in mathematics and have a wide range of applications. They are also closely related to the golden ratio, which is often found in nature. Fibonacci numbers can be generated by starting with 0 and 1, and then adding the two previous numbers to get the next number in the sequence. This relationship is known as the **Fibonacci recurrence**.

The Fibonacci numbers are also related to each other by a plethora of (**Fibonacci identities**) identities. These identities can be proved using mathematical induction. How? First, the base case must be proven true for $n = 0$. Then, the inductive step, it must be shown that if the Fibonacci identities are true for $n = k$, then they are also true for $n = k + 1$. By following this process, it can be shown that a Fibonacci identity holds. As a result, these identities provide a powerful tool for understanding and manipulating Fibonacci numbers.

After having studied mathematical induction the Fibonacci numbers are a good topic to test ones abilities to perform induction. There are two obvious reasons for this. Firstly, many of the results (exercises) for are relatively straight-forward. Secondly, many of the results obtain are quite surprising. For instance, the sum of the squares of the first $n$ Fibonacci numbers is the same as the product of the $n$-th and the $n + 1$-th. This fact is easily provable by mathematical induction. We now study the Fibonacci Numbers and the Euler-Binet Formula.

Fibonacci numbers are defined as a *recursive sequence* by starting with 0 and 1, and then adding the previous two integers together. It has long been noticed that the Fibonacci numbers arise in many places throughout the natural world. Fibonacci numbers have many special mathematical properties.

**Definition 1.6. Fibonacci numbers** are the positive integers defined by $f_0 = 0$, $f_1 = 1$, and

$$f_n = f_{n-1} + f_{n-2}$$

for $n \geq 2$.

The first 21 Fibonacci numbers are

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 5 | 8 | 13 |
| 21 | 34 | 55 | 89 | 144 | 233 | 377 |
| 610 | 987 | 1597 | 2584 | 4181 | 6765 | 10946 |

Here we prove several identities involving Fibonacci numbers. The idea is to provide several interesting examples on how mathematical induction can be applied to give rigorous arguments on (perhaps) experimentally found identities.

**Example 1.19.** Prove that for all positive integers $n$,

$$\sum_{i=0}^{n} f_i^2 = f_n f_{n+1}. \tag{1.58}$$

*Solution.* Let $P$ be the set of positive integers for which (Equation 1.58) is true. Since $f_0^2 = 0 = f_0 f_1$ we see $0 \in P$. Assume $k \in P$. It follows $k+1 \in P$ by

$$\sum_{i=0}^{k+1} f_i^2 = \sum_{i=0}^{k} f_i^2 + f_{k+1}^2 \tag{1.59}$$

$$= f_k f_{k+1} + f_{k+1}^2 \tag{1.60}$$

$$= f_{k+1}(f_k + f_{k+1}) \tag{1.61}$$

$$= f_{k+1} f_{k+2}. \tag{1.62}$$

By mathematical induction $P = \mathbb{N}$ as desired. □

**Example 1.20.** Prove that for all positive integers $n$,

$$\sum_{j=1}^{n} f_{2j} = f_{2n+1} - 1. \tag{1.63}$$

*Solution.* For $n = 1$, $f_2 = 1 = f_3 - 1$ so the base case holds. Assume, for some positive integer $k$, that (Equation 1.63) holds. Then we find

$$\sum_{j=1}^{k+1} f_{2j} = \sum_{j=1}^{k} f_{2j} + f_{2k+2} \tag{1.64}$$

$$= f_{2k+1} - 1 + f_{2k+2} \tag{1.65}$$

$$= f_{2k+3} - 1. \tag{1.66}$$

By mathematical induction, (Equation 1.63) holds for all positive integers $n$. □

**Example 1.21.** Prove that for all positive integers $n$,

$$\sum_{i=1}^{n} f_{2i-1} = f_{2n}. \tag{1.67}$$

*Solution.* Since $f_1 = 1 = f_2$ we see the base case holds. Assume, for some positive integer $k$, that (Equation 1.67) holds. Then we find

$$\sum_{i=1}^{k+1} f_{2i-1} = \sum_{i=1}^{k} f_{2i-1} + f_{2(k+1)-1} \tag{1.68}$$

$$= f_{2k} + f_{2k+1} \tag{1.69}$$

$$= f_{2k+2} \tag{1.70}$$

$$= f_{2(k+1)}. \tag{1.71}$$

By mathematical induction, (Equation 1.67) holds for all positive integers $n$. □

**Example 1.22.** Prove that for all positive integers $n$,

$$\sum_{i=1}^{n} f_i = f_{n+2} - 1. \tag{1.72}$$

*Solution.* For $n = 1$, $f_1 = 1 = f_3 - 1$ so the bases case holds. Assume, for some positive integer $k$, that (Equation 1.72) holds. Then we find

$$\sum_{j=1}^{k+1} f_j = \sum_{j=1}^{k} f_j + f_{k+1} \tag{1.73}$$

$$= f_{k+2} - 1 + f_{k+1} \tag{1.74}$$

$$= f_{k+1} + f_{k+2} - 1 \tag{1.75}$$

$$= f_{k+3} - 1. \tag{1.76}$$

By mathematical induction, (Equation 1.72) holds for all positive integers $n$. □

**Example 1.23.** Prove that for all positive integers $n$,

$$f_{n+1} f_{n-1} - (f_n)^2 = (-1)^n. \tag{1.77}$$

*Solution.* For $n = 1$, $f_2 f_0 - (f_1)^2 = (-1)^1$ so the base case holds. Assume, for some positive integer $k$, that (Equation 1.77) holds. Then we find

$$f_{k+2} f_k - (f_{k+1})^2 = (f_{k+1} + f_k) f_k - (f_{k+1})(f_{k-1} + f_k) \tag{1.78}$$

$$= f_{k+1} f_k + (f_k)^2 - f_{k+1} f_{k-1} - f_{k+1} f_k \tag{1.79}$$

$$= (-1)\left(-(f_k)^2 + f_{k+1} f_{k-1}\right) \tag{1.80}$$

$$= (-1)(-1)^k \tag{1.81}$$

$$= (-1)^{k+1}. \tag{1.82}$$

By mathematical induction, (Equation 1.77) holds for all positive integers $n$. □

From our previous video, we recall the definition of the Fibonacci numbers.

**Definition 1.7. Fibonacci numbers** are the positive integers defined by $f_0 = 0$, $f_1 = 1$, and

$$f_n = f_{n-1} + f_{n-2}$$

for $n \geq 2$.

The first 21 Fibonacci numbers are

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 5 | 8 | 13 |
| 21 | 34 | 55 | 89 | 144 | 233 | 377 |
| 610 | 987 | 1597 | 2584 | 4181 | 6765 | 10946 |

In our previous lecture we also proved the following 5 Fibonacci identities.

**Example 1.24.** Prove that for all positive integers $n$,

$$\sum_{i=0}^{n} f_i^2 = f_n f_{n+1}.$$

**Example 1.25.** Prove that for all positive integers $n$,

$$\sum_{j=1}^{n} f_{2j} = f_{2n+1} - 1.$$

**Example 1.26.** Prove that for all positive integers $n$,

$$\sum_{i=1}^{n} f_{2i-1} = f_{2n}.$$

**Example 1.27.** Prove that for all positive integers $n$,

$$\sum_{i=1}^{n} f_i = f_{n+2} - 1.$$

**Example 1.28.** Prove that for all positive integers $n$,

$$f_{n+1}f_{n-1} - (f_n)^2 = (-1)^n.$$

Now let's see what this infamous formula is all about.

The Fibonacci numbers also have an interesting relationship to the **golden ratio**. This relationship is expressed by a formula called the **Euler-Binet formula**. And this simple equation has surprising implications, and it has been used to derive many other results in mathematics. The Fibonacci numbers and the golden ratio continue to fascinate mathematicians and laypeople alike, and they are sure to continue to yield new insights in the future.

Firstly, we notice that the Euler-Binet formula gives us a **closed form** for calculating the $n$-th Fibonacci number. In fact, the formula is in terms of the golden ratio $\phi$. To prove the formula we first need the following lemma involving the golden ratio.

**Lemma 1.17.** *For any solution $x$ of $x^2 - x - 1 = 0$ and any positive integer $n$,*

$$x^n = xf_n + f_{n-1}.$$

*Proof.* Proof by mathematical induction. Clearly, $x^1 = xf_1 + f_0 = x(1) + 0 = x$ so the base case holds. Assume now that, for some positive integer $k$, that

$$x^k = xf_k + f_{k-1}.$$

We wish to prove that

$$x^{k+1} = xf_{k+1} + f_k.$$

To this end, multiply the identity by $x$ to obtain

$$\begin{aligned} x^{k+1} &= x^2 f_k + xf_{k-1} && (1.83)\\ &= (x+1)f_k + xf_{k-1} && (1.84)\\ &= x(f_k + f_{k-1}) + f_k && (1.85)\\ &= xf_{k+1} + f_k && (1.86) \end{aligned}$$

as needed.

□

The **golden ratio** is the positive root of the quadratic equation $x^2 - x - 1 = 0$, that is,

$$\phi = \frac{1+\sqrt{5}}{2}.$$

The conjugate of $\phi$ is denoted using $\tau$ and is

$$\tau = \frac{1-\sqrt{5}}{2}.$$

It is easily verified that $\phi\tau = -1$ and $\phi - \tau = \sqrt{5}$. We now give a closed formula to compute the $n$-th Fibonacci number.

**Theorem 1.13** (Euler-Binet Formula)**.** *For all positive integers $n$,*

$$f_n = \frac{1}{\sqrt{5}}(\phi^n - \tau^n).$$

*Proof.* By (Lemma 1.17),

$$\phi^n = \phi f_n + f_{n-1} \quad \text{and} \quad \tau^n = \tau f_n + f_{n-1}.$$

It follows that $f_n = \frac{\phi^n - \tau^n}{\phi - \tau}$. Now observe that (Theorem 1.13) follows since $\phi - \tau = \sqrt{5}$.

$\square$

The first 75 Fibonacci numbers.

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987,
1597, 2584, 4181, 6765, 10946, 17711, 28657, 46368, 75025,
121393, 196418, 317811, 514229, 832040, 1346269, 2178309,
3524578, 5702887, 9227465, 14930352, 24157817, 39088169,
63245986, 102334155, 165580141, 267914296, 433494437,
701408733, 1134903170, 1836311903, 2971215073, 4807526976,
7778742049, 12586269025, 20365011074, 32951280099,
53316291173, 86267571272, 139583862445, 225851433717,
365435296162, 591286729879, 956722026041, 1548008755920,
2504730781961, 4052739537881, 6557470319842, 10610209857723,
17167680177565, 27777890035288, 44945570212853, 72723460248141,
117669030460994, 190392490709135, 308061521170129,
498454011879264, 806515533049393, 1304969544928657,
2111485077978050

The next example shows that the Fibonacci numbers grow exponentially fast.

**Example 1.29.** Prove that $f_n > \left(\frac{3}{2}\right)^{n-1}$, for all $n \geq 6$.

*Solution.* We verify that

$$f_6 = 8 > \left(\frac{3}{2}\right)^5 \approx 7.59375.$$

We also must verify

$$f_7 = 13 > \left(\frac{3}{2}\right)^6 \approx 11.390625.$$

Now let $k > 7$, and assume (the inductive hypothesis) that $f_i > (3/2)^{i-1}$ for $i = k-1$ and $i = k-2$. Then we have

$$\begin{aligned}
f_k &= f_{k-1} + f_{k-2} \\
&> \left(\frac{3}{2}\right)^{k-2} + \left(\frac{3}{2}\right)^{k-3} \\
&= \left(\frac{3}{2}\right)^{k-3} \left(\frac{3}{2} + 1\right) \\
&= \left(\frac{3}{2}\right)^{k-3} \left(\frac{5}{2}\right) \\
&> \left(\frac{3}{2}\right)^{k-3} \left(\frac{9}{4}\right) \\
&= \left(\frac{3}{2}\right)^{k-3} \left(\frac{3}{2}\right)^{2} = \left(\frac{3}{2}\right)^{k-1}
\end{aligned}$$

as desired.

The golden ratio $\phi$ is approximately, 1.61803398875. We can use the golden ratio to improve our understanding of the growth rate of the Fibonacci sequence.

**Example 1.30.** Prove that $f_n > \phi^{n-2}$, for all $n \geq 3$.

*Solution.* We verify that

$$f_3 = 3 > \phi^1 \approx 1.618 \qquad \text{and} \qquad f_4 = 5 > \phi^2 \approx 2.618.$$

Now let $k > 4$, and assume (the inductive hypothesis) that $f_i > \phi^{i-2}$ for $i = k-1$ and $i = k-2$. Now using $\phi^2 = \phi + 1$, we have

$$\begin{aligned}
f_k &= f_{k-1} + f_{k-2} \\
&> \phi^{k-3} + \phi^{k-4} \\
&= \phi^{k-4} (\phi + 1) \\
&= \phi^{k-4} \phi^2 \\
&= \phi^{k-2}
\end{aligned}$$

as desired.

This may seem like a slight improvement (i.e. the base has increased from 1.5 to $\phi$), but this small change in base means much more growth in the long term.

## 1.7 Universal Property of Natural Numbers

**Theorem 1.14** (Universal Property of Natural Numbers)**.** *Let $S$ be any set, $f : S \to S$ be any function, and let $x_0 \in S$. Then there exists a unique function $\phi : \mathbb{N} \to S$ such that $\phi(1) = x_0$ and $\phi \circ s = f \circ \phi$.*

*Proof.* We will rely upon the set-theoretic principle that a subset $\Gamma \subseteq A \times B$ is the graph of a function from $A$ to $B$ if and only if $p : \Gamma \to A$ is a bijection. We wish to construct a mapping $\phi : \mathbb{N} \to S$ and so $p : \Gamma \to \mathbb{N}$ must be a bijection with graph $\Gamma \subseteq \mathbb{N} \times S$. We also insist that $\phi(1) = x_0$ which means $(1, x_0) \in \Gamma$. Since $\Gamma$ is expected to be the graph of the yet unconstructed function $\phi$, for any $n \in \mathbb{N}$, we must have elements of the form $(n, \phi(n)) \in \Gamma$. So, if $(n, t) \in \Gamma$, then $t$ is expected to be $\phi(n)$. Then, the second condition says that $\phi(s(n)) = f(\phi(n))$ and hence $(s(n), f(t)) \in \Gamma$. This says, if we prescribe $\theta : \mathbb{N} \times S \to \mathbb{N} \times S$ as $\theta(n, t) = (s(n), f(t))$, then $\theta(\Gamma) \subseteq \Gamma$. So let $\theta$ be so prescribed, we see that these three conditions ensure what we need:

- $p : \Gamma \to A$ is a bijection
- $(1, x_0) \in \Gamma$
- $\theta(\Gamma) \subseteq \Gamma$.

Let $\mathcal{C}$ be the set of all subsets of $\mathbb{N} \times S$ satisfying $(ii)$ and $(iii)$. Notice that $(1, x_0) \in \mathbb{N} \times S$, and so $\mathbb{N} \times S$ satisfies $(ii)$. If $(s(n), f(t)) \in \theta(\mathbb{N} \times S)$, then by the definitions of $s$ and $f$ we see that $(s(n), f(t)) \in \mathbb{N} \times S$, and so $\mathbb{N} \times S$ satisfies $(iii)$. Then $\mathbb{N} \times S \in \mathcal{C}$, and hence this collection is nonempty.

$b)$ and $c)$: Let $\Gamma$ be the intersection of all elements in $\mathcal{C}$. First let us check that $\Gamma \in \mathcal{C}$. This is easy, since $(1, x_0) \in X$ for all $X \in \mathcal{C}$ and $\Gamma$ being the intersection of such sets, $(1, x_0) \in \Gamma$. Similarly, for any $X \in \mathcal{C}$, $\theta(\Gamma) \subseteq \theta(X) \subseteq X$ and thus $\theta(\Gamma) \subseteq X$ for all $X \in \mathcal{C}$. So, by definition of $\Gamma$, $\theta(\Gamma) \subseteq \Gamma$. So, $\Gamma$ satisfies $b)$ and $c)$, and hence $\Gamma \in \mathcal{C}$.

$a)$: First, consider the set $G = \theta(\Gamma) \cup \{(1, x_0)\}$. Then clearly $G \subseteq \Gamma$. On the other hand, $(1, x_0) \in G$ and

$$\theta(G) \subseteq \theta(\theta(\Gamma)) \cup \theta(\{(1, x_0)\} \subseteq \theta(\Gamma) \subseteq G.$$

So, $G \in \mathcal{C}$ and thus by definition of $\Gamma$, we get $\Gamma \subseteq G$. This shows that

$$\theta(\Gamma) \cup \{(1, x_0)\} = G = \Gamma. \tag{1.87}$$

We prove that $p : \Gamma \to \mathbb{N}$ is a bijection by applying induction to the set,

$$T = \{n \in \mathbb{N} \mid p^{-1}(n) \subseteq \Gamma \text{ has exactly one element}\}.$$

Notice that if $T = \mathbb{N}$, then $p$ is a bijection.

We have $p(1, x_0) = 1$ and we wish to show that $p^{-1}(1) = \{(1, x_0)\}$. If not, say $(1, t) \in p^{-1}(1)$ with $t \neq x_0$. By (1.87), we see that $(1, t) \in \theta(\Gamma)$. So, there exists an element $(n, u) \in \Gamma$ such that $(1, t) = \theta(n, u) = (s(n), f(u))$. This says in particular, $1 = s(n)$ contradicting Peano's axiom. This proves that $p^{-1}(1) = \{(1, x_0)\}$ and hence $1 \in T$.

Next, assume that $n \in T$. Then by definition, we have $p^{-1}(n) = \{(n, w)\}$. Since $(n, w) \in \Gamma$, we know that $\theta(n, w) = (s(n), f(w)) \in \Gamma$, since $\theta(\Gamma) \subseteq \Gamma$. Thus $p^{-1}(s(n))$ contains $(s(n), f(w))$. If we can show this is the only element in this set, we would have shown $s(n) \in T$ and then by induction, we would be done. So, assume that $(s(n), x) \in \Gamma$ and we want to show that $x = f(w)$. By Peano's axiom, $(s(n), x) \neq (1, x_0)$ and hence, from (1.87), we see that $(s(n), x) \in \theta(\Gamma)$ and thus there is an element $(m, y) \in \Gamma$ with $\theta(m, y) = (s(n), x)$. Then $s(m) = s(n)$ and $f(y) = x$. By injectivity of $s$, we get $m = n$. Since $(m, y) = (n, y) \in \Gamma$ and $n \in T$ implies $y = w$. Then $x = f(w)$ and thus $(s(n), x) = (s(n), f(w))$ proving what we set out to prove. Thus $T = \mathbb{N}$ and hence $p$ is a bijection.

□

## 1.8 Exercises

**Exercise 1.1.** Conjecture a formula for the sum of the first $n$ even positive integers. Prove your result using mathematical induction.

**Exercise 1.2.** Show that the sum of consecutive odd natural numbers beginning with 1 is a square.

**Exercise 1.3.** Prove that $2^{n+1} > n + 2$ for every positive integer $n$.

**Exercise 1.4.** Prove that a set with $n$ elements has exactly $2^n$ subsets.

**Exercise 1.5.** Prove that, for all positive integers $n$,

$$\sum_{j=1}^{n} (-1)^{j-1} j^2 = (-1)^{n-1} \frac{n(n+1)}{2}.$$

**Exercise 1.6.** Prove that, for all positive integers $n$,

$$\sum_{j=1}^{n} j \cdot j! = (n+1)! - 1.$$

**Exercise 1.7.** Use mathematical induction to show that the sum of the first $n$ odd cubes is $n^2\left(2n^2-1\right)$.

**Exercise 1.8.** Use mathematical induction to prove that $2^n < n!$ for $n \geq 4$.

**Exercise 1.9.** Use mathematical induction to prove that $3^n > 3n-1$ for every positive integer $n$.

**Exercise 1.10.** Prove that $0 < a < b$ then $0 < a^n < b^n$ for all positive integers $n$.

**Exercise 1.11.** Use mathematical induction to prove that $3^n > n^3$ for $n > 4$.

**Exercise 1.12.** Use the strong form of mathematical induction to establish that for all $n \geq 1$,

$$a^n - 1 = (a-1)\left(a^{n-1} + a^{n-2} + a^{n-3} + \cdots + a + 1\right).$$

**Exercise 1.13.** Show that any amount of postage that is an integer number of cents greater than 53 cents can be formed using just 7-cent and 10-cent stamps.

**Exercise 1.14.** Use mathematical induction to prove that $x-y$ is a factor of $x^n - y^n$, where $x$ and $y$ are variables.

**Exercise 1.15.** Use mathematical induction to prove the inequality. For all $n \geq 1$,

$$\frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \cdots + \frac{n}{2^n} \leq 2 - \frac{n+2}{2^n}.$$

**Exercise 1.16.** Use mathematical induction to prove that $2^n > n^2$ for $n > 4$.

**Exercise 1.17.** Use mathematical induction to show that for every positive integer $n$,

$$\sum_{i=1}^{n} 2^k = 2^{n+1} - 2.$$

**Exercise 1.18.** You have a supply of 32 cent stamps and 21 cent stamps. You need to mail a package which requires 1.48 dollars in postage. How many of each type of stamp should you use? Can you prove it?

**Exercise 1.19.** Prove $2n < 7^n$ whenever $n$ is a positive integer.

**Exercise 1.20.** Find the Fibonacci numbers $f_{24}$, $f_{32}$, and $f_{44}$.

**Exercise 1.21.** Write out the first 50 Fibonacci numbers.

**Exercise 1.22.** Show that $f_{n+3} + f_n = 2f_{n+2}$ whenever $n$ is a positive integer.

**Exercise 1.23.** Show that $f_{n+3} - f_n = 2f_{n+1}$ whenever $n$ is a positive integer.

**Exercise 1.24.** Show that $f_{n-2} + f_{n+2} = 3f_n$ whenever $n$ is a positive integer with $n \geq 2$.

**Exercise 1.25.** Show that $f_{2n} = f_n^2 + 2f_{n-1}f_n$ whenever $n$ is a positive integer with $n \geq 2$.

**Exercise 1.26.** Show that $f_{2n+1} = f_{n+1}^2 + f_n^2$ whenever $n$ is a positive integer.

**Exercise 1.27.** Show that $f_{2n} = f_{n+1}^2 - f_{n-1}^2$ whenever $n$ is a positive integer.

**Exercise 1.28.** Show that for all positive integers $n$,

$$f_1f_2 + (f_2f_3 + f_3f_4) + \cdots + (f_{2n-2}f_{2n-1} + f_{2n-1}f_{2n}) = (f_{2n})^2 .$$

**Exercise 1.29.** Prove that $f_{n+2}^2 - f_{n+1}^2 = f_nf_{n+3}$ , for all $n \geq 1$.

**Exercise 1.30.** Prove that $f_{n+1}f_n - f_{n-1}f_{n-2} = f_{2n-1}$ for every positive integer $n$, $n > 2$.

**Exercise 1.31.** Prove that $f_1f_2 + f_2f_3 + \cdots + f_{2n-1}f_{2n} = f_{2n}^2$ for every positive integer $n$.

**Exercise 1.32.** Prove that $f_{m+n} = f_mf_{n+1} + f_nf_{m-1}$ for every positive integer $n$.

**Exercise 1.33.** Prove that $f_n > \left(\frac{5}{3}\right)^{n-1}$, for all $n \geq 2$.

**Exercise 1.34.** Show that for $n \geq 2$,

$$f_n = \frac{f_{n-1} + \sqrt{5f_{n-1}^2 + 4(-1)^n}}{2}$$

Notice that this formula gives $f_n$ in terms of one predecessor rather than two predecessors.

**Exercise 1.35.** Let $F = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. Show that

$$F^n = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}$$

for all $n \geq 1$.

**Exercise 1.36.** Let $a_0 = 1$ and, for $n > 0$, let $a_n = 2a_{n-1} + 1$. The first few terms of the sequence are 1,3,7,15. What are the next fews terms? Prove that $a_n = 2^{n+1} - 1$ for all positive integers.

**Exercise 1.37.** Let $b_0 = 1$ and, for $n > 0$, let $b_n = 3b_{n-1} - 1$. What are the first five terms of the sequence? Prove that $b_n = (3^n + 1)/2$ for all positive integers.

**Exercise 1.38.** Find the first 50 Lucas numbers.

**Exercise 1.39.** Find and prove a formula for the sum of the first $n$ Lucas numbers when $n$ is a positive integer.

**Exercise 1.40.** Find and prove a formula for the sum of the first $n$ Lucas numbers with odd indices when $n$ is a positive integer.

**Exercise 1.41.** Find and prove a formula for the sum of the first $n$ Lucas numbers with even indices when $n$ is a positive integer.

**Exercise 1.42.** Show that $f_{2n} = f_n L_n$ for all positive integers $n$.

**Exercise 1.43.** Prove that $L_{m+n} = f_{m+1} L_n + f_m L_{n-1}$ whenever $m$ and $n$ are positive integers with $n > 1$.

**Exercise 1.44.** Prove that $L_n = \phi^n + \tau^n$ where $\phi$ is the golden ratio and $\tau$ its conjugate.

**Exercise 1.45.** Establish each of the following for all $n \in \mathbb{N}$.

- $L_n - 5f_n^2 = 4(-1)^n$
- $L_{2n} = L_n^2 - 2(-1)^n$
- $f_{n+1} + f_{n-1} = L_n$
- $L_{n+1} + L_{n-1} = 5f_n$
- $L_{2n+1} = L_n L_{n+1} - (-1^n)$
- $L_{n-1}L_{n+1} - L_n^2 = 5(-1)^{n-1}$, $n \geq 2$

# Chapter 2

# Divisibility

Anyone who has ever taken a high school math class knows that divisibility is an important concept. But what exactly is divisibility, and how can it be used to solve problems? This book provides a comprehensive guide to understanding divisibility and covers topics such as prime numbers, composite numbers, GCDs, and more. If you're looking to improve your understanding of math and want to learn everything there is to know about divisibility, then this is the perfect book for you!

Number theory is the study of integers and their properties. One of the most important concepts in number theory is divisibility. Divisibility is a way of determining whether one number is a multiple of another number. For example, we say that 6 is divisible by 3 because 3 x 2 = 6. We also say that 10 is divisible by 5 because 5 x 2 = 10. In general, we say that a number a is divisible by another number b if there exists an integer c such that a = b x c.

Divisibility is a critical concept for advanced college students because it is the basis for many other number theoretic concepts and results. For example, the Euclidean algorithm for finding the greatest common divisor of two numbers relies on the concept of divisibility. Furthermore, many proofs in number theory involve showing that one number is divisible by another number. As a result, students must have a strong understanding of divisibility and be able to apply it in various contexts.

First focus on specific properties of divisibility such as the division algorithm and modular arithmetic. And then we focus on specific applications of divisibility such as greatest common divisors and least common multiples. We make sure to provide plenty of examples and practice problems for you to work through. By doing so, you'll help ensure that they gain a strong understanding of this important number theoretic concept.

A prime number is a positive integer that has no divisors other than 1 and itself. In other words, a prime number cannot be evenly divided by any other number except for 1 and itself. For example, the number 7 is prime because it can only be evenly divided by 1 and 7. The number 10 is not prime because it can be evenly divided by 1, 2, 5, and 10. Prime numbers are an important concept in mathematics, and they have a wide range of applications in cryptography and coding theory.

Divisibility in the integers is a fundamental topic in number theory, and the study of prime numbers has led to the development of important theoretical tools like the Chinese Remainder Theorem and the Euclidean algorithm. In addition, prime numbers are used in public key cryptography, which is a technique for secure communication that is used by militaries, banks, and other organizations.

The greatest common divisor (GCD) of two integers is the largest integer that evenly divides both numbers. For example, the GCD of 24 and 18 is 6 because 6 is the largest integer that evenly divides 24 and 18. The Euclidean algorithm is a method for finding the GCD of two integers that is based on the concept of divisibility. The algorithm is named after the Greek mathematician Euclid, who first described it in his book Elements, around 300 BC, making it one of the oldest algorithms still in use today.

The Euclidean algorithm is a powerful tool that has a wide range of applications. In particular, it can be used to find the GCD of two numbers when one number is much larger than the other. It can also be used to find the LCM of two numbers and to solve linear Diophantine equations.

The Euclidean algorithm is based on the following property of divisibility: if a is divisible by b, then a - b is also divisible by b. This property can be used to find the GCD of two numbers when one number is much larger than the other.

The Fundamental Theorem of Arithmetic is a theorem that states that every positive integer is divisible by a unique (up to ordering) set of primes. In other words, if a and b are two positive integers with no common factors (i.e., they are co-prime), then a*b is divisible by all of the primes that divide a and by all of the primes that divide b.

This theorem is one of the cornerstones of number theory, and it has many applications in mathematics and computer science. It is also a useful tool for proving other results in number theory. For example, it can be used to show that there are infinitely many prime numbers. The proof of the theorem is relatively simple, but it relies on some interesting ideas.

The theorem is a fundamental result in number theory, and it has important applications in cryptography and security. The theorem was first proved by Euclid in his Elements, and it has been central to number theory ever since.

A linear Diophantine equation is an equation of the form ax + by = c, where a, b, and c are integers. This type of equation has infinitely many integral solutions if a and b are relatively prime, and no solutions if they are not.

In general, the set of all solutions to a linear Diophantine equation forms a line in the plane. However, some equations have special solutions that do not lie on this line. For example, the equation 2x + 3y = 5 has the solution x = 2 and y = -1, which is not on the line 2x + 3y = 5. These special solutions are called non-trivial solutions. The most common method to solve a linear Diophantine equation is the Euclidean algorithm.

The study of linear Diophantine equations is a branch of mathematics known as number theory. Number theory is the study of the positive integers, which are the whole numbers greater than 0. Integer solutions to linear Diophantine equations have applications to many areas of mathematics, including cryptography and coding theory.

I wrote this book for people who want to improve their understanding of mathematics. In it, I cover the basics of divisibility and explain how to use divisibility to solve problems. I also include worked examples and practice problems so that you can test your knowledge as you go.

When teaching divisibility to advanced college students, it is important to stress the importance of writing proofs. A proof is a logical argument that shows that a statement is true. By stressing the importance of writing proofs, students will be better prepared to understand and apply the concept of divisibility in their future studies.

When it comes to teaching mathematics, there is no one-size-fits-all approach. Different students learn in different ways, and what works for one may not work for another. However, some general principles can help to make math instruction more effective.

First, it is important to create a foundation of basic skills. Without a strong understanding of basic concepts, students will struggle to progress to more advanced material. Second, it is important to provide plenty of practice opportunities. Students need to be able to work through problems on their own in order to develop fluency and confidence.

Finally, it is important to emphasize understanding over rote memorization. Understanding the underlying concepts is key to being able to apply mathematics in the real world. By following these principles, you will build a strong foundation that will serve you well throughout your life.

This book is a comprehensive guide to understanding divisibility. If you're looking to improve your understanding of math and want to learn everything there is to know about divisibility, then this is the perfect book for you! The author does a great job of explaining complex concepts in an easy-to-understand way, making it ideal for anyone who wants to strengthen their understanding of divisibility. I would highly recommend this book to anyone looking for a better grasp of how divisibility works.

## 2.1 The Integers

Discuss axioms and the properties of the integers.

## 2.2 Divisibility and The Division Algorithm

We begin by stating the definition of divisibility, the main topic of discussion. We then give a few examples followed by several basic lemmas on divisibility. The Well-Ordering Axiom, which is used in the proof of the Division Algorithm, is then stated. Examples demonstrating how to use the Division Algorithm as a method of proof are then given.

Certainly the sum, difference and product of any two integers is an integer. The same can not be said about the ratio of two integers. For example, while 2 and 3 are integers, the ratio 2/3 is not an integer. We simply can not take any to integers and divide them. The study of the integers is to a great extent the study of divisibility.

**Definition 2.1.** If $a$ and $b$ are integers with $a \neq 0$, we say that $a$ **divides** $b$, written $a|b$, if there exists an integer $c$ such that $b = ac$.

Here are some examples of divisibility:

- $3|6$ since $6 = 2(3)$ and $2 \in \mathbb{Z}$
- $6|24$ since $24 = 4(6)$ and $4 \in \mathbb{Z}$
- $8|0$ since $0 = 0(8)$ and $0 \in \mathbb{Z}$
- $-5| - 55$ since $-55 = 11(-5)$ and $11 \in \mathbb{Z}$
- $-9|909$ since $909 = -101(-9)$ and $-101 \in \mathbb{Z}$

There are other common ways of saying $a$ divides $b$. Namely, $a|b$ is equivalent to all of the following:

- $a$ is a **divisor** of $b$
- $a$ divides $b$
- $b$ is **divisible by** $a$
- $b$ is a **multiple of** $a$
- $a$ is a **factor of** $b$

Any integer $n$, except 0, has just a finite number of divisors. For if $a|n$ where $a$ and $n$ are positive integers, then $n = ak$ for some integer $k$. Since $k$ is a positive integer, we see that $n = ak \geq a$. Hence any nonzero integer $n$ can have a most $2|n|$ divisors.

We now state and prove the transitive and linear combination properties of divisibility.

**Lemma 2.1** (Transitive Property of Divisibility]). *Let $a$, $b$, and $c$ be integers. If $a|b$ and $b|c$, then $a|c$.*

*Proof.* Suppose $a|b$ and $b|c$, then there exists integers $m$ and $n$ such that $b = ma$ and $c = nb$. Thus

$$c = nb = n(ma) = (nm)a.$$

Since $nm \in \mathbb{Z}$ we see that $a|c$ as desired.

□

We say an integer $n$ is a **linear combination** of $a$ and $b$ if there exists integers $x$ and $y$ such that $n = ax + by$. For example, 7 is a linear combination of 3 and 2 since $7 = 2(2)+1(3)$. The next lemma says that if an integer divides to other integers, then it divides any linear combination of these two integers.

**Lemma 2.2** (Linear Combinations). *Let $a$, $b$, and $c$ be integers. If $c|a$ and $c|b$, then $c|(xa + yb)$ for any positive integers $x$ and $y$.*

*Proof.* Suppose $c|a$ and $c|b$. Then there exists integers $m$ and $n$ such that $a = mc$ and $b = nc$. Assume $x$ and $y$ are arbitrary integers. We have

$$xa + yb = x(mc) + y(nc) = c(xm + yn)$$

Since $xm + yn \in \mathbb{Z}$ we see that $c|(xa + yb)$ as desired.

□

We now state and prove the antisymmetric and multiplicative properties of divisibility.

**Lemma 2.3** (Antisymmetric Property of Divisibility). *Let $a$ and $b$ be nonzero positive integers. If $a|b$ and $b|a$, then $a = b$.*

*Proof.* Suppose $a|b$ and $b|a$, then there exists integers $m$ and $n$ such that $b = ma$ and $a = nb$. Notice that both $m$ and $n$ are positive since both $a$ and $b$ are.
Then we have

$$a = nb = n(ma) = (nm)a.$$

Thus, $nm = 1$ and so in particular $n = 1$. Whence, $a = b$ as desired.

□

**Lemma 2.4** (Multiplicative Property of Divisibility)**.** *Let $a$, $b$, and $c$ be integers. If $c \neq 0$ and $a|b$ then $ac|bc$.*

*Proof.* Suppose $a|b$. Then there exists an integer $n$ such that $b = na$. By substitution we find,

$$bc = (nc)a = (ac)n.$$

Since $c \neq 0$, it follows that $ac \neq 0$, and so $ac|bc$ as needed.

□

**Lemma 2.5.** *Let $a$ and $b$ be integers. If $a|b$, then $a^n|b^n$ for any natural number $n$.*

*Proof.* We will use mathematical induction. Since $a|b$ certainly implies $a|b$, the case for $k = 1$ is trivial. Assume that $a^k|b^k$ holds for some natural number $k > 1$. Then there exists an integer $m$ such that $b^k = ma^k$. Then

$$b^{k+1} = bb^k = b\left(ma^k\right) = (bm)a^k = (m'am)a^k = Ma^{k+1}$$

where $m'$ and $M$ are integers. Whence, $a^{k+1}|b^{k+1}$ as desired.

□

Before we state and prove the Division Algorithm, let's recall the Well-Ordering Axiom, namely:

> Every nonempty set of positive integers contains a least element.

This is an incredible important and powerful statement. We will use the Well-Ordering Axiom to prove the **Division Algorithm** .

The proof of the Division Algorithm illustrates the technique of proving **existence** and **uniqueness** and relies upon the Well-Ordering axiom.

**Theorem 2.1** (Division Algorithm)**.** *If $a$ and $b$ are nonzero positive integers, then there are unique positive integers $q$ and $r$ such that*

$$a = bq + r \qquad \textit{and} \qquad 0 \leq r < b.$$

*Proof.* First we prove existence. Let $b$ be an arbitrary natural number greater than 0 and let $S$ be the set of multiples of $b$ that are greater than $a$, namely,

$$S = \{bi \mid i \in \mathbb{N} \text{ and } bi > a\}.$$

Notice $S$ is nonempty since $ab > a$. By the Well-Ordering Axiom, $S$ must contain a least element, say $bk$. Since $k \neq 0$, there exists a natural number $q$ such that $k = q+1$. Notice $bq \leq a$ since $bk$ is the least multiple of $b$ greater than $a$. Thus there exists a natural number $r$ such that $a = bq + r$. Notice $0 \leq r$. Assume, $r \geq b$. Then there exists a natural number $m \geq 0$ such that $b + m = r$. By substitution, $a = b(q+1) + m$ and so $bk = b(q+1) \leq a$. This contradiction shows $r < b$ as needed.

Now we prove uniqueness. Suppose

$$a = bq_1 + r_1, \quad a = bq_2 + r_2, \quad 0 \leq r_1 < b, \quad 0 \leq r_2 < b.$$

If $q_1 = q_2$ then $r_1 = r_2$. Assume $q_1 < q_2$. Then $q_2 = q_1 + n$ for some natural number $n > 0$. This implies

$$r_1 = a - bq_1 = bq_2 + r_2 - bq_1 = bn + r_2 \geq bn \geq b$$

which is contrary to $r_1 < b$. Thus $q_1 < q_2$ cannot happen. Similarly, $q_2 < q_1$ cannot happen either, and thus $q_1 = q_2$ as desired.

□

We say an integer $a$ is of the form $bq + r$ if there exists integers $b$, $q$, and $r$ such that $a = bq + r$. Notice that the division algorithm, in a certain sense, measures the divisibility of $a$ by $b$ using a remainder $r$.

**Example 2.1.** Show 3 divides $a(a^2 + 2)$ for any natural number $a$.

*Solution.* Equivalently, we need to show that $a\left(a^2+2\right)$ is of the form $3k$ for some $k$ for any natural number $a$. By the division algorithm, $a$ has exactly one of the forms $3k$, $3k+1$, or $3k+2$. If $a = 3k+1$ for some $k$, then

$$(3k+1)\left((3k+1)^2+2\right) = 3(3k+1)\left(3k^2+2k+1\right)$$

which shows $3|a(a^2+2)$. If $a = 3k+2$ for some $k$, then

$$(3k+2)\left((3k+2)^2+2\right) = 3(3k+2)\left(3k^2+4k+2\right)$$

which shows $3|a(a^2+2)$. Finally, if $a$ is of the form $3k$ then we have

$$a\left(a^2+2\right) = 3k\left(9k^2+2\right)$$

which shows $3|a(a^2+2)$. Therefore, in all possible cases, $3|a(a^2+2))$ for any positive natural number $a$.

The advantage of the Division Algorithm is that it allows us to prove statements about the positive integers (integers) by considering only a finite number of cases. The next three examples illustrates this.

**Example 2.2.** Show 6 divides the product of any three consecutive positive integers.

*Solution.* Let $m$ be an natural number. We need to show that $m(m+1)(m+2)$ is of the form $6k$. The division algorithm yields that $m$ is either even or odd (not both). In either case, $m(m+1)(m+2)$ must be even. The natural number $m(m+1)(m+2)$ is also divisible by 3, since one of $m$, $m+1$, or $m+2$ is of the form $3k$. Since $m(m+1)(m+2)$ is even and is divisible by 3, it must be divisible by 6.

**Example 2.3.** Prove that, for each natural number $n$, $7^n - 2^n$ is divisible by 5.

*Solution.* Let $P$ be the set of natural number for which $7^n - 2^n$ is divisible by 5. Clearly, $7^1 - 2^1 = 5$ is divisible by 5, so $P$ is nonempty with $0 \in P$. Assume $k \in P$. We find

$$\begin{aligned} 7^{k+1} - 2^{k+1} &= 7 \cdot 7^k - 2 \cdot 2^k \\ &= 7 \cdot 7^k - 7 \cdot 2^k + 7 \cdot 2^k - 2 \cdot 2^k \\ &= 7(7^k - 2^k) + 2^k(7-2) \end{aligned}$$

The induction hypothesis is that $(7^k - 2^k)$ is divisible by 5. Now since both $(7^k - \cdot 2^k)$ and $7-2$ are divisible by 5, so is any linear combination of $(7^k - 2^k)$ and $7-2$. Hence, $7^{k+1} - 2^{k+1}$ is divisible by 5 by **??**. Therefore, $k+1 \in P$ and so $P = \mathbb{N}$ by mathematical induction.

## 2.3 Prime Numbers

Several of the most basic and interesting questions concerning the integers involves the prime numbers. For example,

> Are there infinitely many primes of the form $n^2 + 1$, where $n \in \mathbb{N}$?

This question is easy to understand, but no one has been able to answer it.

From a certain point of very, the prime numbers are the building blocks for the integers; that is to say, every integer greater than 1 has a prime factor. Indeed, every positive integer is a product of primes. This result was known to the ancient Greeks and is sometimes referred to as Euclid{'}s lemma.

One of the first questions that comes to mind is concerning prime numbers is: how many prime numbers are there?" or maybe evenwhy are primes so important to talk about¿‘.
What about these questions: without using trial division, how can one determine whether a given integer is prime or composite?",is it possible for given a function to find all the prime numbers?”, “are there arbitrarily long sequences of integers, all of which are not primes?“. These simple questions have kept mathematicians busy for thousands of years.

**Definition 2.2.** A **prime number** is a natural number greater than 1 that is divisible by no natural numbers other than 1 and itself. A natural number greater than 1 that is not prime is called a **composite number** .

The idea, passing over 1, is to find a prime number and then cross out all of the multiples of this prime number. For example, 2 is prime but every even number is not and so cross all even numbers off the list. Next, 3 is prime and so cross out every multiple of three, because they are not prime. Continue in this fashion, and then the numbers left are the prime numbers. Of course for a given large integer this is not practical, if your time is limited. Since the time of Eratosthenes, sophisticated versions of this algorithm (called the **Sieve of Eratosthenes** ) have achieved new results.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |

Consider the first 5 rows in the above array. How many primes are there in the first 5 rows? How many in the last five rows? If one carries out the sieve of Eratosthenes between 10,000 and 10,050, you will find that there are just 4 prime numbers. Can we find 5 rows where there are no prime numbers? What is the last prime number?

The following lemma, while known to Euclid, is proven using the (modern) Well-Ordering Axiom.

**Lemma 2.6** (Prime Divisor)**.** *Every natural number greater than 1 has a prime divisor.*

*Proof.* Assume, for a contradiction, that there exists an natural number greater than 1 that does not have a prime divisor. Then since the set of all natural numbers greater than 1 without a prime divisor is nonempty, the Well-Ordering Axiom states that this set must have a least positive natural number, say $n$, that does not have a prime divisor and is greater than 1. Since $n$ does not have a prime divisor and $n$ divides $n$, $n$ must not be prime. Thus, $n = ab$ and since $a < n$, $a$ must have a prime divisor and similarly for $b$. Therefore, $n = ab$ must have a prime divisor. This contradiction, leads us to the desired conclusion that every natural number greater than 1 must have a **prime divisor** .

□

2, 3, 5, 7, 11, 13, 17, 19, 23, 29 , 31, 37, 41, 43, 47, 53, 59, 61, 67, 71 , 73, 79, 83, 89, 97, 101, 103, 107, 109, 113 , 127, 131, 137, 139, 149, 151, 157, 163, 167, 173 , 179, 181, 191, 193, 197, 199, 211, 223, 227, 229 , 233, 239, 241, 251, 257, 263, 269, 271, 277, 281 , 283, 293, 307, 311, 313, 317, 331, 337, 347, 349 , 353, 359, 367, 373, 379, 383, 389, 397, 401, 409 , 419, 421, 431, 433, 439, 443, 449, 457, 461, 463 , 467, 479, 487, 491, 499, 503, 509, 521, 523, 541 , 547, 557, 563, 569, 571, 577, 587, 593, 599, 601 , 607, 613, 617, 619, 631, 641, 643, 647, 653, 659 , 661, 673, 677, 683, 691, 701, 709, 719, 727, 733 , 739, 743, 751, 757, 761, 769, 773, 787, 797, 809 , 811, 821, 823, 827, 829, 839, 853, 857, 859, 863 , 877, 881, 883, 887, 907, 911, 919, 929, 937, 941 , 947, 953, 967, 971, 977, 983, 991, 997

Figure 2.1: Prime numbers less than 1000.

The following proof of the infinitude of primes is a great example of what is called proof **by contradiction** . The idea is to suppose that there are finitely many prime numbers, and then use these primes to create another natural number whose prime divisor can not be in the original list of all prime numbers.

**Theorem 2.2** (Euclid)**.** *There are infinitely many primes.*

*Proof.* Assume that the prime numbers are listed in ascending order with $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and so on; and assume (for a contradiction) that $p_k$ is the last prime. Consider the natural number,

$$P = p_1 p_2 \cdots p_k + 1.$$

Since every positive natural number greater than 1 has a prime divisor, $P$ has a prime divisor, say $p_m$. However, $p_m$ can not divide $P$ since $P$ is of the form, $P = cp_m + 1$. Therefore $p_k$, the last prime number, cannot exist.

□

## 2.4 Greatest Common Divisors

Perhaps the most useful result concerning great common divisors is Bezout's lemma. This fact states that the greatest common divisor of two integers is always a linear combination of these two integers. In fact we can say more, the greatest common divisor of two given integers is always the least positive linear combination of these two integers.

**Definition 2.3.** Let $a$ and $b$ be two integers that are not both zero. Then the **greatest common divisor** of $a$ and $b$ is the largest integer that divides both $a$ and $b$. The greatest common divisor of $a$ and $b$ is denoted by $(a, b)$ or sometimes by $\gcd(a, b)$.

The integers 4 and 8 have greatest common divisor of 4 and we write $(4, 8) = 4$ since 4 is the largest integer that divides both 4 and 8. Also $(23, 2) = 1$ and $(9, 51) = 3$.

**Definition 2.4.** A **linear combination** of $a$ and $b$ is an integer of the form $ma + nb$ where $m$ and $n$ are integers.

Note that given 2 and 51 we can form many different linear combinations, here are three examples:

$$3(2) + 7(51) = 363, \qquad 3(2) - 7(51) = -351,$$

and $-31(2) + 0(51) = -62$. The connection between liner combination and greatest command visors is **Bezout's identity** .

**Theorem 2.3** (Bezout's Identity)**.** *Let $a$ and $b$ be integers, not both zero. Then $(a, b) = am + bn$ for some integers $m$ and $n$.*

*Proof.* Assume $a$ and $b$ are integers and w.l.o.g. assume $a \neq 0$. Consider the set

$$S = \{ax + by \mid ax + by > 0, \ x \text{ and } y \text{ are integers}\}.$$

Since $S$ is nonempty, because $|a|$ is in $S$, the Well-Ordering Axiom yields a least positive natural number $d$ such that $d = am+bn$ for some integers $m$ and $n$. The idea is to show that $d = (a, b)$. To do this we use the Division

Algorithm obtaining $q$ and $r$ such that $a = qd + r$ where $0 \leq r < d$. If $r > 0$, then $r$ is in $S$ because

$$r = a - qd = a - q(am + bn) = a(1 - qm) + b(-qn).$$

But we can not have $r$ is in S because $r < d$ and $d$ is the least in $S$. Therefore $r = 0$ and so $d|a$. Using the same argument with $a$ replaced by $b$, it is shown that $d|b$. To show $d = (a, b)$ it remains to show that $d$ is greater than any other common divisor of $a$ and $b$; and so let $c$ be a common divisor of $a$ and $b$. Then, $c \mid am + bn$ that is $c \mid d$ and so $d \geq c$.

□

**Corollary 2.1.** *There are an infinite number of ways to write $(a, b)$ as a linear combination of $a$ and $b$.*

*Proof.* Let $d = (a, b)$. There exists integers $m$ and $n$ such that $d = am+bn$ and thus, for any integer $k$, we have

$$d = (m + k(b/d))a + (n - k(a/d))b$$

which expresses $(a, b)$ as a linear combination of $a$ and $b$.

□

**Corollary 2.2.** *Let $a$ and $b$ be integers, then the set of linear combinations of $a$ and $b$ is the set of multiples of $(a, b)$.*

*Proof.* By **??**, if $d = (a, b)$ then $d = am + bn$ for some integers $m$ and $n$. Thus every multiple of $d$ is also a linear combination of $a$and $b$. Conversely, let $ax + by$ be a linear combination of $a$ and $b$. Then using **??**, $d|am + by$ and so $am + by$ is a multiple of $d$.

□

Two integers are said to be **relatively prime** if their greatest common divisor is 1.

**Definition 2.5.** If $(a, b) = 1$ then $a$ and $b$ are said to be **relatively prime** .

Note that $(2, 5) = 1$ and so 2 and 5 are relatively prime. But $(8, 24) = 8$ and so 8 and 24 are not relatively prime.

**Definition 2.6.** Integers $a_1$, $a_2$, ..., $a_n$ are called **pairwise relatively prime** when $(a_i, a_j) = 1$ for every possible $i$ and $j$ with $i \neq j$.

For example, The integers 3, 5, 7 are pairwise relatively prime because $(3,5) = 1$, $(5,7) = 1$, and $(3,7) = 1$. The integers 4, 19, 27 are pairwise relatively prime because $(4,19) = 1$, $(4,27) = 1$, and $(4,27) = 1$.
The integers 10, 14, and 35 are **mutually relatively prime** because $(10,14,35) = 1$ (there is no common divisor for all three) however they are not pairwise relatively prime because $(10,14) = 2$.

**Example 2.4.** Show that if $k$ is an integer, then the integers $6k-1$, $6k+1$, $6k+2$, $6k+3$, and $6k+5$ are relatively prime.

*Solution.* Suppose that $(6k+a, 6k+b) = d$. Then $d|(b-a)$. We have $a, b \in \{-1,1,2,3,5\}$, so if $a < b$ it follows that $b-a \in \{1,2,3,4,6\}$. Hence $d \in \{1,2,3,4,6\}$. To show that $d = 1$ it is sufficient to show that neither 2 nor 3 divides $(6k+a, 6k+b)$. If $p = 2$ or $p = 3$ and $p|(6k+a, 6k+b)$ then $p|a$ and $p|b$. However, there are no such pairs $a, b$ in the set $\{-1,1,2,3,5\}$.

**Example 2.5.** Show that every positive integer greater than 6 is the sum of two relatively prime integers greater than 1.

*Solution.* By the previous example, we know that $6k-1$, $6k+1$, $6k+2$, $6k+3$, and $6k+5$ are pairwise relatively prime. To represent $n$ as the sum of two relatively prime integers greater than one, let $n = 12k+h$, $0 \leq h < 12$. We now examine the twelve cases, one for each possible value of $h$, in the following tables:

| $h$ | $n$ |
|---|---|
| 0 | $(6k-1)+(6k+1)$ |
| 1 | $(6k-1)+(6k+2)$ |
| 2 | $(6k-1)+(6k+3)$ |
| 3 | $(6k+1)+(6k+2)$ |
| 4 | $(6k+2)+(6k+2)$ |
| 5 | $(6k+2)+(6k+3)$ |

| $h$ | $n$ |
|---|---|
| 6 | $(6k+1)+(6k+5)$ |
| 7 | $(6k+2)+(6k+5)$ |
| 8 | $(6k+3)+(6k+5)$ |
| 9 | $(12k+7)+2$ |
| 10 | $(12k+7)+3$ |
| 11 | $(12k+9)+2$ |

So for all possible cases very positive integer greater than 6 is the sum of two relatively prime integers greater than 1.

**Corollary 2.3.** *Let $a$ and $b$ be integers, then $(a, b) = 1$ if and only if there exists integers $m$ and $n$ such that $am + bn = 1$.*

*Proof.* If $(a, b) = 1$ then by **??** there exists integers $m$ and $n$ such that $1 = am + by$. Conversely, suppose $(a, b) = d$ and that $1 = ax + by$ for some integers $x$ and $y$. Then $d|1$ because $d|a$ and so $d = 1$.

□

**Example 2.6.** Show that $3k + 2$ and $5k + 3$ are relatively prime.

*Solution.* Since $5(3k+2)-3(5k+3) = 1$, the previous proposition implies that $(3k + 2, 5k + 3) = 1$.

**Theorem 2.4.** *Let $a$ and $b$ be integers, then $(a, b)$ is the least positive integer that is a linear combination of $a$ and $b$.*

*Proof.* This follows from the Well-Ordering Axiom as in the proof of (i). The proof is left for the reader as Exercise **??**.

□

**Example 2.7.** What is $\left(a^2 + b^2, a + b\right)$, where $a$ and $b$ are relatively prime integers that are not both 0?

*Solution.* Let $p$ be a prime dividing $\left(a^2 + b^2, a + b\right)$. Then

$$p\,|(a + b)^2 - (a^2 + b^2) = 2ab.$$

Now if $p|a$, then $p|b$ since $p|(a + b)$. But $(a, b) = 1$, so $p \nmid a$. Similarly, $p \nmid b$. Therefore, $p|2$ and so $p = 1$ or $p = 2$. If $a$ and $b$ have the same parity, then $2|(a + b)$ and $2\,\middle|\left(a^2 + b^2\right)$ and so $\left(a^2 + b^2, a + b\right) = 2$. But if $a$ and $b$ have opposite parity, then $a + b$ and $\left(a^2 + b^2, a + b\right) = 1$.

**Corollary 2.4.** *If $(a, b) = d$, then $(a/d, b/d) = 1$.*

*Proof.* If $(a, b) = d$ then $d = am + bn$ for some integers $m$ and $n$. Since $d|a$ and $d|b$ we have $1 = (a/d)m + (b/d)n$ and by **??** $(a/d, b/d) = 1$.

□

**Theorem 2.5.** *Let $a$ and $b$ be integers, then $(a,b)=d$ if and only if $d|a$, $d|b$, and if $c$ is another common divisor then $c|d$.*

*Proof.* If $(a,b)=d$ then by definition, $d|a$ and $d|b$. Let $c$ be a common divisor of $a$ and $b$ with $a=cx$ and $b=cy$ for some integers $x$ and $y$. By **??**, there exists $m$ and $n$ such that $d=am+bn$; and therefore we have $d=c(xm+yn)$. Whence, $c|d$.

□

**Corollary 2.5.** *If $b|ac$ and $(a,b)=1$, then $b|c$.*

*Proof.* If $b|ac$ there exists an integer $k$ such that $ac=bk$. Since $(a,b)=1$ there exists integers $m$ and $n$ such that $am+bn=1$. Then

$$c=c(1)=c(am+bn)=(ac)m+bcn=bkm+bn=b(km+cn)$$

which shows $b|c$ since $km+cn$ is an integer.

□

**Corollary 2.6.** *If $b|a$, $c|a$, and $(b,c)=1$, then $bc|a$.*

*Proof.* If $b|a$, $c|a$, and $(b,c)=1$, there exist natural numbers $s$, $t$, $m$ and $n$ with $a=sb$, $a=tc$, and $bm+nc=1$. Then

$$a=a(1)=a(bm+nc)=abm+anc=tcbm+sbnc=bc(tm+sn)$$

which shows $bc|a$ since $tm+sn$ is an natural number.

□

**Corollary 2.7.** *If $(a,bc)=1$, then $(a,b)=1$ and $(a,c)=1$; and conversely.*

*Proof.* If $(a,bc)=1$, there exists natural numbers $u$ and $v$ such that $au+bcv=1$. Since 1 is a linear combination of $a$ and $b$ and is also a linear combination of $a$ and $c$, it follows $(a,b)=1$ and $(a,c)=1$.

Conversely, if $(a,c)=1$ then $(a,b)=1$ there exists natural numbers $s$, $t$, $m$ and $n$ such that $as+bct=1$ and $am+bn=1$. Multiplying,

$$1=(as+bct)(am+bn)=a(sm+sbn+ctm)+bc(tn)$$

which shows 1 is a linear combination of $a$ and $bc$ and so $(a, bc) = 1$.

□

**Corollary 2.8.** *If* $(a, b) = 1$ *and* $c|a$*, then* $(c, b) = 1$*.*

*Proof.* If $(a, b) = 1$ and $c|a$, then there exists natural numbers $m$, $n$, and $k$ such that $am + bn = 1$ and $a = ck$. Then

$$1 = am + bn = c(km) + bn$$

which shows $(b, c) = 1$.

□

## 2.5 Euclidean Algorithm

Divide $a$ by $b$, obtaining the quotient $q_1$ and the remainder $r_1$. Then, if $r_1$ is not zero, divide $b$ by $r_1$ obtaining the quotient $q_2$ and remainder $r_2$. Then if $r_2$ is not zero then we repeat this process and divide $r_1$ by $r_2$, obtaining the quotient $q_3$ and remainder $r_3$. This process, or *algorithm*, is repeated until we first obtain the remainder of zero. At the conclusion of the process we have the greatest common divisor which is the last nonzero remainder.

The next lemma is used in the proof of the Euclidean Algorithm.

**Lemma 2.7.** *If* $a$ *and* $b$ *are positive integers. If* $a = bq + r$ *for some positive integers* $q$ *and* $r$*, then* $(a, b) = (b, r)$*.*

For example, in the case that $288 = 40(7) + 8$ we have

$$\begin{aligned} S &= \{d \in \mathbb{Z} \mid d \mid 288 \text{ and } d \mid 40\} \\ &= \{\pm 1, \pm 2, \pm 4 \pm, 8 \pm\} \end{aligned}$$

$$\begin{aligned} T &= \{d \in \mathbb{Z} \mid d \mid 40 \text{ and } d \mid 8\} \\ &= \{\pm 1, \pm 2, \pm 4 \pm, 8 \pm\} \end{aligned}$$

Clearly, $S = T$ and both sets are finite.

*Proof.* Assume $a = bq + r$. Let $S$ and $T$ be the set of common divisors of $a$ and $b$ and of $b$ and $r$, respectively; that is,

$$S = \{d \in \mathbb{Z} : d \mid a \text{ and } d \mid b\} \quad \text{and} \quad T = \{d \in \mathbb{Z} : d \mid b \text{ and } d \mid r\}.$$

Let $d \in S$. So $d$ divides $a$ and $b$ and thus divides $b$ and $r = a - bq$. Hence $d \in T$.

To show the reverse inclusion $T \supseteq S$, if $d \in T$ then $d$ divides $b$ and $r$. Then $d$ divides $a = bq + r$ and $b$, and so $d \in S$.

We have shown $S \subseteq T$ and $T \subseteq S$; and therefore, $S = T$. Since these are finite sets the greatest common divisor of $a$ and $b$ is the same as the greatest common divisor of $b$ and $r$.

□

**Example 2.8.** Find $(345688, 245994)$.

*Solution.* By the Division Algorithm,

$$\begin{aligned}
345688 &= 245994(1) + 99694 \text{ with } 0 \leq 99694 < 245994\\
245994 &= 99694(2) + 46606 \text{ with } 0 \leq 46606 < 99694\\
99694 &= 46606(2) + 6482 \text{ with } 0 \leq 6482 < 46606\\
46606 &= 6482(7) + 1232 \text{ with } 0 \leq 1232 < 6482\\
6482 &= 1232(5) + 322 \text{ with } 0 \leq 322 < 1232\\
1232 &= 322(3) + 266 \text{ with } 0 \leq 266 < 322\\
322 &= 266(1) + 56 \text{ with } 0 \leq 56 < 266\\
266 &= 56(4) + 42 \text{ with } 0 \leq 42 < 56\\
56 &= 42(1) + 14 \text{ with } 0 \leq 14 < 42\\
42 &= 14(3) + 0 \text{ with } 0 \leq 0 < 14
\end{aligned}$$

Therefore, $(345688, 245994) = 14$.

**Example 2.9.** Let $d = (328, 288)$. Find $d$ and write it as a linear combination of 328 and 288.

*Solution.* By the Division Algorithm,

$$\begin{aligned}
328 &= 288(1) + 40 \text{ with } 0 \leq 40 < 288\\
288 &= 40(7) + 8 \text{with} 0 \leq 8 < 40\\
40 &= 8(5) + 0 \text{ with } 0 \leq 8 < 40
\end{aligned}$$

Now, $d = (328, 288) = 8$ follows from

$$(328, 288) = (288, 40) = (40, 8) = (8, 0) = 8$$

by **??**. We can use the above computation to write 8 as a line recombination of 328 and 288 using back substitution:

$$\begin{aligned}8 &= 288 - 40(7)\\ 8 &= 288 - [328 - 288(1)](7)\\ 8 &= 8(288) - 7(328)\square\end{aligned}$$

One way to view the **Euclidean algorithm** is as the repeated application of the Division Algorithm and repeated application of **??**.

We can visualize the greatest common divisor. For example, a 24-by-60 rectangular area can be divided into a grid of: 1-by-1 squares, 2-by-2 squares, 3-by-3 squares, 4-by-4 squares, 6-by-6 squares or 12-by-12 squares. Therefore, 12 is the greatest common divisor of 24 and 60.

The greatest common divisor of two numbers $a$ and $b$ is the product of the prime factors shared by the two numbers, where a same prime factor can be used multiple times, but only as long as the product of these factors divides both $a$ and $b$. For example, since 1386 can be factored into $2 \times 3 \times 3 \times 7 \times 11$, and 3213 can be factored into $3 \times 3 \times 3 \times 7 \times 17$, the greatest common divisor of 1386 and 3213 equals $63 = 3 \times 3 \times 7$, the product of their shared prime factors. In particular, if two numbers have no prime factors in common, they are relatively prime.

> A important feature of the Euclidean algorithm is that it can find the gcd efficiently without having to compute the prime factors.

Factorization of large integers is believed to be a computationally very difficult problem, and the security of many modern cryptography systems is based upon its infeasibility.

Consider the question of finding the greatest common divisor of two numbers. For example, let $a = 288$ and $b = 3266$, what is $(3266, 288)$? We apply the Division Algorithm and **??** to obtain

$$3266 = 11(288) + 98 \text{ with } 0 \leq 98 < 288 \text{ and } (3266, 288) = (288, 98).$$

Again, we apply the Division Algorithm and **??** to obtain

$$288 = 2(98) + 92 \text{ with } 0 \leq 92 < 98 \text{ and } (3266, 288) = (288, 98) = (98, 92).$$

Again, we apply the Division Algorithm and **??** to obtain

$$98 = 1(92) + 6 \text{ with } 0 \leq 6 < 92 \text{ and } (3266, 288) = (92, 6) = 2.$$

We now write this process in a general format.

**Theorem 2.6.** *Let $a$ and $b$ be positive positive integers with $a \geq b$. If $b \nmid a$, then apply the division algorithm repeatedly as follows:*

*{2} & $a = bq_0 + r_0$ with $0 \leq r_0 < b$, & & $b = r_0 q_1 + r_1$ with $0 \leq r_1 < r_0$,*
*\ & $r_0 = r_1 q_2 + r_2$ with $0 \leq r_2 < r_1$, & & $r_1 = r_2 q_3 + r_3$ with $0 \leq r_3 < r_2$,*
*\ & $r_2 = r_3 q_4 + r_4$ with $0 \leq r_4 < r_3$, & & $r_3 = r_4 q_5 + r_5$ with $0 \leq r_5 < r_4$, ...*

*This process ends after a finite number of steps; that is, for some $k$:*

$$r_{k-2} = r_{k-1} q_k + r_k \text{ with } 0 \leq r_k < r_{k-1}$$

*where $r_{k-1}=r_k q_{k+1}+0 $ and $r_k = (a, b)$.*

*Proof.* The proof follows from the property: if $a = bq + r$, then $(a, b) = (b, r)$. Thus, if $b|a$, then $a = bq + 0$ and so $(a, b) = (b, 0) = b$. Notice

$$(a, b) = (b, r_0) = (r_0, r_1) = \cdots = (r_{k-2}, r_{k-1}) = (r_{k-1}, r_k) = (r_k, 0) = r_k.$$

by **??** as desired.

□

In the 19th century, the Euclidean algorithm led to the development of new number systems, such as Gaussian integers and Eisenstein integers.

# Chapter 3

# Unique Factorization

The Fundamental Theorem of Arithmetic states that every natural number greater than 1 is either a prime or a product of a finite number of primes and this factorization is unique except for the rearrangement of the factors. Before we prove the fundamental fact, it is important to realize that not all sets of numbers have this property.

For example, let us consider the set of even natural numbers, namely

$$E = \{2k \mid k \in \mathbb{Z}\}.$$

We can add, subtract, even multiply elements of $E$, and obtain elements in $E$, so we say the set $E$ is closed under addition, subtraction, and multiplication. However, this is not the set of natural numbers so we should define what we mean by divisibility; namely for any two elements of E we say $a|b$ means there exists $m \in E$ such that $b = ma$. The importance of $m \in E$ should not be overlooked. For example, $2|8$ because $8 = m(2)$ where $m = 4 \in E$. But $2 \nmid 6$ because there is no $m \in E$ such that $6 = m(2)$.

So what are some primes in $E$?

For example, 2 is prime in $E$ because there does not exist $n, m$ in $E$ such that $2 = nm$. Similarly, 6 is prime in $E$ because there does not exist $n, m$ in $E$ such that $6 = nm$. Also, 10 and 30 are primes, and so $60 = 2(30)$ is not. However since $60 = 10(6)$ we conclude that factorization into primes in $E$ is not unique.

## 3.1 Prime Characterization

Before getting to the Fundamental Theorem of Arithmetic we need an important result.

**Lemma 3.1** (Prime Characterization). *A natural number $p$ is a prime if and only if*

$$p|bc \implies (p|b \text{ or } p|c)$$

*for any natural numbers $b$ and $c$.*

*Proof.* Assume $p$ is prime and $p|bc$. Notice that, since $p$ is prime, either $(p, b) = 1$ or $(p, b) = p$. If $(p, b) = 1$, then $p|c$ by **??**.(**??**). If $(p, b) = p$ then $p|b$. In either case, $p|c$ or $p|b$.
Conversely, suppose

$$\forall\, b, c \in \mathbb{N},\ p|bc \implies p|c \text{ or } p|b. \tag{3.1}$$

To show that $p$ is prime let $d$ be a divisor of $p$.
Then $p = dt$ for some $t$. Hence, by 3.1 we have $p|d$ or $p|t$. Thus, if $t = pk$ for some $k$, then $p = dt = dpk$, and so $d = \pm 1$.
If $d = pk$ for some $k$, then $p = ptk$ and so $d = \pm p$. Therefore, the only divisors of $p$ are $d = \pm 1, \pm p$, and so $p$ is prime.

□

**Example 3.1.** Prove if $p$ is a prime number, $a_1$, $a_2$, ..., $a_n$ are natural numbers, and $p\,|a_1 a_2 \cdots a_n$ , then $p\,|a_i$ for some $1 \leq i \leq n$.

*Solution.* The statement is clearly true when $n = 1$ and $n = 2$ follows from Theorem **??**. Assume the statement is true for $n = k$, and suppose $p\,|a_1 a_2 \cdots a_k a_{k+1}$. Then by Theorem **??**, $p\,|a_1 a_2 \cdots a_k$ or $p\,|a_{k+1}$. If $p\,|a_{k+1}$, the statement is proven. If not, then by the induction hypothesis there is some $0 \leq i \leq k$ such that $p|a_i$. Therefore, there is some $0 \leq i \leq k + 1$ such that $p|a_i$ as desired.

The most basic method of checking the primality of a given integer n is called **trial division** . This method consists of dividing $n$ by each integer $m$ that is greater than 1 and less than or equal to the square root of $n$. If the result of any of these divisions is an integer, then $n$ is not a prime, otherwise it is a prime. For example, for $n = 37$, the trial divisions are by $m = 2, 3, 4, 5,$ and 6. None of these numbers divides 37, so 37 is prime.

**Lemma 3.2.** *Every natural number greater than 1 is a product of primes.*

*Proof.* Consider the set $S$ consisting of all positive natural numbers greater than 1 that are not a product of primes. Assume for a contradiction that $S$ is not empty, then by the Well-Ordering Axiom there is a least element, say $m$. Because $m$ has no prime divisors and $m$ divides $m$, we see that $m$ is not prime.
Thus, $m = ab$ where $1 < a < m$ and $1 < b < m$. Since $m$ is the least element in $S$, $a$ and $b$ are products of primes; and thus so is $m$.
This contradiction shows that $S$ is empty and so every natural number greater than 1 is a product of primes.

□

## 3.2 Fundamental Theorem of Arithmetic

The **Fundamental Theorem of Arithmetic**, also called the **unique factorization theorem** or the unique-prime-factorization theorem, states that every integer greater than 1 is either is prime itself or is the product of prime numbers, and that, although the order of the primes in the second case is arbitrary, the primes themselves are not.

**Theorem 3.1** (Fundamental Theorem of Arithmetic)**.** *Every natural number greater than 1 can be written uniquely in the form*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \tag{3.2}$$

*where $p_1 < p_2 < \cdots < p_k$ are prime numbers and $e_1, e_2, ..., e_k$ are natural numbers.*

*Proof.* Every natural number has a prime factorization by Theorem **??**. Thus existence is proven. Now we prove uniqueness. If there is an natural number greater than 1 for which the factorization is not unique, then by the Well-Ordering Axiom there exists a smallest such natural number, say $m$. Assume that $m$ has two prime factorizations say

$$m = {p_1}^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \qquad \text{and} \qquad m = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t},$$

where

$$p_1 < p_2 < \cdots < p_s \qquad q_1 < q_2 < \cdots < q_t$$

and the $\alpha_i$ and $\beta_j$ are all positive for $0 \le i \le s$ and $0 \le j \le t$. By Theorem **??**,

$$q_1 \mid p_{i^*} \text{ for some } 1 \le i^* \le s \qquad \text{and} \qquad p_1 \mid q_{j^*} \text{ for some } 1 \le j^* \le t.$$

Since all the numbers $p_i$ and $q_j$ are prime, we must have $q_1 = p_{i^*}$ and $p_1 = q_{j^*}$. Then $i^* = j^* = 1$ since

$$q_1 \le q_{j^*} = p_1 \le p_{i^*} = q_1.$$

Let $u$ be the natural number defined as

$$u = \frac{m}{p_1} = \frac{m}{q_1} = {p_1}^{\alpha_1 - 1} {p_2}^{\alpha_2} \cdots {p_s}^{\alpha_s} = {q_1}^{\beta_1 - 1} {q_2}^{\beta_2} \cdots {q_t}^{\beta_t}.$$

If $u = 1$, then $m = p_1$ has a unique factorization contrary to hypothesis. If $u > 1$, then $u < m$ and $u$ has two factorizations. Both cases reveal that $m$ can not exist as desired.

□

**Example 3.2.** Show there are infinitely many primes of the form $4n+3$.

*Solution.* First notice that the product of any two natural numbers of the form $4n+1$ also has the form $4n+1$ which can be seen by letting $a = 4s+1$ and $b = 4r+1$ where $s$ and $r$ are natural numbers, then

$$ab = (4s+1)(4r+1) = 16rs + 4r + 4s + 1 = 4(4rs + r + s) + 1.$$

We assume there are only a finite number of primes of the form $4k+3$, say $p_0 = 3, p_1, ..., p_n$ is all of them; and we consider the natural number

$$Q = 4p_1 p_2 \cdots p_n + 3.$$

Notice that the prime factorization of $Q$, namely $Q = q_1 \cdots q_t \cdots q_m$ must contain at least one prime of the form $4k+3$ because otherwise $Q$ would be of the form $4k+1$. Thus, there is one prime in the prime factorization of $Q$ that is of the form $4k+3$ say $q_t$. Either $q_t = 3$ or $q_t > 3$. If $q_t = 3$, then $3|Q$ which means $3|(Q-3)$ and so $3\,|4p_1 \cdots p_n$ which is absurd. If $q_t > 3$, then $q_t = p_j$ for some $1 \leq j \leq n$ and so $q_t|\,Q$ implies $q_t | Q - 4p_1 \cdots p_n = 3$, which is also absurd. Therefore, there are infinitely many primes of the form $4n+3$.

**Definition 3.1.** The **least common multiple** of two nonzero natural numbers $a$ and $b$ is the smallest positive natural number that is divisible by $a$ and $b$.

The least common multiple of 15 and 21 is $[15, 21] = 105$. The least common multiple of 24 and 36 is $[24, 36] = 72$. The least common multiple of 2 and 20 is $[2, 20] = 20$. The least common multiple of 7 and 11 is $[7, 11] = 77$.

**Corollary 3.1.** *Let $a$ and $b$ be natural numbers. Then*

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_n^{\min(\alpha_1, \beta_1)} \tag{3.3}$$

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_n^{\max(\alpha_1, \beta_1)}. \tag{3.4}$$

*Proof.* By the Fundamental Theorem of Arithmetic is the ability to find the greatest common divisor and least common multiple from a factorization of two given natural numbers. Say we are given $a$ and $b$, and we are able to find the unique factorization of each (and assume that all exponents are nonnegative and the $p_i$ are all primes in both $a$ and $b$), namely

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \qquad \text{and} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}$$

then because for each prime $p_i$, in $a$ and $b$ have exactly $\min(\alpha_i, \beta_i)$ factors of $p_i$ in common; and

□

**Example 3.3.** Find the unique prime factorization of $m = 4463914455$ and $n = 8125921375$. Then factor $m$ and $n$ into a product of primes with the same set of primes with (possibly zero) nonnegative exponents.

*Solution.* Notice $4463914455 = 3^4 \cdot 5 \cdot 7^2 \cdot 11^3 \cdot 13^2$ and $8125921375 = 5^3 \cdot 11^3 \cdot 13^2 \cdot 17^2$. Thus the set of primes in both natural numbers is $\{3, 5, 7, 11, 13, 17\}$ and so we have

$$\begin{aligned} 4463914455 &= 3^4 \cdot 5 \cdot 7^2 \cdot 11^3 \cdot 13^2 \cdot 17^0 \\ 8125921375 &= 3^0 \cdot 5^3 \cdot 7^0 \cdot 11^3 \cdot 13^2 \cdot 17^2 . \square \end{aligned}$$

## 3.3 GCD and LCM

**Corollary 3.2** (Product of GCD and LCM)**.** *If $a$ and $b$ are integers, then*

$$(a, b)[a, b] = ab. \tag{3.5}$$

*Proof.* Let $a$ and $b$ have unique prime factorizations; namely

$$a = p_1^{u_1} p_2^{u_2} \cdots p_n^{u_n} \qquad \text{and} \qquad b = q_1^{v_1} q_2^{v_2} \cdots q_m^{v_m} .$$

Now we can form the set of primes $P_1, ..., P_k$ consists of all the $p_1, p_2, ..., p_n$ and $q_1, q_2, ..., q_m$. So we can write

$$a = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_n^{\alpha_n} \qquad \text{and} \qquad b = P_1^{\beta_1} P_2^{\beta_2} \cdots P_m^{\beta_m}$$

where the exponents are zero where necessary. Now let $X_i = \max(\alpha_i, \beta_i)$ and $x_i = \min(\alpha_i, \beta_i)$ . Then

$$[a, b](a, b) = P_1^{X_1 + x_1} P_1^{X_1 + x_1} \cdots P_n^{X_1 + x_1} = ab.$$

as desired.

□

**Example 3.4.** Prove that, if $a, b$, and $c$ are natural numbers, then

$$[a, b] | c \text{ if and only if } a | c \text{ and } b | c. \tag{3.6}$$

*Solution.* Suppose $[a, b]|c$. Since $a|[a, b]$ and $b|[a, b]$ it follows that $a|c$ and $b|c$. Conversely, suppose $a|c$ and $b|c$. Using prime factorization we can write

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}, \qquad b = p_1{}^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}, \qquad c = p_1^{c_1} \cdot p_2^{c_2} \cdots p_n^{c_n}.$$

Then $\max(a_i, b_i) \leq c_i$ for $i = 1, 2, ..., n$ because $a|c$ and $b|c$. Hence, $[a, b] \mid c$.

Let $p$ be a prime and $n$ a positive integer. If $p^a | n$ but $p^{a+1} \nmid n$, we say that $p^a$ exactly divides $n$ and we write $p^a \| n$.

**Example 3.5.** Prove that, if $a$ and $b$ are positive natural numbers, then

$$(a, b) = (a + b, [a, b]). \tag{3.7}$$

*Solution.* Let $p$ be a prime that divides $a$ or $b$. Then $p$ divides $a + b$ and $[a, b]$. Hence $p$ divides both sides of 3.7. Define, $s$ and $t$ by $p^s \| a$ and $p^t \| b$, say $a = xp^s$ and $b = yp^t$. Without loss of generality, suppose $s \leq t$. Then

$$a + b = p^s \left(x + p^{t-s}\right),$$

so $p^s \| (a + b)$. Also, $p^{\max(s,t)} \| [a, b]$. But $\max(s, t) = t$, so $p^t \| [a, b]$. Therefore,

$$p^{\min(s,t)} \| (a + b, [a, b]).$$

But $\min(s, t) = s$, so the same power of $p$ divides both sides of 3.7. Therefore, the two sides of 3.7 must be equal.

# Chapter 4

# Congruence Equations

## 4.1 Introduction to Congruence

In “Linear Congruence Equations (Fundamental Concepts and Principles)“, the author takes the reader on a comprehensive tour of linear congruence equations and their many applications. The book is ideal for students who want to deepen their knowledge of mathematics as well as professionals who need to use linear congruence equations in their work. It provides a clear and concise explanation of the concepts underlying linear congruence equations, making it an essential resource for anyone looking to understand this important topic.

Congruence in the integers means that two numbers are equivalent if their difference is a multiple of a certain number, called the modulus. In other words, we can say that two numbers are congruent modulo m if they have the same remainder when divided by m. For example, 17 and 29 are Congruent modulo 4 because the remainders when we divide them by 4 are 1 and 1 respectively.

Congruence is an equivalence relation, which means that it satisfies the three properties of reflexivity, symmetry, and transitivity. There are also several lemmas about congruence which we will now state without proof. The first one says that if a is congruent to b modulo m and c is congruent to d modulo m then a+c is congruent to b+d modulo m.

The second lemma states that if a is congruent to b modulo m and c is any integer then a+c is congruent to b+c modulo m. The third and final lemma says that if a is congruent to b modulo m then ac is congruent to bc modulo m. These lemmas show that congruent behaves nicely with addition, subtraction, and multiplication and so it should be clear why it is such a useful concept.

Modular arithmetic is a system that involves the remainders of the division of certain numbers. It is often referred to as “clock arithmetic” because of its similarity to how hours are measured on a clock. The numbers in modular arithmetic are called “objects” and the remainders are called “residues”. The concept of modular arithmetic can be difficult to grasp at first, but it is actually quite simple.

In many applications, it is important to know not only the value of x modulo n, but also its least positive residue. For example, in computer science, when working with very large numbers that are too large to fit into a single data type, it is often necessary to store only the least significant digits of the number; and when performing arithmetic operations on such numbers, it is often necessary to reduce them modulo some number n that is a power of two (such as $216 = 65536$), so that they can be stored in a smaller data type. In both cases, it suffices to know only the least positive residue of x modulo n.

In this chapter, we explain what congruence (modular arithmetic) is in the integers. We also provide some examples to illustrate how it works. Least positive residues are an important part of understanding modular arithmetic. We hope that by the end of this chapter, you will have a good understanding of both least positive residues and congruence in the integers.

In mathematics, modular arithmetic is a system that allows numbers to be divided into congruent classes. This means that the remainders of two numbers when divided by a third number are the same. For example, when we divide 7 by 3, the remainder is 1; when we divide 8 by 3, the remainder is 2; and when we divide 9 by 3, the remainder is 0. In modular arithmetic, these three numbers would be said to be congruent modulo 3.

Modular arithmetic is particularly useful in computer science because it can be used to represent data in a more efficient way. For example, instead of storing the full date (December 21st, 2015), a computer can store just the day of the month (21) and the year (2015). This is possible because we know that there are only 31 days in December, so the modular arithmetic system allows us to store the information more efficiently.

Overall, modular arithmetic is a powerful tool that can be used in a variety of ways. It is particularly useful for computer science applications, but it can also be used for other purposes as well.

In this chapter, we will explain what congruence (modular arithmetic) in the integers is and how it works.

Linear congruence is an equation that produces a set of integers that are evenly spaced apart. The equation has the form $ab \equiv 1 \pmod{n}$, where a, b, and n are integers and $n > 0$. Linear congruence equations are very powerful tools that can be used to solve various mathematical problems.

In fact, they are so versatile that they have even been used to crack codes!

One way to solve for x is to find the modular inverse of a modulo m. This can be done using the Extended Euclidean Algorithm. Once the modular inverse is found, it can be plugged into the equation to solve for x.

The Euclidean algorithm is a fast and straightforward way to solve these equations. Given an equation $ax \equiv b \pmod{m}$, we can use the Euclidean algorithm to find a solution in just a few steps. First, we find the greatest common divisor of a and m using the Euclidean algorithm. Then, we divide b by this greatest common divisor to get an integer c. Finally, we use the Extended Euclidean algorithm to find a number d such that $ad \equiv 1 \pmod{m}$. Plugging in these values for x in our original equation gives us the solution: $x \equiv cd \pmod{m}$. By using the Euclidean algorithm, we can quickly and easily solve linear congruence equations.

Linear congruence equations are a powerful tool that can be used to solve many different types of problems. With a little practice, anyone can learn how to use them.

These equations have a solution if and only if a and m are relatively prime. If an equation has a solution, then all solutions can be found by repeated addition of m to any one solution. In particular, if x is a solution of the equation, then so are x + km for any integer k. The set of all solutions of the equation is called the residue class of x (modulo m).

In this chapter, you'll learn that two numbers in the same residue class modulo m give the same remainder when divided by m. For example, 7 and 17 are in the same residue class modulo 6 because they both leave the same remainder, 1, when divided by 6. On the other hand, 14 is not in this residue class because it leaves a different remainder, 2, when divided by 6.

Linear Congruence Equations are useful in many situations, including finding the inverse of an integer with modular arithmetic. If we have an integer a such that there is no integer b for which $ab \equiv 1 \pmod{m}$, then there is no inverse of a (modulo m). However, if $ab \equiv 1 \pmod{m}$, then a has an inverse modulo m, and this inverse is given by b.

Thus, to find the inverse of an integer with modular arithmetic, we must first determine whether or not it has an inverse. We can do this by solving a linear congruence equation. In summary, in this chapter, you'll learn that linear congruence equations are both necessary and sufficient for finding the inverse of an integer with modular arithmetic.

This book is a comprehensive guide to understanding linear congruence equations and their various applications. It is ideal for students who are looking to further their knowledge of mathematics and for professionals who need to use linear congruence equations in their work. The author takes the reader on a clear and concise tour of the concepts underlying linear congruence equations, making it an essential resource for anyone looking to understand this important topic. I highly recommend this book to anyone interested in learning more about linear congruence equations.

## 4.2 Introduction to Congruence

A modern treatment of congruences was introduced by Karl Friedrich Gauss. Congruence, or modular arithmetic, arises naturally in common everyday situations. For example, odometers usually work modulo 100,000 and utility meters often operate modulo 1000. In trigonometry, it is common to work in degrees, that is modulo 360 degrees, and indeed, it is common to work in minutes and seconds both of which are working modulo 60.

**Definition 4.1.** Let $n$ be a positive integer. Integers $a$ and $b$ are **congruent modulo** $n$ if $a - b$ is divisible by $n$ and is denoted by $a \equiv b \pmod{n}$.

Notice $24 \equiv 4 \pmod{5}$ since $5|(24-4)$ but $24 \not\equiv 3 \pmod{5}$ since $5 \mid (24-3)$ does not hold. Also, $111 \equiv 9 \pmod{40}$ since $40|(111-9)$ and $111 \not\equiv 8 \pmod{40}$ since $40 \mid (111-8)$ does nto hold.

Next we show that congruence modulo $n$ is an equivalence relation on the set of integers.

**Theorem 4.1.** *For each positive integer $n$, congruence modulo $n$ is an equivalence relation on the set of integers.*

*Proof.* If $a$ is an integer, then $a \equiv a \pmod{n}$ since $n|(a-a)$ and so $\equiv$ is reflexive. If $a$ and $b$ are integers and $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$ since $n|(b-a) \iff n|(a-b)$ and so the relation $\equiv$ is symmetric. If $a, b$ and $c$ are integers, $a \equiv b \pmod{n}$, and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$ because $n|(b-a)$ and $n|(c-b)$ implies $n|(a-c)$ and so the relation $\equiv$ is also transitive.

□

**Theorem 4.2.** *If $a$ and $b$ are integers, then $a \equiv b \pmod{n}$ if and only if there exists an integer $k$ such that $a = b + kn$.*

*Proof.* If $a \equiv b \pmod{n}$, then $n|(a-b)$ and this means there exists an integer $k$ such that $kn = a - b$ and so $a = b + kn$. Conversely, if there is an integer $k$ such that $a = b + kn$, then $n|(a-b)$; and so $a \equiv b \pmod{n}$.

□

**Lemma 4.1.** *For all integers $a$, $b$, $c$, and $d$, if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a \pm b \equiv c \pm d \pmod{n}$ and $ab \equiv cd \pmod{n}$.*

*Proof.* If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $n|a-c$ and $n|b-d$. It follows that, $n|(a \pm b) - (c \pm d)$ and thus $a \pm b \equiv c \pm d \pmod{n}$. It also follows that, $n|(ab-cb)$ and $n|(cb-cd)$; thus $n|(ab-cd)$. Therefore, $ab \equiv cd \pmod{n}$.

□

**Lemma 4.2.** *For all integers $a$, $c$, and $d$, if $a+c \equiv a+d \pmod{n}$, then $c \equiv d \pmod{n}$.*

*Proof.* If $a+c \equiv a+d \pmod{n}$, then $n|(a+c)-(a+d)$ and so $n|c-d$ which means $c \equiv d \pmod{n}$.

□

**Lemma 4.3.** *For all integers $a$, $c$, and $d$, if $ac \equiv ad \pmod{n}$ and $(a,n) = 1$, then $c \equiv d \pmod{n}$.*

*Proof.* If $ac \equiv ad \pmod{n}$, then $n|(ac-ad)$ which means $n|a(c-d)$. Since $(a,n) = 1$, it follow that $n|(c-d)$ and so $c \equiv d \pmod{n}$.

□

**Lemma 4.4.** *For all integers $a$, there exists an integer $h$ such that $ah \equiv 1 \pmod{n}$ if and only if $(a,n) = 1$.*

*Proof.* If $(a,n) = 1$, then there exists integers $s$ and $t$ such that $sa+tn = 1$. Let $h = s$, then $ah \equiv 1 \pmod{n}$ as desired. Conversely, if there is such a $h$ then $ah = 1+qn$ for some $q$. Thus, $ah+(-q)n = 1$ and so $(a,n) = 1$.

□

**Lemma 4.5.** *For all integers $a$, $b$, and $c$, if $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/(c,n)}$.*

*Proof.* If $ac \equiv bc \pmod{n}$, we know that $n|(ac - bc) = c(a - b)$. Thus there exists an integer $k$ such that $c(a - b) = kn$ and dividing both sides by $d = (c, n)$, we have $(c/d)(a - b) = k(n/d)$. Because $(n/d, c/d) = 1$ it follows that $(n/d)|(a - b)$. Therefore, $a \equiv b \pmod{n/(c, n)}$.

□

**Lemma 4.6.** *For all integers $a$ and $b$, if $k, n > 0$ and $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.*

*Proof.* Because $a \equiv b \pmod{n}$ we have by definition, $n|(a - b)$ and since

$$a^k - b^k = (a - b)\left(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}\right)$$

we see that $(a - b)\left|\left(a^k - b^k\right)\right.$; whence $n\left|\left(a^k - b^k\right)\right.$. Therefore, $a^k \equiv b^k \pmod{n}$.

□

**Definition 4.2.** Given a modulus $n$ and an integer $a$ the **least positive residue** of $a$ modulo $n$ is the smallest positive integer $r$ such that $a \equiv r \pmod{n}$.

For example, the remainder of $n$ when divided by 9 is the same as the remainder of the sum of its digits when divided by 9 which follows from writing $n = d_t 10^t + d_{t-1}10^{t-1} + ... + d_1 10 + d_0$ where $0 \leq d_i \leq 9$ by noting that $10^k \equiv 1 \pmod{9}$ for any $k$. Notice also that the remainder of $n$ when divided by 11 is the same as the remainder of the alternating sum of its digits when divided by 11 which follows from writing $n$ in decimal form and noting that $10^k \equiv (-1)^k \pmod{11}$ for any $k$.

Let $\{0, 1, 2, ..., n - 1\}$ be a complete set of on $\mathbb{Z}$ for congruence modulo $n$, then define $\mathbb{Z}_n$:=$\{[1], [2], [3], ..., [n - 1]\}$ and define the operation $+$ on $\mathbb{Z}_n$ by $[a] + [b] = [a + b]$. Arithmetic using this operation is referred to as **equivalence class representatives} on $\mathbb{Z}$ for congruence modulo $n$, then define $\mathbb{Z}_n$:=$\{[1], [2], [3], ..., [n - 1]\}$ and define the operation $+$ on $\mathbb{Z}_n$ by $[a] + [b] = [a + b]$. Arithmetic using this operation is referred to as \index{modular arithmetic** .

The operation $+$ is a well-defined binary operation; meaning, if $[a] = [b]$ and $[c] = [d]$ in $\mathbb{Z}_n$, then $[a] + [b] = [a + b] = [c + d] = [c] + [d]$ which follows from $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$.

For example, the arithmetic tables for $\mathbb{Z}_6$ are

| $+$ | 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 |

| $\times$ | 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 | 4 | 1 | 2 |
| 4 | 0 | 4 | 2 | 0 | 1 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

**Theorem 4.3.** *Let $n$ be a positive integer, then $+$ is associative and commutative, each element has an inverse, and $[0]$ is the identity element.*

*Proof.* By the definition of $+$ and the use of associativity in the integers, it follows that

$$\begin{aligned}[a] + ([b] + [c]) = [a] + [b + c] &= [a + (b + c)] = [(a + b) + c] \\ &= [a + b] + [c] = ([a] + [b]) + [c]\end{aligned}$$

for any $[a]$, $[b]$, and $[c] \in \mathbb{Z}_n$. The element $[0]$ is the identity because

$$[a] + [0] = [a + 0][a]$$

for any $[a] \in \mathbb{Z}_n$. For every element $[a]$ of $\mathbb{Z}_n$ there is an inverse because

$$[a] + [-a] = [a + (-a)] = [0]$$

and indeed $[-a] \in \mathbb{Z}_n$. Commutativity follows since

$$[a] + [b] = [a + b] = [b + a] = [b] + [a]$$

for $[a]$, $[b] \in \mathbb{Z}_n$.

□

**Theorem 4.4.** *Let $n$ be a positive integer. Then a complete set of equivalence class representatives on $\mathbb{Z}$ for congruence modulo $n$ is $\{0, 1, 2, ..., n - 1\}$.*

*Proof.* Given an integer $x$, the Division Algorithm yields unique integers $q$ and $r$ such that $x = nq + r$ and $0 \leq r < n$. Then $x \equiv r \pmod{n}$ and so $x$ is congruent to at least one of $\{0, 1, 2, .., n - 1\}$. In fact $r$ is unique because otherwise, say $x \equiv s \pmod{n}$ and $x = nt + s$ with $0 \leq s < n$ for some $t$, would contradict the uniqueness of the Division Algorithm.

□

## 4.3 Linear Diophantine Equations

In the following Diophantine equations, $x$, $y$, and $z$ are the unknowns and the other letters are given constants.

$$ax + by = 1 \tag{4.1}$$

This is a linear Diophantine equation.

$$x^n + y^n = z^n \tag{4.2}$$

For n = 2 there are infinitely many solutions (x,y,z): the Pythagorean triples. For larger integer values of n, Fermat's Last Theorem states there are no positive integer solutions $(x, y, z)$.

$$x^2 - ny^2 = \pm 1 \tag{4.3}$$

This is Pell's equation, which is named after the English mathematician John Pell. It was studied by Brahmagupta in the 7th century, as well as by Fermat in the 17th century.

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \tag{4.4}$$

The Erdos-Straus conjecture states that, for every positive integer n ? 2, there exists a solution in x, y, and z, all as positive integers. Although not usually stated in polynomial form, this example is equivalent to the polynomial equation $4xyz = yzn + xzn + xyn = n(yz + xz + xy)$.

The term **Diophantine equation** usually refers to any equation in one or more unknowns that is to be solved in the integers.

The simplest kind of Diophantine equation is the **linear Diophantine equation** , namely $ax+by = c$. In general, Diophantine equations furnish a natural vehicle for puzzles and problems of a mathematical nature.

**Theorem 4.5** (Linear Diophantine Equation)**.** *The linear Diophantine equation $ax + by = c$ has a solution if and only if $d|c$, where $d = (a, b)$. Moreover, if $(x_0, y_0)$ is a solution, then the set of solutions of the equation consists of pairs $(x, y)$ where*

$$x = x_0 + \frac{tb}{d} \qquad \textit{and} \qquad y = y_0 - \frac{ta}{d} \tag{4.5}$$

*and $t$ is an arbitrary integer.*

*Proof.* Since $d = (a, b)$ there exists integers $m$ and $n$ such that $am + bn = d$. Since $d|c$ we have an integer $k$ such that $c = dk$ and thus we have $(am + bn)k = dk$. Thus, $a(mk) + b(nk) = c$ and so we have a solution.

Conversely, suppose $ax + by = c$ has a solution say $x_1$ and $y_1$. Then $ax_1 + by_1 = c$ and since $d|a$ and $d|b$ we have $d|c$. Let $x_0$ and $y_0$ be any solution. Then we have $ax_0 + by_0 = c$ and so

$$ax_0 + \frac{tab}{d} + by_0 - \frac{tab}{d} = c$$

for any integer $t$. Therefore, 4.5 holds for any integer $t$.

It remains to show that all solutions $(x, y)$ have the correct form. Let $(x, y)$ be an arbitrary solution and let $(x_0, y_0)$ be any particular solution. Then we have $a\left(x - x_0\right) + b\left(x - x_0\right) = 0$ and thus $a\left(x - x_0\right) = b\left(y_0 - y\right)$. Now enter $d$. Dividing by $d$, we have

$$\frac{a}{d}\left(x - x_0\right) = \frac{b}{d}\left(y_0 - y\right).$$

Observe that

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

and so $\frac{a}{d} \mid \left(y_0 - y\right)$. Therefore, there exists an integer $s$ such that $y = y_0 - \left(\frac{a}{d}\right) s$ and by substitution, $x = x_0 + \left(\frac{b}{d}\right) s$ as desired.

□

While solving linear Diophantine equations are straightforward, this is not true for general Diophantine equations. In 1900, in recognition of their depth, David Hilbert proposed the solvability of all Diophantine problems as the tenth of his celebrated problems. In 1970, a novel result in mathematical logic known as Matiyasevich's theorem settled the problem negatively: in general Diophantine problems are unsolvable.

Using **??** we can check if a linear Diophantine equations is solvable and if solvable, actually find its solutions. The key ingredient is finding a particular solution is the Euclidean algorithm.

**Example 4.1.** Solve the linear Diophantine equation $14x + 34y = 90$.

*Solution.* Since $(14, 34) = 2$ and $2|90$. There is a solution and they are all given by 4.5 and so we need to find an initial solution. Since an initial solution is $x = 4$ and $y = 1$ we have all solutions \$x=4+17 t \$ and $y = 1 - 7t$ where $t \in \mathbb{Z}$.

**Example 4.2.** Solve the linear Diophantine equation $14x + 35x = 91$.

*Solution.* Since $(14, 35) = 7$ and $7|91$ the equation is solvable.
Since an initial solution is $x = 4$ and $y = 1$ we have all solutions $x = 4+2t$ and $y = 1 - 5t$ where $t \in \mathbb{Z}$.

**Example 4.3.** Solve the linear Diophantine equation $14x + 36y = 93$.

*Solution.* Since $(14, 36) = 2$ and $2 \nmid 93$ there are no solution to the linear Diophantine equation $14x + 36y = 93$..

**Corollary 4.1.** *If $(a, b) = 1$ and if $x_0$ and $y_0$ is a particular solution of the linear Diophantine equation $ax + by = c$, then all solutions are given by $x = x_0 + bt$ and $y = y_0 - at$ for integral values of $t$.*

*Proof.* The proof follows mediately from **??**.

□

For example, the equation $5x + 22y = 18$ has $x_0 = 8$, $y_0 = -1$ as one solution and so a complete solution is given by $x = 8+22t$ and $ y=-1-5t$ for arbitrary integral values of $t$.

A problem in Diophantus' **Arithmetica** is to find four natural numbers whose sums by three are 20, 22, 24, and 27. Can you find these four integers?

**Theorem 4.6** (General Linear Diophantine Equation)**.** *If $a_1, a_2, \dots, a_n$ are nonzero positive integers, then the equation*

$$a_1x_1 + \cdots + a_nx_n = c$$

*has an integral solution if and only if $d = (a_1, \dots, a_n)$ divides $c$. Furthermore, when there is a solution, there are infinitely many solutions.*

*Proof.* The proof is left for the reader.

□

**Example 4.4.** Which combinations of pennies, dimes, and quarters have a total value of 99 cents.

Diophantus made important advances in mathematical notation, becoming the first person known to use algebraic notation and symbolism. Before him everyone wrote out equations completely. Diophantus introduced an algebraic symbolism that used an abridged notation for frequently occurring operations, and an abbreviation for the unknown and for the powers of the unknown.

*Solution.* Let $x, y$, and $z$ be the number of pennies, dimes, and quarters, respectively. To solve this question we will solve the linear Diophantine equation: $x + 10y + 25z = 99$. Since $x, y$, and $z$ are all positive integers, it follows that $z = 0, 1, 2, 3$; and so we can solve the 4 corresponding equations in only $x$ and $y$. First, we solve $x + 10y = 99$. Clearly, $x_0 = 99$ and $y_0 = 0$ is a particular solution and since $(1, 10) = 1$ all solutions are given by $x = 99 + 10t$ and $y = 0 - t$. By letting $t$ range from 0 to $-9$, we find some combinations of pennies, dimes, and quarters that total 99 cents:

| $x$ | 99 | 89 | 79 | 69 | 59 | 49 | 39 | 29 | 19 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $y$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| $z$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $t$ | 0 | $-1$ | $-2$ | $-3$ | $-4$ | $-5$ | $-6$ | $-7$ | $-8$ | $-9$ |

Next, we solve $x + 10y = 74$. Clearly, $x_0 = 74$ and $y_0 = 0$ is a particular solution and since $(1, 10) = 1$ all solutions are given by $x = 74 + 10t$ and $y = 0 - t$. By letting $t$ range from 0 to $-7$, we find more combinations of pennies, dimes, and quarters that total 99 cents:

| $x$ | 74 | 64 | 54 | 44 | 34 | 24 | 14 | 4 |
|---|---|---|---|---|---|---|---|---|
| $y$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| $z$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $t$ | 0 | $-1$ | $-2$ | $-3$ | $-4$ | $-5$ | $-6$ | $-7$ |

Next, we solve $x + 10y = 49$. Clearly, $x_0 = 49$ and $y_0 = 0$ is a particular solution and since $(1, 10) = 1$ all solutions are given by $x = 49 + 10t$ and $y = 0 - t$. By letting $t$ range from 0 to $-4$, we find more combinations of pennies, dimes, and quarters that total 99 cents:

| $x$ | 49 | 39 | 29 | 19 | 9 |
|---|---|---|---|---|---|
| $y$ | 0 | 1 | 2 | 3 | 4 |
| $z$ | 2 | 2 | 2 | 2 | 2 |
| $t$ | 0 | $-1$ | $-2$ | $-3$ | $-4$ |

| $x$ | 24 | 14 | 4 |
|---|---|---|---|
| $y$ | 0 | 1 | 2 |
| $z$ | 2 | 2 | 2 |
| $t$ | 0 | $-1$ | $-2$ |

Finally, we solve $x + 10y = 24$. Clearly, $x_0 = 24$ and $y_0 = 0$ is a particular solution and since $(1, 10) = 1$ all solutions are given by $x = 49 + 10t$ and $y = 0 - t$. By letting $t$ range from 0 to $-2$, we find even more combinations of pennies, dimes, and quarters that total 99 cents.

## 4.4 Exercises

**Exercise 4.1.** Solve the linear Diophantine equation by either finding all solutions or by showing there are none.

- $3x + 4y = 7$
- $17x + 13y = 100$
- $30x + 47y = -11$
- $25x + 95y = 970$
- $102x + 1001y = 1$
- $7x + 21y + 35z = 8.$
- $6x + 51y = 22$
- $33x + 14y = 115$
- $14x + 35y = 93$
- $56x + 72y = 40$
- $24x + 138y = 18$
- $221x + 35y = 11$
- $18x + 5y = 48$
- $54x + 21y = 906$
- $158x - 57y = 7$
- $41x - 51y = 223$

**Exercise 4.2.** Solve the linear Diophantine equation

$$7101x + 102y + 103z = 1$$

by either finding all solutions or by showing there are none.

**Exercise 4.3.** A grocer order apples and oranges at a total cost of \$8.39. If apples cost him 25 cents each and oranges cost him 18 cents each, how many of each type of fruit did he order?

**Exercise 4.4.** A postal clerk has only 14 cents and 21 cent stamps to sell. What combination of these may be used to mail a package requiring postage of exactly \$4.00.

**Exercise 4.5.** Divide 100 into two summands such that one is divisible by 7 and the other by 11.

**Exercise 4.6.** Is it possible to have 50 coins, all of which are pennies, dimes, or quarters, with a total worth 3 dollars.

**Exercise 4.7.** When Mr. Smith cached a check at his bank, the teller mistook the number of cents for the number of dollars and vice versa. Unaware of this, Mr. Smith spent 68 cents and then noticed to his surprise that he had twice the amount of the original check. Determine the smallest value for which the check could have been written.

**Exercise 4.8.** Divide 100 into two summands such that one is divisible by 7 and the other by 11.

**Exercise 4.9.** A man has 5 diamonds, 8 rubies, 7 sapphires, and 83 gold coins; a second man has 7,9,6, and 74 of these items, respectively; a third man has 3, 13, 11, and 80. If the collections are considered equally valuable, how many gold coins is each diamond, ruby, and sapphire writ?

**Exercise 4.10.** Solve the linear Diophantine equation, $714x+7007y = 7$.

**Exercise 4.11.** Solve the linear Diophantine equation by either finding all solutions or by showing there are none for $17x + 13y = 100$.

**Exercise 4.12.** Solve the linear congruence $5x \equiv 7(\text{mod} 57)$ using basic properties of congruence (no linear Diophantine equation). Show all your steps.

**Exercise 4.13.** Explain why the linear Diophantine equation $2x-101y = 82$ is solvable or not solvable. If possible find all solutions.

**Exercise 4.14.** Solve the linear congruence $5x \equiv 15(\text{mod} 35)$ by solving a linear Diophantine equation. Show all your steps.

**Exercise 4.15.** Solve the congruence $3x \equiv 5(\text{mod} 16)$ by writing a linear Diophantine equation and solving it.

**Exercise 4.16.** Show that the sum of two even or two odd integers is even and also show that the sum of an odd and an even is odd.

**Exercise 4.17.** Show that the product of two odd integers is odd and also show that the product of two integers is even if either or one of them is even.

**Exercise 4.18.** Show that if $a$ and $b$ are positive integers and $a|b$, then $a \leq b$.

**Exercise 4.19.** Show that if $a$ is an integer, then 3 divides $a^3 - a$.

**Exercise 4.20.** Show that the square of every of odd integer is of the form $8k + 1$.

**Exercise 4.21.** Show that the product of every two integers of the form $6k + 5$ is of the form $6k + 1$.

**Exercise 4.22.** Find the number of positive integers not exceeding 1000 that are divisible by 3 but not by 4.

**Exercise 4.23.** Show that any integer of the form $6k + 5$ is also of the form $3j + 2$, but not conversely.

**Exercise 4.24.** Prove that if $a$ ad $b$ are integers, with $b > 0$, then there exists unique integers $q$ and $r$ satisfying $a = bq + r$, where $2b \leq r < 3b$.

**Exercise 4.25.** Extend the Division Algorithm by allowing negative divisors. Specifically, prove that whenever $a$ and $b \neq 0$ are integers, there are unique integers $q$ and $r$ such that $a = bq + r$, where $0 \leq r < |b|$.

**Exercise 4.26.** Prove that the square of any integer is either of the form $3k$ or $3k + 1$.

**Exercise 4.27.** Prove that the cube of any integer has one of the forms: $9k$, $9k + 1$, $9k + 8$.

**Exercise 4.28.** Prove that the cube of any integer has one of the forms: $7k$, $7k+1$, $7k-1$.

**Exercise 4.29.** Prove that the fourth power of any integer is either of the form $5k$ or $5k+1$.

**Exercise 4.30.** Let $a$ and $b$ be positive integers. Prove if $a|b$, then $a^n|b^n$ for any positive integer $n$.

**Exercise 4.31.** Use mathematical induction to show that $n^5-n$ is divisible by 5 for every positive integer $n$.

**Exercise 4.32.** Prove that if $a$, $b$, and $c$ are integers with $a$ and $c$ nonzero, such that $a|b$ and $c|d$, then $ac|bd$.

**Exercise 4.33.** Prove or disprove with a counterexample. There are integers $a$, $b$, and $c$ such that $a|bc$, but $a \nmid b$ and $a \nmid c$.

**Exercise 4.34.** Prove or disprove with a counterexample. If $a$, $b$ and $c \neq 0$ are integers, then $a|b$ if and only if $ac|bc$.

**Exercise 4.35.** Prove or disprove with a counterexample. If $a|m$ and $a|(ms+nt)$ for some integers $a \neq 0$, $m$, $s$, $n$, and $t$, then $a|nt$.

**Exercise 4.36.** Prove that $7^n-1$ is divisible by 6 for $n \geq 1$.

**Exercise 4.37.** Prove that $5^n-2^n$ is divisible by 3 for $n \geq 1$.

**Exercise 4.38.** Show that $f_n \mid f_m$ when $n$ and $m$ are positive integers with $n \mid m$.

**Exercise 4.39.** Show that the product of every two integers of the form $6k+1$ is also of the form $6k+1$.

**Exercise 4.40.** Show that any integer of the form $6k+5$ is also of the form $3k+2$, but not conversely.

**Exercise 4.41.** Given nonzero integers $a, b$, and $c$ show that $a|b$ and $a|c$ implies $a|(bx+cy)$ for any integers $x$ and $y$.

**Exercise 4.42.** Determine which of the following integers are prime: 201, 207, 213, 203, 211, 221.

**Exercise 4.43.** Find the smallest prime in the arithmetic progression $an+b$.

- $a = 3, b = 1$,
- $a = 5, b = 4$,
- $a = 7, b = 12$,
- $a = 11, b = 16$.

**Exercise 4.44.** Using the sieve of Eratosthenes, find the prime numbers less than 200.

**Exercise 4.45.** Show that $x^2 - x + 41$ is prime for all integers $x$ with $0 \leq x \leq 40$. Show that it is composite for $x = 41$.

**Exercise 4.46.** Show that $2x^2 + 11$ is prime for all integers $x$ with $0 \leq x \leq 10$. Show that it is composite for $x = 11$.

**Exercise 4.47.** Show that $2x^2 + 29$ is prime for all integers $x$ with $0 \leq x \leq 28$. Show that it is composite for $x = 29$.

**Exercise 4.48.** It has been conjectured that there are infinitely many primes of the form $n^2 - 2$. Exhibit five such examples.

**Exercise 4.49.** Show that any prime of the form $3n+1$ is also of the form $6m+1$.

**Exercise 4.50.** Show that each integer of the form $3n + 2$ has a prime factor of this form.

**Exercise 4.51.** Show the only prime $p$ for which $3p + 1$ is perfect square is $p = 5$.

**Exercise 4.52.** Find all primes that are the difference of the fourth powers of two integers.

**Exercise 4.53.** Show that no integer of the form $n^3 + 1$ is a prime, other than 2.

**Exercise 4.54.** Prove that all odd primes are either of the form $4n + 1$ or $4n - 1$ for some $n \in \mathbb{N}$.

**Exercise 4.55.** Prove that, if $n \in \mathbb{N}$ s a product of primes of the form $4m + 1$, then $n$ must be of that form.

**Exercise 4.56.** Let $Q_n = p_1 p_2 \cdots p_n + 1$ where $p_1, p_2, \cdots, p_n$ are the smallest primes. Determine the smallest prime factor of $Q_n$ for $n = 1, 2, 3, 4, 5$, and 6. Do you think that $ Q_n$ is prime infinitely often?

**Exercise 4.57.** Show there are infinitely prime numbers of the form $4k + 3$.

**Exercise 4.58.** Give an example to show that the following conjecture is not true: Every positive integer can be written in the form $p + a^2$, where $p$ is either a prime or 1, and $a \geq 0$.

**Exercise 4.59.** Another unproven conjecture is that there are an infinitude of primes that are 1 less than a power of 2, such as $3 = 2^2 - 1$. Find four more of these primes.

**Exercise 4.60.** It has been conjectured that every even integer can be written as the difference of consecutive primes in finitely many ways. For example, $6 = 29 - 23 = 137 - 131 = 599 - 593 = 1019 - 1013 = ...$ Express the integer 10 as the difference of two consecutive primes in 15 ways.

**Exercise 4.61.** Find four primes of the form $2^n + 1$ for $n \in \mathbb{N}$.

**Exercise 4.62.** Prove that if $2^n + 1$ is prime, then $n = 0$ or $n = 2k$ for some integer $k$.

**Exercise 4.63.** Prove that $p$ is prime if and only if it has no divisors $d$ that satisfy $1 < d \leq \sqrt{p}$.

**Exercise 4.64.** Show there are infinitely many primes of the form $6k+5$.

**Exercise 4.65.** Show that no integer of the form $n^3+1$ is a prime, other than 2.

**Exercise 4.66.** Explain why $(a, a^2) = a$ where $a$ is a positive integer. Explain why 201 is not a prime. Explain why 11 is a prime number.

**Exercise 4.67.** Find the greatest common divisor of each of the following pairs of integers.

- $5, 15$
- 0,100
- $-27, -45$
- $-90, 100$
- 100, 121
- 1001, 289

**Exercise 4.68.** Find the greatest common divisor of each of the following.

- $(a, 2a)$
- $(a, a^2)$
- $(a, a+1)$
- $(a, a+2)$

**Exercise 4.69.** Show that $(n, 1) = 1$ for all integers $n$.

**Exercise 4.70.** Show that $(n+1, n) = 1$ for all integers $n$.

**Exercise 4.71.** Show that $(2n+1, 2n-1) = 1$ for all integers $n$.

**Exercise 4.72.** Show that if $a$ is an even integer and $b$ is an odd integer, then $(a, b) = \left(\frac{a}{2}, b\right)$.

**Exercise 4.73.** Show that if $a, b$, and $c$ are integers, then $[a, b] | c$ if and only if $a|c$ and $b|c$.

**Exercise 4.74.** Show that if $a$ and $b$ are positive integers, then $(a, b) = (a+b, [a, b])$.

**Exercise 4.75.** Show that $8a+3$ and $5a+2$ are relatively prime for all integers $a$.

**Exercise 4.76.** For any integer $a$ show that $(2a+1, 9a+4) = 1$.

**Exercise 4.77.** For any integer $a$ show that $(5a+2, 7a+3) = 1$.

**Exercise 4.78.** Show that if $a$ is odd, then $(3a, 3a+2) = 1$.

**Exercise 4.79.** Show that if $a$ and $b$ are integers with $(a, b) = 1$, then $(a+b, a-b) = 1$ or $2$.

**Exercise 4.80.** Show that if $a$ and $b$ are even integers that are not both zero, then $(a, b) = 2\left(\frac{a}{2}, \frac{b}{2}\right)$.

**Exercise 4.81.** Show that if $a, b$, and $c$ are integers such that $(a, b) = 1$ and $c|(a+b)$, then $(c, a) = (c, b) = 1$.

**Exercise 4.82.** Show that if $a, b$, and $c$ are integers with $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.

**Exercise 4.83.** Show that if $a$ and $b$ are relatively prime integers, then $(a + 2b, 2a + b) = 1$ or $3$.

**Exercise 4.84.** Show that if $(a, b) = 1$ and $a|bc$ then $a|c$.

**Exercise 4.85.** Show that if $r|a$, $r|b$, and $r|c$, then $r|\gcd(a, b, c)$.

**Exercise 4.86.** Which of the following are true and which are false? For those that are false provide a counterexample.

- If $a|b$ and $b|c$, then $a|c$.
- If $a|c$ and $b|d$, then $ab|cd$.
- If $m^2|n^2$, then $m|n$.
- If $m|n$, then $m^2|n^2$.
- If $m$ is a positive integer, then $\gcd(ma, mb) = m\gcd(a, b)$.
- If $n|ab$ and $n\nmid a$, then $n|b$.
- If $n|ab$ and $\gcd(n, a) = 1$, then $n|b$.
- If $n$ is a positive integer, then $\gcd(a^n, b^n) = \gcd(a, b)^n$.
- If $n$ is an integer, then $\gcd(a, b) = \gcd(a, b + na)$.
- If $n$ is composite and $n|ab$, then $n|a$ or $n|b$.

**Exercise 4.87.** What is $\left(a^2 + b^2, a + b\right)$, where $a$ and $b$ are relatively prime integers that are not both 0? ::: {.proof } Let $p$ be a prime dividing $\left(a^2 + b^2, a + b\right)$. Then

$$p \,\big|(a + b)^2 - \left(a^2 + b^2\right) = 2ab.$$

Now if $p|a$, then $p|b$ since $p|(a + b)$. But $(a, b) = 1$, so $p \nmid a$. Similarly, $p \nmid b$. Therefore, $p|2$ and so $p = 1$ or $p = 2$. If $a$ and $b$ have the same parity, then $2|(a + b)$ and $2\,\big|\left(a^2 + b^2\right)$ and so $\left(a^2 + b^2, a + b\right) = 2$. But if $a$ and $b$ have opposite parity, then $a + b$ and $\left(a^2 + b^2, a + b\right) = 1$.

:::

**Exercise 4.88.** Show that if $k$ is a positive integer, then $3k+2$ and $5k+3$ are relatively prime.

**Exercise 4.89.** Show that if $(a, b) = 1$ and $c|a$, then $(c, b) = 1$.

**Exercise 4.90.** Show that if $a$, $b$, and $c$ are integers such that $(a, b) = 1$ and $c|(a + b)$, then $(c, a) = (c, b) = 1$.

**Exercise 4.91.** Find the greatest common divisor of each of the following pairs of integers.

- $5, 15$
- 0,100
- $-27, -45$
- $-90, 100$
- 100, 121
- 1001, 289

**Exercise 4.92.** What is the greatest common divisor of each of the following?

- $(a, 2a)$
- $(a, a^2)$
- $(a, a + 1)$
- $(a, a + 2)$

**Exercise 4.93.** Use the Euclidean Algorithm to find the following greatest common divisors.

- $(221, 187)$
- $(51, 87)$
- $(105, 300)$
- $(34709, 100313)$
- $(64, 38, 190)$
- $(15, 35, 90)$
- $(100, 210, 540)$
- $(300, 2160, 5040)$
- $(240, 660, 5540, 9980)$
- $(1240, 6660, 15540, 19980)$

**Exercise 4.94.** Find $(143, 227)$, $(306, 657)$, and $(272, 1479)$.

**Exercise 4.95.** Use the Euclidean Algorithm to find integers $x$ and $y$ satisfying the following.

- $(56, 72) = 56x + 72y$
- $(24, 138) = 24x + 138y$
- $(119, 272) = 119x + 272y$
- $(1769, 2378) = 1769x + 2378y$

**Exercise 4.96.** Find integers $x$ and $y$ satisfying

$$(198, 288, 512) = 198x + 288y + 512z.$$

**Exercise 4.97.** Find $\gcd(143, 227)$, $\gcd(306, 657)$, and $\gcd(272, 1479)$.

**Exercise 4.98.** Show that if $k > 0$ then $\gcd(ka, kb) = k \gcd(a, b)$.

**Exercise 4.99.** Which of the following are true and which are false? For those that are false provide a counterexample.

- If $a|b$ and $b|c$, then $a|c$.
- If $a|c$ and $b|d$, then $ab|cd$.
- If $m^2|n^2$, then $m|n$.
- If $m|n$, then $m^2|n^2$.
- If $m$ is a positive integer, then $\gcd(ma, mb) = m \gcd(a, b)$.
- If $n|ab$ and $n \not| \, a$, then $n|b$.
- If $n|ab$ and $\gcd(n, a) = 1$, then $n|b$.
- If $n$ is a positive integer, then $\gcd(a^n, b^n) = \gcd(a, b)^n$.
- If $n$ is an integer, then $\gcd(a, b) = \gcd(a, b + na)$.
- If $n$ is composite and $n|ab$, then $n|a$ or $n|b$.

**Exercise 4.100.** Show that if $r|a$, $r|b$, and $r|c$, then $r| \gcd(a, b, c)$.

**Exercise 4.101.** Prove that, if $a_1, a_2, \ldots a_m$ are pairwise relatively prime, then

$$(a_1, a_2, \ldots a_n) = 1.$$

**Exercise 4.102.** Use the Euclidean algorithm to find $(1372, 490)$ and write the GCD as a linear combination of 1372 and 490.

**Exercise 4.103.** Use the Euclidean algorithm to find $d = (500, 50, 40)$ and write $d$ as a linear combination of the three given integers.

**Exercise 4.104.** Use the Euclidean Algorithm to find $(28, 48, 24)$.

**Exercise 4.105.** Use the Euclidean Algorithm to find $(28, 48, 24)$.

**Exercise 4.106.** Use the Euclidean Algorithm to find $(34709, 100313)$.

**Exercise 4.107.** Use the Euclidean Algorithm to find the greatest common divisor $(105, 300)$ and then write this as a linear combination of these integers.

**Exercise 4.108.** Use the Euclidean Algorithm to find the multiplicative inverse for 91 modulo 191.

**Exercise 4.109.** Find the unique prime factorization of 12446784 and of 2293834752.

**Exercise 4.110.** Factor 12446784 and 2293834752 into a product of primes with the same set of primes with (possibly zero) nonnegative exponents.

**Exercise 4.111.** Find a prime factorization of

- $111111$,
- $100,000$,
- $10,500,000$, and
- $10!$.

**Exercise 4.112.** Show that all of the prime powers in the prime-power factorization of an integer $n$ are even if and only if $n$ is a perfect square.

**Exercise 4.113.** Show that if $a$ and $b$ are positive integers and $a^3 | b^2$, then $a | b$.

**Exercise 4.114.** Find the greatest common divisor of each of the following pairs of integers:

- $2^1 3^2 5^3$, \$$2^{23}$37^2 \$
- \$2(3)(5)(7), 7(11)(13) \$
- $2^8 3^6 5^4 11^{13}$, \$2(3)(5)(11)(13) \$
- $41^{101} 47^{43} 103^{1001}$, $41^{11} 43^{47} 83^{111}$

**Exercise 4.115.** Find the least common multiple of each of the following pairs of integers:

- $2^2 3^3 5^5 7^7$, $2^7 3^5 5^3 7^2$
- $2(3)(5)(7)(11)$, $17(19)(23)(29)$
- $2^3 5^7 11^{13}$, $2(3)(5)(7)(11)(13)$
- $47^{11} 79^{111} 101^{1001}$, $41^{11} 83^{111} 101^{1000}$

**Exercise 4.116.** Find the least common multiple of each of the following pairs of integers:

- $2^2 3^3 5^5 7^7$, $2^7 3^5 5^3 7^2$
- $2(3)(5)(7)(11)$, $17(19)(23)(29)$
- $2^3 5^7 11^{13}$, $2(3)(5)(7)(11)(13)$
- $47^{11} 79^{111} 101^{1001}$, $41^{11} 83^{111} 101^{1000}$

**Exercise 4.117.** If $p$ is a prime and $a$ is an integer with $p \left| a^2 \right.$ then $p|a$.

**Exercise 4.118.** Show that if $a$, $b$, and $c$ are integers with $c|ab$ then $c|(a,c)(b,c)$.

**Exercise 4.119.** Find the prime factorization of

- $33,776,925$
- $210,733,237$
- $1,359,170,111$
- $33,108,075$
- $7,300,977,607$
- $4,165,073,376,607$.

**Exercise 4.120.** Show that any number of the form $2^{4n+2}+1$ can be factored easily and then show how to factor $2^{18}+1$.

**Exercise 4.121.** Find the unique prime factorization of 12446784 and of 2293834752. Factor 12446784 and 2293834752 into a product of primes with the same set of primes with (possibly zero) nonnegative exponents.

**Exercise 4.122.** Find a prime factorization of 111111, $100,000$, $10,500,000$, and 10!.

**Exercise 4.123.** Show that all of the prime powers in the prime-power factorization of an integer $n$ are even if and only if $n$ is a perfect square.

**Exercise 4.124.** Show that if $a$ and $b$ are positive integers and $a^3|b^2$, then $a|b$.

**Exercise 4.125.** Show that if $a$, $b$, and $c$ are integers with $c|ab$ then $c|(a,c)(b,c)$.

**Exercise 4.126.** Show that if $p$ is prime, $a$ is an integer, and $n$ is a positive integer such that $p\,|a^n$ , then $p|a$.

**Exercise 4.127.** Show that if $p^a\| m$ and $p^b\Big\| n$, then $p^{a+b}\Big\| nm$.

**Exercise 4.128.** Show that if $p^a\| m$ then $p^{ka}\|m^k$ for any positive integer $k$.

**Exercise 4.129.** Show that if $p^a\| m$ and $p^b\Big\| n$ with $a \neq b$, then $p^{\min(a,b)}\Big\| (m+n)$.

**Exercise 4.130.** Use the unique factorizations of $n = 5248$ and $m = 1280$ to determine the unique factorizations of $(n, m)$and $[n, m]$.

**Exercise 4.131.** Show that if $a$ and $b$ are positive integers, then $(a, b) = (a + b, [a, b])$.

**Exercise 4.132.** Write out the unique prime factorization of 1494411775. Show each step.

## 4.5 Linear Congruence Equations

**Definition 4.3.** Given integers $a, b$ and a modulus $n$, a congruence equation of the form $ax \equiv b \pmod{n}$ is called a **linear congruence** where $x$ is an unknown.

Solvability of a linear congruence $ax \equiv b \pmod{n}$ can easily be described by the following: (i) if $a$ and $n$ are relatively prime then there is precisely one incongruent solution modulo $n$, (ii) if the greatest common divisor of $a$ and $n$ does not divide $b$, then the linear congruence has no solution, and (iii) if the gcd of $a$ and $n$ **does** divide $b$ then there are exactly $(a, n)$ distinct incongruent solutions modulo $n$. Knowing whether there are solutions to a given linear congruence is often the first step, but as we will see, the work of computing $(a, n)$ can be also used in finding solutions, if there are any.

**Theorem 4.7.** *Let $x$ be an unknown in the linear congruence equation $ax \equiv b \pmod{n}$ and $d = (a, n)$.*

- *If $d = 1$, then there is precisely one solution.*
- *If $d|b$ there are exactly $d$ distinct solutions, otherwise there are no solutions.*

*Proof.* By the Euclidean algorithm there are integers $s$ and $t$ such that $as + nt = 1$, and then $a(sb) + n(tb) = b$ and thus we find that $x = sb$ is a solution of the congruence. If $y$ is any other solution, then $ay \equiv b \pmod{n}$. Thus, $ax \equiv ay \pmod{n}$ and since $(a, n) = 1$ we have $x \equiv y \pmod{n}$.

Since the congruence is equivalent to $ax + n(-y) = b$ in integers $x$ and $y$, the existence of solutions $x$ and $y$ requires that $d = (a, n)$ divide $b$. Suppose then that this requirement is satisfied and let $x = x_0 + (n/d)t$ and $y = y_0 + (a/d)t$ where $x = x_0$ and $y = y_0$ is a particular solution, be all solutions to $ax + n(-y) = b$. Therefore, for any integer $t$, $x$ is a solution to $ax \equiv b \pmod{n}$.
To determine that there are $d$ incongruent solutions, we find the condition that describes when two solutions are congruent modulo $n$. Suppose we have two solutions, namely,

$$x_0 + \left(\frac{n}{d}\right) t_1 \equiv x_0 + \left(\frac{n}{d}\right) t_2 \pmod{n}.$$

Since

$$\left(\frac{n}{d}, n\right) = \frac{n}{d},$$

it follows that $t_1 \equiv t_2 \pmod{d}$. This show that a complete set of incongruent solutions is obtained by taking $x = x_0 + \left(\frac{n}{d}\right) t$ and $t$ ranges through a complete system of residues modulo $d$; one such set is given by $t = 0, 1, 2, \dots, d-1$.

□

**Example 4.5.** Solve the linear congruence $131x \equiv 21 \pmod{77}$.

*Solution.* Because $1 = (131, 77)|21$ there is a unique solution modulo 77. We have $54x \equiv 21 \pmod{77}$ and dividing by 3 we have $18x \equiv 7 \pmod{77}$. Next multiplying by 4 we have $72x \equiv 28 \pmod{77}$ and so $-5x \equiv 28 \equiv 105 \pmod{77}$. Therefore, $x \equiv -21 \equiv 56 \pmod{77}$.

**Example 4.6.** Solve the linear congruence $6x \equiv (10)^k \pmod{21}$.

*Solution.* There is no solution because $(6, 21) = 3$ does not divide $2^k 5^k$ for any positive integer $k$.

**Example 4.7.** Solve the linear congruence $91x \equiv 98 \pmod{119}$.

*Solution.* Because $7 = (91, 119)|98$ there are 7 incongruent solutions modulo 119. We use cancellation to simplify the congruence to $13x \equiv 14 \pmod{17}$. We have $-4x \equiv -3 \equiv -20 \pmod{17}$. Therefore, in terms of the original modulus, the solutions are

$$x \equiv 5, 22, 39, 56, 73, 90, 107 \pmod{199}.\square$$

**Example 4.8.** Solve the linear congruence $31x \equiv 12 \pmod{24}$.

*Solution.* Since $(31, 24) = 1$ and $1|12$ there is exactly one incongruent solution modulo 24. To find this solution we use $31 \equiv 7 \pmod{24}$ so $31x \equiv 7x \pmod{24}$ which means we now solve the linear congruence $7x \equiv 12 \pmod{24}$. Next we multiply by 7, to obtain $49x \equiv 84 \pmod{24}$. Then since $49 \equiv 1 \pmod{24}$ and $84 \equiv 12 \pmod{24}$ we now have $x \equiv 12 \pmod{24}$ as our solution to the linear congruence $31x \equiv 12 \pmod{24}$.

**Example 4.9.** Solve the linear congruence $987x \equiv 610 \pmod{1597}$.

*Solution.* Solving the linear congruence equation is equivalent to solving the linear Diophantine equation $987x + 1597(-y) = 610$ for $x$ and $y$. There is a solution because $(987, 1597) = 1$ and it is unique modulo 1597.

A particular solution is $x = -1$ and $y = -1$. Thus all solutions to the Diophantine equations are

$$x = -1 + \frac{1597}{1}t \quad \text{and} \quad y = -1 + \frac{987}{1}t.$$

Suppose that

$$-1 + \frac{1597}{1}t_1 \equiv -1 + \frac{1597}{1}t_2 \pmod{1597}$$

are two solutions to the congruence equation. Then clearly, $t_1 \equiv t_2 \pmod{1597}$. This show that a complete set of incongruent solutions is obtained by taking $x = -1 + 1597t$ and $t = 0$. Therefore, the unique solution is $x \equiv 1596 \pmod{1597}$.

**Example 4.10.** Solve the linear congruence $42x \equiv 50 \pmod{76}$.

*Solution.* Solving the linear congruence equation is equivalent to solving the linear Diophantine equation $42x + 76(-y) = 50$ for $x$ and $y$. There is a solution because $(42, 76) = 2$ and $2|50$; and so there are exactly two solutions modulo 76. A particular solution is $x = -35$ and $y = 20$. Thus all solutions for $42x + 76(-y) = 50$ are

$$x = -35 + \frac{76}{2}t \qquad \text{and} \qquad y = 20 + \frac{42}{2}t.$$

Suppose that $-35 + 38t_1 \equiv -35 + 38t_2 \pmod{76}$ are two solutions. Since $(38, 76) = 38$, we have, $t_1 \equiv t_2 \pmod{2}$. This show that a complete set of incongruent solutions is obtained by taking $x = -35 + 38t$ and $t = 0, 1, 2, \dots, d-1$ where $d = (42, 76) = 2$. Therefore, the solutions are $x \equiv 3 \pmod{76}$ and $x \equiv 41 \pmod{76}$.

Notice that to solve a linear congruence equation $ax \equiv b \pmod{n}$ we find, (if possible) an integer $h$ such that $ah \equiv 1 \pmod{n}$ and then using $h$ we solve by multiplying by $h$, obtaining $x \equiv hb \pmod{n}$.

**Definition 4.4.** Let $a$ be an integer with $(a, n) = 1$. Then a solution of the linear congruence $ax \equiv 1 \pmod{n}$ is called an **inverse** of $a$.

**Theorem 4.8.** *Let $p$ be a prime. The positive integer $a$ is its own inverse modulo $p$ if and only if $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.*

*Proof.* If $a$ is its own inverse modulo $p$, then $a^2 \equiv 1 \pmod{p}$. Thus, $p \,\big|\, (a^2 - 1)$ and so either $p|(a-1)$ or $p|(a+1)$. Therefore, $a \equiv 1 \pmod{p}$

or $a \equiv -1 \pmod{p}$. Conversely, if $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$, then $a^2 \equiv 1 \pmod{p}$, so that $a$ is its own inverse modulo $p$.

□

**Example 4.11.** By finding an inverse, solve the linear congruence $37x \equiv b \pmod{53}$.

*Solution.* First we solve, $37x \equiv 1 \pmod{53}$. We have $-16x \equiv 1 \equiv 54 \pmod{53}$. Now dividing by 2 and simplifying, we have $8x \equiv -27 \equiv 26 \equiv 132 \pmod{53}$ Again dividing by 2 and simplifying, we have $2x \equiv 33 \equiv 86 \pmod{53}$ Therefore, $x \equiv 43 \pmod{53}$. Now to solve $37x \equiv b \pmod{53}$ we multiply by 43 and we have $(43)37x \equiv 43b \pmod{53}$. Thus $x \equiv 43b \pmod{53}$ is the solution.

**Example 4.12.** By finding an inverse, solve the linear congruence $31x \equiv 12 \pmod{24}$.

*Solution.* Recall that since $(31, 24) = 1$ and $1|12$ there is exactly one incongruent solution modulo 24. To find this solution let's use the definition of congruence, namely $24|(31x - 12)$ which means there exists an integer $y$ such that $31x - 12 = 24y$ and so we will solve the linear Diophantine equation $31x + 24(-y) = 12$. Now notice that we merely need the $x$ solutions because of our original linear congruence involves only $x$. But first we need a particular solution to this linear Diophantine equation, which can be found using the Euclidean algorithm, $31 = 1(24) + 7$ with $0 \leq 7 < 24$ $24 = 3(7) + 3$, with $0 \leq 2 < 7$ $7 = 2(3) + 1$, with $0 \leq 1 < 2$ so $(31, 24) = 1$ which we already knew but now we can use back substitution to find 1 as a linear combination of 31 and 24, namely, $1 = 7 - 2(3)$, $1 = 7 - 2(24 - 3(7))$, $1 = (7)7 + (-2)(24)$, $1 = (7)(31 - 1(24)) + (-2)(24)$, $1 = (7)(31) + (-9)(24)$. Then multiplying by 12 yields a particular solution with $x_0 = 84$ since, $12 = (31)(84) + (24)(-108)$, So all solutions to the linear Diophantine equation $31x + 24(-y) = 12$ are given $x = 84 + 24t$ where $t \in \mathbb{Z}$. In particular when $t = -3$ we find the solution $x \equiv 12 \pmod{24}$.

**Example 4.13.** By finding an inverse, solve the linear congruence $78x \equiv 12 \pmod{240}$.

*Solution.* Since $(78, 240) = 6$ and $6|12$ there are exactly six incongruent solution modulo 240. To find these solutions let's use the definition of congruence, namely $240|(78x - 12)$ which means there exists an integer $y$ such that $78x - 12 = 240y$ and so we will solve the linear Diophantine equation $78x + 240(-y) = 12$. Using the Euclidean algorithm,

$240 = 3(78) + 6, \text{with} 0 \leq 7 < 24$ and now we can write 6 as a linear combination of 78 and 240, namely, $6 = (-3)(78) + (1)(240)$ Then multiplying by 2 yields a particular solution with $x_0 = -6$ since,
$12 = (-6)(78) + (2)(240)$, So all solutions to the linear Diophantine equation $78x - 12 = 240y$ are given
$x = -6 + \frac{240}{6}t = -6 + 40t$ where $t \in \mathbb{Z}$. In particular, when $t = 1, 2, 3, 4, 5, 6, 7$ we find the six incongruent solutions modulo 240, $x \equiv 34, 74, 114, 154, 194, 234 \pmod{240}$.

**Example 4.14.** For which integers $c$, $0 \leq c \leq 1001$, does the congruence $154x \equiv c \pmod{1001}$ have solutions? When there are solutions, how many incongruent solutions are there?

## 4.6 Chinese Remainder Theorem

The Chinese Remainder Theorem is a staple in many high-level mathematics courses. This theorem has been used for centuries to help mathematicians solve complex problems, and it's an essential tool for anyone looking to pursue a career in mathematics. In this Definitive Guide, you'll learn everything you need to know about the Chinese Remainder Theorem, from its history to its many applications.

The Chinese Remainder Theorem is a mathematical theorem that states that if there are a certain number of integers that are all coprime to each other, then for any integer N that is congruent to each modulo ni, there is exactly one such congruence class modulo M. In other words, the Chinese Remainder Theorem allows you to solve a system of linear congruence equations with a unique solution. The Chinese Remainder Theorem is an important tool in number theory and has a wide range of applications, including cryptography and computer science.

The Chinese Remainder Theorem is a mathematical theorem with a wide range of applications. In its simplest form, the theorem states that if one knows the remainders of a number when it is divided by a set of coprime numbers, then one can determine the number itself. The theorem has a wide range of applications, from helping to solve simple arithmetic problems to more complex applications in cryptography and computer science. For example, the Chinese Remainder Theorem can be used to find the last digit of a very large number, something that is often useful in mathematical contests. It can also be used to design algorithms for factoring large numbers, a critical task in cryptography.

Chinese Remainder Theorem is a mathematics theorem that helps one to find the value of a certain number when its value is unknown. It was developed by Chinese mathematician Sun Zi during the 3rd century BC, and it has since been used by mathematicians and scientists all over the world.

Chinese Remainder Theorem is a powerful tool that can be used to solve a variety of mathematical problems. However, it is not without its challenges. One of the biggest challenges is that it can be difficult to find the values of x that satisfy all the congruences.

This can be particularly tricky when there are a large number of congruences. Additionally, the Chinese Remainder Theorem can only be used when the moduli are relatively prime. This can sometimes be difficult to determine, especially when working with larger numbers. Despite these challenges, the Chinese Remainder Theorem remains a valuable tool for mathematicians and can be used to solve a variety of problems.

The theorem has been used in a variety of applications, ranging from number theory to cryptography. However, the Chinese Remainder Theorem was not always so well-known.

In fact, it was not until the 19th century that the theorem began to be widely used. This is largely due to the work of Chinese mathematician Sun Tzu, who provided the first complete proof of the theorem. Since then, the Chinese Remainder Theorem has been studied by mathematicians all over the world and has become an essential tool in many different fields.

The Chinese Remainder Theorem has a wide range of applications, from cryptography to music composition. In cryptography, the theorem is used to design schemes for secret sharing and public-key encryption. In music composition, it can be used to create patterns that are both complex and pleasing to the ear.

The theorem can also be used to solve certain number theory problems, such as finding the order of an element in a finite group. In addition, the Chinese Remainder Theorem has applications in computer science, particularly in the area of error-correcting codes. Overall, the Chinese Remainder Theorem is a powerful tool with a wide range of applications.

Today, the theorem is still an active area of research, with new applications being discovered regularly. As such, it is clear that the Chinese Remainder Theorem has had a significant impact on Mathematics and its development.

This book is written for people who want to learn about the Chinese Remainder Theorem. It will cover the basics of the theorem, as well as some more advanced topics. I'll also share my own experience teaching this theorem to students.

One of the most essential subjects in mathematics is number theory. This branch of mathematics deals with the properties and relationships between integers, which are the building blocks of all other numbers. It is a critical tool for solving problems in other areas of mathematics, as well as in physics and engineering.

Despite its importance, number theory can be challenging for students to grasp. In this book, we will cover the fundamental concepts of the Chinese Remainder Theorem, and provide tips on how to make the material engaging and relevant.

The Chinese Remainder Theorem is a staple in many high-level mathematics courses for good reason. This theorem has been used for centuries to help mathematicians solve complex problems, and it's an essential tool for anyone looking to pursue a career in mathematics. In this Definitive Guide, you'll learn everything you need to know about the Chinese Remainder Theorem, from its history to its many applications. If you're looking for a comprehensive guide to the Chinese Remainder Theorem, then look no further than this book.

## 4.7 Chinese Remainder Theorem

When solving a linear congruence with a large modulus it is sometimes useful to reduce the linear congruence to a system of linear congruences with smaller moduli. Being able to construct a solution to the original congruence from a linear system of congruence equations is where the Chinese Remainder Theorem is often applied.

The Chinese Remainder Theorem is also useful of resolving elementary word problems, as such some are given in the exercises at the end of the section.

Now to see how the Chinese Remainder Theorem works it's useful to see an example first. Let's solve the following linear system of congruence equations.

$$\begin{cases} x \equiv 15 \pmod{27} \\ x \equiv 16 \pmod{20} \end{cases} \tag{4.6}$$

Notice, 20 and 27 are relatively prime, so we can find integers $a$ and $b$ such that $20a + 27b = 1$.
In fact by inspection, we find $a = -4$ and $b = 3$ since $20(-4) + 27(3) = 1$. We claim $x = 15(20)(-4) + 16(27)(3) = 96$ is a solution to both linear congruence equations in 4.6. More specifically, we will say, $x \equiv 96 \pmod{540}$ is *the* solution to the system in 4.6 where $540 = (20)(27)$. This strategy and the uniqueness is justified in the following well-known theorem.

**Example 4.15.** Solve the linear system of congruences

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 5 \pmod{4} \\ x \equiv -3 \pmod{7} \end{cases}$$

*Solution.* We find $N = (3)(4)(7) = 84$ and we use a table to construct the solution.

| $i$ | $n_i$ | $a_i$ | $\bar{n}_i$ | $u_i$ |
|---|---|---|---|---|
| 1 | 3 | 2 | $84/3 = 28$ | $28u_1 \equiv 1 \pmod{3} \Longrightarrow u_1 = 1$ |
| 2 | 4 | 5 | $84/4 = 21$ | $21u_2 \equiv 1 \pmod{4} \Longrightarrow u_2 = 1$ |
| 3 | 7 | $-3$ | $84/7 = 12$ | $12u_3 \equiv 1 \pmod{7} \Longrightarrow u_3 = 3$ |

By 4.9 the solution to the system is

$$x = (2)(28)(1) + (5)(21)(1) + (-3)(12)(3) = 53 \pmod{84}. \tag{4.7}$$

as wanted.

**Theorem 4.9.** *[Chinese Remainder I] Suppose $n_1$, $n_2$, ..., $n_s$ are pairwise relatively prime positive integers. Then the system of congruences*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad\vdots \\ x \equiv a_s \pmod{n_s} \end{cases} \tag{*}$$

*has a unique solution modulo $N = n_1 n_2 \cdots n_s$.*

*Proof.* Let $\bar{n}_i = N/n_i$. We know that $(n_i, \bar{n}_i) = 1$ for $i = 1, ..., s$ because $(n_i, n_j) = 1$ whenever $i \neq j$. Therefore, for each $i$, there are integers $v_i$ and $u_i$ such that $v_i n_i + u_i \bar{n}_i = 1$; and using these $u_i$ we can construct a solution to the system as

$$x = a_1 \bar{n}_1 u_1 + a_2 \bar{n}_2 u_2 + \cdots + a_s \bar{n}_s u_s.$$

To verify this is a solution, check the $i^{\text{th}}$ congruence equation in *, namely,

$$x = \sum_{k=1}^{s} a_k \bar{n}_k u_k \equiv a_i \bar{n}_i u_i \equiv a_i \pmod{n_i}$$

for $1 \leq i \leq s$. To prove uniqueness, assume $y$ is a solution to the system of congruences. Then $x_0 \equiv a_i \equiv y \pmod{n_i}$ for $1 \leq i \leq s$. Hence, $n_i | (x_0 - y)$ for each $n_i$ and since no two of the $n_i$ have a common factor, $n_1 n_2 \cdots n_s | (x_0 - y)$, that is $N | (x_0 - y)$. Thus, $y \equiv x_0 \pmod{N}$.

□

**Example 4.16.** Solve the linear system of congruences.

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{6} \\ x \equiv 4 \pmod{7}. \end{cases}$$

*Solution.* We find $N = (5)(6)(7) = 210$ and we use a table to construct the solution.

| $i$ | $n_i$ | $a_i$ | $\bar{n}_i$ | $u_i$ |
|---|---|---|---|---|
| 1 | 5 | 3 | $210/5 = 42$ | $42u_1 \equiv 1 \pmod{5} \Longrightarrow u_1 = 3$ |
| 2 | 6 | 2 | $210/6 = 35$ | $35u_2 \equiv 1 \pmod{6} \Longrightarrow u_2 = 5$ |
| 3 | 7 | 4 | $210/7 = 30$ | $30u_3 \equiv 1 \pmod{7} \Longrightarrow u_3 = 4$ |

By 4.9 the solution is

$$x = (3)(42)(3) + (2)(35)(5) + (4)(30)(4) = 1208 \equiv 158 \pmod{210}.$$

as desired.

**Example 4.17.** Solve the linear system of congruences.

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7}. \end{cases}$$

*Solution.* We find $N = (3)(5)(7) = 105$ and we use a table to construct the solution.

| $i$ | $n_i$ | $a_i$ | $\bar{n}_i$ | $u_i$ |
|---|---|---|---|---|
| 1 | 3 | 2 | $105/3 = 35$ | $35u_1 \equiv 1 \pmod{3} \Longrightarrow u_1 = 2$ |
| 2 | 5 | 3 | $105/5 = 21$ | $21u_2 \equiv 1 \pmod{5} \Longrightarrow u_2 = 1$ |
| 3 | 7 | 2 | $105/7 = 15$ | $15u_3 \equiv 1 \pmod{7} \Longrightarrow u_3 = 1$ |

Therefore,

$$x_0 = (2)(35)(2) + (3)(21)(1) + (2)(15)(1) = 263 \equiv 23 \pmod{105}.$$

is the solution by the 4.9.

**Example 4.18.** Solve the linear system of congruences.

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7}. \end{cases}$$

*Solution.* We find $N = (2)(3)(5)(7) = 210$ and we use a table to construct the solution.

| $i$ | $n_i$ | $a_i$ | $\bar{n}_i$ | $u_i$ |
|---|---|---|---|---|
| 1 | 2 | 1 | $210/2 = 105$ | $105u_1 \equiv 1 \pmod 2 \Longrightarrow u_1 = 1$ |
| 2 | 3 | 2 | $210/3 = 70$ | $70u_2 \equiv 1 \pmod 3 \Longrightarrow u_2 = 1$ |
| 3 | 5 | 3 | $210/5 = 42$ | $42u_3 \equiv 1 \pmod 5 \Longrightarrow u_3 = 3$ |
| 4 | 7 | 4 | $210/7 = 30$ | $30u_4 \equiv 1 \pmod 7 \Longrightarrow u_3 = 4$ |

By 4.9 the solution is

$$x_0 = (1)(105)(1)+(2)(70)(1)+(3)(42)(3)+(4)(30)(4) = 1103 \equiv 53 \pmod{210}.$$

as desired.

**Theorem 4.10.** *[Chinese Remainder Theorem II] Suppose $n_1, n_2, , \dots n_s$ are pairwise relatively prime positive integers and that $(a_i, n_i) = 1$ for each $i$. Then the system of congruences $a_1 x \equiv b_1 \pmod{n_1}$, $a_2 x \equiv b_2 \pmod{n_2}$, ..., $a_s x \equiv b_s \pmod{n_s}$ has a unique solution modulo $N = n_1 n_2 \cdots n_s$.*

*Solution.* Since $(a_i, n_i) = 1$ for each $i$, we know that each congruence in the system has a solution, we first choose integers $x_1, x_2, \dots, x_s$ such that $a_i x_i \equiv b_i \pmod{n_i}$. Let $\bar{n}_i = N/n_i$ and since no two of the $n_i$ have a common factor, we see that $(n_i, \bar{n}_i) = 1$. Thus there is integer $u_i$ such that $\bar{n}_i u_i \equiv 1 \pmod{n_i}$. We now show that the number $x_0$ defined by

$$x_0 = \sum_{i=1}^{s} x_i \bar{n}_i u_i$$

is a solution of the original system of congruences. First note that $n_i$ divides each $\bar{n}_i$ when $j \neq i$. Thus for each $i$, we have,

$$a_i x_0 = \sum_{k=1}^{s} a_k x_k \bar{n}_k u_k \equiv a_i x_i \equiv b \pmod{n_i}.$$

Hence, $x_0$ is s solution of each congruence. If $y$ is a solution to the system of congruences, then $x_0 \equiv x_i \equiv y \pmod{n_i}$. Hence, $n_i | (x_0 - y)$ for each $n_i$ and since no two of the $n_i$ have a common factor, $n_1 n_2 \cdots n_s | (x_0 - y)$, that is $N | (x_0 - y)$. Thus, $y \equiv x_0 \pmod N$.

**Example 4.19.** Solve the linear system of congruences.

$$\begin{cases} 2x \equiv 3 \pmod 7 \\ 3x \equiv 4 \pmod 5 \\ 5x \equiv 46 \pmod{51} \end{cases}$$

*Solution.* We find $N = (7)(5)(51) = 1785$ and we use a table to construct the solution.

| $i$ | $n_i$ | $a_i$ | $b_i$ | $a_i x_i \equiv b_i \pmod{n_i}$ | $\bar{n}_i$ | $\bar{n}_i u_i \equiv 1 \pmod{n_i}$ |
|---|---|---|---|---|---|---|
| 1 | 7 | 2 | 3 | $x_1 = 5$ | 255 | $u_1 = 5$ |
| 2 | 5 | 3 | 4 | $x_2 = 3$ | 357 | $u_2 = 3$ |
| 3 | 51 | 5 | 46 | $x_3 = 50$ | 35 | $u_3 = 35$ |

By 4.10 the solution is

$$x_0 = (5)(255)(5)+(3)(357)(3)+(50)(35)(35) = 70838 \equiv 1223 \pmod{1785}.$$

as required.

## 4.8 Exercises

**Exercise 4.133.** Show that each of the following congruences hold.

- $13 \equiv 1 \pmod{2}$
- $-2 \equiv 1 \pmod{3}$
- $22 \equiv 7 \pmod{5}$
- $-3 \equiv 30 \pmod{11}$
- $91 \equiv 0 \pmod{13}$
- $111 \equiv -9 \pmod{40}$
- $69 \equiv 62 \pmod{7}$
- $666 \equiv 0 \pmod{37}$
- $166 \equiv 13 \pmod{17}$

**Exercise 4.134.** Determine whether each of the following pairs of integers is congruent modulo 7.

- \$1,15 \$
- \$-1,8 \$
- \$0,42 \$
- \$-9,5 \$
- \$2,99 \$
- $-1, 699$

**Exercise 4.135.** Show that if $a$ is an even integer, then $a^2 \equiv 0 \pmod{4}$, and if $a$ is an odd integer then $a^2 \equiv 1 \pmod{4}$.

**Exercise 4.136.** Show that if $a$ is an odd integer, then $a^2 \equiv 1 \pmod{8}$.

**Exercise 4.137.** Show that if $a, b, m$, and $n$ are integers such that $m > 0$, $n > 0$, $n|m$, and $a \equiv b \pmod{m}$, then $a \equiv b \pmod{n}$.

**Exercise 4.138.** Show that if $a, b, c$, and $m$ are integers such that $c > 0$, $m > 0$, and $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$.

**Exercise 4.139.** Show that if $a, b$, and $c$ are integers such that $c > 0$, such that $a \equiv b \pmod{c}$, then $(a, c) = (b, c)$.

**Exercise 4.140.** Find the least nonnegative residue modulo 13 of each of the following integers:

- 22
- $-1$
- 100
- $-100$
- 1001
- $-1000$

**Exercise 4.141.** Find the least positive residue of $1! + 2! + 3! + \cdots + 100!$ modulo each of the following integers.

- 2
- 12
- 7
- 25

**Exercise 4.142.** Find the least residue of $a$ modulo $n$.

- $a = 1348, n = 45$
- $a = 341123, n = 234$
- $a = 809834, n = 112$
- $a = 20934, n = 29$
- $a = 20034, n = 23$
- $a = 3407, n = 128$
- $a = 29976, n = 134$
- $a = 34534, n = 93$
- $a = 345996, n = 238$
- $a = 88629, n = 34$
- $a = 929001, n = 222$
- $a = 987559, n = 367$

**Exercise 4.143.** Construct tables for addition modulo 8, subtraction modulo 8, and multiplication modulo 8.

**Exercise 4.144.** What can you conclude if $a^2 \equiv b^2 \pmod{p}$, where $a$ and $b$ are integers and $p$ is prime?

**Exercise 4.145.** Show that if $n$ is odd positive integer, then $1+2+3+\cdots+(n-1) \equiv 0 \pmod{n}$.

**Exercise 4.146.** Show by mathematical induction that if $n$ is a positive integer, then $4^n \equiv 1+3n \pmod{9}$.

**Exercise 4.147.** Show by mathematical induction that if $n$ is a positive integer, then $5^n \equiv 1+4n \pmod{16}$.

**Exercise 4.148.** Determine which of the following are true:
- $7 \equiv -34 \pmod{9}$ - $-50 \equiv 2 \pmod{13}$ - $17 \equiv 62 \pmod{90}$
- $-73 \equiv -29 \pmod{128}$

**Exercise 4.149.** Find the least residue of $b$ modulo $m$ given:

- $m = 41,522$; $b = -16,115$
- $m = 91,631$; $b = -2152$
- $m = 63$; $b = 752 \cdot 571$
- $m = 51$; $b = 414 \cdot 566$

**Exercise 4.150.** What is the least residue of $100^6$ modulo 49? What is the least residue of $49^4$ modulo 23?

**Exercise 4.151.** Show that the following statements are true or determine if they are false by providing a counterexample.

- If $a \equiv b \pmod{n}$ and $m|n$ then $a \equiv b \pmod{m}$.
- If $a \equiv b \pmod{n}$ and $c > 0$, then $ca \equiv cb \pmod{cn}$.

- If $a \equiv b \pmod{n}$ and the integers $a, b, n$ are divisible by $d > 0$, then $a/d \equiv b/d \pmod{n/d}$.

- If $a^2 \equiv b^2 \pmod{n}$ then $a \equiv b \pmod{n}$.

- If $a \equiv b \pmod{n}$ then $(a, n) = (b, n)$.

**Exercise 4.152.** Show that $53^{103} + 103^{53}$ is divisible by 39.

**Exercise 4.153.** Show that $111^{333} + 333^{111}$ is divisible by 7.

**Exercise 4.154.** Show by mathematical induction that if $n$ is a positive integer, then $5^n \equiv 1 + 4n \pmod{16}$.

**Exercise 4.155.** What can you conclude if $a^2 \equiv b^2 \pmod{p}$, where $a$ and $b$ are integers and $p$ is prime?

**Exercise 4.156.** Show that if $n$ is an odd positive integer, then $1 + 2 + 3 + \cdots + (n - 1) \equiv 0 \pmod{n}$. Is this statement true if $n$ is even?

**Exercise 4.157.** Show that if $n$ is an odd integer or if $n$ is a positive integer divisible by 4, then $1^3 + 2^3 + 3^3 + \cdots + (n - 1)^3 \equiv 0 \pmod{n}$. Is this statement true if $n$ is not divisible by 4?

**Exercise 4.158.** For which positive integers $n$ is it true that $1^2 + 2^2 + 3^2 + \cdots + (n - 1)^2 \equiv 0 \pmod{n}$.

**Exercise 4.159.** Construct the multiplication and addition tables for modular arithmetic for $n = 6$.

**Exercise 4.160.** Prove that if $a \equiv b (\text{mod} m)$ then $a^k \equiv b^k (\text{mod} m)$ for every positive integer $k$.

**Exercise 4.161.** For which integers $c$, $0 \leq c \leq 1001$, does the congruence $154x \equiv c \pmod{1001}$ have solutions? When there are solutions, how many incongruent solutions are there?

**Exercise 4.162.** Solve the linear congruence equation $ax \equiv b \pmod{n}$.

- $a = 1348, b = 123, n = 45$
- $a = 341123, b = 325, n = 234$
- $a = 809834, b = 239, n = 112$
- $a = 20934, b = 198, n = 29$
- $a = 20034, b = 314, n = 23$
- $a = 3407, b = 349, n = 128$
- $a = 29976, b = 276, n = 134$
- $a = 34534, b = 39, n = 93$
- $a = 345996, b = 967, n = 238$
- $a = 88629, b = 865, n = 34$
- $a = 929001, b = 229, n = 222$
- $a = 987559, b = 143, n = 367$

**Exercise 4.163.** Determine which integers $a$, where $1 \leq a \leq 14$, have an inverse modulo 14 and for each one find its inverse.

**Exercise 4.164.** Determine which integers $a$, where $1 \leq a \leq 30$, have an inverse modulo 30 and for each one find its inverse.

**Exercise 4.165.** Show that if $\bar{a}$ is an inverse of $a$ modulo $m$ and $\bar{b}$ is an inverse of $b$ modulo $m$, then $\bar{a}\bar{b}$ is an inverse of $ab$ modulo $m$.

**Exercise 4.166.** Find all solutions to the following linear congruence equations.

- $3x \equiv 2 \pmod{7}$
- $6x \equiv 3 \pmod{9}$
- $17x \equiv 14 \pmod{21}$
- $15x \equiv 9 \pmod{25}$
- $128x \equiv 833 \pmod{1001}$
- $987x \equiv 610 \pmod{1597}$
- $36x \equiv 30 \pmod{42}$
- $143x \equiv 169 \pmod{110}$

- $51x \equiv 0 \pmod{17}$
- $52x \equiv 0 \pmod{17}$
- $253x \equiv 341 \pmod{299}$
- $441x \equiv 465 \pmod{640}$
- $36x \equiv 8 \pmod{102}$
- $34x \equiv 60 \pmod{98}$
- $140x \equiv 133 \pmod{30}$
- $140x \equiv 133 \pmod{31}$

**Exercise 4.167.** Find all solutions of the linear congruence

$$3x - 7y \equiv 11 \pmod{13}.$$

**Exercise 4.168.** What can you conclude if $a^2 \equiv b^2 \pmod{p}$, where $a$ and $b$ are integers and $p$ is prime?

**Exercise 4.169.** Show that if $n$ is an odd positive integer, then

$$1 + 2 + 3 + \cdots + (n-1) \equiv 0 \pmod{n}.$$

Is this statement true of $n$ is even?

**Exercise 4.170.** Show that if $n$ is an odd integer or if $n$ is a positive integer divisible by 4, then

$$1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 \equiv 0 \pmod{n}.$$

Is this statement true if $n$ is not divisible by 4?

**Exercise 4.171.** For which positive integers $n$ is it true that

$$1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 \equiv 0 \pmod{n}.$$

**Exercise 4.172.** Show by mathematical induction that if $n$ is a positive integer, then $5^n \equiv 1 + 4n \pmod{16}$.

**Exercise 4.173.** Give a complete system of residues modulo 13 consisting of entirely odd integers.

**Exercise 4.174.** An astronomer knows that a satellite orbits the Earth in a period that is an exact multiple of 1 hour that is less than 1 day. If the astronomer notes that the satellite completes 11 orbits in an interval that starts when a 24-hour clock reads 0 hours and ends when the clock reads 17 hours, how long is the orbital period of the satellite?

**Exercise 4.175.** Solve the linear congruence equation $987x \equiv 610(\text{mod}1597)$.

**Exercise 4.176.** Solve the linear congruence equation $987x \equiv 610(\text{mod}1597)$. If you find solutions explain why you have found them all.

**Exercise 4.177.** Suppose $p \equiv 3 \pmod 4$. Show that $(p+1)/4$ is an integer and is the multiplicative inverse of 4 modulo $p$.

**Exercise 4.178.** Explain why the linear congruence equation $3x \equiv 81(\text{mod}910)$ is solvable or not solvable. If possible solve it.

**Exercise 4.179.** Find an integer that leaves remainder of 1 when divided by either 2 or 5, but that is divisible by 3.

**Exercise 4.180.** Find an integer that leaves remainder of 9 when it is divided by either 10 or 11, but that is divisible by 13.

**Exercise 4.181.** A certain integer between 1 and 1200 leaves the remainder $1, 2, 6$ when divided by $9, 11, 13$ respectively. What is the integer?

**Exercise 4.182.** For which integers $c$, does $12x \equiv c \pmod{30}$ have solutions? When there are solutions are many are there?

**Exercise 4.183.** Determine which integers $a$ have inverse modulo 14 and then find each of the inverses.

**Exercise 4.184.** Find all solutions to the linear congruence equations $6x + 3y \equiv 12 \pmod{13}$ and $10x + 5y \equiv 9 \pmod{15}$.

**Exercise 4.185.** A professor feeds his pet python every fours days and bathes it once a week. This week he fed it on Tuesday and washed it on Wednesday. When if ever, will he feed and wash the Python on the same day? How often will this happen?

**Exercise 4.186.** A professor buys a new car every three years; he bought his first in 1981. He gets a sabbatical leave every seven years, starting in 1992. When will he first get both during a leap year?

**Exercise 4.187.** On the Fourth of July, a professor took a red pill at 8 a.m. and a green pill at noon. The next day he took a white pill at 10 p.m. He takes the red, green, and white pill every 5, 7, and 24 hours, respectively. How often does he take all three together? When in August will this first happen, if at all?

**Exercise 4.188.** Solve the linear system of congruences.
$x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 5 \pmod{17}$, $x \equiv 3 \pmod{5}$;

**Exercise 4.189.** Solve the linear system of congruences.
$x \equiv 0 \pmod{2}$, $x \equiv 0 \pmod{3}$, $x \equiv 1 \pmod{5}$, $x \equiv 6 \pmod{7}$.

**Exercise 4.190.** Solve the linear system of congruences.

- $x \equiv 4 \pmod{6}$, $x \equiv 13 \pmod{15}$
- $x \equiv 7 \pmod{10}$, $x \equiv 4 \pmod{15}$
- $x \equiv 7 \pmod{15}$, $x \equiv 4 \pmod{10}$
- $x \equiv 5 \pmod{6}$, $7x \equiv 3 \pmod{10}$, $4x \equiv 8 \pmod{15}$
- $x \equiv 1 \pmod{999}$, $x \equiv 2 \pmod{1001}$, $x \equiv 3 \pmod{1003}$, $x \equiv 4 \pmod{1004}$, $x \equiv 5 \pmod{1007}$.

**Exercise 4.191.** Find the smallest even integer $m$ such that $3|m$, $5|(m+3)$, and $11|(m+5)$.

**Exercise 4.192.** Find three consecutive integers divisible by $2, 3$, and $5$, respectively.

**Exercise 4.193.** Find a single congruence that is equivalent to the system of congruences $x \equiv r_1 \pmod{m}$ and $x \equiv r_2 \pmod{m+1}$.

**Exercise 4.194.** The three children in a family have feet that are 5 inches, 7 inches, and 9 inches long. When they measure the length of the dining room of their house using their feet, they each find that there are 3 inches left over. How long is the dining room?

**Exercise 4.195.** A professor feeds his pet python every fours days and bathes it once a week. This week he fed it on Tuesday and washed it on Wednesday. When if ever, will he feed and wash the Python on the same day? How often will this happen?

**Exercise 4.196.** A professor buys a new car every three years; he bought his first in 1981. He gets a sabbatical leave every seven years, starting in 1992. When will he first get both during a leap year?

**Exercise 4.197.** On the Fourth of July, a professor took a red pill at 8 a.m. and a green pill at noon. The next day he took a white pill at 10 p.m. He takes the red, green, and white pill every 5, 7, and 24 hours, respectively. How often does he take all three together? When in August will this first happen, if at all?

**Exercise 4.198.** If eggs are removed form a basket 2, 3, 4, 5, and 6, at a time, there remain, respectively, 1, 2, 3, 4, and 5 eggs. But if the eggs are removed 7 at a time, no eggs remain. What is the least number of eggs that could have been in the basket?

**Exercise 4.199.** Use the Chinese Remainder Theorem to solve the linear congruence equation $3x \equiv 11 \; (\mathrm{mod} 245)$.

**Exercise 4.200.** Find three consecutive integers divisible by $2, 3$, and $5$, respectively.

**Exercise 4.201.** Find the smallest even integer $m$ such that $3|m$, $5|(m+3)$, and $11|(m+5)$.

**Exercise 4.202.** Find a single congruence that is equivalent to the system of congruences $x \equiv r_1 \pmod{m}$ and $x \equiv r_2 \pmod{m+1}$. ::: {.solution } Solve the linear system of congruences $x \equiv 2 \pmod{3}$, $x \equiv 5 \pmod{4}$, $x \equiv -3 \pmod{7}$. We find $N = (3)(4)(7) = 84$ and we use a table to construct the solution.

| $i$ | $n_i$ | $a_i$ | $\bar{n}_i$ | $u_i$ |
|---|---|---|---|---|
| 1 | 3 | 2 | $84/3 = 28$ | $28u_1 \equiv 1 \pmod{3} \Longrightarrow u_1 = 1$ |
| 2 | 4 | 5 | $84/4 = 21$ | $21u_2 \equiv 1 \pmod{4} \Longrightarrow u_2 = 1$ |
| 3 | 7 | $-3$ | $84/7 = 12$ | $12u_3 \equiv 1 \pmod{7} \Longrightarrow u_3 = 3$ |

The solution is

$$x_0 = (2)(28)(1) + (5)(21)(1) + (-3)(12)(3) = 53 \pmod{84}.$$

:::

**Exercise 4.203.** Using the Chinese Remainder Theorem, solve the system of linear congruence equations $2x \equiv 3(\text{mod}4)$, $3x \equiv 5(\text{mod}6)$, and $4x \equiv 1(\text{mod}7)$.

**Exercise 4.204.** Solve the system $2x \equiv 3(\text{mod}4)$, $5x \equiv 6(\text{mod}7)$, $9x \equiv 10(\text{mod}11)$ using the Chinese Remainder theorem.

# Chapter 5

# Euler's Theorem

Euler's theorem is a fundamental statement in modular arithmetic. While it may seem daunting at first, this theorem is actually quite simple to understand once you break it down into its component parts.

In this book, the author takes you through the basics of Euler's theorem step-by-step, explaining everything in a clear and concise manner. The accompanying illustrations are also very helpful, making it easy for beginners to follow along. By the end of the book, you will have a solid understanding of this important theorem and be able to apply it to various real-world scenarios.

Euler's theorem is a statement in modular arithmetic that says that for any integer a and any prime number p, the congruence relation $a^{\phi}(p) \equiv 1 \pmod{p}$ holds. Here, $\phi(p)$ is Euler's totient function, which gives the number of positive integers less than or equal to p that are coprime to p. This theorem is named after Leonhard Euler, who proved it in 1736.

Euler's theorem has several important applications. For instance, it can be used to demonstrate Fermat's little theorem, which states that for any prime number p and any integer a coprime to p, the congruence relation $a^{(p-1)} \equiv 1( \pmod{p}$ holds.

Additionally, Euler's theorem can be used to find modular multiplicative inverses. That is, given an integer a and a modulus m, Euler's theorem can be used to calculate the modular multiplicative inverse of a modulo m. This is significant because modular multiplicative inverses are essential for many algorithms, such as the Extended Euclidean algorithm and the Chinese remainder theorem.

In summary, Euler's theorem is an important result with many applications in mathematics and computer science. Overall, Euler's theorem is a powerful tool that can be used to understand and manipulate numbers in modular arithmetic.

One way to apply Euler's theorem is to find the modular inverse of a number. Suppose we want to find the modular inverse of 7 (modulo 11). We can use Euler's theorem to do this as follows: since 7 is relatively prime to 11, we have $7^10 = 1 \pmod{11}$. This means that the modular inverse of 7 is 10 (modulo 11).

Euler's theorem can also be used to solve Congruence equations. For example, suppose we want to solve the equation $3x \equiv 5 \pmod 7$. Using Euler's theorem, we can rewrite this equation as $3x \equiv 5 \pmod 7 = 3x^6 \equiv 5x^6 \pmod 7$, which can be further simplified to $x^6 \equiv 35 \pmod 7$. This equation can then be solved using modular exponentiation.

Thus, Euler's theorem has many applications in mathematics and other fields. It is a useful tool for simplifying equations and solving Congruence equations.

Wilson's theorem states that a natural number n is prime if and only if the factorial of its predecessor is congruent to negative one modulo the number itself. This theorem is named after Edward Wilson, who proved it in 1836.

Wilson's theorem has a number of applications in cryptography and number theory. For example, it can be used to test whether a given number is prime; if the number passes the test, then it is probably prime, but if it fails, then it definitely isn't prime. The theorem can also be used to find prime numbers in certain sequences of numbers. In general, Wilson's theorem is a simple yet powerful tool for working with prime numbers.

In number theory, Fermat's little theorem states that if p is a prime number, then for any integer a, the number $a^p - a$ is an integer multiple of p. In other words, if we divide $a^p - a$ by p, the remainder is always zero. This theorem is named after Pierre de Fermat, who first proved it in 1640.

The modular arithmetic properties of primes are important in number theory and have applications to computer science, cryptography, and other areas of mathematics.

For example, modular arithmetic is used in RSA encryption, which is a widely used method of data security. In RSA encryption, two large prime numbers are used to generate a public key and a private key. The public key can be shared with anyone, but the private key must be kept secret. To encrypt a message, the sender uses the recipient's public key. To decrypt the message, the recipient uses their private key. Fermat's little theorem is used to ensure that only the intended recipient can decrypt the message; if someone else tries to decrypt the message using the public key, they will not be able to because they do not have the correct private key. Without this security feature, RSA encryption would not be possible.

Fermat's little theorem is a simple but powerful result with far-reaching implications. It is one of the building blocks of modern number theory and has helped to pave the way for many advances in mathematics and computer science.

Euler's Totient-Function is a function named after 18th-century mathematician Leonhard Euler, who first described it. Basically, the Totient-Function takes a positive integer as input and outputs how many positive integers less than or equal to the input are relatively prime to the input.

In modular arithmetic, two numbers are said to be relatively prime if they have no common factors other than 1. For example, the numbers 3 and 4 are relatively prime because the only factor they have in common is 1. On the other hand, the numbers 6 and 8 are not relatively prime because they have the common factor 2. The Totient-Function is useful in modular arithmetic because it can be used to find modular inverses.

A modular inverse is an integer that when multiplied by another integer produces 1 modulo some number. For example, the modular inverse of 3 modulo 7 is 5 because 3*5 = 15 and 15 mod 7 = 1. Finding modular inverses can be useful for things like decrypting messages that have been encrypted using the RSA algorithm.

This theorem is extremely important because it allows mathematicians to work with very large numbers by breaking them down into smaller pieces.

For example, suppose we want to find the value of $2^1$000000 (two to the one-millionth power). This number is too large to calculate directly, but we can use Euler's Theorem to break it down into smaller pieces. Thus, Euler's Theorem is a vital tool and without this theorem, many problems would be intractable.

Euler's Theorem is probably the single most important theorem in modular arithmetic. This book will take you through the basics of Euler's theorem step-by-step, explaining everything in a clear and concise manner. The accompanying illustrations are also very helpful, making it easy for beginners to follow along. By the end of the book, you will have a solid understanding of this important theorem and be able to apply it to various real-world scenarios. Conclusion

This book is an excellent introduction to Euler's theorem and would be ideal for anyone who wants to learn more about it. The author takes you through the basics of the theorem step-by-step, explaining everything in a clear and concise manner. The accompanying illustrations are also very helpful, making it easy for beginners to follow along. By the end of the book, you will have a solid understanding of this important theorem and be able to apply it to various real-world scenarios.

## 5.1 Wilson's Theorem

This theorem is named after one of Edward Waring's students, John Wilson. But actually, Wilson only observed the result to be true and did not provide its proof. Later Euler proved Wilson's theorem and then Gauss gave a generalization. Basically, the theorem states that the factorial of a prime number minus one is congruent to minus one modulo the prime. Interestingly, its converse is also well-known and gives a sufficient condition for an integer to be a prime.

Before we state and prove Wilson's theorem let's Illustrate with $p = 13$. For $p = 13$ we have $(13-1)! \equiv -1 \pmod{13}$ which we can prove by using the $(13-3)/2$ congruences
$2 \cdot 7 \equiv 1 \pmod{13}$, $3 \cdot 9 \equiv 1 \pmod{13}$,
$4 \cdot 10 \equiv 1 \pmod{13}$,
$5 \cdot 8 \equiv 1 \pmod{13}$, and
$6 \cdot 11 \equiv 1 \pmod{13}$. When these $(13-3)/2$ congruences are multiplied together and the factors are rearranged, we get $2 \cdot 3 \cdot 4 \cdots (13-2) \equiv 1 \pmod{13}$ and thus $(13-2)! \equiv 1 \pmod{13}$; whence $(13-1)! \equiv -1 \pmod{13}$.

**Theorem 5.1.** *[Wilson] If $p$ is prime, then $(p-1)! \equiv -1 \pmod{p}$.*

*Proof.* The cases $p = 2$ and $p = 3$ are evident. Choose any integer $a$ from the list $1, 2, 3, ..., p-1$. Recall that the linear congruence $ax \equiv 1 \pmod{p}$ has a unique solution $x$, since $(a, p) = 1$. Notice that if $ax \equiv 1 \pmod{p}$ and $a = x$ then $a \equiv \pm 1 \pmod{p}$ and so there are exactly $\left(\frac{p-3}{2}\right)$ pairs left. If we omit the numbers 1 and $p-1$, the effect is to group the remaining integers $2, 3, ..., p—2$ into pairs $a$ and $b$ where $a \neq b$, such that their product $ab \equiv 1 \pmod{p}$. When these $(p—3)/2$ congruences are multiplied together and the factors are rearranged, we get $2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \pmod{p}$ and thus $(p-2)! \equiv 1 \pmod{p}$; whence $(p-1)! \equiv -1 \pmod{p}$ as desired.

□

**Theorem 5.2.** *[Converse of Wilson's Theorem] If $n > 2$ is a positive integer such that $(n-1)! \equiv -1 \pmod{n}$, then $n$ is prime.*

*Proof.* Assume that $n$ is not prime and $(n-1)! \equiv -1 \pmod{n}$; and so there is some nontrivial factor $a$ of $n$ for which $a|(n-1)!$; whence $a|1$ since $nk - (n-1)! = 1$ for some integer $k$. Therefore, $a$ can not exist and so $n$ is prime.

□

## 5.2 Fermat's Theorem

Given a prime number $p$ and a positive integer $a$, Fermat's Theorem says that $a$ to the $p-1$ power is congruent to 1 modulo $p$. Fermat's Theorem takes care of solving linear congruences with prime modulus and provides a formula for finding the solution.

**Example 5.1.**

Before stating and proving Fermat's Theorem let's consider the congruence $5^{22} \equiv 1 \pmod{23}$. To illustrate why this is true, let $p = 23$ and $a = 5$. Notice that $1 \cdot 5 \equiv 5 \pmod{23}$ and see 5.1 for the other congruences.

Table 5.1: Fermat's Theorem in the case $p = 23$ and $a = 5$.

| | | |
|---|---|---|
| $2 \cdot 5 \equiv 10 \pmod{23}$ | $3 \cdot 5 \equiv 15 \pmod{23}$ | $4 \cdot 5 \equiv 20 \pmod{23}$ |
| $5 \cdot 5 \equiv 2 \pmod{23}$ | $6 \cdot 5 \equiv 7 \pmod{23}$ | $7 \cdot 5 \equiv 12 \pmod{23}$ |
| $8 \cdot 5 \equiv 17 \pmod{23}$ | $9 \cdot 5 \equiv 22 \pmod{23}$ | $10 \cdot 5 \equiv 4 \pmod{23}$ |
| $11 \cdot 5 \equiv 9 \pmod{23}$ | $12 \cdot 5 \equiv 14 \pmod{23}$ | $13 \cdot 5 \equiv 19 \pmod{23}$ |
| $14 \cdot 5 \equiv 1 \pmod{23}$ | $15 \cdot 5 \equiv 6 \pmod{23}$ | $16 \cdot 5 \equiv 11 \pmod{23}$ |
| $17 \cdot 5 \equiv 16 \pmod{23}$ | $18 \cdot 5 \equiv 21 \pmod{23}$ | $19 \cdot 5 \equiv 3 \pmod{23}$ |
| $20 \cdot 5 \equiv 8 \pmod{23}$ | $21 \cdot 5 \equiv 13 \pmod{23}$ | $22 \cdot 5 \equiv 18 \pmod{23}$ |

Consequently, we have,

$$\prod_{k=1}^{22} (k \cdot 5) = 5^{22} 22! \equiv 22! \pmod{23}$$

Whence, $5^{22} \equiv 1 \pmod{23}$.

**Theorem 5.3.** *[Fermat] If $p$ is prime and $a$ is a positive integer with $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$*

*Proof.* Consider the $p-1$ integers: $a, 2a, 3a, ..., (p-1)a$. These integers have the following property: if $ra \equiv sa \pmod{p}$ with $1 \leq r < s \leq p-1$, then $r \equiv s \pmod{p}$ because $(a, p) = 1$. Therefore, these integers must be congruent modulo $p$ to $1, 2, 3, ..., p-1$ taken in some order. Multiplying all of these congruence together yields $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$ and since $((p-1)!, p) = 1$, we have $a^{p-1} \equiv 1 \pmod{p}$ as desired.

□

If $p$ is prime and $a$ is a positive integer with $(a, p) = 1$, then $a^p \equiv a \pmod{p}$ follows as well because $a^{p-1} \equiv 1 \pmod{p}$ and so $a^p \equiv a \pmod{p}$.

If $(a, p) = p$ then $a^p \equiv a \equiv 0 \pmod{p}$ and so in either case we have $a^p \equiv a \pmod{p}$.

**Example 5.2.** Use Fermat's theorem to solve $23x \equiv 1 \pmod{53}$.

*Solution.* Since 53 is prime and $(23, 53) = 1$ we can apply Fermat's theorem, to find $23^{52} \equiv 1 \pmod{53}$. Therefore a solution is $x \equiv 23^{51} \pmod{53}$. Using $23^{25} \equiv 23 \pmod{53}$, we find the solution to be $x \equiv 23 \cdot 23 \cdot 23 \equiv 30 \pmod{53}$.

**Example 5.3.** Compute $2^{340}$ modulo 341. Use this to show that the converse of Fermat's Theorem is not true.

*Solution.* Since $2^{340} \equiv 1 \pmod{341}$, if the converse of Fermat's Theorem were true then 341 would be prime. However, $341 = 11 \cdot 13$ and so the converse of Fermat Little Theorem is not true.

**Example 5.4.** Show that if $p$ is a prime and $a$ is an integer such that $(a, p) = 1$, then $a^{p-2}$ is an inverse of $a$ modulo $p$.
Find the inverse of 5 modulo 23.

*Solution.* By Fermat's Theorem we know that $a^{p-1} \equiv 1 \pmod{p}$ and so $a \cdot a^{p-2} \equiv 1 \pmod{p}$. Therefore, $a^{p-2}$ is an inverse of $a$ modulo $p$.
Since $5^{22} = 5 \cdot 5^{21} \equiv \pmod{23}$ and $5^{21} \equiv 14 \pmod{23}$. We see that $5 \cdot 14 \equiv 1 \pmod{23}$ and so 14 is the inverse of 5 modulo 23.

**Example 5.5.** Show that if $a$ and $b$ are positive integers and $p$ is a prime with $(a, p) = 1$, then the solutions of the linear congruence $ax \equiv b \pmod{p}$ are the integers $x$ such that $x \equiv a^{p-2}b \pmod{p}$.

**Example 5.6.** Solve the two linear congruences $4x \equiv 11 \pmod{19}$ and $5x \equiv 19 \pmod{23}$.

*Solution.* Since $a^{p-2}$ is the inverse of $a$ modulo $p$ we have

$$ax \equiv a\left(a^{-1}b\right) = \left(aa^{p-2}\right)b = a^{p-1}b \equiv b \pmod{p}$$

by Fermat's Theorem.

**Example 5.7.** By Fermat's Theorem we have $4^{18} \equiv 1 \pmod{19}$ and $5^{22} \equiv 1 \pmod{23}$; so $x \equiv 4^{17} \cdot 11 \equiv 17 \pmod{19}$ is the solution to

$4x \equiv 11 \pmod{19}$ and $x \equiv 5^{21} \cdot 19 \equiv 13 \pmod{23}$ is the solution to $5x \equiv 19 \pmod{23}$.

**Example 5.8.** Show $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ when $p$ and $q$ are distinct primes.

*Solution.* By Fermat's Theorem we have $p^{q-1} \equiv 1 \pmod{q}$ and $q^{p-1} \equiv 1 \pmod{p}$; thus we consider the system $x \equiv 1 \pmod{p}$ and $x \equiv 1 \pmod{q}$. Using the Chinese Remainder Theorem we have,

$$x \equiv 1\left(\frac{pq}{q}\right)p^{q-2} + 1\left(\frac{pq}{p}\right)q^{q-2} \pmod{pq}.$$

Finally since $(p,q) = 1$, we have $x \equiv p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ as desired.

## 5.3 Euler's $\phi$-function

**Definition 5.1.** For each integer $n > 1$, let $\phi(n)$ denote the number of positive integers less than $n$ and relatively prime to $n$ and let $\phi(1) = 1$. The function $\phi$ is called the **totient function**, or sometimes, Euler's $\phi$-function.

Euler's totient function as many amazing properties.
For example, notice that

$$\begin{aligned}
&\phi(13) = 13 - 1 = 12 \\
&\phi\left(5^3\right) = 5^2 - 5^1 = 20 \\
&\phi(35) = \phi(5)\phi(7) = (5-1)(7-1) = 24.
\end{aligned}$$

### Properties of the Euler Function

**Lemma 5.1.** *If $p$ is a prime number, then $\phi(p) = p - 1$.*

*Proof.* Since 1, 2, 3, ..., $p-1$ are relatively prime to the prime $p$, $\phi(p) = p - 1$.

□

**Lemma 5.2.** *If $p$ is a prime number, then $\phi\left(p^r\right) = p^r - p^{r-1}$.*

*Proof.* By Euclid's Lemma, the integers $k$ such that $1 \leq k \leq p^r$ and $k$ is divisible by $p$ are $p, 2p, 3p, ..., \left(p^{r-1}\right)p$. Thus the number of positive integers less than $p^r$ and relatively prime to $p^r$ is

$$p^r - 1 - \left(p^{r-1} - 1\right) = p^r - p^{r-1}$$

as desired.

□

**Lemma 5.3.** *If $p$ and $q$ are distinct primes, then $\phi(pq) = (p-1)(q-1)$.*

*Proof.* By Euclid's Lemma, an integer $k$ will satisfy $(k, pq) > 1$ if and only if $p|k$ or $q|k$ and the number of such $k$ is $(p-1) + (q-1)$.
Thus the number of $k$ such that $(k, pq) = 1$ and $1 \leq k < pq$ is

$$pq - 1 - ((p-1) + (q-1)) = (p-1)(q-1)$$

as desired.

□

**Lemma 5.4.** *If $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.*

*Proof.* There are $\phi(n)$ congruence classes which are represented by an integer relatively prime to $n$ in $\mathbb{Z}_n$. Let these representatives be $a_1, ..., a_{\phi(n)}$. The products $aa_1, ..., aa_{\phi(n)}$ are all distinct because $(a, n) = 1$ and since each product is still relatively prime to $n$, there is a representative from each of the $\phi(n)$ congruence classes $a_1, ..., a_{\phi(n)}$. Therefore,

$$a_1 a_2 \cdots a_{\phi(n)} \equiv (aa_1)(aa_2) \cdots \left(aa_{\phi(n)}\right) \equiv a^{\phi(n)} \left(a_1 \cdots a_{\phi(n)}\right) \pmod{n}.$$

Since $\left(a_1 \cdots a_{\phi(n)}, n\right) = 1$, we have $a^{\phi(n)} \equiv 1 \pmod{n}$ as desired.

□

**Theorem 5.4.** *If $n = {p_1}^{e_1} {p_2}^{e_2} \cdots {p_k}^{e_k}$ is the unique prime factorization of $n$, then*

$$\phi(n) = \left({p_1}^{e_1} - {p_1}^{e_1 - 1}\right)\left({p_2}^{e_2} - {p_2}^{e_2 - 1}\right) \cdots \left({p_k}^{e_k} - {p_k}^{e_k - 1}\right).$$

**Example 5.9.** Show that if $n$ is an odd integer, then $\phi(4n) = 2\phi(n)$.

::: {.proof }[Solution] Since $n$ is an odd integer $(4,n)=1$ and so $\phi(4n)=\phi(4)\phi(n)=2\phi(n)$.
:::

**Example 5.10.** Show that if $m$ and $n$ are positive integers then, $m|n \Longrightarrow \phi(m)|\phi(n)$.

::: {.proof }[Solution] Let $n=p_1^{e_1}\cdots {p_s}^{e_s}$ be the unique prime factorization of $n$. Since $m|n$ we have $m={p_1}^{f_1}\cdots {p_s}^{f_s}$ where $0\leq f_i\leq e_i$ for $i=1,2,...,s$. Using $\phi\left(p^\alpha\right)=p^\alpha-p^{\alpha-1}$
we have

$$\begin{aligned}
\phi(n) &= \phi\left(p_1^{e_1}\cdots p_s^{e_s}\right)\\
&= \phi\left(p_1^{e_1}\right)\cdots\phi\left(p_s^{e_s}\right)\\
&= \left(p_1^{e_1}-p_1^{e_1-1}\right)\cdots\left(p_s^{e_s}-p_s^{e_s-1}\right)\\
&= p_1^{e_1-1}\left(p_1-1\right)\cdots {p_s}^{e_s-1}\left(p_s-1\right)\\
&= p_1^{e_1-f_1}p_1^{f_1-1}\left(p_1-1\right)\cdots p_s^{e_s-f_s}{p_s}^{f_s-1}\left(p_s-1\right)\\
&= p_1^{e_1-f_1}\cdots {p_s}^{e_s-f_s}p_1^{f_1-1}\left(p_1-1\right)\cdots {p_s}^{f_s-1}\left(p_s-1\right)\\
&= p_1^{e_1-f_1}\cdots {p_s}^{e_s-f_s}\phi\left({p_1}^{f_1}\right)\cdots\phi\left({p_s}^{f_s}\right)\\
&= {p_1}^{e_1-f_1}\cdots {p_s}^{e_s-f_s}\phi(m)
\end{aligned}$$

Therefore, $\phi(m)|\phi(n)$ as desired.
:::

## Solving Euler Functional Equations

**Example 5.11.** Solve the functional equation $\phi(n)=10$.

::: {.proof }[Solution] The claim is that $n=2^a3^b11^c$ for some integers $a,b$, and $c$. To see this let $\alpha$ be the highest power of $p$ dividing $n$, then there is an integer $k$ with $(p,k)=1$ and $\phi(n)=\phi\left(p^\alpha k\right)=\phi\left(p^\alpha\right)\phi(k)=\left(p^\alpha-p^{\alpha-1}\right)\phi(k)=p^{\alpha-1}(p-1)\phi(k)=10$. Since $(p-1)|10$ we must have $p-1=1,2,5$, or $10$ and so $p=2,3$, or $11$. Now we should try to bound the exponents $a,b$, and $c$. Since,

$$\phi(n)=\phi\left(2^a3^b11^c\right)=\left(2^a-2^{a-1}\right)\left(3^b-3^{b-1}\right)\left(11^c-11^{c-1}\right)=10 \quad (5.1)$$

the exponents $a,b$, and $c$ must be less than or equal to $2,1$, and $1$ respectively. We tabulate to find the solutions.

| $a$ | $b$ | $c$ | $n$ | $\phi(n)$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 |
| 0 | 0 | 1 | 11 | 10 |
| 0 | 1 | 0 | 3 | 2 |
| 0 | 1 | 1 | 33 | 20 |
| 0 | 2 | 0 | 9 | 6 |
| 0 | 2 | 1 | 99 | 60 |

| $a$ | $b$ | $c$ | $n$ | $\phi(n)$ |
|---|---|---|---|---|
| 1 | 0 | 0 | 2 | 1 |
| 1 | 0 | 1 | 22 | 10 |
| 1 | 1 | 0 | 6 | 2 |
| 1 | 1 | 1 | 66 | 20 |
| 1 | 2 | 0 | 18 | 6 |
| 1 | 2 | 1 | 198 | 60 |

| $a$ | $b$ | $c$ | $n$ | $\phi(n)$ |
|---|---|---|---|---|
| 2 | 0 | 0 | 4 | 2 |
| 2 | 0 | 1 | 44 | 20 |
| 2 | 1 | 0 | 12 | 4 |
| 2 | 1 | 1 | 132 | 40 |
| 2 | 2 | 0 | 36 | 12 |
| 2 | 2 | 1 | 396 | 120 |

:::

**Example 5.12.** Solve the functional equation $\phi(n) = 12$. ::: {.proof }[Solution] The claim is that $n = 2^a 3^b 5^c 7^d 13^e$ for some integers $a, b, c, d$, and $e$. To see this let $\alpha$ be the highest power of $p$ dividing $n$, then $\phi(n) = 12 = p^{\alpha-1}(p-1)\phi(k)$ for some integer $k$. Since $(p-1)|12$ we must have $p - 1 = 1, 2, 3, 4, 6, 12$ and so $p = 2, 3, 5, 7, 13$. Now we should try to bound the exponents if we can. If $\alpha = 2$, then $p|12$ and so $p = 2$ or $p = 3$. Therefore, $c, d$ and $e$ must be 0 or 1. If $\alpha = 3$, the $p^2\big|12$ and so $p = 2$. Therefore, $b$ must be 0,1, or 2. If $a = 4$, then $p^3\big|12$ and so $p \neq 2$. Therefore, $a$ must be 3 or less. If $p = 5$, then $12 = 4\phi(k)$ and so $\phi(k) = 3$ which is not possible. We are left with $n = 2^a 3^b 7^d 13^e$ and $0 \leq a \leq 3$, $0 \leq b \leq 2$, $0 \leq d \leq 1$, and $0 \leq e \leq 1$. These results are summarized in 5.2.

:::

Table 5.2: The functional equation $\phi(n) = 12$.

| $a$ | $b$ | $d$ | $e$ | $n$ | $\phi(n)$ |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 |
| 0 | 0 | 0 | 1 | 13 | 12 |
| 0 | 0 | 1 | 0 | 7 | 6 |
| 0 | 0 | 1 | 1 | 91 | 72 |
| 0 | 1 | 0 | 0 | 3 | 2 |
| 0 | 1 | 0 | 1 | 39 | 24 |
| 0 | 1 | 1 | 0 | 21 | 12 |
| 0 | 1 | 1 | 1 | 273 | 144 |
| 0 | 2 | 0 | 0 | 9 | 6 |
| 0 | 2 | 0 | 1 | 117 | 72 |
| 0 | 2 | 1 | 0 | 63 | 36 |
| 0 | 2 | 1 | 1 | 819 | 432 |
| 1 | 0 | 0 | 0 | 2 | 1 |
| 1 | 0 | 0 | 1 | 26 | 12 |
| 1 | 0 | 1 | 0 | 14 | 6 |
| 1 | 0 | 1 | 1 | 182 | 72 |

| $a$ | $b$ | $d$ | $e$ | $n$ | $\phi(n)$ |
|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 6 | 2 |
| 1 | 1 | 0 | 1 | 78 | 24 |
| 1 | 1 | 1 | 0 | 42 | 12 |
| 1 | 1 | 1 | 1 | 546 | 144 |
| 1 | 2 | 0 | 0 | 18 | 6 |
| 1 | 2 | 0 | 1 | 234 | 72 |
| 1 | 2 | 1 | 0 | 126 | 36 |
| 1 | 2 | 1 | 1 | 1638 | 432 |
| 2 | 0 | 0 | 0 | 4 | 2 |
| 2 | 0 | 0 | 1 | 52 | 24 |
| 2 | 0 | 1 | 0 | 28 | 12 |
| 2 | 0 | 1 | 1 | 364 | 144 |
| 2 | 1 | 0 | 0 | 12 | 4 |
| 2 | 1 | 0 | 1 | 156 | 48 |
| 2 | 1 | 1 | 0 | 84 | 24 |
| 2 | 1 | 1 | 1 | 1092 | 288 |

| $a$ | $b$ | $d$ | $e$ | $n$ | $\phi(n)$ |
|---|---|---|---|---|---|
| 2 | 2 | 0 | 0 | 36 | 12 |
| 2 | 2 | 0 | 1 | 468 | 144 |
| 2 | 2 | 1 | 0 | 252 | 72 |
| 2 | 2 | 1 | 1 | 3276 | 864 |
| 3 | 0 | 0 | 0 | 8 | 4 |
| 3 | 0 | 0 | 1 | 104 | 48 |
| 3 | 0 | 1 | 0 | 56 | 24 |
| 3 | 0 | 1 | 1 | 728 | 288 |
| 3 | 1 | 0 | 0 | 24 | 8 |
| 3 | 1 | 0 | 1 | 312 | 96 |
| 3 | 1 | 1 | 0 | 168 | 48 |
| 3 | 1 | 1 | 1 | 2184 | 576 |
| 3 | 2 | 0 | 0 | 72 | 24 |
| 3 | 2 | 0 | 1 | 936 | 288 |
| 3 | 2 | 1 | 0 | 504 | 144 |
| 3 | 2 | 1 | 1 | 6552 | 1728 |

## Reduced Residue System

**Definition 5.2.** A **reduced residue system** modulo $n$ is a set of $\phi(n)$ integers such that each element of the set is relatively prime to $n$, and no two different elements of the set are congruent modulo $n$.

Notice the set $A = \{1,2,3,4,5,6,7,8,9,10,11,12\}$ is a reduced residue system modulo 13 since $A$ contains $\phi(13) = 12$ integers which are all relatively prime with 13 and no two integers of $A$ are congruent modulo 13. The set $B = \{1,5,7,11\}$ is a reduced residue system modulo 12 since $B$ contains $\phi(12) = 4$ integers which are all relatively prime with 12 and no two integers of $B$ are congruent modulo 12. It is not hard to check that the following sets $C$, $D$, and $E$ are each a reduced residue system modulo 28.

$$C = \{1,3,5,9,11,13,15,17,19,23,25,27\}$$

$$D = \{\pm 1, \pm 3, \pm 5, \pm 9, \pm 11, \pm 13\}$$

$$E = \{\pm 5, \pm 15, \pm 25, \pm 45, \pm 55, \pm 65\}$$

Notice $E$ was obtain from $D$ by multiplying every integer of $D$ by 5.

**Lemma 5.5.** *If*

$$\left\{r_1, r_2, \dots, r_{\phi(m)}\right\}$$

*is a reduced residue system modulo* $m$ *and* $(a,m) = 1$, *then*

$$\left\{ar_1, ar_2, \dots, ar_{\phi(m)}\right\}$$

*is also a reduced residue system modulo* $m$.

*Proof.* For $\left\{ar_1, ar_2, \dots, ar_{\phi(m)}\right\}$ to be a reduced residue system modulo $m$ we need to show that

$$ar_i \not\equiv ar_j \qquad \text{for all } 1 \leq i < j \leq \phi(m). \tag{5.2}$$

and

$$(ar_i, m) = 1 \qquad \text{for all } 1 \leq i \leq \phi(m) \tag{5.3}$$

To prove 5.2, assume the contrary, $1 \leq i < j \leq \phi(m)$ and $ar_i \equiv ar_j \pmod{m}$. Then $r_i \equiv r_j \pmod{m}$ because $(a,m) = 1$. But $r_i \equiv r_j \pmod{m}$ can not happen because $\left\{r_1, r_2, \dots, r_{\phi(m)}\right\}$ is a reduced residue system modulo $m$. Therefore, $ar_i \not\equiv ar_j \pmod{m}$ and so 5.2 is proven.

To show 5.3 we suppose $1 \leq i \leq \phi(m)$ and that $p$ is a prime divisor of $(ar_i, m)$. Since $p|m$ we can not have $p\,|r_i$ because $(r_i, m) = 1$. It follows that, $(p, r_i) = 1$ and $p\,|ar_i$.
By Euclid's lemma $p|a$. Clearly, $p|a$ and $p|m$ contradict $(a,m) = 1$. Thus there is no prime divisor of $(ar_i, m)$ for any $1 \leq i \leq \phi(m)$ and so 5.3 is

proven.
Therefore, $\left\{ar_1, ar_2, \dots, ar_{\phi(m)}\right\}$ is also a reduced residue system modulo $m$.

□

## 5.4 Euler's Theorem

**Theorem 5.5.** *[Euler] If* $(a,m)=1$, *then*

$$a^{\phi(m)} \equiv 1 \pmod{m}. \tag{5.4}$$

*Proof.* Let $\left\{r_1, r_2, \dots, r_{\phi(m)}\right\}$ denote the reduced residue system modulo $m$ consisting of positive integers less than $m$. By 5.5, we know that

$$\left\{ar_1, ar_2, \dots, ar_{\phi(m)}\right\}$$

is also a reduced residue system modulo $m$. Moreover, the integers $r_1, r_2, \dots, r_{\phi(m)}$ are congruent to the integers $ar_1, ar_2, \dots, ar_{\phi(m)}$ modulo $m$ in some order. It follows that

$$a^{\phi(m)} r_1 \cdot r_2 \cdots r_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} \pmod{m}$$

and since $\left(r_1 \cdot r_2 \cdots r_{\phi(m)}, m\right) = 1$ we divide by $r_1 \cdot r_2 \cdots r_{\phi(m)}$ to obtain 5.4.

□

**Example 5.13.** Prove that the solution to the linear congruence $ax \equiv b \pmod{m}$ is $x \equiv a^{\phi(m)-1} b \pmod{m}$ provided $(a,m)=1$.
Then use Euler's $\phi$-function to solve the linear congruence $4x \equiv 781 \pmod{1183}$.

*Solution.* If $(a,m)=1$, then by Euler's theorem $a^{\phi(m)} \equiv 1 \pmod{m}$ and so multiplying by $b$ we have

$$a^{\phi(m)} b = a\left(a^{\phi(m)-1} b\right) \equiv b \pmod{m}$$

and so $x \equiv a^{\phi(m)-1} b \pmod{m}$ is a solution. By 4.7, this solution is unique. To solve the given linear congruence equation notice $(4, 1183) = 1$, and so by Euler's theorem, the solution is $x \equiv a^{\phi(m)-1} b \pmod{m}$ where $a = 4$, $m = 1183$, $b = 781$, and $\phi(1183) = 936$. Therefore the unique solution is $x \equiv 4^{935}(781) \equiv 491 \pmod{1183}$.

**Example 5.14.** Find the last digit in the decimal expansion of

$$n = 2 \cdot (7^{1000}) + 7 \cdot (3^{99,999}).$$

*Solution.* Since $\phi(10) = 4$ and $7^{1000} = 7^{4(250)}$, by Euler's Theorem we have,

$$7^{1000} = \left(7^4\right)^{250} \equiv 1^{250} \equiv 1 \pmod{10}.$$

So the last digit in the expansion of $7^{1000}$ is 1 and thus the last digit in the expansion of $2\left(7^{1000}\right)$ is of course 2.
Since $\phi(10) = 4$ and $3^{99,999} = 3^{4(24999)+3}$ by Euler's Theorem we have,

$$3^{99,999} = \left(3^4\right)^{24999} 3^3 \equiv 27 \equiv 7 \pmod{10}.$$

So the last digit in the expansion of $3^{99,999}$ is 7 and thus the last digit in the expansion of $7\left(7^{1000}\right)$ is of course 9. Since the sum of integers with last digit of 2 and last digit of 9 is 1, the last digit of $2\left(7^{1000}\right) + 3^{99,999}$ is 1.

## 5.5 Exercises

**Exercise 5.1.** What is the remainder when 16! is divided by 19?

**Exercise 5.2.** What is the remainder when 5! 25! is divided by 31?

**Exercise 5.3.** What is the remainder when 18! is divided by 437?

**Exercise 5.4.** What is the remainder when 40! is divided by 1763?

**Exercise 5.5.** Find the least positive residue of $8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13$ modulo 7.

**Exercise 5.6.** Show that $10! + 1$ is divisible by 11 by grouping together pairs of inverses modulo 11 that occur in 10!.

**Exercise 5.7.** Show that $12! + 1$ is divisible by 13 by grouping together pairs of inverses modulo 13 that occur in 12!.

**Exercise 5.8.** Show that if $m$ and $k$ are positive integers, then $\phi(m^k) = m^{k-1}\phi(m)$.

**Exercise 5.9.** Show that if $p$ is prime then

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}.$$

**Exercise 5.10.** Show that if $p > 2$ is prime then

$$1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod{p}.$$

**Exercise 5.11.** Show that if $p$ is prime and $p \equiv 3 \pmod{4}$, then

$$\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}.$$

**Exercise 5.12.** What is the remainder when 18! is divided by 437?

**Exercise 5.13.** Use Fermat's theorem to solve $23x \equiv 1 \pmod{91}$.

**Exercise 5.14.** Find the least positive residue of $9! + 10! + 11! + 12! + 13!$ modulo 11.

**Exercise 5.15.** Determine $\phi(n)$ for $n = 1, 2, 3, 4, 5$ and 6.

**Exercise 5.16.** Show that $\phi(5186) = \phi(5187) = \phi(5188)$.

**Exercise 5.17.** Find the least positive residue of $3^{999,999,999}$ modulo 7 and of $2^{1,000,000}$ modulo 17.

**Exercise 5.18.** Use Euler's theorem to find the least positive residue of $3^{100,000}$ modulo 35.

**Exercise 5.19.** Suppose $p \equiv 3 \pmod 4$. Show that $(p+1)/4$ is an integer and is the multiplicative inverse of 4 modulo $p$.

**Exercise 5.20.** Which is true:

- if $m|n$, then $\phi(m)|\phi(n)$ or
- if $\phi(m)|\phi(n)$, then $m|n$.

Both, neither, or one of them.

**Exercise 5.21.** Show that if $m$ and $k$ are positive integers, then

$$\phi\left(m^k\right) = m^{k-1}\phi(m).$$

**Exercise 5.22.** Show that if $a$ and $m$ are positive integers with $(a, m) = (a-1, m) = 1$, then

$$1 + a + a^2 + \cdots + a^{\phi(m)-1} \equiv 0 \pmod m.$$

**Exercise 5.23.** Show that if $c_1, c_2, ..., c_{\phi(m)}$ is a reduced residue system modulo $m$, where $m$ is a positive integer greater than 2, then $c_1 + c_2 + c_3 + \cdots + c_{\phi(m)} \equiv 0 \pmod m$.

**Exercise 5.24.** Find the value of the Euler phi-function for the given integer.

- 100
- 256
- 1001
- $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
- 10!
- 20!

**Exercise 5.25.** Find all positive integers $n$ such that $\phi(n) = 6$.

**Exercise 5.26.** Find all positive integers $n$ such that $\phi(n) = 14$.

**Exercise 5.27.** Find a reduced residue system modulo for each of the following integers.

- 9
- 10
- 14
- 16
- 17

**Exercise 5.28.** Solve the congruence $5x \equiv 3(\text{mod}14)$ by using Euler's theorem.

**Exercise 5.29.** Show that $\phi(5186) = \phi(5187) = \phi(5188)$.

**Exercise 5.30.** Show that if $n$ is an odd integer, then $\phi(4n) = 2\phi(n)$.

**Exercise 5.31.** Solve the functional equation $\phi(n) = 6$.

**Exercise 5.32.** Find the second to last digit in the decimal expansion of $43^{52}$.

**Exercise 5.33.** Show that if $n$ is an odd integer, then $\phi(4n) = 2\phi(n)$.

**Exercise 5.34.** Solve the functional equation $\phi(n) = 6$.

**Exercise 5.35.** Show that if $m$ and $k$ are positive integers, then $\phi(m^k) = m^{k-1}\phi(m)$.

*Solution.* If $n = {p_1}^{e_1}{p_2}^{e_2} \cdots p_k^{e_k}$ is the unique prime factorization of $n$, then

$$\phi(n) = \left(p_1^{e_1} - p_1^{e_1-1}\right)\left(p_2^{e_2} - p_2^{e_2-1}\right)\cdots\left(p_k^{e_k} - p_k^{e_k-1}\right).$$

**Exercise 5.36.** Determine which of the following quadratic congruences has solutions \ (a) $16x^2 + 5x + 1 \equiv 0 \pmod{31}$
\ (b) $16x^2 - 5x + 1 \equiv 0 \pmod{101}$.

*Solution.* Let $y = 2ax + b$ and $d = b^2 - 4ac$, then we have a simplified version $y^2 \equiv d \pmod{p}$.

**Exercise 5.37.** Let $p$ be an odd prime. Show that the quadratic congruence equation $ax^2 + bx + c \equiv 0 \pmod{p}$ has a solution if and only if

$$\left(\frac{b^2 - 4ac}{p}\right) = 1.$$

**Exercise 5.38.** Find the second to last digit in the decimal expansion of $43^{52}$.

**Exercise 5.39.** Use Euler's theorem to find any $x$ that satisfies the linear congruence equation $3x \equiv 13(\text{mod} 17)$.

**Exercise 5.40.** Determine $\phi(10440125)$.

# Chapter 6

# Quadratic Congruences

Math can be a difficult subject for some students, but with the right guide, anyone can understand it. Quadratic Congruence Equations is a comprehensive guide to the topic of quadratic congruence equations, written by an experienced math teacher. It provides clear explanations of all the basic concepts, as well as more advanced theories, and is perfect for students who want to learn more about the subject.

Most number theory book I've seen points out that the general problem of solving $x^2 \equiv a \pmod{m}$ can be reduced to solving the special case where m is a prime then spends most of the time studying this special case in detail. However, in this book, you'll learn how to reduce the general problem to the problem of prime moduli, or how you can unwind the reduction to produce a solution to the original problem.

Quadratic congruence equations are a type of equation that involves finding the remainder when a certain number is divided by another number. For example, the equation $x^2 \equiv 2 \pmod{3}$ is a quadratic congruence equation. The general form of a Quadratic Congruence Equation is $ax^2 + bx + c \equiv 0 \pmod{m}$, where $a, b, c$, and $m$ are integers.

Quadratic congruence equations can be a challenge to solve, but with the help of this book, you will find that they are much easier than most people think. I'll provide step-by-step instructions on how to reduce any general quadratic equation into its own specific case where the modulus is prime and then explain both methods for solving $x$ when it comes time! With these few tips under your belt, not only should things become more clear; however puzzles like these might even seem like child's play after all.

In number theory, an integer q is called a quadratic residue modulo n if it is congruent to a perfect square modulo n; i.e., if there exists an integer x such that: $q \equiv x^2 \pmod{n}$. Otherwise, q is called a quadratic nonresidue modulo n. For example, 3 is a quadratic residue modulo 5 because $32 \equiv 25 \equiv 0 \pmod{5}$, but 10 is not a quadratic residue modulo 5 because $102 \equiv 100 \equiv 25 \equiv 0 \pmod{5}$.

Quadratic residues play an important role in many areas of number theory, including the construction of various cryptographic systems. In addition, they have applications to engineering and physics. Quadratic residues are also interesting from the point of view of combinatorics: for example, the study of Gaussian binomials leads to the study of quadratic residues.

In Number Theory, they are used in Quadratic Sieve Methods to factorize large numbers. In Cryptography, they are used in various algorithms, such as the Quadratic Sieve algorithm and the Generalized Fermat Primality Test. Thus, Quadratic Residues are important in both Math and Computer Science.

In other words, the value of the Legendre symbol at a (nonzero) quadratic residue mod p is 1 and at a non-quadratic residue (non-residue) is $-1$. And the value of the Legendre symbol at 0 is 0.

The Legendre symbol was introduced by Adrien-Marie Legendre in 1798 in the course of his attempts to prove the law of quadratic reciprocity. The notational convenience of the Legendre symbol inspired the introduction of several other "symbols" used in algebraic number theory, such as the Hilbert symbol and the Artin symbol.

The Legendre symbol is important in many ways, one being that it provides a way to calculate whether a given number is a quadratic residue modulo a prime number. It also serves as a building block for other more complicated symbols in algebraic number theory, such as the Jacobi symbol and Dirichlet characters. Consequently, the Legendre symbol has many applications in fields such as mathematics, cryptography, and physics.

Two of the most celebrated mathematicians of all time, Leonhard Euler and Carl Friedrich Gauss, both made significant contributions to the study of quadratic congruences. In particular, they each developed a criterion for determining when a given quadratic equation has a solution modulo a prime number. These criteria, known as Euler's criterion and Gauss's criterion, are both still widely used today.

Euler's criterion states that a quadratic equation has a solution modulo a prime number $p$ if and only if the quantity $(a/p)$ is congruent to 1 or $-1$ modulo $p$. In other words, the equation must have at least one real solution when reduced modulo p. Gauss's criterion is similar, but rather than considering the quantity $(a/p)$, it looks at $(ab/p)$. This criterion states that a quadratic equation has a solution modulo a prime number $p$ if and only if the quantity $(ab/p)$ is congruent to 1 or $-1$ modulo $p$.

Both of these criteria are still widely used in number theory and other branches of mathematics. Indeed, they are both special cases of a more general theorem known as Quadratic Reciprocity. As such, they continue to be of great interest today.

The Law of Quadratic Reciprocity is a fundamental theorem in number theory that gives a condition for the solvability of quadratic congruences. Quadratic congruences are equations of the form $x^2 \equiv a \pmod{p}$, where $p$ is a prime number. The Law of Quadratic Reciprocity states that if p and q are prime numbers and p is not equal to q, then the following conditions are equivalent:

- $-x^2 \equiv a \pmod{p}$ is solvable if and only if $x^2 \equiv a \pmod{q}$ is solvable.
- $-p$ is a quadratic residue modulo $q$ if and only if $q$ is a quadratic residue modulo $p$.

This theorem has many applications in cryptography, as it can be used to construct efficient algorithms for factoring numbers. In general, the Law of Quadratic Reciprocity is a powerful tool for studying the properties of prime numbers.

The Tonelli-Shanks algorithm is a method for solving the Quadratic congruence equation. It is named after Italian mathematician Giuseppe Tonelli and British mathematician Alan M. Shanks. The Quadratic congruence equation is an equation of the form $ax^2 + bx + c \equiv 0 \pmod{n}$, where $a, b$, and $c$ are integers and $x$ is an unknown integer. The Tonelli-Shanks algorithm can be used to find the value of $x$ that satisfies the equation.

To do so, the algorithm first uses the Beijing theorem to factor the Quadratic congruence equation into a product of two linear factors. Then, it uses the Chinese remainder theorem to solve for $x$. The Tonelli-Shanks algorithm is a powerful tool for solving Quadratic congruence equations, and it can be used to find the values of x that satisfy any such equation.

The Tonelli-Shanks algorithm is significant because it provides an efficient way to solve quadratic congruences, which are equations that arise frequently in number theory and cryptography. In particular, the algorithm has applications for factoring integers and computing discrete logarithms. As such, it has been studied extensively by mathematicians and computer scientists alike.

This book is a comprehensive guide to the topic of quadratic congruence equations, written by an experienced math teacher. It provides clear explanations of all the basic concepts, as well as more advanced theories, and is perfect for students who want to learn more about the subject.

Anyone who wants to brush up on their skills will find this book helpful, whether they are struggling with math or not. My teaching style makes the material easy to understand, and the exercises at the end of each chapter help reinforce what has been learned. I highly recommend this book to anyone looking to improve their understanding of quadratic congruence equations.

## 6.1 General Quadratic Congruence

Consider the general quadratic congruence,

$$ax^2 + bx + c \equiv 0 \pmod{p} \tag{6.1}$$

where $p$ is an odd prime and $(a, p) = 1$. Inspired by completing the square, we have

$$\begin{aligned}
&ax^2 + bx + c \equiv 0 \pmod{p}\\
&4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}\\
&4a^2x^2 + 4abx + 4ac + (b^2 - 4ac) \equiv (b^2 - 4ac) \pmod{p}\\
&4a^2x^2 + 4abx + b^2 \equiv b^2 - 4ac \pmod{p}\\
&(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}
\end{aligned}$$

Let $y = 2ax + b$ and $d = b^2 - 4ac$, then we have a simplified version of (6.1), namely

$$y^2 \equiv d \pmod{p}. \tag{6.2}$$

Thus, solving 6.2 becomes the impetus.

### Quadratic Residues

**Definition 6.1.** Let $m$ be a positive integer with $(a, m) = 1$. If $x^2 \equiv a \pmod{m}$ has a solution then $a$ is a **quadratic residue** of $m$. If $x^2 \equiv a \pmod{m}$ does not have solution then $a$ is a **quadratic nonresidue** of $m$.

**Theorem 6.1.** *Let $p$ be an odd prime. If $(a, p) = 1$, then $x^2 \equiv a \pmod{p}$ either has no solutions or exactly two incongruent solutions modulo $p$.*

*Proof.* If $x_0$ is a solution for $x^2 \equiv a \pmod{p}$ then so is $-x_0$. If $x_0 \equiv -x_0 \pmod{p}$ then $2x_0 \equiv 0 \pmod{p}$ and so $x_0 \equiv 0 \pmod{p}$ since $p$ is odd. Clearly, this can not happen and so if there are any solutions there are at least two incongruent solutions. If $x_0$ and $x_1$ are both solutions then ${x_0}^2 - {x_1}^2 \equiv (x_0 - x_1)(x_0 + x_1) \equiv 0 \pmod{p}$ and so either $x_0 \equiv -x_1 \pmod{p}$ or $x_0 \equiv x_1 \pmod{p}$.

□

### The Legendre Symbol

**Definition 6.2.** Let $p$ be an odd prime with $(a,p)=1$. The **Legendre symbol** is defined as follows:

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

Since the quadratic residues of 13 are $1,3,4,9,10,12$ and the quadratic non-residues of 13 are $2,5,6,7,8,11$. We can rewrite using the Legendre symbol,

$$\left(\frac{1}{13}\right)=\left(\frac{3}{13}\right)=\left(\frac{4}{13}\right)=\left(\frac{9}{13}\right)=\left(\frac{10}{13}\right)=\left(\frac{12}{13}\right)=1$$

and

$$\left(\frac{2}{13}\right)=\left(\frac{5}{13}\right)=\left(\frac{6}{13}\right)=\left(\frac{7}{13}\right)=\left(\frac{8}{13}\right)=\left(\frac{11}{13}\right)=-1.$$

Notice the relationship the quadratic residues and quadratic non-residues of 13 satisfies:

$$1^6\equiv 3^6\equiv 4^6\equiv 9^6\equiv 10^6\equiv 12^6\equiv 1 \pmod{13}$$

and

$$2^6\equiv 5^6\equiv 6^6\equiv 7^6\equiv 8^6\equiv 11^6\equiv -1 \pmod{13}.$$

So for each of these $a's$ we have $\left(\frac{a}{13}\right)\equiv a^{(13-1)/2} \pmod{13}$. Also notice that for $p=17$,

$$1^8\equiv 2^8\equiv 4^8\equiv 8^8\equiv 9^8\equiv 13^8\equiv 15^8\equiv 16^8\equiv 1 \pmod{17}$$

and

$$3^8\equiv 5^8\equiv 6^8\equiv 7^8\equiv 10^8\equiv 11^8\equiv 12^8\equiv 14^8\equiv -1 \pmod{17}.$$

So again for each of these $a's$ we have $\left(\frac{a}{17}\right)\equiv a^{(17-1)/2} \pmod{17}$.

## 6.2 Euler's and Gauss's Criterion

**Theorem 6.2.** *[Euler's Criterion] Let $p$ be an odd prime and $(a,p)=1$. Then*

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

*Proof.* The only values for $a^{(p-1)/2}$ are $\pm 1 \pmod p$. So it suffices to consider the cases $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{a}{p}\right) = -1$. If $\left(\frac{a}{p}\right) = 1$ then $x^2 \equiv a \pmod p$ has a solution say $x_0$. Then by Fermat's Little theorem,

$$a^{(p-1)/2} \equiv \left(x_0^2\right)^{(p-1)/2} \equiv x_0^{p-1} \equiv 1 \pmod p$$

since $(x_0, p) = 1$. Conversely, if $\left(\frac{a}{p}\right) = -1$ then $x^2 \equiv a \pmod p$ has no solution. The key idea is that we can group together the integers $1, 2, 3...., p{-}1$ into $(p{-}1)/2$ pairs each with product of $a$. Then multiplying these pairs together, and using Wilson's theorem, we have

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

To see why we can do this, note that $(y, p) = 1$ means $yx \equiv a \pmod p$ has exactly one solution say $x$ and this must happen precisely when $x \neq y$.

□

**Example 6.1.** Use Euler's Criterion to determine $\left(\frac{5}{23}\right)$ and $\left(\frac{9}{53}\right)$.

*Solution.* Since $(5, 23) = 1$ we have, by Euler's criterion,
$\left(\frac{5}{23}\right) \equiv 5^{11} \equiv 22 \equiv -1 \pmod{23}$ and so 5 is a quadratic nonresidue of 23.
Similarly,
$\left(\frac{9}{53}\right) \equiv 9^{26} \equiv 1 \pmod{53}$ and so 9 is a quadratic residue of 53.

::: {#thm- }[Gauss's Criterion] Let $p$ be an odd prime with $(a, p) = 1$. If $n$ is the number of least positive residues of the integers $a, 2a, 3a, ..., ((p-1)/2)a$ that exceed $p/2$, then

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

:::

*Proof.* Let

$$A = \left\{a, 2a, 3a, ..., \left(\frac{p-1}{2}\right)a\right\},$$

$\{r_1, r_2, ..., r_n\}$ be those least positive residues of $A$ that exceed $p/2$, and $\{s_1, s_2, ..., s_m\}$ be those least positive residues of $A$ that do not exceed $p/2$. It follows that

$$\{p - r_1, p - r_2, ..., p - r_n, s_1, s_2, ..., s_m\}$$

is a permutation of the set $\left\{1, 2, 3, ..., \left(\frac{p-1}{2}\right)\right\}$, and so

$$(p - r_1)(p - r_2) \cdots (p - r_n)\, s_1 s_2 \cdots s_m = 1 \cdot 2 \cdot 3 \cdots \left(\frac{p-1}{2}\right).$$

Simplifying with modulus $p$, we have

$$(-1)^n r_1 r_2 \cdots r_n s_1 s_2 \cdots s_m \equiv \left(\frac{p-1}{2}\right)! \pmod{p}$$

By definition of the $r_i's$ and $s_i's$ we know,

$$(-1)^n a(2a)(3a) \cdots \left(\frac{p-1}{2}\right) a \equiv \left(\frac{p-1}{2}\right) \pmod{p}$$

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

By Euler's Criterion $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv (-1)^n \pmod{p}$ as desired.

□

**Example 6.2.** Find $\left(\frac{7}{13}\right)$ and $\left(\frac{9}{53}\right)$ using Gauss's Lemma.

*Solution.* Since $(13-1)/2 = 6$ we look at the first 6 multiples of 7 namely: $7, 14, 21, 28, 35, 42$. The least positive residues $\pmod{13}$ are $7, 1, 8, 2, 9, 3$. The number of them that exceed $13/2$ is 3 namely: $7, 8, 9$. Therefore, $\left(\frac{7}{13}\right) = (-1)^3 = -1$. Since $(53-1)/2 = 26$ we look at the first 26 multiples of 9 $\pmod{53}$ namely

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 9 | 18 | 27 | 36 | 45 | 1 | 10 | 19 | 28 | 37 | 46 | 2 | 11 |
| 20 | 29 | 38 | 47 | 3 | 12 | 21 | 30 | 39 | 48 | 4 | 13 | 22. |

The number of them that exceeds $53/2$ is 12. Therefore,

$$\left(\frac{9}{53}\right) = (-1)^{12} = 1. \square$$

## 6.3 Quadratic Characters

**Example 6.3.** Quadratic Characters Show that if $p$ is an odd prime, then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4}. \end{cases} \tag{6.3}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1 \text{ or } 7 \pmod{8} \\ -1 & p \equiv 3 \text{ or } 5 \pmod{8}. \end{cases} \tag{6.4}$$

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv 1 \text{ or } 11 \pmod{12} \\ -1 & p \equiv 5 \text{ or } 7 \pmod{12}. \end{cases} \tag{6.5}$$

*Solution.* To verify 6.3, notice every odd prime is of the form $p = 4k + 1$ (that is $p \equiv 1 \pmod 4$) or of the form $p = 4k+3$ (that is $p \equiv -1 \pmod 4$). In the first case, Euler's Criterion yields $1 \equiv (-1)^{(p-1)/2} \equiv \left(\frac{-1}{p}\right)$ because $(p-1)/2$ is even. In the latter case, $(p-1)/2$ is odd and so Euler's Criterion yields
$-1 \equiv (-1)^{(p-1)/2} \equiv \left(\frac{-1}{p}\right)$.
The reader should verify the remaining formulas.

## 6.4 Properties of the Legendre Symbol

**Lemma 6.1.** *Let $p$ be an odd prime with $(a,p) = (b,p) = 1$. If $a \equiv b \pmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

*Proof.* The congruence $x^2 \equiv a$ has a solution if and only if $x^2 \equiv b \pmod p$ does because $a \equiv b \pmod p$.

□

**Lemma 6.2.** *If $p$ is an odd prime with $(a,p) = (b,p) = 1$, then*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right). \tag{6.6}$$

*Proof.* By Euler's Criterion we know

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right), \qquad b^{(p-1)/2} \equiv \left(\frac{b}{p}\right), \qquad \text{and} \qquad (ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right).$$

Therefore,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

and because the only values possible are ±1, 6.6 follows immediately.

□

**Lemma 6.3.** *If $p$ is an odd prime with $(a,p) = 1$, then $\left(\frac{a^2}{p}\right) = 1$.*

*Proof.* 6.2 yields $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1$ as desired.

□

**Lemma 6.4.** *If $p$ is an odd prime with $(a,p)=(b,p)=1$, then*

$$\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right).$$

*Proof.* By 6.2 and 6.3,

$$\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right)=\left(\frac{a}{p}\right)$$

follows immediately.

□

**Theorem 6.3.** *If $n$ has prime factorization*

$$n={p_1}^{2t_1+1}\cdots {p_k}^{2t_k+1}p_{k+1}^{2t_{k+1}}\cdots p_m^{2t_m}$$

*and $q$ is a prime not dividing $n$, then*

$$\left(\frac{n}{q}\right)=\left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right)\cdots\left(\frac{p_k}{q}\right).$$

*Proof.* By 6.4,

$$\left(\frac{n}{q}\right)=\left(\frac{{p_1}^{2t_1+1}}{q}\right)\left(\frac{{p_2}^{2t_2+1}}{q}\right)\cdots\left(\frac{{p_k}^{2t_k+1}}{q}\right)\left(\frac{{p_{k+1}}^{2t_k}}{q}\right)\cdots\left(\frac{{p_m}^{2t_m}}{q}\right)$$

By 6.3, we see that $\left(\frac{n}{q}\right)=\left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right)\cdots\left(\frac{p_k}{q}\right)$ as desired.

□

## 6.5 Law of Quadratic Reciprocity

**Theorem 6.4.** *Law of Quadratic Reciprocity Let $p$ and $q$ be distinct odd primes, then*

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

Notice that the Law of Quadratic Reciprocity is equivalent to the following.

$$\left(\frac{p}{q}\right)=\begin{cases}-\left(\frac{q}{p}\right) & \text{if } p\equiv q\equiv 3 \pmod 4\\ \left(\frac{q}{p}\right) & \text{otherwise}\end{cases}$$

**Example 6.4.** Evaluate $\left(\frac{29}{53}\right)$.

*Solution.* Since $29 \equiv 1 \pmod 4$ we have $\left(\frac{29}{53}\right) = \left(\frac{53}{29}\right)$. Since $53 \equiv 24 \pmod{29}$ and $24 = 2^2 6$,

$$\begin{aligned}\left(\frac{29}{53}\right) = \left(\frac{24}{29}\right) = \left(\frac{6}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right)\\ = (-1)\left(\frac{3}{29}\right) = (-1)\left(\frac{29}{3}\right) = (-1)\left(\frac{2}{3}\right) = 1.\end{aligned}$$

which shows $x^2 \equiv 29 \pmod{53}$ is not solvable.

**Example 6.5.** Evaluate $\left(\frac{30}{43}\right)$.

*Solution.* To evaluate $\left(\frac{30}{43}\right)$ we note that $30 = 2 \cdot 3 \cdot 5$. So we have

$$\left(\frac{30}{43}\right) = \left(\frac{2}{43}\right)\left(\frac{3}{43}\right)\left(\frac{5}{43}\right)$$

and since $43 \equiv 3 \pmod 4$, we see that $\left(\frac{30}{43}\right) = \left(\frac{2}{43}\right)(-1)\left(\frac{43}{3}\right)\left(\frac{43}{5}\right)$. Finally since $43 \equiv 3 \pmod 8$, $43 \equiv 1 \pmod 3$, and $43 \equiv 3 \pmod 5$ and so

$$\left(\frac{30}{43}\right) = (-1)\left(\frac{1}{3}\right)\left(\frac{3}{5}\right) = (-1)\left(\frac{3}{5}\right) = (-1)\left(\frac{5}{3}\right) = (-1)\left(\frac{2}{3}\right) = -1$$

which shows $x^2 \equiv 30 \pmod{43}$ is not solvable.

**Example 6.6.** Evaluate $\left(\frac{713}{1009}\right)$.

*Solution.* Since $713 = 23 \cdot 31$ we have $\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)$. So we break these down into the two parts 23 and 31 as follows:

$$\begin{aligned}
\left(\frac{23}{1009}\right) &= \left(\frac{1009}{23}\right) && \text{since } 1009 \equiv 1 \pmod 4 \\
\left(\frac{1009}{23}\right) &= \left(\frac{20}{23}\right) && \text{since } 1009 \equiv 20 \pmod{23} \\
\left(\frac{20}{23}\right) &= \left(\frac{5}{23}\right) && \text{since } 20 = 4^2 \cdot 5 \\
\left(\frac{5}{23}\right) &= \left(\frac{23}{5}\right) && \text{since } 5 \equiv 1 \pmod 4 \\
\left(\frac{23}{5}\right) &= \left(\frac{3}{5}\right) && \text{since } 23 \equiv 3 \pmod 5 \\
\left(\frac{3}{5}\right) &= \left(\frac{5}{3}\right) && \text{since } 5 \equiv 1 \pmod 4 \\
\left(\frac{5}{3}\right) &= \left(\frac{2}{3}\right) && \text{since } 5 \equiv 2 \pmod 3 \\
\left(\frac{2}{3}\right) &= -1 && \text{since } 3 \equiv 3 \pmod 8
\end{aligned}$$

and the second part follows from,

$$\begin{aligned}
\left(\frac{31}{1009}\right) &= \left(\frac{1009}{31}\right) && \text{since } 1009 \equiv 1 \pmod 4 \\
\left(\frac{1009}{31}\right) &= \left(\frac{17}{31}\right) && \text{since } 1009 \equiv 17 \pmod{31} \\
\left(\frac{17}{31}\right) &= \left(\frac{31}{17}\right) && \text{since } 17 \equiv 1 \pmod 4 \\
\left(\frac{31}{17}\right) &= \left(\frac{14}{17}\right) && \text{since } 31 \equiv 14 \pmod{17} \\
\left(\frac{14}{17}\right) &= \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) && \text{since } 14 = 2 \cdot 7 \\
\left(\frac{2}{17}\right)\left(\frac{7}{17}\right) &= \left(\frac{7}{17}\right) && \text{since } 17 \equiv 1 \pmod 8 \\
\left(\frac{7}{17}\right) &= \left(\frac{17}{7}\right) && \text{since } 17 \equiv 1 \pmod 4 \\
\left(\frac{17}{7}\right) &= \left(\frac{3}{7}\right) && \text{since } 17 \equiv 3 \pmod 7 \\
\left(\frac{3}{7}\right) &= (-1)\left(\frac{7}{3}\right) && \text{since } 7 \equiv 3 \pmod 4 \text{ and } 3 \equiv 3 \pmod 4 \\
(-1)\left(\frac{7}{3}\right) &= (-1)\left(\frac{1}{3}\right) = -1 && \text{since } 7 \equiv 1 \pmod 3.
\end{aligned}$$

Therefore, $\left(\frac{713}{1009}\right) = 1$.

**Example 6.7.** Solve the quadratic congruence $5x^2 - 3x + 21 \equiv 0 \pmod{53}$.

::: {.proof }[Solution] Let $y = 2ax+b = 10x-3$ and $d = (-3)^2-4(5(21) = -411 \equiv 13 \pmod{53}$. So the congruence becomes $y^2 \equiv 13 \pmod{53}$. We find that $y \equiv 15 \pmod{53}$ and $y \equiv 38 \pmod{53}$. Therefore we solve, $10x - 3 \equiv 15 \pmod{53}$ and $10x - 3 \equiv 38 \pmod{53}$. We find $x \equiv 23 \pmod{53}$ and $x \equiv 20 \pmod{53}$. :::

## 6.6 Tonelli–Shanks Algorithm

The Tonell–Shanks algorithm (sometimes called the RESSOL algorithm[1]) is used within modular arithmetic to solve a quadratic congruence equation of the form

$$x^2 \equiv a \pmod{p}$$

where $a$ is a quadratic residue (mod $p$), and $p$ is an odd prime. Tonelli–Shanks cannot be used for composite moduli. Note that, finding square roots modulo composite numbers is a computational problem equivalent to integer factorization [**?**].

::: {#thm- }[Shanks] Let $p$ be an odd prime and assume $(a, p) = 1$. Let $x$ be a solution to $x^2 \equiv a \pmod{p}$ and let $n$ and $k$ be integers such that $p-1 = 2^n k$ where $n \geq 1$ and $k$ is odd, and let $q$ be a quadratic nonresidue modulo $p$. Then $x$ can be found by repeating the following loop:

- Set $t = a^{(k+1)/2} \pmod{p}$ and find the least $i$ such that $r^{2^i} \equiv 1 \pmod{p}$ where $r = a^k \pmod{p}$.
- If $i = 0$ then the solutions are $x \equiv \pm t \pmod{p}$ else set $u \equiv q^{k(2^{n-i-1})} \pmod{p}$ and goto (i) and replace $t$ by $tu$ and $r$ by $ru^2$.

:::

### Examples of Shank's Algorithm

We solve three examples illustrating the use of 6.6.

**Example 6.8.** Solve the quadratic congruence $x^2 \equiv 29 \pmod{53}$.

::: {.proof }[Solution] First we find $53 - 1 = 52 = 2^2(13)$ and so we set $n = 2$ and $k = 13$. Next we find the a quadratic nonresidue. Since $\left(\frac{2}{53}\right) = -1$, we use $q = 2$. With $a = 29$, $q = 2$, $n = 2$, and $k = 13$ we perform Shanks algorithm.

Loop 1: We find $t = 29^7 \equiv 17 \pmod{53}$ and $r = 29^{13} \equiv 52 \pmod{53}$. Next we find $i$:

| $i$ | $52^{2^i}$ |
|---|---|
| 0 | $52^{2^0} \equiv 52 \pmod{53}$ |
| 1 | $52^{2^1} \equiv 1 \pmod{53}$ |

[1] or just Shank's Algorithm for short

Since $i \neq 0$ we find $u = 2^{13(2^{2-1-1})} \equiv 30 \pmod{53}$.

Loop 2: We find $t = 17(30) \equiv 33 \pmod{53}$ and $r = 52(30)^2 \equiv 1 \pmod{53}$. Next we find $i$:

| $i$ | $1^{2^i}$ |
|---|---|
| 0 | $1^{2^0} \equiv 1 \pmod{53}$ |

Since $i = 0$, we find $x = \pm 33 \pmod{53}$. Therefore the solutions are $x \equiv 20, 33 \pmod{53}$. :::

**Example 6.9.** Solve the quadratic congruence $x^2 \equiv 37 \pmod{137}$.

::: {.proof }[Solution] We let $a = 37$. Since $137 - 1 = 2^3 17$ we let $n = 3$, $k = 17$. Also, since $\left(\frac{3}{137}\right) = -1$ we let $q = 3$ and perform Shanks algorithm.

Loop 1: We find $t = 37^9 \equiv 37 \pmod{137}$ and $r = 37^{17} \equiv 37 \pmod{137}$. Next we find $i$:

| $i$ | $37^{2^i}$ |
|---|---|
| 0 | $37^{2^0} \equiv 37 \pmod{137}$ |
| 1 | $37^{2^1} \equiv 136 \pmod{137}$ |
| 2 | $37^{2^2} \equiv 1 \pmod{137}$ |

Since $i \neq 0$ we find $u = 127 \pmod{137}$.

Loop 2: We find $t = 37(127) \equiv 41 \pmod{137}$ and $r = 37(127)^2 \equiv 1 \pmod{137}$. Next we find $i$:

| $i$ | $1^{2^i}$ |
|---|---|
| 0 | $1^{2^0} \equiv 1 \pmod{137}$ |

Since $i = 0$ we find $x \equiv \pm 41 \pmod{137}$. Therefore the solutions are $x \equiv 41, 96 \pmod{137}$. :::

**Example 6.10.** Solve the quadratic congruence $x^2 \equiv 11 \pmod{257}$.

::: {.proof }[Solution] We let $a = 11$. Since $257 - 1 = 256 = 2^8(1)$ we let $n = 8$, $k = 1$. Also, since $\left(\frac{5}{257}\right) = -1$ we let $q = 5$ and perform Shanks algorithm.

Loop 1: We find $t = 11^1 \equiv 11 \pmod{257}$ and $r = 11^1 \equiv 11 \pmod{257}$.

Next we find $i$:

| $i$ | $11^{2^i}$ |
|---|---|
| 0 | $11^{2^0} \equiv 11 \pmod{257}$ |
| 1 | $11^{2^1} \equiv 121 \pmod{257}$ |
| 2 | $11^{2^2} \equiv 249 \pmod{257}$ |
| 3 | $11^{2^3} \equiv 64 \pmod{257}$ |
| 4 | $11^{2^4} \equiv 241 \pmod{257}$ |
| 5 | $11^{2^5} \equiv 256 \pmod{257}$ |
| 6 | $11^{2^6} \equiv 1 \pmod{257}$ |

Since $i \neq 0$ we find $u = 5^{1(2^{8-6-1})} \equiv 25 \pmod{257}$.

Loop 2: We find $t = 11(25) \equiv 18 \pmod{257}$ and $r = 11(25)^2 \equiv 193 \pmod{257}$. Next we find $i$:

| $i$ | $193^{2^i}$ |
|---|---|
| 0 | $193^{2^0} \equiv 193 \pmod{257}$ |
| 1 | $193^{2^1} \equiv 241 \pmod{257}$ |
| 2 | $193^{2^2} \equiv 256 \pmod{257}$ |
| 3 | $193^{2^3} \equiv 1 \pmod{257}$ |

Since $i \neq 0$ we find $u = 5^{1(2^{8-3-1})} \equiv 225 \pmod{257}$.

Loop 3: We find $t = 18(225) \equiv 195 \pmod{257}$ and $r = 193(225)^2 \equiv 256 \pmod{257}$. Next we find $i$:

| $i$ | $256^{2^i}$ |
|---|---|
| 0 | $256^{2^0} \equiv 256 \pmod{257}$ |
| 1 | $256^{2^1} \equiv 1 \pmod{257}$ |

Since $i \neq 0$ we find $u = 5^{1(2^{8-1-1})} \equiv 16 \pmod{257}$.

Loop 4: We find $t = 195(16) \equiv 36 \pmod{257}$ and $r = 256(16)^2 \equiv 1 \pmod{257}$. Next we find $i$:

| $i$ | $1^{2^i}$ |
|---|---|
| 0 | $1^{2^0} \equiv 1 \pmod{257}$ |

Since $i = 0$ we find $x \equiv \pm 36 \pmod{257}$. Therefore the solutions are $x \equiv 36, 221 \pmod{257}$. :::

## 6.7 Solving Quadratic Congruences

**Example 6.11.** Find all solutions to the quadratic congruence equation

$$f(x) = 2x^2 + 10x + 1 \equiv 0 \pmod{1429530274918301}. \qquad (6.7)$$

::: {.proof }[Solution] The first step in our method is to find the unique factorization of the modulus namely,

$$m = 1429530274918301 = 101^3 193^4.$$

Now we divide this problem into solving both of the following equations.

$$2x^2 + 10x + 1 \equiv 0 \pmod{101} \tag{6.8}$$

$$2x^2 + 10x + 1 \equiv 0 \pmod{193} \tag{6.9}$$

First we solve (6.8) by making the linear change of variables $y = 4x + 10$ and $d = 92$ because solving (6.8) is equivalent to solving $y^2 \equiv 92 \pmod{101}$ since

$$y^2 - 92 = (4x + 10)^2 - 92 \equiv 2x^2 + 10x + 1 \equiv 0 \pmod{101}.$$

To determine if $y^2 \equiv 92 \pmod{101}$ is solvable we compute the Legendre symbol $\left(\frac{92}{101}\right)$ by first factoring $92 = 2^2 23$ and then we apply the law of quadratic reciprocity to find,

$$\left(\frac{92}{101}\right) = \left(\frac{2^2}{101}\right)\left(\frac{23}{101}\right) = \left(\frac{23}{101}\right) = \left(\frac{101}{23}\right) = \left(\frac{9}{23}\right) = 1.$$

So now we use Shank's algorithm to solve $y^2 \equiv 92 \pmod{101}$. First we find $101 - 1 = 100 = 2^2(25)$ and so we set $n = 2$ and $k = 25$. With $a = 92$, $n = 2$, and $k = 25$ we perform Shanks algorithm and find $t \equiv 92^{13} \equiv 71 \pmod{101}$ and $r \equiv 92^{25} \equiv 1 \pmod{101}$. Therefore, Shank's algorithm terminates during the first loop and the solutions are $y = \pm 71$.

So we need to solve

$$71 \equiv 4x + 10 \pmod{101} \qquad \text{and} \qquad -71 \equiv 4x + 10 \pmod{101}.$$

For the first congruence equation we obtain $x \equiv 91 \pmod{101}$ and for the second we obtain $x \equiv 5 \pmod{101}$. Therefore the two solutions of the quadratic congruence $2x^2 + 10x + 1 \equiv 0 \pmod{101}$ are $x \equiv 91 \pmod{101}$ and $x \equiv 5 \pmod{101}$.

Next we solve (6.9) by making the linear change of variables $y = 4x + 10$ and $d = 92$ because solving $2x^2 + 10x + 1 \equiv 0 \pmod{193}$ is equivalent to solving $y^2 \equiv 92 \pmod{193}$. To determine if this equation is solvable we compute the Legendre symbol $\left(\frac{92}{193}\right)$ by first factoring $92 = 2^2 23$. Then

$$\left(\frac{92}{193}\right) = \left(\frac{2^2}{193}\right)\left(\frac{23}{193}\right) = \left(\frac{23}{193}\right) = \left(\frac{193}{23}\right) = \left(\frac{9}{23}\right) = 1$$

Therefore, $y^2 \equiv 92 \pmod{193}$ is solvable.

Now we use Shank's algorithm to solve $y^2 \equiv 92 \pmod{193}$. First we find $193 - 1 = 192 = 2^6(3)$ and so we set $n = 6$ and $k = 3$. Next we find a

quadratic nonresidue of 193 namely $q = 5$ since $\left(\frac{5}{193}\right) = -1$.
Now with $a = 92$, $q = 5$, $n = 6$, and $k = 3$ we perform Shank's algorithm

Loop 1: We find $t = 92^2 \equiv 165 \pmod{193}$ and $r = 92^3 \equiv 126 \pmod{193}$. Next we find $i$:

| $i$ | $126^{2^i}$ |
|---|---|
| 0 | $126^{2^0} \equiv 126 \pmod{193}$ |
| 1 | $126^{2^1} \equiv 50 \pmod{193}$ |
| 2 | $126^{2^2} \equiv 184 \pmod{193}$ |
| 3 | $126^{2^3} \equiv 81 \pmod{193}$ |
| 4 | $126^{2^4} \equiv 192 \pmod{193}$ |
| 5 | $126^{2^5} \equiv 1 \pmod{193}$ |

Since $i \neq 0$ we find $u = 5^{3(2^{6-5-1})} \equiv 125 \pmod{193}$.

Loop 2: We find $t = 165(125) \equiv 167 \pmod{193}$ and $r = 126(125)^2 \equiv 150 \pmod{193}$. Next we find $i$:

| $i$ | $150^{2^i}$ |
|---|---|
| 0 | $150^{2^0} \equiv 150 \pmod{193}$ |
| 1 | $150^{2^1} \equiv 112 \pmod{193}$ |
| 2 | $150^{2^2} \equiv 192 \pmod{193}$ |
| 3 | $150^{2^3} \equiv 1 \pmod{193}$ |

Since $i \neq 0$ we find $u = 5^{3(2^{6-3-1})} \equiv 64 \pmod{193}$.

Loop 3: We find $t = 167(64) \equiv 73 \pmod{193}$ and $r = 150(64)^2 \equiv 81 \pmod{193}$. Next we find $i$:

| $i$ | $81^{2^i}$ |
|---|---|
| 0 | $81^{2^0} \equiv 81 \pmod{193}$ |
| 1 | $81^{2^1} \equiv 192 \pmod{193}$ |
| 2 | $81^{2^2} \equiv 1 \pmod{193}$ |

Since $i \neq 0$ we find $u = 5^{3(2^{6-2-1})} \equiv 43 \pmod{193}$.

Loop 4: We find $t = 73(43) \equiv 51 \pmod{193}$ and $r = 81(43)^2 \equiv 1 \pmod{193}$.

Therefore, Shank's algorithm terminates and the solutions are $y = \pm 51$. So we need to solve $51 \equiv 4x+10 \pmod{193}$ and $-51 \equiv 4x+10 \pmod{193}$. For the first congruence equation we obtain $x \equiv 155 \pmod{193}$ and for the second we obtain $x \equiv 33 \pmod{193}$. Therefore the two solutions of the quadratic congruence $2x^2 + 10x + 1 \equiv 0 \pmod{193}$ are $x \equiv 155 \pmod{193}$ and $x \equiv 33 \pmod{193}$.

Next we will use Hensel's lifting theorem to lift to solutions modulo $101^3$ and $193^4$. Thus we compute $f'(x) = 4x + 10$ and we notice that

$$\begin{aligned} f'(5) &\equiv 30 \neq 0 \pmod{101} & f'(91) &\equiv 71 \neq 0 \pmod{101} \\ f'(33) &\equiv 142 \neq 0 \pmod{193} & f'(155) &\equiv 51 \neq 0 \pmod{193} \end{aligned}$$

Since these values of the derivative are nonzero we know each of these four solutions lift (uniquely) up to the necessary powers. To do so we compute the inverses of each, namely,

$$\begin{aligned} 30u_1 &\equiv 1 \pmod{101} \Rightarrow u_1 = 64 & 71u_2 &\equiv 1 \pmod{101} \Rightarrow u_2 = 37 \\ 142u_3 &\equiv 1 \pmod{193} \Rightarrow u_3 = 140 & 51u_4 &\equiv 1 \pmod{193} \Rightarrow u_4 = 53 \end{aligned}$$

Now using the inverses we just computed we can lift our 4 solutions as follows.

| $k$ | $x_k = x_{k-1} - f\left(x_{k-1}\right) 64$ |
|---|---|
| 1 | $x_1 \equiv 5 \pmod{101^1}$ |
| 2 | $x_2 = 5 - f(5) * 64 \equiv 3742 \pmod{101^2}$ |
| 3 | $x_3 = 3742 - f(3742) * 64 \equiv 64948 \pmod{101^3}$ |

| $k$ | $x_k = x_{k-1} - f\left(x_{k-1}\right) 37$ |
|---|---|
| 1 | $x_1 \equiv 91 \pmod{101^1}$ |
| 2 | $x_2 = 6454 - f(6454) * 37 \equiv 6454 \pmod{101^2}$ |
| 3 | $x_3 = 6454 - f(6454) * 37 \equiv 965348 \pmod{101^3}$ |

| $k$ | $x_k = x_{k-1} - f\left(x_{k-1}\right) 140$ |
|---|---|
| 1 | $x_1 \equiv 33 \pmod{193^1}$ |
| 2 | $x_2 = 33 - f(33) * 140 \equiv 21263 \pmod{193^2}$ |
| 3 | $x_3 = 21263 - f(21263) * 140 \equiv 6055601 \pmod{193^3}$ |
| 4 | $x_4 = 6055601 - f(6055601) * 140 \equiv 811229985 \pmod{193^4}$ |

| $k$ | $x_k = x_{k-1} - f\left(x_{k-1}\right) 53$ |
|---|---|
| 1 | $x_1 \equiv 155 \pmod{193^1}$ |
| 2 | $x_2 = 155 - f(155) * 53 \equiv 15981 \pmod{193^2}$ |
| 3 | $x_3 = 15981 - f(15981) * 53 \equiv 1133451 \pmod{193^3}$ |
| 4 | $x_4 = 1133451 - f(1133451) * 53 \equiv 576258011 \pmod{193^4}$ |

To recap, $2x^2 + 10x + 1 \equiv 0 \pmod{101^3}$ has solutions 64948 and 965348 and $2x^2 + 10x + 1 \equiv 0 \pmod{193^4}$ has solutions 811229985 and 576258011.

Finally, to solve our originally congruence equation we use the Chinese remainder theorem to solve the 4 linear systems:

$$(1)\begin{cases} x \equiv 64948 \pmod{101^3} \\ x \equiv 811229985 \pmod{193^4} \end{cases} \qquad (2)\begin{cases} x \equiv 64948 \pmod{101^3} \\ x \equiv 576258011 \pmod{193^4} \end{cases}$$

$$(3)\begin{cases} x \equiv 965348 \pmod{101^3} \\ x \equiv 811229985 \pmod{193^4} \end{cases} \qquad (4)\begin{cases} x \equiv 965348 \pmod{101^3} \\ x \equiv 576258011 \pmod{193^4} \end{cases}$$

We use the following tables to construct the four solutions.

| $i$ | $n_i$ | $a_i$ | $\bar{n}_i$ | $u_i$ |
|---|---|---|---|---|
| 1 | $101^3$ | 64948 | $193^4$ | $193^4 u_1 \equiv 1 \pmod{101^3} \Longrightarrow u_1 = 970433$ |
| 2 | $193^4$ | 811229985 | $101^3$ | $101^3 u_2 \equiv 1 \pmod{193^4} \Longrightarrow u_2 = 80623169$ |

So a solution to (1) is

$$\begin{aligned} x_1 &= (64948)\left(193^4\right)(970433) + (811229985)\left(101^3\right)(80623169) \\ &\equiv 1193121168121899 \pmod{m}. \end{aligned}$$

| $i$ | $n_i$ | $a_i$ | $\bar{n}_i$ | $u_i$ |
|---|---|---|---|---|
| 1 | $101^3$ | 64948 | $193^4$ | $193^4 u_1 \equiv 1 \pmod{101^3} \Longrightarrow u_1 = 970433$ |
| 2 | $193^4$ | 576258011 | $101^3$ | $101^3 u_2 \equiv 1 \pmod{193^4} \Longrightarrow u_2 = 80623169$ |

So the solution to (2) is

$$\begin{aligned} x_2 &= (64948)\left(193^4\right)(970433) + (576258011)\left(101^3\right)(80623169) \\ &\equiv 1386887794953578 \pmod{m}. \end{aligned}$$

| $i$ | $n_i$ | $a_i$ | $\bar{n}_i$ | $u_i$ |
|---|---|---|---|---|
| 1 | $101^3$ | 965348 | $193^4$ | $193^4 u_1 \equiv 1 \pmod{101^3} \Longrightarrow u_1 = 970433$ |
| 2 | $193^4$ | 811229985 | $101^3$ | $101^3 u_2 \equiv 1 \pmod{193^4} \Longrightarrow u_2 = 80623169$ |

So the solution to (3) is

$$\begin{aligned} x_3 &= (965348)\left(193^4\right)(970433) + (811229985)\left(101^3\right)(80623169) \\ &\equiv 42642479964718 \pmod{m}. \end{aligned}$$

| $i$ | $n_i$ | $a_i$ | $\bar{n}_i$ | $u_i$ |
|---|---|---|---|---|
| 1 | $101^3$ | 965348 | $193^4$ | $193^4 u_1 \equiv 1 \pmod{101^3} \Longrightarrow u_1 = 970433$ |
| 2 | $193^4$ | 576258011 | $101^3$ | $101^3 u_2 \equiv 1 \pmod{193^4} \Longrightarrow u_2 = 80623169$ |

So the solution to (4) is

$$\begin{aligned} x_4 &= (965348)\left(193^4\right)(970433) + (576258011)\left(101^3\right)(80623169) \\ &\equiv 236409106796397 \pmod{m}. \end{aligned}$$

Therefore, the four and only four solutions to 6.7 are 1193121168121899, 1386887794953578, 42642479964718, and 236409106796397. :::

## 6.8 Exercises

**Exercise 6.1.** Find a congruence describing all primes for which 5 is a quadratic residue.

**Exercise 6.2.** Find a congruence describing all primes for which 7 is a quadratic residue.

**Exercise 6.3.** Evaluate the Legendre symbol.

- $\left(\frac{7}{79}\right)$
- $\left(\frac{15}{101}\right)$
- $\left(\frac{31}{641}\right)$
- $\left(\frac{111}{991}\right)$
- $\left(\frac{105}{1009}\right)$
- $\left(\frac{1005}{10009}\right)$

**Exercise 6.4.** Solve the quadratic congruence.

- $x^2 + x + 1 \equiv 0 \pmod{7}$
- $x^2 + 5x + 1 \equiv 0 \pmod{7}$
- $x^2 + 3x + 1 \equiv 0 \pmod{7}$
- $x^2 \equiv 1 \pmod{15}$
- $x^2 \equiv 58 \pmod{77}$
- $x^2 \equiv 207 \pmod{1001}$

**Exercise 6.5.** Evaluate the Legendre symbols $\left(\frac{221}{881}\right)$ and $\left(\frac{855}{1009}\right)$.

**Exercise 6.6.** Determine which of the following quadratic congruences has solutions

- $16x^2 + 5x + 1 \equiv 0 \pmod{31}$
- $16x^2 - 5x + 1 \equiv 0 \pmod{101}$

**Exercise 6.7.** Let $p$ be an odd prime. Show that the quadratic congruence equation $ax^2 + bx + c \equiv 0 \pmod{p}$ has a solution if and only if $\left(\frac{b^2-4ac}{p}\right) = 1$

**Exercise 6.8.** Solve $2x^2 - 17x + 1 \equiv 0 \pmod{111400}$.

**Exercise 6.9.** Let $a$ and $b$ be integers not divisible by the prime $p$. Show that either one or all three of the integers $a, b$, and $ab$ are quadratic residues of $p$.

**Exercise 6.10.** Using the law of quadratic reciprocity to show each of the following is true.

- $\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{12} \\ -1 & p \equiv \pm 5 \pmod{12} \end{cases}$
- $\left(\frac{-3}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{6} \\ 1 & p \equiv -1 \pmod{6} \end{cases}$

**Exercise 6.11.** Find all of the quadratic residues of the following integers.

- 7
- 8
- 15
- 18

**Exercise 6.12.** Find the value of the Legendre symbol $\left(\frac{j}{11}\right)$ for $j = 1, 2, 3, 4, 5$, and 6.

**Exercise 6.13.** Evaluate the Legendre symbol $\left(\frac{7}{11}\right)$ using Euler's criterion.

**Exercise 6.14.** Evaluate the Legendre symbol $\left(\frac{7}{11}\right)$ using Gauss's lemma.

**Exercise 6.15.** Let $a$ and $b$ be integers not divisible by the prime $p$. Show that either one or all three of the integers $a$, $b$, and $ab$ are quadratic residues of $p$.

**Exercise 6.16.**

(a) Find a congruence describing all primes for which 5 is a quadratic residue.

(b) Find a congruence describing all primes for which 7 is a quadratic residue.

**Exercise 6.17.** Let $p$ be an odd prime. Show that the quadratic congruence equation $ax^2 + bx + c \equiv 0 \pmod{p}$ has a solution if and only if $\left(\frac{b^2-4ac}{p}\right) = 1$

**Exercise 6.18.** Find all the quadratic residues of 13.

**Exercise 6.19.** Determine if $x^2 \equiv 105( \pmod{1009}$ is solvable using Legendre symbols.

**Exercise 6.20.** Use Hensel's lifting theorem and the Chinese Remainder Theorem to solve the quadratic congruence equation $3x^2 + 11x + 2 \equiv 0(\text{mod}72)$.

**Exercise 6.21.** Determine whether (or not) Shank's Algorithm applies to $x^2 \equiv 6 \pmod{37}$.

**Exercise 6.22.** Determine whether (or not) Shank's Algorithm applies to $x^2 \equiv 21 \pmod{37}$.

**Exercise 6.23.** Rewrite an equivalent quadratic congruence (in standard form) and test whether (or not) Shank's Algorithm applies: $3x^2-2x+7 \equiv 0 \pmod{23}$.

**Exercise 6.24.** Solve $x^2 \equiv 25 \pmod{127}$.

**Exercise 6.25.** Solve $x^2 \equiv 35 \pmod{127}$.

**Exercise 6.26.** Determine whether (or not) Shank's Algorithm applies to $x^2 \equiv 6 \pmod{37}$.

**Exercise 6.27.** Determine whether (or not) Shank's Algorithm applies to $x^2 \equiv 21 \pmod{37}$.

**Exercise 6.28.** Rewrite an equivalent quadratic congruence (in standard form) and test whether (or not) Shank's Algorithm applies: $3x^2 - 2x + 7 \equiv 0 \pmod{23}$.

**Exercise 6.29.** Solve $x^2 \equiv 25 \pmod{127}$. [Hint: You may use Shank's Algorithm, but you do not need to.]

**Exercise 6.30.** Solve $x^2 \equiv 35 \pmod{127}$ using Shank's Algorithm.

# Chapter 7

# Polynomial Congruences

Polynomial Congruence Equations is a mathematics book designed for undergraduate number theory students. The purpose of this book is to provide students with a step-by-step guide on how to solve polynomial congruence equations. It also aims to help students understand the different concepts related to polynomials and their applications.

Two numbers are said to be congruent modulo m if they have the same remainder when divided by m. For example, 15 and 28 are congruent modulo 13 because both numbers leave a remainder of 12 when divided by 13. Congruence is an equivalence relation, which means that it is reflexive, symmetric, and transitive. Congruence modulo m is often written as $a \equiv b \pmod{m}$.

The set of all integers that are congruent modulo m is called an equivalence class. Congruence classes can be used to form a group, which is called the modular arithmetic group. The modular arithmetic group is isomorphic to the quotient group Z/mZ, where Z is the set of all integers.

Modular arithmetic has many applications in mathematics and computer science. For example, it can be used to define division on fields that do not have an inverse element (such as the field of real numbers). It can also be used to solve linear Diophantine equations, which are equations that involve only integer variables.

Congruence reduction is one of the most powerful techniques in solving congruence equations. The idea is to replace a large congruence equation with a smaller system of equations by using factorization. This is a much simpler system of equations and is easier to solve. In fact, congruence reduction can be used to solve much more complex equations as well, along with the assistance of other theorems such as the Chinese remainder theorem.

In this chapter, you'll learn about using Hensel's Lifting Theorem to solve polynomial congruence equations. Here's where you'll see the statement of the theorem, followed by some examples showing how to use it.

Hensel's Lifting Theorem says that if you have two congruence equations, you can find a solution by solving a series of smaller congruence equations. In other words, you can break down a large problem into smaller pieces and then put them back together to find the overall solution. This theorem is particularly useful in number theory, where congruence equations are often used to solve problems. However, it can also be applied to other areas of mathematics. So next time you're stuck on a problem, remember Hensel's Lifting Theorem and try to break it down into smaller pieces. You might just find the solution you're looking for.

Solving polynomial congruences is a fundamental problem in mathematics and has a wide range of applications, from primality testing to cryptography.

In general, the problem is to find all solutions to the equation $f(x) \equiv 0 \pmod{n}$, where f is a polynomial with integer coefficients and n is a positive integer. When n is a prime power, this problem can be solved using Lagrange's Theorem.

However, when n is not a prime power, there is no analog of Lagrange's Theorem that can be used to Solve the problem. However, there is an algorithm for determining when a solution modulo p generates solutions to higher power moduli.

The motivation for this algorithm comes from Newton's method for approximating roots over the real numbers.

Given a polynomial $f(x)$ and an initial guess $x_0$, Newton's method produces a sequence of approximations $x_1, x_2, ...$ that converges to a root of $f(x)$. If we start with a guess that is congruent to a root of $f(x)$ modulo $p$, then the sequence produced by Newton's method will be congruent to a root of $f(x)$ modulo $p^k$ for all $k > 0$.

This provides a way to solve the polynomial congruence $f(x) \equiv 0 \pmod{p^k}$ for all $k > 0$, without having to solve the congruence $f(x) \equiv 0 \pmod{p}$.

This algorithm can be used to solve any polynomial congruence $f(x) \equiv 0 \pmod{n}$, where n is not a prime power. Consequently, it can be used to solve any instance of the general problem mentioned above. Given the wide range of applications of this problem, this algorithm is sure to be of great interest to mathematicians and computer scientists alike.

Overall, Polynomial Congruence Equations is an excellent book that provides students with a step-by-step guide on how to solve polynomial congruence equations. The exercises provided are also very helpful in reinforcing the concepts covered in the main text. I would definitely recommend this book to any undergraduate number theory student looking for a comprehensive guide on solving polynomial congruences.

## 7.1 Congruence Reduction

**Theorem 7.1.** *Congruence Reduction Let* $n = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_s}^{e_s}$ *be the unique factorization of* $n$*. Then the linear congruence* $ax \equiv b \pmod{n}$ *has the same set of solutions as the system of simultaneous congruences*

$$\begin{cases} ax \equiv b \pmod{{p_1}^{e_1}} \\ ax \equiv b \pmod{{p_2}^{e_2}} \\ \quad\vdots \\ ax \equiv b \pmod{{p_s}^{e_s}}. \end{cases}$$

*Proof.* As consequence of the Fundamental Theorem of Arithmetic, $n|m$ if and only if $p_i^{e_i}\big|\,m$ for each $i$. This follows easily since, for some integer $k$,

$$n|m \Longleftrightarrow m = nk \Longleftrightarrow m = kp_1^{e_1}p_2^{e_2}\cdots p_s^{e_s} \Longleftrightarrow p_i^{e_i}\big|\,m$$

for each $i$. Hence, $A \equiv B \pmod{n}$ if and only if all of the congruences $A \equiv B \pmod{{p_1}^{e_1}}$, $A \equiv B \pmod{{p_2}^{e_2}}$,
$\cdots$, $A \equiv B \pmod{{p_s}^{e_s}}$ also hold.

□

**Example 7.1.** Solve the linear congruence equation $17x \equiv 9 \pmod{276}$ by reducing to a linear system of congruence equations.

*Solution.* Since $276 = (2^2)\,(3)(23)$ the given congruence may be replaced by the system $17x \equiv 9 \pmod{4}$, $17x \equiv 9 \pmod{3}$, $17x \equiv 9 \pmod{23}$. We find $N = (4)(3)(23) = 276$ and we use a table to construct the solution.

| $i$ | $n_i$ | $a_i$ | $b_i$ | $a_ix_i \equiv b_i \pmod{n_i}$ | $\bar{n}_i$ | $\bar{n}_iu_i \equiv 1 \pmod{n_i}$ |
|---|---|---|---|---|---|---|
| 1 | 4 | 17 | 9 | $x_1 = 1$ | 69 | $u_1 = 1$ |
| 2 | 3 | 17 | 9 | $x_2 = 0$ | 92 | $u_2 = 2$ |
| 3 | 23 | 17 | 9 | $x_3 = 10$ | 12 | $u_3 = 2$ |

The solution is

$$x_0 = (1)(69)(1) + (0)(92)(2) + (10)(12)(2) = 309 \equiv 33 \pmod{276}$$

and so the solution to $17x \equiv 9 \pmod{276}$ is $x \equiv 33 \pmod{276}$.

**Example 7.2.** Solve the linear congruence equation $3x \equiv 11 \pmod{2275}$ by reducing to a linear system of congruence equations.

*Solution.* Since $2275 = (5^2)(7)(13)$ the given congruence may be replaced by the system

$$\begin{cases} 3x \equiv 11 \pmod{25} \\ 3x \equiv 11 \pmod{7} \\ 3x \equiv 11 \pmod{13}. \end{cases}$$

We find $N = (25)(7)(13) = 2275$ and we use a table to construct the solution.

| $i$ | $n_i$ | $a_i$ | $b_i$ | $a_i x_i \equiv b_i \pmod{n_i}$ | $\bar{n}_i$ | $\bar{n}_i u_i \equiv 1 \pmod{n_i}$ |
|---|---|---|---|---|---|---|
| 1 | 25 | 3 | 11 | $x_1 = 12$ | 91 | $u_1 = 11$ |
| 2 | 7 | 3 | 11 | $x_2 = 6$ | 325 | $u_2 = 5$ |
| 3 | 13 | 3 | 11 | $x_3 = 8$ | 175 | $u_3 = 11$ |

The solution is

$$x_0 = (12)(91)(11)+(6)(325)(5)+(8)(175)(11) = 37162 \equiv 762 \pmod{2275}.$$

and so the solution to $2275 = (5^2)(7)(13)$ is $x \equiv 762 \pmod{2275}$.

## 7.2 Simple Examples of Polynomial Congruence

Given a polynomial $f$ with integer coefficients, the congruence equation $f(x) \equiv 0 \pmod{n}$ is called a **polynomial congruence**.

**Example 7.3.** Solve the polynomial congruence,

$$x^3 + 2 \equiv 0 \pmod{9}. \tag{7.1}$$

*Solution.* Any solution of 7.1 also satisfies $x^3 + 2 \equiv 0 \pmod{3}$. Trying $x = 0, 1$ and $2$ in the latter congruence gives us $x = 1$. Thus we can restrict our search for solutions of 7.1 to the integers in some complete residue system modulo 9 congruent to 1 modulo 3; namely, $1, 4,$ and $7$. Substitution shows that none of these work, and therefore 7.1 has no solutions.

**Example 7.4.** Solve the polynomial congruence,

$$f(x) = x^3 + 3 \equiv 0 \pmod{16}. \tag{7.2}$$

*Solution.* We start with $x^3+3 \equiv 0 \pmod 2$; and find $x=1$ is a solution. Thus the only possible solutions of $x^3+3 \equiv 0 \pmod 4$ are $x=1$ and $x=3$. Substitution shows that only $x=1$ works. Since all solutions of $x^3+3 \equiv 0 \pmod 8$ must be congruent to 1 modulo 4, we try $x=1$ and $x=5$.

Since $f(1)=4$ and $f(5)=128$, only $x=5$ works. We note that $x=5$ is a solution of 7.2 and $x=13$ is the only other possibility. But $f(13) \not\equiv 0 \pmod{16}$ and so $x=5$ is a complete solution to 7.2.

**Theorem 7.2.** *Let $n = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ be the unique factorization of $n$. Then the polynomial congruence $f(x) \equiv 0 \pmod n$ has the same set of solutions as the system of simultaneous congruences*

$$f(x) \equiv 0 \pmod{p_1^{e_1}}, \quad f(x) \equiv 0 \pmod{p_2^{e_2}}, \quad ..., \quad f(x) \equiv 0 \pmod{p_s^{e_s}} \ .$$

*Proof.* As consequence of the fundamental theorem of arithmetic, $n|m$ if and only if $p_i^{e_i}\big| m$ for each $i$. This follows easily since, for some integer $k$,

$$n|m \iff m = nk \iff kp_1^{e_1}p_2^{e_2}\cdots p_s^{e_s} \iff p_i^{e_i}\big| m$$

for each $i$. Hence, $A \equiv B \pmod n$ if and only if all of the congruences $A \equiv B \pmod{p_1^{e_1}}$, $A \equiv B \pmod{p_2^{e_2}}$, $\cdots$, $A \equiv B \pmod{p_s^{e_s}}$ are satisfied.

□

## 7.3 Hensel's Lifting Theorem

In general, in order to solve a polynomial congruence $f(x) \equiv 0 \pmod n$ we can reduce, by 7.2, to the case of moduli that are powers of primes. Thus solving these polynomial congruences becomes the main focus. In order to solve $f(x) \equiv 0 \pmod{p^i}$ where $p^i$ is some prime power, we would actually like to reduce even further and just solve, $f(x) \equiv 0 \pmod p$. So our first goal will be how to solve polynomial congruences with a prime moduli, and then to see how to lift these solutions to $f(x) \equiv 0 \pmod{p^i}$. However, the general procedure for solving $f(x) \equiv 0 \pmod p$ is non-trivial; instead, we set a limit to the number of solutions, which will help in some cases.

Let $f(x) = \sum_{k=1}^{n} a_k x^k$ with integers $a_k$ and $p$ is a prime such that $p \nmid a_n$, then the congruence $f(x) \equiv 0 \pmod p$ has at most $n$ mutually incongruent solutions modulo $p$. Solving $f(x) \equiv 0 \pmod{p^i}$ where $p^i$ is some prime power, our strategy is to solve the case for when $f(x) \equiv 0 \pmod p$ (if possible) and then to **lift** these solutions to the case for $f(x) \equiv 0 \pmod{p^2}$, and then to the case for $f(x) \equiv 0 \pmod{p^3}$, eventually we can reach $f(x) \equiv 0 \pmod{p^i}$.

Given $f(x) = \sum_{k=1}^{m} a_k x^k$ recall that the derivative is $f'(x) = \sum_{k=1}^{m} k a_k x^{k-1}$. Assuming $f, g$ and $h$ are polynomials with integer coefficients, here are three other properties from calculus that we will use,

$$h(x) = f(x) + g(x) \Longrightarrow h'(x) = f'(x) + g'(x)$$

$$f(x) = x^m \Longrightarrow f^{(k)}(x) = m(m-1)(m-2)\cdots(m-k+1)x^{m-k}$$

and (the Taylor expansion),

$$f(a+b) = \sum_{k=0}^{n} \frac{f^{(n)}(a)b^n}{n!}$$

where $f^0(x) = f(x)$.
These tools will lead to a proof of the next theorem which states when a solution to $f(x) \equiv 0 \pmod{p^{k-1}}$ lifts to a unique solution of $f(x) \equiv 0 \pmod{p^k}$ and when such a solution lifts to $p$ incongruent solutions modulo $p^k$ or to none at all.

Let $\bar{a}$ denote the inverse $a$ modulo $p$; that is, given a prime $p$ and an integer $a$ any integer $\bar{a}$ for which $a\bar{a} \equiv 1 \pmod{p}$.

Hensel's lemma, also known as Hensel's lifting lemma, named after Kurt Hensel, is a result in modular arithmetic, stating that if a polynomial equation has a simple root modulo a prime number $p$, then this root corresponds to a unique root of the same equation modulo any higher power of $p$, which can be found by iteratively "lifting" the solution modulo successive powers of $p$.

::: {#thm- }[Hensel's Lifting] If $f$ is a polynomial with integers coefficients and $r$ is a solution to $f(x) \equiv 0 \pmod{p^{k-1}}$ with $k \geq 2$ and prime $p$, then

- if $f'(r) \not\equiv 0 \pmod{p}$, then there is a unique integer $t$, $0 \leq t < p$, such that $f\left(r + tp^{k-1}\right) \equiv 0 \pmod{p^k}$ given by $t \equiv -\overline{f'(r)}\frac{f(r)}{p^{k-1}} \pmod{p}$
- if $f'(r) \equiv 0 \pmod{p}$ and $f(r) \equiv 0 \pmod{p^k}$, then $f\left(r + tp^{k-1}\right) \equiv 0 \pmod{p^k}$ for all integers $t$;
- if $f'(r) \equiv 0 \pmod{p}$ and $f(r) \not\equiv 0 \pmod{p^k}$, then $f(x) = 0 \pmod{p^k}$ has no solutions with $x \equiv r \pmod{p^{k-1}}$.

Furthermore, if $f(r) \equiv 0 \pmod{p}$ and $f'(r) \not\equiv 0 \pmod{p}$, then there is a unique solution $r_k$ modulo $p^k$ for $k = 2, 3, \ldots$ such that $r_k = r_{k-1} - f\left(r_{k-1}\right)\overline{f'(r)}$. :::

**Example 7.5.** Solve the polynomial congruence equation

$$f(x) = x^2 + x + 47 \equiv 0 \pmod{2401}. \tag{7.3}$$

*Solution.* Since $2401 = 7^4$, first we consider the equation $f(x) \equiv 0 \pmod{7}$. By inspection, we see that the solutions are $x = 1$ and $x = 5$. Note that, $f'(x) = 2x + 1$.

For $x = 1$ we find that $f'(1) \equiv 3 \pmod{7}$. Thus $x = 1$ lifts successively to unique solutions modulo each power of 7.
We set $x_1 = 1$.
Then, since $(3)(5) \equiv 1 \pmod{7}$ we have $\overline{f'(1)} = 5$, and so

$$\begin{aligned}
x_2 &= x_1 - f\left(x_1\right)\overline{f'(1)} = 1 - f(1)(5) = 1 - (49)(5) = -244 \equiv 1 \pmod{49}\\
x_3 &= x_2 - f\left(x_2\right)\overline{f'(1)} = 1 - f(1)(5) = 1 - (49)(5) = -244 \equiv 99 \pmod{343}\\
x_4 &= x_3 - f\left(x_3\right)\overline{f'(1)} = 99 - f(99)(5) = 99 - (9947)(5) \equiv 785 \pmod{2401}
\end{aligned}$$

So we have lifted $x \equiv 1 \pmod{7}$ to a solution $x = 785 \pmod{2401}$.

For $x = 5$ we find that $f'(5) \equiv 4 \pmod{7}$. Thus $x = 5$ lifts successively to unique solutions modulo each power of 7.
We set $x_1 = 5$. Then, since $(4)(2) \equiv 1 \pmod{7}$ we have $\overline{f'(5)} = 2$, and so

$$\begin{aligned}
x_2 &= 5 - f(5)(2) = 5 - (77)(2) \equiv 47 \pmod{49}\\
x_3 &= 47 - f(47)(2) = 47 - (2303)(2) = 243 \equiv 243 \pmod{343}\\
x_4 &= 243 - f(243)(2) = 243 - (59339)(2) \equiv 1615 \pmod{2401}
\end{aligned}$$

So we have lifted $x \equiv 5 \pmod{7}$ to a solution $x = 1615 \pmod{2401}$. Therefore the solutions to 7.3 are $x \equiv 785 \pmod{2401}$ and $x \equiv 1615 \pmod{2401}$.

| $x$ | $f(x)$ | $f'(x)$ | $\overline{f'(x)}$ | $\pmod{7}$ |
|---|---|---|---|---|
| 0 | 5 | – | – | – |
| 1 | 0 | 3 | 5 | $k$ \| $x_k = x_{k-1} - f\left(x_{k-1}\right)\overline{f'(x)}$<br>$k = 1$ \| $x_1 \equiv 1 \pmod{7^1}$<br>$k = 2$ \| $x_2 = 1 - f(1) * 5 \equiv 1 \pmod{7^2}$<br>$k = 3$ \| $x_2 = 1 - f(1) * 5 \equiv 99 \pmod{7^3}$<br>$k = 4$ \| $x_2 = 99 - f(99) * 5 \equiv 785 \pmod{7^4}$ |
| 2 | 4 | – | – | – |
| 3 | 3 | – | – | – |
| 4 | 4 | – | – | – |
| 5 | 0 | 4 | 2 | $k$ \| $x_k = x_{k-1} - f\left(x_{k-1}\right)\overline{f'(x)}$<br>$k = 1$ \| $x_1 \equiv 5 \pmod{7^1}$<br>$k = 2$ \| $x_2 = 5 - f(5) * 2 \equiv 47 \pmod{7^2}$<br>$k = 3$ \| $x_2 = 47 - f(47) * 2 \equiv 243 \pmod{7^3}$<br>$k = 4$ \| $x_2 = 243 - f(243) * 2 \equiv 1615 \pmod{7^4}$ |
| 6 | 5 | – | – | – |

## 7.4 Solving Polynomial Congruences

**Example 7.6.** Consider trying to solve the polynomial congruence equation

$$f(x) = x^5 - 3x^4 + 7x^3 - 2x^2 - 9x + 6 \equiv 0 \pmod{165}. \tag{7.4}$$

*Solution.* Since $165 = (3)(5)(11)$, by inspection we solve the following congruences, and we have

$$f(x) \equiv 0 \pmod 3 \Longrightarrow x \equiv 0, 1 \pmod 3$$

$$f(x) \equiv 0 \pmod 5 \Longrightarrow x \equiv 1, 2, 3 \pmod 5$$

$$f(x) \equiv 0 \pmod{11} \Longrightarrow x \equiv 1, 6, 8 \pmod{11}$$

Thus there are a total of $(2)(3)(3) = 18$ solutions to (7.4); for example to find one of them we solve the system $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 5$, $x \equiv 1 \pmod{11}$. Using the Chinese remainder theorem we obtain the solution $x \equiv 111 \pmod{165}$. The other 17 solutions are also found using the Chinese remainder theorem.

| $x$ | $f(x) \pmod{25}$ |
|---|---|
| 0 | $15 \not\equiv 0$ |
| 5 | $15 \not\equiv 0$ |
| 10 | $15 \not\equiv 0$ |
| 15 | $15 \not\equiv 0$ |
| 20 | $15 \not\equiv 0$ |

| $x$ | $f(x) \pmod{25}$ |
|---|---|
| 0 | $14 \not\equiv 0$ |
| 7 | $14 \not\equiv 0$ |
| 14 | $14 \not\equiv 0$ |
| 21 | $14 \not\equiv 0$ |
| 28 | $14 \not\equiv 0$ |
| 35 | $14 \not\equiv 0$ |
| 42 | $14 \not\equiv 0$ |

**Example 7.7.** Solve the polynomial congruence equation

$$f(x) = x^6 - 2x^5 - 35 \equiv 0 \pmod{6125}. \tag{7.5}$$

*Solution.* Since $6125 = 5^3 7^2$, first we consider the equation $f(x) \equiv 0 \pmod 5$. By inspection, we see that the solutions are $x = 0$ and $x = 2$ modulo 5. Note that, $f'(x) = 6x^5 - 10x^4$.
For $x = 0$ we find that $f'(0) \equiv 0 \pmod 5$. Thus we check, $f(0) = -35 \equiv 15 \pmod{25}$ and so $x = 0$ does not lift to a solution modulo $5^k$. For $x = 2$ we find that $f'(2) = 32 \equiv 2 \pmod 5$ and so $x = 2$ has unique lifts modulo $5^k$. We set $x_1 = 2$. Then, since $(2)(3) \equiv 1 \pmod 5$ we have $\overline{f'(2)} = 3$, and so

$$\begin{aligned} x_2 &= 2 - f(2)(3) = 2 - (-35)(3) \equiv 7 \pmod{25} \\ x_3 &= 7 - f(7)(3) = 7 - (76832)(3) \equiv 7 \pmod{125}. \end{aligned}$$

So we have lifted $x \equiv 5 \pmod 5$ to a solution $x \equiv 7 \pmod{125}$; that is we have solved $f(x) \equiv 0 \pmod{125}$. Now we consider the case for $f(x) \equiv 0 \pmod 7$. By inspection, we see that the solutions are $x = 0$ and $x = 2 \pm 7$. For $x = 0$ we find that $f'(0) \equiv 0 \pmod 7$. Thus we check, $f(0) = -35 \equiv 7 \pmod{49}$ and so $x = 0$ does not lift to a solution modulo $7^k$. For $x = 2$ we find that $f'(2) = 32 \equiv 4 \pmod 7$ and so $x = 2$ has unique lifts modulo $7^k$. We set $x_1 = 2$. Then, since $(4)(2) \equiv 1 \pmod 7$ we have $\overline{f'(2)} = 2$, and so

$$x_2 = 2 - f(2)(2) = 2 - (-35)(2) \equiv 23 \pmod{49}.$$

So we have lifted $x \equiv 2 \pmod 7$ to a solution $x \equiv 23 \pmod{49}$; that is we have solved $f(x) \equiv 0 \pmod{49}$. It remains to solve the system $x \equiv 7 \pmod{125}$, $x \equiv 23 \pmod{49}$. This is easy since $(125, 49) = 1$ and we have $125(-29) + 49(74) = 1$ and so $x = 125(-29)(23) + 49(74)(7) = -57993 \equiv 3257 \pmod{6125}$ as desired.

**Example 7.8.** Outline how to solve the polynomial congruence equation.

$$-82 + 12x - 10x^2 + x^3 \equiv 0 \pmod{33075} \tag{7.6}$$

*Solution.* The unique factorization of 33075, is $3^3 5^2 7^2$ and the derivative is $f'(x) = 3x^2 - 20x + 12$.

| $x$ | $f(x)$ | $f'(x)$ | $\overline{f'(x)}$ | $\pmod 3$ | |
|---|---|---|---|---|---|
| 0 | 2 | – | – | – | |
| 1 | 2 | – | – | – | |
| 2 | 0 | 2 | 2 | $k$ | $x_k = x_{k-1} - f(x_{k-1})\overline{f'(x)}$ |
| | | | | 1 | $x_1 \equiv 2 \pmod{3^1}$ |
| | | | | 2 | $x_2 = 2 - f(2) * 2 \equiv 2 \pmod{3^2}$ |
| | | | | 3 | $x_3 = 2 - f(2) * 2 \equiv 20 \pmod{3^3}$ |

| $x$ | $f(x)$ | $f'(x)$ | $\overline{f'(x)}$ | $\pmod 5$ | |
|---|---|---|---|---|---|
| 0 | 3 | – | – | – | |
| 1 | 1 | – | – | – | |
| 2 | 0 | 4 | 4 | $k$ | $x_k = x_{k-1} - f(x_{k-1})\overline{f'(x)}$ |
| | | | | $k = 1$ | $x_1 \equiv 2 \pmod{5^1}$ |
| | | | | $k = 2$ | $x_2 = 2 - f(2) * 4 \equiv 12 \pmod{5^2}$ |
| 3 | 1 | – | – | – | |
| 4 | 0 | 0 | – | $f(x) \not\equiv 0 \pmod{25} \therefore x$ does not lift where $x = 4, 9, 14, 19, 24$ | |

| $x$ | $f(x)$ | $f'(x)$ | $\overline{f'(x)}$ | (mod 7) |
|---|---|---|---|---|
| 0 | 2 | – | – | – |
| 1 | 5 | – | – | – |
| 2 | 1 | – | – | – |
| 3 | 3 | – | – | – |
| 4 | 3 | – | – | – |
| 5 | 0 | 1 | 1 | $\begin{array}{cc} k & x_k = x_{k-1} - f\left(x_{k-1}\right)\overline{f'(x)} \\ \hline k=1 & x_1 = 5 \pmod{7^1} \\ k=2 & x_2 = 5 - f(5) * 1 \equiv 5 \pmod{7^2} \end{array}$ |
| 6 | 0 | 0 | – | $f(x) \not\equiv 0 \pmod{49} \therefore x$ does not lift where $x = 6, 13, 20, 27, 34, 4$ |

After applying Hensel's Lifting theorem, we now must solve the system $x \equiv 20 \pmod{27}$, $x \equiv 12 \pmod{25}$, $x \equiv 5 \pmod{49}$. The Chinese remainder theorem yields

$$x \equiv 20\left(\frac{33075}{27}\right)y_1 + 12\left(\frac{33075}{25}\right)y_2 + 5\left(\frac{33075}{49}\right)y_3 \pmod{33075}$$

where $y_1, y_2$, and $y_3$ are solutions to

$$\frac{33075}{27}y_1 \equiv 1 \pmod{27} \Longrightarrow y_1 = 19$$

$$\frac{33075}{25}y_2 \equiv 1 \pmod{25} \Longrightarrow y_2 = 12$$

$$\frac{33075}{49}y_3 \equiv 1 \pmod{49} \Longrightarrow y_3 = 40$$

Therefore, $x \equiv 20\left(\frac{33075}{27}\right)19 + 12\left(\frac{33075}{25}\right)12 + 5\left(\frac{33075}{49}\right)40 \equiv 30287 \pmod{33075}$ is THE solution.

**Example 7.9.** Solve the polynomial congruence equation

$$2308 - 567x - 6x^2 + 35x^3 \equiv 0 \pmod{148225}. \tag{7.7}$$

*Solution.* The unique factorization of 148225, is $5^2 7^2 11^2$ and the derivative is $f'(x) = 105x^2 - 12x - 567$. We apply Hensel's Lifting theorem and display the computations in the following tables. %**??**, **??**, and **??**.

| $x$ | $f(x)$ | $f'(x)$ | $\overline{f'(x)}$ | $\pmod{5}$ | |
|---|---|---|---|---|---|
| 0 | 3 | — | — | — | |
| 1 | 0 | 1 | 1 | $k$ | $x_k = x_{k-1} - f\left(x_{k-1}\right)\overline{f'(x)}$ |
| | | | | $k=1$ | $x_1 \equiv 1 \pmod{5^1}$ |
| | | | | $k=2$ | $x_2 = 1 - f(1) * 1 \equiv 6 \pmod{5^2}$ |
| 2 | 0 | 4 | 4 | $k$ | $x_k = x_{k-1} - f\left(x_{k-1}\right)\overline{f'(x)}$ |
| | | | | $k=1$ | $x_1 \equiv 2 \pmod{5^1}$ |
| | | | | $k=2$ | $x_2 = 2 - f(2) * 4 \equiv 7 \pmod{5^2}$ |
| 3 | 3 | — | — | — | |
| 4 | 4 | — | — | — | |

| $x$ | $f(x)$ | $f'(x)$ | $\overline{f'(x)}$ | $\pmod{7}$ | |
|---|---|---|---|---|---|
| 0 | 5 | — | — | — | |
| 1 | 6 | — | — | — | |
| 2 | 2 | — | — | — | |
| 3 | 0 | 6 | 6 | $k$ | $x_k = x_{k-1} - f\left(x_{k-1}\right)\overline{f'(x)}$ |
| | | | | $k=1$ | $x_1 \equiv 3 \pmod{7^1}$ |
| | | | | $k=2$ | $x_2 = 3 - f(3) * 6 \equiv 31 \pmod{7^2}$ |
| 4 | 0 | 1 | 1 | $k$ | $x_k = x_{k-1} - f\left(x_{k-1}\right)\overline{f'(x)}$ |
| | | | | $k=1$ | $x_1 \equiv 4 \pmod{7^1}$ |
| | | | | $k=2$ | $x_2 = 4 - f(4) * 1 \equiv 25 \pmod{7^2}$ |
| 5 | 2 | — | — | — | |
| 6 | 6 | — | — | — | |

| $x$ | $f(x)$ | $f'(x)$ | $\overline{f'(x)}$ | $\pmod{11}$ | |
|---|---|---|---|---|---|
| 0 | 9 | — | — | — | |
| 1 | 10 | — | — | — | |
| 2 | 0 | $f'(x) \equiv 5$ | 9 | $k$ | $x_k = x_{k-1} - f\left(x_{k-1}\right)\overline{f'(x)}$ |
| | | | | $k=1$ | $x_1 \equiv 2 \pmod{11^1}$ |
| | | | | $k=2$ | $x_2 = 2 - f(2) * 9 \equiv 79 \pmod{11^2}$ |
| 3 | 2 | — | — | — | |
| 4 | 6 | — | — | — | |
| 5 | 2 | — | — | — | |
| 6 | 2 | — | — | — | |
| 7 | 7 | — | — | — | |
| 8 | 7 | — | — | — | |
| 9 | 3 | — | — | — | |
| 10 | 7 | — | — | — | |

We now must solve the four systems

$$\begin{cases} x \equiv 6 & \pmod{25} \\ x \equiv 31 & \pmod{49} \\ x \equiv 79 & \pmod{121} \end{cases} \quad \begin{cases} x \equiv 7 & \pmod{25} \\ x \equiv 31 & \pmod{49} \\ x \equiv 79 & \pmod{121} \end{cases}$$

$$\begin{cases} x \equiv 6 & \pmod{25} \\ x \equiv 25 & \pmod{49} \\ x \equiv 79 & \pmod{121} \end{cases} \quad \begin{cases} x \equiv 7 & \pmod{25} \\ x \equiv 25 & \pmod{49} \\ x \equiv 79 & \pmod{121} \end{cases}$$

The Chinese remainder theorem yields the four solutions,

$$x \equiv 6\left(\frac{148225}{25}\right)u_1 + 31\left(\frac{148225}{49}\right)u_2 + 79\left(\frac{148225}{121}\right)u_3 \pmod{148225}$$
$$x \equiv 7\left(\frac{148225}{25}\right)u_1 + 31\left(\frac{148225}{49}\right)u_2 + 79\left(\frac{148225}{121}\right)u_3 \pmod{148225}$$
$$x \equiv 6\left(\frac{148225}{25}\right)u_1 + 25\left(\frac{148225}{49}\right)u_2 + 79\left(\frac{148225}{121}\right)u_3 \pmod{148225}$$
$$x \equiv 7\left(\frac{148225}{25}\right)u_1 + 25\left(\frac{148225}{49}\right)u_2 + 79\left(\frac{148225}{121}\right)u_3 \pmod{148225}$$

where $u_1, u_2$ and $u_3$ are found via

$$(148225/25)\,u_1 \equiv 1 \pmod{25} \implies u_1 = 19$$
$$(148225/49)\,u_2 \equiv 1 \pmod{49} \implies u_2 = 15$$
$$(148225/121)\,u_3 \equiv 1 \pmod{121} \implies u_3 = 113$$

Therefore the solutions to 7.7 are $x \equiv 122531 \pmod{148225}$, $x \equiv 86957 \pmod{148225}$, $x \equiv 146731 \pmod{148225}$, and $x \equiv 111157 \pmod{148225}$ as the only solutions.

## 7.5 Exercises

The following polynomial congruences all have 10 or fewer solutions. Use unique factorization,
Hensel's Lifting theorem and the Chinese remainder theorem to solve them.

**Exercise 7.1.** $2 + 3x - 2x^2 \equiv 0 \pmod{1155}$

**Exercise 7.2.** $5 + 11x - 12x^2 \equiv 0 \pmod{8085}$

**Exercise 7.3.** $2 + 3x - 2x^2 \equiv 0 \pmod{3465}$

**Exercise 7.4.** $5 + 11x - 12x^2 \equiv 0 \pmod{24255}$

**Exercise 7.5.** $2 + 3x - 2x^2 \equiv 0 \pmod{12705}$

**Exercise 7.6.** $5 + 11x - 12x^2 \equiv 0 \pmod{5775}$

**Exercise 7.7.** $2 + 3x - 2x^2 \equiv 0 \pmod{8085}$

**Exercise 7.8.** $5 + 11x - 12x^2 \equiv 0 \pmod{63525}$

**Exercise 7.9.** $3 + 11x + 10x^2 \equiv 0 \pmod{1925}$

**Exercise 7.10.** $120 - 9x + 8x^2 \equiv 0 \pmod{1155}$

**Exercise 7.11.** $3 + 11x + 10x^2 \equiv 0 \pmod{5775}$

**Exercise 7.12.** $120 - 9x + 8x^2 \equiv 0 \pmod{5775}$

**Exercise 7.13.** $3 + 11x + 10x^2 \equiv 0 \pmod{17325}$

**Exercise 7.14.** $120 - 9x + 8x^2 \equiv 0 \pmod{40425}$

**Exercise 7.15.** $3 + 11x + 10x^2 \equiv 0 \pmod{63525}$

**Exercise 7.16.** $120 - 9x + 8x^2 \equiv 0 \pmod{698775}$

**Exercise 7.17.** $180 - 15x + 11x^2 \equiv 0 \pmod{1155}$

**Exercise 7.18.** $46 - 5x - 9x^2 \equiv 0 \pmod{315}$

**Exercise 7.19.** $180 - 15x + 11x^2 \equiv 0 \pmod{56595}$

**Exercise 7.20.** $46 - 5x - 9x^2 \equiv 0 \pmod{10395}$

**Exercise 7.21.** $180 - 15x + 11x^2 \equiv 0 \pmod{24255}$

**Exercise 7.22.** $46 - 5x - 9x^2 \equiv 0 \pmod{51975}$

**Exercise 7.23.** $180 - 15x + 11x^2 \equiv 0 \pmod{17325}$

**Exercise 7.24.** $46 - 5x - 9x^2 \equiv 0 \pmod{121275}$

**Exercise 7.25.** $4 + 6x + 2x^2 \equiv 0 \pmod{312987}$

**Exercise 7.26.** $4 + 6x + 2x^2 \equiv 0 \pmod{521645}$

Solve the polynomial congruence.

**Exercise 7.27.** $x^2 + 4x + 2 \equiv 0 \pmod{7}$

**Exercise 7.28.** $x^2 + 4x + 2 \equiv 0 \pmod{49}$

**Exercise 7.29.** $x^2 + 4x + 2 \equiv 0 \pmod{343}$

**Exercise 7.30.** $x^3 + 8x^2 - x - 1 \equiv 0 \pmod{11}$

**Exercise 7.31.** $x^3 + 8x^2 - x - 1 \equiv 0 \pmod{121}$

**Exercise 7.32.** $x^3 + 8x^2 - x - 1 \equiv 0 \pmod{1331}$

**Exercise 7.33.** $x^2 + x + 47 \equiv 0 \pmod{2401}$

**Exercise 7.34.** $x^2 + x + 34 \equiv 0 \pmod{81}$

**Exercise 7.35.** $13x^7 - 42x - 649 \equiv 0 \pmod{1323}$

**Exercise 7.36.** $x^8 - x^4 + 1001 \equiv 0 \pmod{539}$

**Exercise 7.37.** $x^4 + 2x + 36 \equiv 0 \pmod{4375}$

**Exercise 7.38.** $x^6 - 2x^5 - 35 \equiv 0 \pmod{6125}$

Each of the following polynomial congruence equations have fewer than 50 solutions.

**Exercise 7.39.** $9x^5 + 10x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{12960}$

**Exercise 7.40.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{12960}$

**Exercise 7.41.** $6x^5 + 6x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{19440}$

**Exercise 7.42.** $9x^5 + 10x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{19440}$

**Exercise 7.43.** $9x^5 + 10x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{38880}$

**Exercise 7.44.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{38880}$

**Exercise 7.45.** $6x^5 + 6x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{10800}$

**Exercise 7.46.** $8x^5 + 10x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{10800}$

**Exercise 7.47.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{21600}$

**Exercise 7.48.** $6x^5 + 10x^4 + 5x^3 + x^2 + x + 1 \equiv 0 \pmod{21600}$

**Exercise 7.49.** $3x^5 + 4x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{16200}$

**Exercise 7.50.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{16200}$

**Exercise 7.51.** $6x^5 + 6x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{32400}$

**Exercise 7.52.** $8x^5 + 10x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{32400}$

**Exercise 7.53.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{64800}$

**Exercise 7.54.** $6x^5 + 10x^4 + 5x^3 + x^2 + x + 1 \equiv 0 \pmod{64800}$

**Exercise 7.55.** $4x^5 + 4x^4 + 5x^3 + 5x^2 + x + 1 \equiv 0 \pmod{12150}$

**Exercise 7.56.** $3x^5 + 2x^4 + 5x^3 + 6x^2 + x + 1 \equiv 0 \pmod{12150}$

**Exercise 7.57.** $3x^5 + 4x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{24300}$

**Exercise 7.58.** $4x^5 + 3x^4 + x^3 + 2x^2 + x + 1 \equiv 0 \pmod{24300}$

**Exercise 7.59.** $3x^5 + 4x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{48600}$

**Exercise 7.60.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{48600}$

**Exercise 7.61.** $6x^5 + 6x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{97200}$

**Exercise 7.62.** $8x^5 + 10x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{97200}$

**Exercise 7.63.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{194400}$

**Exercise 7.64.** $6x^5 + 10x^4 + 5x^3 + x^2 + x + 1 \equiv 0 \pmod{194400}$

**Exercise 7.65.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{12000}$

**Exercise 7.66.** $7x^5 + 10x^4 + 4x^3 + x^2 + x + 1 \equiv 0 \pmod{12000}$

**Exercise 7.67.** $6x^5 + 6x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{18000}$

**Exercise 7.68.** $8x^5 + 10x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{18000}$

**Exercise 7.69.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{36000}$

**Exercise 7.70.** $6x^5 + 10x^4 + 5x^3 + x^2 + x + 1 \equiv 0 \pmod{36000}$

**Exercise 7.71.** $3x^5 + 4x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{13500}$

**Exercise 7.72.** $4x^5 + 3x^4 + x^3 + 2x^2 + x + 1 \equiv 0 \pmod{13500}$

**Exercise 7.73.** $3x^5 + 4x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{27000}$

**Exercise 7.74.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{27000}$

**Exercise 7.75.** $6x^5 + 6x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{54000}$

**Exercise 7.76.** $8x^5 + 10x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{54000}$

**Exercise 7.77.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{108000}$

**Exercise 7.78.** $6x^5 + 10x^4 + 5x^3 + x^2 + x + 1 \equiv 0 \pmod{108000}$

**Exercise 7.79.** $3x^5 + 2x^4 + 5x^3 + 6x^2 + x + 1 \equiv 0 \pmod{20250}$

**Exercise 7.80.** $3x^5 + 5x^4 + 4x^3 + 3x^2 + 2x + 1 \equiv 0 \pmod{20250}$

**Exercise 7.81.** $3x^5 + 4x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{40500}$

**Exercise 7.82.** $4x^5 + 3x^4 + x^3 + 2x^2 + x + 1 \equiv 0 \pmod{40500}$

**Exercise 7.83.** $3x^5 + 4x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{81000}$

**Exercise 7.84.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{81000}$

**Exercise 7.85.** $6x^5 + 6x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{162000}$

**Exercise 7.86.** $8x^5 + 10x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{162000}$

**Exercise 7.87.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{324000}$

**Exercise 7.88.** $6x^5 + 10x^4 + 5x^3 + x^2 + x + 1 \equiv 0 \pmod{324000}$

**Exercise 7.89.** $3x^5 + 2x^4 + 5x^3 + 6x^2 + x + 1 \equiv 0 \pmod{60750}$

**Exercise 7.90.** $3x^5 + 5x^4 + 4x^3 + 3x^2 + 2x + 1 \equiv 0 \pmod{60750}$

**Exercise 7.91.** $3x^5 + 4x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{121500}$

**Exercise 7.92.** $4x^5 + 3x^4 + x^3 + 2x^2 + x + 1 \equiv 0 \pmod{121500}$

**Exercise 7.93.** $3x^5 + 4x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{243000}$

**Exercise 7.94.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{243000}$

**Exercise 7.95.** $6x^5 + 6x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{486000}$

**Exercise 7.96.** $8x^5 + 10x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{486000}$

**Exercise 7.97.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{972000}$

**Exercise 7.98.** $6x^5 + 10x^4 + 5x^3 + x^2 + x + 1 \equiv 0 \pmod{972000}$

**Exercise 7.99.** $1x^5 + 10x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{20000}$

**Exercise 7.100.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{20000}$

**Exercise 7.101.** $3x^5 + 4x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{15000}$

**Exercise 7.102.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{15000}$

**Exercise 7.103.** $6x^5 + 6x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{30000}$

**Exercise 7.104.** $8x^5 + 10x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{30000}$

**Exercise 7.105.** $4x^5 + 6x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{60000}$

**Exercise 7.106.** $7x^5 + 10x^4 + 4x^3 + x^2 + x + 1 \equiv 0 \pmod{60000}$

**Exercise 7.107.** $5x^5 + 3x^4 + 3x^3 + 5x^2 + x + 1 \equiv 0 \pmod{11250}$

**Exercise 7.108.** $2x^5 + 3x^4 + 6x^3 + 5x^2 + x + 1 \equiv 0 \pmod{11250}$

**Exercise 7.109.** $3x^5 + 4x^4 + 2x^3 + x^2 + x + 1 \equiv 0 \pmod{22500}$

**Exercise 7.110.** $4x^5 + 3x^4 + x^3 + 2x^2 + x + 1 \equiv 0 \pmod{22500}$

**Exercise 7.111.** $3x^5+4x^4+2x^3+x^2+x+1\equiv 0 \pmod{45000}$

**Exercise 7.112.** $4x^5+6x^4+3x^3+x^2+x+1\equiv 0 \pmod{45000}$

**Exercise 7.113.** $6x^5+6x^4+x^3+x^2+x+1\equiv 0 \pmod{90000}$

**Exercise 7.114.** $8x^5+10x^4+3x^3+x^2+x+1\equiv 0 \pmod{90000}$

**Exercise 7.115.** $4x^5+6x^4+3x^3+x^2+x+1\equiv 0 \pmod{180000}$

**Exercise 7.116.** $6x^5+10x^4+5x^3+x^2+x+1\equiv 0 \pmod{180000}$

**Exercise 7.117.** $6x^5+9x^4+8x^3+5x^2+x+1\equiv 0 \pmod{33750}$

**Exercise 7.118.** $3x^5+2x^4+5x^3+6x^2+x+1\equiv 0 \pmod{33750}$

**Exercise 7.119.** $3x^5+4x^4+2x^3+x^2+x+1\equiv 0 \pmod{67500}$

**Exercise 7.120.** Let $a$ be an integer and $p$ a prime such that $(a,p)=1$. Use Hensel's Lifting theorem to solve the polynomial congruence equation $ax\equiv 1 \pmod{p^k}$ for all positive integer $k$.

**Exercise 7.121.** Solve the polynomial congruence equation $2x^2-3x+12\equiv 0(\mathrm{mod}343)$.

# References

Burton, D. M. 2006. *Elementary Number Theory.* Tata McGraw-Hill Publishing Company Limited. https://books.google.com/books?id=XMQjuoTqqRMC.

Davenport, H. 2008. *The Higher Arithmetic: An Introduction to the Theory of Numbers.* Cambridge University Press. https://books.google.com/books?id=VdMhAwAAQBAJ.

Rosen, K. H. 2005. *Elementary Number Theory and Its Applications.* Alternative eText Formats Series. Pearson/Addison Wesley. https://books.google.com/books?id=jD0lAQAAIAAJ.

William, S. 2016. *Cryptography and Network Security - Principles and Practice, 7th Edition.* Pearson Education India. https://books.google.com/books?id=AhDCDwAAQBAJ.

# Index