ELEMENTARY NUMBER THEORY

Puguh Wahyu Prasetyo
Uha Isnaini
Rully Charitas Indra Prahmana
Burhanudin Arif Nurnugroho

ISBN (Online):
978-602-0737-75-1

Universitas Ahmad Dahlan Press

ELEMENTARY NUMBER THEORY

ELEMENTARY NUMBER THEORY

Puguh Wahyu Prasetyo

Uha Isnaini

Burhanudin Arif Nurnugroho
Rully Charitas Indra Prahmana

UNIVERSITAS AHMAD DAHLAN PRESS

Kampus 4 Universitas Ahmad Dahlan, Tamanan, Bantul
Email : uadpress@uad.ac.id

First Print **2020**

Published by:
UNIVERSITAS AHMAD DAHLAN PRESS
Member of IKAPI

ISBN (Online):978-602-0737-75-1

PREFACE

We thank to Allah Subhanahu wa Ta'ala, because for His blessings, mercy, and grace, the compilation of the book Elementary Number Theory can be completed. This book is prepared as teaching material in the learning activities of the Number Theory Course. This book can be used for both pure mathematics and education students. In this book, a summary of Number Theory learning materials is presented in a simple, effective, and easy to understand manner. This book is also equipped with competitive questions.

Our gratitude goes to all those who helped to complete this book so that it can be presented. However, this book is certainly not free from shortcomings. Therefore, we hope that various kinds of improvements, including suggestions and criticisms from readers, for the perfection of this book.

Yogyakarta, October 13, 2020

Authors

CONTENTS

CHAPTERS 1
BASIC CONCEPT

1.1 Number System

Number theory is one of the oldest branch of Mathematics. Based on the constructivism thinking of the human being, the numbers $1, 2, 3, ...$ were believed as the human's first mathematical creation in history. Human invented this mathematical creation to represent the number of things. Now days, we call the numbers $1, 2, 3, ...$ as the set of positive integers. This mathematical creation helped the human at that time to count. Hence, the numbers $1, 2, 3, ...$ are also called the counting numbers. On the other hand, some historical objects showed that the ancient human culture had used the zero to express "there is nothing". We start from Ancient Near East, Ancient Egyptian numerals were of base 10.[14] They used hieroglyphs for the digits and were not positional. By 1770 BC, the Egyptians had a symbol for zero in accounting texts. The symbol nfr, meaning beautiful, was also used to indicate the base level in drawings of tombs and pyramids, and distances were measured relative to the base line as being above or below this line. By the middle of the 2nd millennium BC, the Babylonian mathematics had a sophisticated sexagesimal positional numeral system. The lack of a positional value (or zero) was indicated by a space between sexagesimal numerals. By 300 BC, a punctuation symbol (two slanted wedges) was co-opted as a placeholder in the same Babylonian system. In a tablet unearthed at Kish (dating from about 700 BC), the scribe Bł-bn-aplu wrote his zeros with three hooks, rather than two slanted wedges. The Babylonian placeholder was not a true zero because it was not used alone, nor was it used at the end of a number. Thus numbers like 2 and

$120\ (2 \times 60), 3$ and $180(3 \times 60), 4$ and $240(4 \times 60)$ looked the same, because the larger numbers lacked a final sexagesimal placeholder. Only context could differentiate them. Furthermore, the symbol expressing zero were also found in the historical objects from the ancient Greek, China, Pre-Columbian Americas, and India. This condition motivated the existence of the symbol 0 to express zero as the universal language. Finally, human life has a new set of numbers, we recently call it, the set $\mathbb{N} = \{0, 1, 2, ...\}$ of all natural numbers.

We believe that mathematics is built for human life. In the development of the using of the set $\mathbb{N}$ of all natural numbers, human needs a negatives as the opposites of the set of $\{1, 2, 3, ...\}$ positive number since the ancient human may had used the subtraction in their calculation. This condition motivated the existence of the set of all integers. The set of integers is often denoted by a boldface letter $'Z'(\text{"}Z\text{"})$ or blackboard bold $\mathbb{Z}$ standing for the German word Zahlen which means "numbers". Furthermore, we will use the letter $\mathbb{Z}$ to express the set of all integers $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$.

1.2 Mathematical Induction

In the early part of this chapter, we will learn how to prove the correctness of a formula using mathematical induction. We will start this chapter by recalling the history of mathematical induction. In 370 BC, Plato's Parmenides might have an early example of an implicit inductive proof. The earliest implicit traces of mathematical induction can be found in Euclid's proof stating the number of primes is infinite and in Bhaskara's "cyclic method". An opposite iterated technique, counting down rather than up, is found in the Sorites paradox, where it was argued that if 1,000,000 grains of sand formed a heap and removing one grain from a heap left it a heap, then a single grain of sand (or even no grains) forms a heap.

An implicit proof by mathematical induction for arithmetic sequences was introduced in al-Fakhri written by al-Karaji around 1000

AD, who used it to prove the binomial theorem and properties of Pascal′s triangle. None of these ancient mathematicians, however, explicitly stated the induction hypothesis. Another similar case (contrary to what Vacca has written, as Freudenthal carefully showed) was that of Francesco Maurolico in his Arithmeticorum libri duo (1575), who used the technique to prove that the sum of the first n odd integers is n^2. The first explicit formula of the principle of induction was given by Pascal in his Traite du triangle arithmetique (1665). Another Frenchman, Fermat, made ample use of a related principle, indirect proof by infinite descent. The induction hypothesis was also employed by the Jakob Bernoulli, and from then on it became more or less well known. The modern rigorous and systematic treatment of the principle came only in the 19th century, with George Boole, Augustus de Morgan, Charles Sanders Peirce, Giuseppe Peano, and Richard Dedekind.

Mathematical induction is a way of establishing the correctness of formulas involving integer variables. It also applies to inequalities, algorithms and other assertions involving integer variables. Moreover, it applies to algorithms and assertions involving string variables. Let's see how it works first in the case of a formula.

You have a formula that involves an integer variable n and want to prove that it is true for all positive integers n. In order to do this, you do the following two things.

1.2.1 Principle of Mathematical Induction

Let $S(n)$ be a statement. The mathematical induction steps are:

- Prove that the statement $S(1)$ is true.
- Suppose that the statement $S(k)$ is true for all positive integers $k \geq 1$. This is called the induction hypothesis step.
- Prove that statement $S(k+1)$ is true for all positive integers $k \geq 1$.

In conclusion, the statement is true for all positive integers n.

Example 1.1 Use mathematical induction to prove that

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

for all integers $n \geq 1$, and then find $2 + 4 + 6 + \cdots + 500$.

Solution. For every positive integer $n \geq 1$, we have

$$S(n) : 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Step 1. $S(1) : 1 = \frac{1(1+1)}{2}$ is true.

Step 2. (Inductive step) Suppose that

$$S(k) : 1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$$

is true for all positive integers k.

Step 3. We want to prove

$$S(k+1) : 1 + 2 + 3 + \cdots + k + (k+1)$$

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

We have

$$\begin{aligned}
[1 + 2 + 3 + k] + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2} \\
&= \frac{(k+1)((k+1)+1)}{2}.
\end{aligned}$$

Thus, the statement $S(k+1) : 1+2+3+\cdots+k+(k+1) = \frac{(k+1)((k+1+1))}{2}$ is true. By the principle of mathematical induction, this implies the statement

$$S(n) : 1+2+3+\cdots+n = \frac{n(n+1)}{2}.$$

is true for every positive integer n. As an example when $n = 5$, we have

$$1+2+3+4+5 = \frac{5\times(5+1)}{2} = 15.$$

For the second question, we have

$$\begin{aligned} 2+4+6+\cdots+500 =& 2(1+2+3+\cdots+250) \\ =& 2\times\frac{(250\times(250+1))}{2} \\ =& 62750 \end{aligned}$$

Example 1.2 Use mathematical induction to prove that for every positive integer n,

$$\sum_{i=1}^{n}(2i-1) = 1+3+5+\cdots+(2n-1) = n^2.$$

Solution. For every positive integer n, we set

$$S(n) : 1+3+5+\cdots+(2n-1) = n^2.$$

Step 1. $S(1) : 1 = 1^2$. Thus $S(1)$ is true.

Step 2. (Inductive step) Suppose that

$$S(k) : 1+3+5+\cdots+(2k-1) = k^2$$

is true for every positive integer k.

Step 3. We want to prove

$$S(k+1) : 1+3+5+\cdots+(2k-1)+(2(k+1)-1) = (k+1)^2.$$

We have

$$\begin{aligned} 1+3+5+\cdots+(2k-1)+(2(k+1)-1) &= k^2+(2(k+1)-1) \\ &= k^2+2k+2-1 \\ &= k^2+2k+1 \\ &= (k+1)^2. \end{aligned}$$

Thus, the statement

$$S(k+1): 1+3+5+\cdots+(2k-1)+(2(k+1)-1) = (k+1)^2$$

is true. By the principle of mathematical induction, this implies for every positive integer n,

$$S(n): 1+3+5+\cdots+(2n-1) = n^2.$$

As an example, when $n = 5$ we have

$$1+3+5+7+9 = 5^2 = 25.$$

Example 1.3 Use mathematical induction to prove that for every positive integer n,

$$\sum_{i=1}^{n} i^2 = 1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Solution. For every positive integer n, we set

$$S(n): 1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Step 1. $S(1): 1^2 = \frac{1\times 2\times(1+1)}{6} = 1$. Thus $S(1)$ is true.

Step 2. (Inductive step) Suppose that

$$S(k): 1^2+2^2+3^2+\cdots+k^2 = \frac{k(k+1)(2k+1)}{6}$$

is true for every positive integer k.

Step 3. We want to prove

$$S(k+1): 1^2+2^2+3^2+\cdots \\ +k^2+(k+1)^2=\frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}.$$

We have

$$\begin{aligned}1^2+2^2+3^2+\cdots+k^2+(k+1)^2 \\ &=\frac{k(k+1)(2k+1)}{6}+(k+1)^2 \\ &=\frac{k(k+1)(2k+1)+6(k+1)^2}{6} \\ &=\frac{(k+1)[k(2k+1)+6(k+1)]}{6} \\ &=\frac{(k+1)(2k^2+k+6k+6)}{6} \\ &=\frac{(k+1)(2k^2+7k+6)}{6} \\ &=\frac{(k+1)(k+2)(2k+3)}{6} \\ &=\frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}.\end{aligned}$$

Thus, the statement

$$S(k+1): 1^2+2^2+3^2+\cdots \\ +k^2+(k+1)^2=\frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}$$

is true. By the principle of mathematical induction, this implies for every positive integer n,

$$S(n): 1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

As an example, when $n=5$ we have

$$1^2+2^2+3^2+4^2+5^2=\frac{5\times(5+1)(10+1)}{6}=55.$$

Example 1.4 Use mathematical induction to prove that for every positive integer n, $2^{2n} - 1$ is divisible by 3 denoted by $3 \mid (2^{2n} - 1)$.

Solution. For every positive integer n, we set

$$S(n) : 3 \mid (2^{2n} - 1).$$

Step 1. We have $2^2 - 1 = 3$. Thus $S(1) : 3 \mid 2^{(2)-1}$ is true.

Step 2. (Inductive step) Suppose that

$$S(k) : 3 \mid (2^{2k} - 1)$$

is true for every positive integer k. This means there exist an integer x such that $2^{2k} - 1 = 3x$.

Step 3. We want to prove

$$S(k+1) : 3 \mid (2^{2(k+1)} - 1).$$

We have

$$\begin{aligned} 2^{2(k+1)} - 1 =& 2^{2k+2} - 1 \\ =& 4 \times 2^{2k} - 1 \\ =& (3+1)2^{2k} - 1 \\ =& 3 \times 2^{2k} + (2^{2k} - 1) \\ =& 3 \times 2^{2k} + 3x \\ =& 3 \times (2^{2k} + x). \end{aligned}$$

Thus, the statement

$$S(k+1) : 3 \mid (2^{2(k+1)} - 1)$$

is true. By the principle of mathematical induction, this implies for every positive integer n,

$$S(n) : 3 \mid (2^{2n} - 1).$$

Let $S(n)$ be a statement. In general, the mathematical induction steps can be formulated as:

1. Prove that the statement $S(a)$ is true for a starting integer a.
2. Suppose that the statement $S(k)$ is true for every integer $k \geq a$. This is called the induction hypothesis step.
3. Prove that the statement $S(k+1)$ is true for every integer $k \geq a$.
4. We can conclude that the statement $S(n)$ is true for every integer $n \geq a$.

Example 1.5 Use mathematical induction to prove that for every positive integer $n \geq 3$, $2n + 1 < 2^n$.

Solution. For every positive integer $n \geq 3$, we set

$$S(n) : 2n + 1 < 2^n.$$

Step 1. We have $2 \times 3 + 1 = 7 < 8 = 2^3$. Thus $S(3)$ is true.

Step 2. (Inductive step) Suppose that

$$S(k) : 2k + 1 < 2^k$$

is true for every positive integer $k \geq 3$.

Step 3. We want to prove

$$S(k+1) : 2(k+1) + 1 < 2^{k+1}.$$

We have

$$\begin{aligned} 2(k+1) + 1 =& 2k + 2 + 1 \\ =& 2k + 1 + 2 \\ <& 2^k + 1, \text{since } S(k) \text{ is true} \\ <& 2^k + 2^k, \text{since } k \geq 3 = 2^{k+1}. \end{aligned}$$

Thus, the statement

$$S(k+1): 2(k+1)+1 < 2^{k+1}$$

is true. By the principle of mathematical induction, this implies for every positive integer $n \geq 3$,

$$S(n): 2n+1 < 2^n.$$

Example 1.6 Use mathematical induction to prove that for every positive integer $n \geq 1$,

$$\sum_{i=1}^{n} i(i+1) = 2+6+12+\cdots+n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

Solution. For every positive integer $n \geq 1$, we set

$$S(n): \sum_{i=1}^{n} i(i+1) = 2+6+12+\cdots+n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

Step 1. $S(1): 1 \times (1+1) = 2 = \frac{1\times(1+1)\times(1+2)}{3}$. Thus $S(3)$ is true.

Step 2. (Inductive step) Suppose that

$$S(k): \sum_{i=1}^{k} i(i+1) = 2+6+12+\cdots+k(k+1) = \frac{k(k+1)(k+2)}{3}$$

is true for every positive integer $k \geq 1$.

Step 3. We want to prove

$$\begin{aligned} S(k+1): \sum_{i=1}^{k+1} i(i+1) =& 2+6+12+\cdots \\ &+ k(k+1)+(k+1)((k+1)+1) \\ &= \frac{(k+1)((k+1)+1)((k+1)+2)}{3} \\ =& \frac{(k+1)(k+2)(k+3)}{3}. \end{aligned}$$

We have

$$\begin{aligned}\sum_{i=1}^{k} i(i+1) =& [2+6+12+\cdots+k(k+1)]+(k+1)((k+1)+1)\\ =& \frac{k(k+1)(k+2)}{3}+(k+1)(k+2)\\ =& \frac{k(k+1)(k+2)+3(k+1)(k+2)}{3}\\ =& \frac{(k+1)(k+2)(k+3)}{3}.\end{aligned}$$

Thus, the statement

$$\begin{aligned}S(k+1): \sum_{i=1}^{k+1} i(i+1) =& 2+6+12+\cdots\\ &+k(k+1)+(k+1)((k+1)+1)\\ =& \frac{(k+1)(k+2)(k+3)}{3}\end{aligned}$$

is true. By the principle of mathematical induction, this implies for every positive integer $n \geq 1$,

$$S(n): \sum_{i=1}^{n} i(i+1) = 2+6+12+\cdots+n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

As an example, when $n = 5$ we have $2+6+12+20+30 = \frac{5\times6\times7}{3} = 70$.

Example 1.7 Use mathematical induction to prove that for every positive integer $n \geq 4$, $2^n < n!$.

Solution. For every positive integer $n \geq 4$, we set

$$S(n): 2^n < n!.$$

Step 1. $S(4): 2^4 = 16 < 24 = 4!$. Thus $S(4)$ is true.

Step 2. (Inductive step) Suppose that

$$S(k) : 2^k < k!$$

is true for every positive integer $k \geq 4$.

Step 3. We want to prove

$$S(k+1) : 2^{k+1} < (k+1)!.$$

We have

$$\begin{aligned} 2^{k+1} =& 2 \times 2^k \\ =& 2 \times (k!), \text{ since } S(k) \text{ is true} \\ =& (k+1) \times (k!), \text{ since } k \geq 4, 2 < (k+1) \\ =& (k+1)!. \end{aligned}$$

Thus, the statement

$$S(k+1) : 2^{k+1} < (k+1)!$$

is true. By the principle of mathematical induction, this implies for every positive integer $n \geq 4$,

$$S(n) : 2^n < n!.$$

As an example, when $n = 5$ we have $2^5 = 32 < 120$.

Example 1.8 Use mathematical induction to prove that for every nonnegative integer n,

$$\begin{aligned} \sum_{i=0}^{n} r^i &= 1 + r + r^2 + r^3 + \cdots + r^n \\ &= \frac{r^{n+1} - 1}{r - 1}, r \neq 1. \end{aligned}$$

Solution. For every nonnegative integer n, we set

$$S(n) : \sum_{i=0}^{n} r^i = 1 + r + r^2 + r^3 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1},\ r \neq 1.$$

Step 1. $S(0) : \sum_{i=0}^{0} r^i = 1 = \frac{r^{0+1} - 1}{r - 1}$. Thus $S(0)$ is true.

Step 2. (Inductive step) Suppose that

$$S(k) : \sum_{i=0}^{k} r^i = 1 + r + r^2 + r^3 + \cdots + r^k = \frac{r^{k+1} - 1}{r - 1},\ r \neq 1.$$

is true for every nonnegative integer k.

Step 3. We want to prove

$$\begin{aligned} S(k+1) : \sum_{i=0}^{k+1} r^i &= 1 + r + r^2 + r^3 + \cdots + r^k + r^{k+1} \\ &= \frac{r^{(k+1)+1} - 1}{r - 1} \\ &= \frac{r^{k+2} - 1}{r - 1},\ r \neq 1. \end{aligned}$$

We have

$$\begin{aligned} 1 + r + r^2 + r^3 + \cdots + r^k + r^{k+1} &= \frac{r^{k+1} - 1}{r - 1} + r^{k+1} \\ &= \frac{(r^{k+1} - 1) + r^{k+1}(r - 1)}{r - 1} \\ &= \frac{r^{k+1} - 1 + r^{k+2} - r^{k+1}}{r - 1} \\ &= \frac{r^{k+2} - 1}{r - 1}. \end{aligned}$$

Thus, the statement

$$S(k+1) : \sum_{i=0}^{k+1} r^i = 1 + r + r^2 + r^3 + \cdots + r^k + r^{k+1} = \frac{r^{k+2} - 1}{r - 1},\ r \neq 1,$$

is true. By the principle of mathematical induction, this implies for every nonnegative integer n,

$$S(n): \sum_{i=0}^{n} r^i = 1 + r + r^2 + r^3 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1},\ r \neq 1.$$

Example 1.9 Use mathematical induction to prove that for every positive integer n,

$$\frac{\mathrm{d}^n}{\mathrm{d}x^n}(x^{-1}) = (-1)^n n! x^{-(n+1)}.$$

Solution. For every nonnegative integer n, we set

$$S(n): \frac{\mathrm{d}^n}{\mathrm{d}x^n}(x^{-1}) = (-1)^n n! x^{-(n+1)}.$$

Step 1. $S(1): \dfrac{\mathrm{d}}{\mathrm{d}x}(x^{-1}) = (-1) \times 1! \times x^{-(1+1)} = -x^{-2}$ Thus $S(1)$ is true.

Step 2. (Inductive step) Suppose that

$$S(k): \frac{\mathrm{d}^k}{\mathrm{d}x^k}(x^{-1}) = (-1)^k k! x^{-(k+1)}$$

is true for every positive integer k.

Step 3. We want to prove

$$S(k+1): \frac{\mathrm{d}^{k+1}}{\mathrm{d}x^{k+1}}(x^{-1}) = (-1)^{k+1}(k+1)! x^{-((k+1)+1)}.$$

We have

$$\begin{aligned}
\frac{\mathrm{d}^{k+1}}{\mathrm{d}x^{k+1}}(x^{-1}) =& \frac{\mathrm{d}}{\mathrm{d}x}\left[\frac{\mathrm{d}^k}{\mathrm{d}x^k}(x^{-1})\right] \\
=& \frac{\mathrm{d}}{\mathrm{d}x}(-1)^k k! x^{-(k+1)} \\
=& (-1)^k k!(-(k+1)) x^{-(k+2)} \\
=& (-1)^{k+1}(k+1)! x^{-(k+2)}.
\end{aligned}$$

Thus, the statement

$$S(k+1): \frac{\mathrm{d}^{k+1}}{\mathrm{d}x^{k+1}}(x^{-1}) = (-1)^{k+1}(k+1)!x^{-((k+1)+1)}$$

is true. By the principle of mathematical induction, this implies for every nonnegative integer n,

$$S(n): \frac{\mathrm{d}^{n}}{\mathrm{d}x^{n}}(x^{-1}) = (-1)^{n}n!x^{-(n+1)}.$$

We give the following problems related to mathematical induction. Learn and solve them.

Use mathematical induction to prove:

1. $\sum_{i=1}^{n} i^3 = 1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$, for every integer $n \geq 1$.
2. $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n(n+1)}$, for every integer $n \geq 1$.
3. $\sum_{i=1}^{n} 2i^2 = 2 \times 1^2 + 2 \times 2^2 + 2 \times 3^2 + \cdots + 2 \times n^2 = n^3 + n$, for every integer $n \geq 1$.
4. $\sum_{i=1}^{n} (2i-1)^2 = 1^2 + 3^2 + 5^2 + \cdots + (2n-1)$, for every integer $n \geq 1$.
5. $7^n - 1$ is divisible by 6, denoted by $6 \mid (7^n - 1)$, for every integer $n \geq 1$.
6. $n^3 - n$ is divisible by 3 for every integer $n \geq 1$.
7. $7^n - 2^n$ is divisible by 5 for every integer $n \geq 1$.
8. $3^n - 1$ is divisible by 2 for every integer $n \geq 1$.

9. $\sum_{i=1}^{n} 2i+3 = 5+7+9+\cdots+(2n+3) = n(n+4)$, for every integer $n \geq 1$.

1.3 Binomial Theorem

1.3.1 Binomial Expansion

A binomial is an expression of the form $(a+b)^n$. In general, the expansion of these binomials for various values of n can be obtained by multiplying $(a+b)$ for n times. We have

$$(a+b)^n = \underbrace{(a+b)\times\cdots\times(a+b)}_{n \text{ times}}$$

We note that every term in the expansion of $(a+b)^n$ appears as $a^{n-i}b^i$, for some $0 \leq i \leq n$. The coefficient of $a^{n-i}b^i$ comes from the multiplication of $n-i$ times of a and i times of b. This equals to the number of choosing $n-i$ of a from n number of a or equivalently the number of choosing i of b from n number of b. Thus, the coefficient of $a^{n-i}b^i$ is

$$\begin{pmatrix} n \\ n-i \end{pmatrix} = \begin{pmatrix} n \\ i \end{pmatrix}$$

where

$$\binom{n}{r} = \frac{n!}{(n-r)!r!}, 0 \leq r \leq n.$$

Furthermore, we have the following table in the next page.

Table 1.1 Binomial Expansion

Term	Expansion	Coefficients
$(a+b)^0$	1	$\binom{0}{0}$
$(a+b)^1$	$a+b$	$\binom{1}{0}, \binom{1}{1}$
$(a+b)^2$	$a^2+2ab+b^2$	$\binom{2}{0}, \binom{2}{1}, \binom{2}{2}$
$(a+b)^3$	$a^3+3a^2b+3ab^2+b^3$	$\binom{3}{0}, \binom{3}{1}, \binom{3}{2}, \binom{3}{3}$

In general, we have the binomial theorem

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + ...+ \\ + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

We note that the triangle of numbers in the third column in Table 1.1 is related to Pascal's triangle. In Pascal's triangle, the sum of each pair of adjacent numbers gives the number underneath the pair. In other words, the numbers in Pascal's triangle correspond to the coefficients in the binomial expansions. We will prove the Binomial Theorem for $a = 1$ and $b = x$ in the further subsection.

Example 1.10 Use Pascal's triangle to expand $(2+3x)^5$.

Solution. The coefficients in the next row in Table 1.1 are $1, 5, 10, 10, 5, 1$. We have the following expansion:

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

By substituting $a = 2$ and $b = 3x$, we obtain

$$\begin{aligned}(2+3x)^5 &= 2^5 + 5 \times 2^4 \times (3x) + 10 \times 2^3 \times (3x)^2 \\ &\quad + 10 \times 2^2 \times (3x)^3 + 5 \times 2 \times (3x)^4 + (3x)^5 \\ &= 32 + 240x + 720x^2 + 1080x^3 + 910x^4 + 243x^5.\end{aligned}$$

Example 1.11 Use Pascal's triangle to expand $(5x - \frac{1}{x})^4$.

Solution. From the fifth row in Table 1.1, we have

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$

By substituting $a = 5x$ and $b = -\frac{1}{x}$, we obtain

$$\begin{aligned}(5x - \frac{1}{x})^4 &= (5x)^4 + 4 \times (5x)^3 \times \left(-\frac{1}{x}\right) \\ &\quad + 6 \times (5x)^2 \times \left(-\frac{1}{x}\right)^2 + 4 \times (5x) \times \left(-\frac{1}{x}\right)^3 + \left(-\frac{1}{x}\right)^4 \\ &= 625x^4 - 500x^2 + 150 - \frac{20}{x^2} + \frac{1}{x^4}.\end{aligned}$$

Example 1.12 Find the coefficient of x^3 in the expansion of $(7 - 2x)^5$.

Solution. We note that in the expansion of $(7 + (-2x))^5$, only $10 \times (7) \times (-2x)^3$ contributes x^3. We have

$$10 \times 7 \times (-2x)^3 = -3920x^3.$$

We obtain the coefficient of x^3 in the expansion of $(7 - 2x)^5$ is -3920.

Example 1.13 Find the coefficient of x^5 in the expansion of $(3x + 1)^7$.

Solution. We note that in the expansion of $(3x + 1)^7$, only $\binom{7}{2} \times (3x^5) \times 1^2$ contributes x^5. We have

$$\binom{7}{2} \times (3x^5) \times 1^2 = 5103x^5.$$

We obtain the coefficient of x^5 in the expansion of $(3x + 1)^7$ is 5103.

Example 1.14 Find the constant term in the expansion of $\left(5x + \frac{1}{x^2}\right)^6$.

Solution. The solution of $x^{6-i}\left(\frac{1}{x^2}\right)^i = x^0$ is $i = 2$. This means the required term is

$$\begin{aligned}\binom{6}{2}(5x)^4\left(\frac{1}{x^2}\right)^2 &= 15 \times 625x^4 \times \frac{1}{x^4} \\ &= 9375.\end{aligned}$$

Example 1.15 Find the term in x^8 the expansion of $(x + \sqrt{x})^1\, 2$.

Solution. The solution of $x^{12-i}\left(\sqrt{x}\right)^i = x^8$ is $i = 8$. This means the required term is

$$\binom{12}{8}(x)^4\left(\sqrt{x}\right)^8 = 495x^8.$$

When $a = 1$ and $b = x$, we have the following special case of binomial theorem

$$(1+x)^n = 1 + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n-1}x^{n-1} + x^n$$

Example 1.16 Use the binomial theorem to expand $(1 + \sqrt{x})^4$ then write $(1 + \sqrt{3})^4$ in the simplest form.

Solution. We have

$$\begin{aligned}\left(1+\sqrt{x}\right)^4 &= 1 + \binom{4}{1}\sqrt{x} + \binom{4}{2}\left(\sqrt{x}\right)^2 + \binom{4}{3}\left(\sqrt{x}\right)^3 + \left(\sqrt{x}\right)^4 \\ &= 1 + 4\sqrt{x} + 6x + 4x\sqrt{x} + x^2\end{aligned}$$

which implies

$$\begin{aligned}(1+\sqrt{3})^4 &= 1 + 4\sqrt{3} + 6 \times 3 + 4 \times 3\sqrt{3} + 3^2 \\ &= 28 + 16\sqrt{3}.\end{aligned}$$

Example 1.17 Using binomial theorem, count 1.1^5!

Solution. We have

$$\begin{aligned}(1+x)^5 &= 1 + \binom{5}{1}x + \binom{5}{2}x^2 + \binom{5}{3}x^3 + \binom{5}{4}x^4 + x^5 \\ &= 1 + 5x + 10x^2 + 10x^3 + 5x^4 + x^5\end{aligned}$$

which implies

$$\begin{aligned}1.1^5 &= (1+0.1)^5 \\ &= 1 + 0.5 + 0.10 + 0.010 + 0.0005 + 0.000001 \\ &= 1.61051.\end{aligned}$$

1.3.2 Approximations Using the Binomial Theorem

If successive terms of a binomial expansion get smaller and smaller, we can ignore negligible terms and hence make approximations.

Example 1.18 Expand $(1+2x)^5$ up to x^3 and find an approximation for 1.02^5.

Solution. We have

$$\begin{aligned}(1+2x)^5 &= 1 + \binom{5}{1}(2x) + \binom{5}{2}(2x)^2 + \binom{5}{3}(2x)^3 + \dots \\ &= 1 + 10x + 40x^2 + 80x^3 + \dots\end{aligned}$$

Substituting $x = 0.01$, we obtain

$$\begin{aligned}(1.02)^5 &= 1 + 10 \times 0.01 + 40 \times 0.0001 + 80 \times 0.000001 + \dots \\ &\approx 1.10408.\end{aligned}$$

This is very close to the exact value 1.1040808031.

Example 1.19 Expand $(2-3x)^{10}$ up to x^3 and find an approximation for 1.97^{10}.

Solution. We have

$$\begin{aligned}(2-3x)^{10} &= 2^{10} + \binom{10}{1} 2^9(-3x) + \binom{10}{2} 2^8(-3x)^2 \\ &\quad + \binom{10}{3} 2^7(-3x)^3 + \dots \\ &= 1024 - 15360x + 103680x^2 - 414720x^3 + \dots\end{aligned}$$

Substituting $x = 0.01$ provides us

$$\begin{aligned}(1.97)^{10} &= 1024 - 153.60 + 10.3680 - 0.414720 + \dots \\ &\approx 880.35328.\end{aligned}$$

This is very close to the exact value 1.1040808031.

1.3.3 Problems where the Power is Unknown

In some cases, the value of n in $(a+b)^n$ is unknown. We are able to count n when certain expansion is given.

Example 1.20 In the expansion of $(1+3x)^n$, the coefficient of x^2 is 105. Find the value of n.

Solution. We have

$$\begin{aligned}\binom{n}{2}(3x)^2 &= \frac{n(n-1)}{2} \times 9x^2 \\ &= 105x^2.\end{aligned}$$

This gives us

$$\begin{aligned} & \frac{n(n-1)}{2} \times 9 = 105 \\ \Leftrightarrow \quad & n(n-1) = 30 \\ \Leftrightarrow \quad & n^2 - n - 30 = 0 \\ \Leftrightarrow \quad & (n-6)(n+5) = 0.\end{aligned}$$

Since n is nonnegative, we get $n = 6$.

Example 1.21 In the expansion of $(1+px)^q$, the coefficients of x and x^2 are -28 and 336, respectively. Find the values of p and q.

Solution. The corresponding expansion is

$$(1+px)^q = 1 + q(px) + \frac{q(q-1)}{2!}(px)^2 + \dots$$

Equating the coefficients of both sides provides us $pq = -28$ and $\frac{q(q-1)}{2!}p^2 = 336$. Combining both equations give us

$$\begin{aligned}
\frac{q(q-1)}{2!} \times \left(-\frac{28}{q}\right)^2 &= 336 \\
\Leftrightarrow \quad \frac{391(q-1)}{q} &= 336 \\
\Leftrightarrow \quad 392q - 336q &= 392 \\
\Leftrightarrow \quad 56q &= 392 \\
\Leftrightarrow \quad q &= 7.
\end{aligned}$$

We get $p = -\frac{28}{7} = -4$.

Example 1.22 In the expansion of $(a+x)(1+x)^n$, the first two terms are $3 + 16x$. Find the coefficients of x^2 and x^3.

Solution. We have

$$\begin{aligned}
(a+x)(1+x)^n &= (a+x) \\
&\quad \left(1 + nx + \frac{n(n-1)}{2!}x^2 + \frac{n(n-1)(n-2)}{3!}x^3 + \cdots\right) \\
&= a + (1+an)x + \left(n + \frac{an(n-1)}{2!}\right)x^2 \\
&\quad + \left(\frac{n(n-1)}{2!} + \frac{an(n-1)(n-2)}{3!}\right)x^3 + \dots \\
&= 3 + 16x
\end{aligned}$$

Equating the coefficients gives us $a = 3$ and $1 + an = 1 + 3n = 16$. This gives us $n = 5$. We get the coefficient of x^2 is

$$5 + \frac{3 \times 5 \times 4}{2} = 5$$

and the coefficent of x^3 is

$$\frac{5 \times 4}{2} + \frac{3 \times 5 \times 4 \times 3}{6} = 40.$$

In the next part, we will give some basic properties which are very important in the binomial theorem section.

Theorem 1.23 *If $r \leq n$, then $\binom{n}{r} = \binom{n}{n-r}$.*

Proof. Now let $r \leq n$. It follows from the definition that

$$\binom{n}{r} = \frac{n!}{(n-r)!r!} = \frac{n}{(n-(n-r))!(n-r)!} = \binom{n}{n-r}.$$

■

The theorem which has been explain above is called the symmetric property of the binomial coefficient. In order to make the property more readable, we provide some examples below.

Example 1.24 The following examples explained the symmetric property of the binomial coefficient.

1. $\binom{10}{2} = \binom{10}{8} = 45$
2. $\binom{12}{10} = \binom{12}{2} = 66$

We believe that mathematics is a tool to help the human to solve their problem. In the following example, we will describe the motivation of the existing property of binomial coefficient.

Example 1.25 Now we assume that there is a meeting. There are 10 persons in this meeting. Moreover, we will choose 3 persons from 10. Hence, there are $\binom{10}{3}$ ways to choose. In case, if the election proses for 3 persons does not enclose one of the attendants, then we have $\binom{9}{3}$ ways. Furthermore, if one person does not enclosed in every election

for the 3 chosen person, then we actually only choose for 2 person from 9. Hence, we have the following conclusion.

$$\binom{10}{3} = \binom{9}{3} + \binom{9}{2}.$$

Please, clarify the conclusion explained above by checking the result of $\binom{10}{3}$ and $\binom{9}{3} + \binom{9}{2}$.

In general case, we have the following property as a generalization of the case explain in the Example 1.25.

Theorem 1.26 *If k and r are natural numbers such that $k > r$, the we therefore have*

$$\binom{k}{r-1} + \binom{k}{r} = \binom{k+1}{r}$$

Proof.

$$\begin{aligned}
\binom{k}{r-1} + \binom{k}{r} &= \frac{k!}{(k-r+1)!(r-1)!} + \frac{k!}{(k-r)!r!} \\
&= \frac{k!r + k!(k-r+1)}{k+1-r)!r!} \\
&= \frac{k!(r+k-r+1)}{(k+1-r)!r!} \\
&= \frac{k!(k+1)}{(k+1-r)!r!} \\
&= \frac{(k+1)!}{(k+1-r)!r!} \\
\binom{k}{r-1} + \binom{k}{r} &= \binom{k+1}{r}
\end{aligned}$$

■

Now, we are ready to prove the another form of Binomial Theorem as follows

Theorem 1.27 *For every natural number n, we have*

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + ... + \binom{n}{n-1}x^{n-1} + \binom{n}{n}x^n$$

Proof. We will prove the Binomial Theorem by using mathematical induction.

1. $S(1)$: We have $(1+a)^1 = \binom{1}{0} + \binom{1}{1}a = a+a$. Thus $S(1)$ is true.

2. Inductive step. Suppose that $S(k)$:

   $$(1+x)^k = \binom{k}{0} + \binom{k}{1}x + ... + \binom{k}{k-1}x^{k-1} + \binom{k}{k}x^k$$

   is true for every integer k.

3. We want to prove Suppose that $S(k+1)$:

   $$(1+x)^k = \binom{k+1}{0} + \binom{k+1}{1}x + ... + \binom{k+1}{k}x^k + \binom{k+1}{k+1}x^{k+1}$$

$$\begin{aligned}(1+a)^{k+1} &= (1+a)^k(1+a)\\ &= [\binom{k}{0} + \binom{k}{1}x + ... + \binom{k}{k-1}x^{k-1} + \binom{k}{k}x^k]\\ &\quad (1+a)\\ &= \binom{k}{0} + [\binom{k}{0} + \binom{k}{1}]a + ... + [\binom{k}{k-1} + \binom{k}{k}]a^k\\ &\quad + \binom{k}{k}a^{k+1}\\ (1+a)^{k+1} &= \binom{k+1}{0} + \binom{k+1}{1}x + ... + \binom{k+1}{k}x^k\\ &\quad + \binom{k+1}{k+1}x^{k+1}\end{aligned}$$

Hence, we may infer that

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + ... + \binom{n}{n-1}x^{n-1} + \binom{n}{n}x^n$$

for every integers n. ■

Theorem 1.28 *For every integers n, we have*

$$2^n = \binom{n}{0} + \binom{n}{1} + ... + \binom{n}{n-1} + \binom{n}{n}$$

Proof. It follows from Theorem 1.27, in case $x = 1$, we already have

$$2^n = \binom{n}{0} + \binom{n}{1} + ... + \binom{n}{n-1} + \binom{n}{n}$$

■

We will use Theorem 1.27 and Theorem 1.28 to solve the following problem.

Example 1.29 Prove that

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + ... = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + ... = 2^{n-1}$$

Proof. Substitute $x = -1$ in the Theorem 1.27, we therefore have

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} ... + (-1)^k \binom{n}{k} + ... + (-1)^n \binom{n}{n}$$

This implies

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + ... = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + ...$$

Applying the Theorem 1.28, we have

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + ... = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + ... = \frac{2^n}{2} = 2^{n-1}$$

■

Theorem 1.30 *If n, m, and k are natural numbers such that $n > k > m$, then*

$$\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$$

Proof.

$$\begin{aligned}\binom{n}{k}\binom{k}{m} &= \frac{n!}{(n-k)!k!}\frac{k!}{(k-m)!m!} \\ &= \frac{n!}{(n-m)!m!}\frac{(n-m)!}{(n-m-k+m)!(k-m)!} \\ \binom{n}{k}\binom{k}{m} &= \binom{n}{m}\binom{n-m}{k-m}\end{aligned}$$

■

Example 1.31 In a class, there are 15 students. We will choose 5 students from 15 and 2 student from 5 chosen students to be the main team. We would like to determine how many ways we can use to choose these 5 students.

1. The first method. We can start to choose 5 student from 15 and then we continue to choose 2 student from 5 who were chosen before. Hence, we have

$$\binom{15}{5}\binom{5}{2} = 30.030$$

2. The second method, we can start to choose 2 students for the main team from 15 students as the first step. Then, we can continue to choose 5-2 students from 15-2. Hence, we have

$$\binom{15}{2}\binom{13}{3} = 30.030$$

The example which is explained above can be generalized in the following theorem

Theorem 1.32 *If n and k are natural integers such that $n \geq k$, then*

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

Proof.

$$\begin{aligned} k\binom{n}{k} &= k\frac{n!}{(n-k)!k!} \\ &= k\frac{n(n-1)!}{(n-k)!k(k-1)!} \\ &= n\frac{(n-1)!}{(n-1-(k-1))!(k-1)} \\ k\binom{n}{k} &= n\binom{n-1}{k-1} \end{aligned}$$

■

If the binomial coefficient is arranged recursively, we have the Pascal's triangle. In case, $n \in \{0, 1, 2, 3, 4, 5, 6\}$, we have the following Pascal's triangle.

$n = 0$						1						
$n = 1$					1		1					
$n = 2$				1		2		1				
$n = 3$			1		3		3		1			
$n = 4$		1		4		6		4		1		
$n = 5$	1		5		10		10		5		1	
$n = 6$	1		6		15		20		15		6	1

The representation of Pascal's triangle using binomial coefficient symbol is shown below.

$$\begin{array}{ccccccccccccc}
 & & & & & & \binom{0}{0} & & & & & & \\
 & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
 & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
 & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & \\
\binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6}
\end{array}$$

Example 1.33 The following examples will generate another property of binomial coefficient.

1. $\binom{2}{0} + \binom{3}{1} + \binom{4}{2} + \binom{5}{3} + \binom{6}{4} = \binom{7}{3}$
2. $\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \binom{5}{2} + \binom{6}{2} = \binom{7}{3}$

Finally, for the general case, we have the following property.

Theorem 1.34 *If k and r are natural numbers such that $k \geq r$, then*

1. $\binom{k}{0} + \binom{k+1}{1} + ... + \binom{k+r}{r} = \binom{k+r+1}{r}$
2. $\binom{k}{k} + \binom{k+1}{k} + ... + \binom{k+r}{k} = \binom{k+r+1}{k+1}$

Proof.

1. (a) $S(1) : \binom{1}{0} + \binom{1}{1} = \binom{2}{1}$. Thus $S(1)$ is true.

   (b) Assume the statement is also valid for $S(n)$, that is, $S(n)$: $\binom{n}{0} + \binom{n+1}{1} + \binom{n+2}{3} + ... + \binom{n+r}{r} = \binom{n+r+1}{r}$

   (c) We will prove the statement is true for $S(n+1)$

   $$\binom{n+1}{0} + \binom{n+2}{1} + \binom{n+3}{2} + ... + \binom{n+r}{r-1} + \binom{n+1+r}{r} = \binom{n+r+1}{r}$$

   It follows from Theorem 1.26 that the left side can be represented as follows

$$\binom{n}{0}+\binom{n+1}{0}+\binom{n+1}{1}+...+\binom{n+r}{r-1}+\binom{n+r}{r}$$
$$=\binom{n+r+1}{r-1}+\binom{n+r+1}{r}$$
$$=\binom{n+r+1}{r}.$$

Hence, we can infer that the statement is also valid for $n+1$. Thus $S(n+1)$ is true.

2. The authors suggest the reader to prove by themselves.

■

The implementation of Theorem 1.34 in solving problem in number theory will be explained in the following examples.

Example 1.35 Evaluate the following statements

1. $1.2.3+2.3.4+3.4.5+...+(n-2)(n-1)n=3!\binom{n+1}{4}$
2. $1^2+2^2+3^2+4^2+...+n^2=2\binom{n+1}{3}+\binom{n+1}{2}$

Proof.

1. We have the following hint to solve the example number 1.

$$(k-2)(k-1)k=\frac{k!}{(k-3)!}=\frac{3!k!}{(k-3)!3!}=3!\binom{k}{3}$$

Hence, the left side of the problem in the example number 1 can be represented as

$$3!\binom{3}{3}+3!\binom{4}{3}+...+3!\binom{n}{3}=3!(\binom{3}{3}+\binom{4}{3}+...+\binom{n}{3})$$

It follows from Theorem 1.34 part (2) that

$$3!(\binom{3}{3}+\binom{4}{3}+...+\binom{n}{3})=3!\binom{n+1}{4}$$

2. We have the following hint to solve the example number 2.

$$k^2 = k(k-1) + k$$

Hence, the left side of the problem in the example number 2 can be represented as

$$\begin{aligned}
1^2 + 2^2 + ... + n^2 &= (1.0 + 1) + ... + (n(n-1) + n) \\
&= (2.1 + 3.2 + ... + n(n-1))(1 + 2 + ... + n) \\
&= 2\binom{2}{2} + ... + 2\binom{n}{2} + \binom{1}{1} + ... + \binom{n}{1} \\
&= 2(\binom{2}{2} + ... + \binom{n}{2}) + \binom{1}{1} + ... + \binom{n}{1} \\
1^2 + 2^2 + ... + n^2 &= 2\binom{n+1}{3} + \binom{n+1}{2}
\end{aligned}$$

■

Homework Chapter 1

1. Show that $1 + 2 + 3 + ... + n = \binom{n+1}{2}$

2. Prove the following statement using mathematical induction for every positive integer n.

   a $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{1}{3}n(4n^2 - 1)$.

   b $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$.

3. Prove that

$$1 + 2 + 3 + 4 + \cdots + n = \binom{n+1}{2} \ !$$

4. Prove that for any $n \geq 1$, $\binom{n}{k} = \binom{n}{k+1}$ if and only if n is an odd number and $k = \frac{1}{2}(n-1)$.

5. Prove that $n\binom{n-1}{k} = (k+1)\binom{n}{k+1}$!

6. Let k, r, n be natural numbers such that $0 \leq k \leq r \leq n$. Prove that

$$\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}$$

7. Prove that

$$\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + ... + n\binom{n}{n} = n2^{n-1}$$

8. Determine the result of the following sums

$$n\binom{n}{1} + n\binom{n}{3} + n\binom{n}{5} + ... + n\binom{n}{n}$$

   where n is an even integer.

9. Evaluate the result of the following sums

$$\sum_{k=1}^{n} 12(k-1)k(k+1)$$

10. Prove that

$$\binom{k}{k} + \binom{k+1}{k} + ... + \binom{k+r}{k} = \binom{k+r+1}{k+1}$$

11. Prove that

$$\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + ... + 2^n\binom{n}{n} = 3^n$$

12. Determine the result

$$\binom{n}{0} + 2\binom{n}{1} + \binom{n}{2} + \binom{n}{4} + ...$$

13. Prove that

$$\binom{2n}{n} + \binom{2n}{n-1} = \frac{1}{2}\binom{2n+2}{n+1}$$

14. Calculate the following sums

    a. $\sum_{k=1}^{n} 12(k-1)k(k+1)$

    b. $\sum_{k=1}^{n}(-1)^k k\binom{n}{k}$

15. Prove that

$$\binom{n}{r} = \binom{n}{r+1} \iff r = \frac{1}{2}(n-1)$$

    and n is an odd integer.

CHAPTERS 2
DIVISIBILITY

2.1 DIVISIBILITY RELATION

In the number theory, we will be considering the set of all integers as the largest set since we dont use the set of all real numbers and the set of all rational numbers. The set of all integers is denoted by $\mathbb{Z}$ and the element of $\mathbb{Z}$ is usually denoted by small letter as $a, b, c, \ldots, m, n, \ldots, x, y, z$ We start by the following definition.

Definition 2.1 *Let a, b are integers. The integer a divides the integer b if there exists an integer k such that $b = ka$ and this condition is denoted by $a|b$. In other words, the integer a is a factor of the integer b. Otherwise $a \nmid b$.*

Example 2.2 The following examples describe the divisibility of integers.

1. $6|30$ since there exists 5 such that $30 = 5 \times 6$.
2. $8 \nmid 25$ since there is no integer a satisfying $25 = a \times 8$.

We summarize some basic properties of divisibility in the following proposition.

Proposition 2.3 *Let a, b, and c be integers. We have the following basic properties:*

i. $a \mid a$ *(reflexivity property)*

ii. If $a \mid b$ *and* $b \mid c$ *then* $a \mid c$ *(transitivity property)*

iii. *If* $a|b$ *then* $a|cb$

iv. *If* $a \mid b$ *and* $b \neq 0$ *then* $|a| \leq |b|$

v. *If* $a|b$ *and* $a|c$ *then* $a|\alpha b + \beta c$ *for any integers* α *and* β

vi. *If* $a \mid b$ *and* $a \mid b \pm c$ *then* $a \mid c$

vii. *If* $a \mid b$ *and* $b \mid a$ *then* $|a| = |b|$

viii. *If* $a \mid b$ *and* $b \neq 0$ *then* $\frac{b}{a} \mid b$

ix. *For* $c \neq 0$, $a \mid b$ *if and only if* $ac \mid bc$

Proof. The proofs of the above properties are rather straightforward from the definition. We present proofs for some of them to give the reader some relevant examples of writing proofs.

(Proof of ii) Let a, b and c be integers such that $a \mid b$ and $b|c$. Since $a|b, b = ka$, where k is an integer and $b|c$ implies $c = lb$,, where l is an integer. Therefore $c = lb = l(ka) = (lk)a$. Hence $a|c$.

(Proof of iii) Let $a|b$ and $b = ka$, for any integer k. Multiplying the both sides of the equation $b = ka$ by c gives us $bc = cka$. Thus $a|bc$.

■

Theorem 2.4 *If* $a|b$ *and* $a|c$*, then the following conditions hold.*

i. $a|b + c$

ii. $a|b - c$

iii. $a|bc$

Proof. Now let $a|b$ and $a|c$. Then $b = ka$ for an integer k, and $c = la$ for an integer l. Moreover, we have

i. $b + c = ka + la = (k + l)a \Rightarrow a|b + c$

ii. $b - c = ka - la = (k - l)a \Rightarrow a|b - c$

iii. $bc = (ka)(la) = (kal)a \Rightarrow a|bc$

■

Theorem 2.5 *If $a|b$ and $a|c$, then $a|mb + nc$ for any integers a, b, c, m and n.*

Proof. Now let $a|b$ and $a|c$. Then $b = ka$ for an integer k, and $c = la$ for an integer l. Furthermore, multiplying the both sides of the equation $b = ka$ with m, we have $mb = mka$ and multiplying the both sides of the equation $c = la$ with n, we have $nc = nla$. Thus $mb + nc = mka + nla = (mk + nl)a \Rightarrow a|mb + nc$. ■

Theorem 2.6 *For any integers a, b and m the following conditions hold.*

i. If $ma|mb$ and $m \neq 0$, then $a|b$.

ii. $1|a$ and $a|0$.

iii. If $a|b$ and $b \neq 0$,then $|a| \leq |b|$.

Proof.

i. Now let $ma|mb, m \neq 0$. Then $mb = kma$ for an integer k, since $m \neq 0$, divide the both side of the previous equation, we have $b = ka$. This implies $a|b$.

ii. It is clear that $a = a.1$. Hence $1|a$ for any integer a. Furthermore, $0 = 0.a$ for any integer a. Thus $a|0$.

iii. The proof is left as an exercise to the reader.

■

2.2 Greatest Common Divisor (GCD)

We have learned to determine some factors of any integers. For example, the integers 1, 2, 3, 5,9,15 and 45 are factors or divisors of the integer 45. On the other hand, the factors of 60 are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20 and 30. In fact, the greatest factor of 45 and 60 is 15. Now, we are ready to define what the greatest common divisor is. We start with the definition of a common divisor as described below.

Definition 2.7 *Let a and b be integers. Then an integer d is said to be common divisor of a and b if $d|a$ and $d|b$.*

Example 2.8 The integer 2 is a common divisor of 30 and 40.

Definition 2.9 *Let a and b be integers. Then an integer d is said to be greatest common divisor of a and b if*

1. *$d|a$ and $d|b$.*
2. *there exists an integer e such that $e|a$ and $e|b$, then a and $e \leq d$.*

Example 2.10 Take a look at the following examples.

1. Positive divisors of -15 are 1,3,5,15.
2. Positive divisors of 40 are 1,2,4,5,8,10,20,40.
3. The common divisors of -15 and 40 are 1,5.
4. The greatest common divisor of -15 and 40 is 5 will be denoted by $gcd(-15, 40) = 5$

We use $gcd(a, b) = d$ to denote d is the greatest common divisor of a and b. We start form the following property.

Theorem 2.11 *If $gcd(a, b) = d$, then*

$$gcd(\frac{a}{d}, \frac{b}{d}) = 1.$$

Proof. The number $\frac{a}{d}$ and $\frac{b}{d}$ seem to be fractions, but they are integers since d is a divisor both of a and b. In fact, we have $gcd(a, b) = d$. So, it is possible to find integers y such that $d = ax + by$ (we will discuss this property later in this chapter). Upon dividing each side of this equation by the integer d, we therefore have the expression

$$1 = \left(\frac{a}{d}\right) x + \left(\frac{b}{d}\right) y$$

Since $\frac{a}{d}$ and $\frac{b}{d}$ are integers, we may conclude that $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime. Thus

$$gcd(\frac{a}{d}, \frac{b}{d}) = 1.$$

■

Theorem 2.12 ***Division Algorithm*** *Let a and b are integers such that $b > 0$. If there exists a unique pair of integers q and r such that*

$$a = bq + r, 0 \leq r < b.$$

The integer q is called the quotient, and the integer r is called the remainder in the division of a by b

Proof. Define a set as follows

$$S = \{a - xb | x \text{ an integer } ; a - xb \geq 0\}$$

We will show that the set S is nonempty by exhibiting a value of x implying $a - xb$ nonnegative. Since the integer $b \geq 1$, we have $|a|b \geq |a|$, and so

$$a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$$

For the choice $x = -|a|$, then, $a - xb$ belongs to S. This gives $S \neq \emptyset$. Moreover, the set S contains a smallest integer, say r. By the definition of S, there exists an integer q satisfying

$$r = a - qb \qquad 0 \leq r$$

We claim that $r < b$. If this were not the case, then $r \geq b$ and

$$a - (q+1)b = (a - qb) - b = r - b \geq 0$$

The consequence is that the integer $a - (q+1)b$ has the proper form to belong to the set S. However, $a - (q+1)b = r - b < r$, contrary to the choice of r as the smallest member of S. Hence, $r < b$. Furthermore, we will show the uniqueness of q and r. Suppose that a has two representation as follow.

$$a = qb + r = q'b + r'$$

where $0 \leq r < b, 0 \leq r' < b$. Then $r' - r = b(q - q')$. This implies

$$|r' - r| = b|q - q'|$$

Upon adding the two inequalities $-b < -r \leq 0$ and $0 \leq r' < b$, we obtain $-b < r' - r < b$ or in equivalent terms, $|r' - r| < b$. Thus, $b|q - q'| < b$, which gives

$$0 \leq |q - q'| < 1$$

Since $|q-q'|$ is a nonnegative integer, the only possible value for $|q-q'|$ is 0. This implies $|q - q'| = 0 \Rightarrow q = q'$ and $r = r'$. This completes the proof. ■

The following property is the consequence when the integer $b < 0$.

Corollary 2.13 *If a and b are integers such that $a \neq 0$, then there exists a unique pair of integers q and r such that $a = qb+r$, where $0 \leq r < |b|$.*

Proof. Prove this corollary as exercise. ■

Theorem 2.14 *If $b = aq + r$, then $gcd(b, a) = gcd(a, r)$.*

Proof. Let $gcd(b, a) = d$ and $gcd(a, r) = c$. We will show that $c = d$. Since $gcd(b, a) = d, d|b$ and $d|a$ and since $b = aq + r$, $d|q$. This implies

d is a common divisor of both a and r. But, since $gcd(a, r) = c$, $d \leq c$. Furthermore, since $gcd(a, r) = c, c|a$ and $c|r$ and since $b = aq + r, c|b$. It follows from $c|a$ and $c|b$ that c is a common divisor of both a and b. However, $gcd(a, b) = d$, then $d \geq c$. Since $d \geq c$ and $c \geq d, c = d$. This yields $gcd(b, a) = gcd(a, r)$ which completes the proof. ■

Theorem 2.15 *If a and b are integers such that $a, b \neq 0$, then there exist integers x and y such that $ax + by = gcd(a, b)$.*

Proof. Define a set as follows

$$S = \{a - xb | x \text{ an integer } ; a - xb \geq 0\}$$

We will show that the set S is nonempty. For any integer $a \neq 0$, then the integer $|a| = au + b.0$ belongs to S where $u = 1$ or $u = -1$ depending on the integer a is positive of negative. It is clear that the set S consists of positive integers which leads that S contains the smallest element, say d. It follows from the definition of S, there exists integers x and y for which $d = ax + by$. We claim that $d = gcd(a, b)$.

It follows from Division Algorithm, we can obtain integers q and r such that $a = qd + r$, where $0 \leq r < d$. Then r can be represented as the form

$$\begin{aligned} r &= a - qd \\ &= a - q(ax + by) \\ r &= a(1 - qx) + b(-qy) \end{aligned}$$

Now, if r were positive integers, then the representation would imply that r belongs to S, contrary to the fact that d is the smallest member of S. Therefore, $r = 0$ and so $a = qd$ or equivalently $d|a$. By using the similar reasoning, we therefore have $d|b$ which gives d is a common divisor of a and b.

Furthermore, if c is an arbitrary positive common divisor of the integers a and b, then $c|(ax + by), c|d$. Moreover, $c = |c| \leq |d| = d$, so

that d is greater than every positive common divisor of a and b. Thus, we may deduce that $d = gcd(a, b)$. ■

It follows from Theorem 2.15 that if $gcd(a, b) = 1$ then there exists positive integers x and y such that $ax + by = 1$. Conversely, if there exists positive integers x and y such that $ax + by = 1$, whether the statement $gcd(a, b) = 1$ is true?. In the following theorem, we give a necessary and sufficient condition for $gcd(a, b) = 1$.

Theorem 2.16 *Let $a, b \neq 0$ be integers. Then the following conditions are equivalent.*

i. $gcd(a, b) = 1$.

ii. There exists integers x and y such that $ax + by = 1$.

Proof. The first step, we will prove from (i) to (ii). Now, suppose $gcd(a, b) = 1$. It follows from Theorem 2.15 that there exists integers x and y such that $ax + by = gcd(a, b) = 1$. Conversely, suppose $ax + by = 1$ for some integers x and y and $d = gcd(a, b)$. We will show that $d = 1$. Since $d = gcd(a, b), d|a$ and $d|b$. This implies $d|(ax + by)$ or $d|1$. The possible value for d is only 1 since there is no positive integer greater than 1 which divides 1. Hence, $d = 1 \Rightarrow gcd(a, b) = 1$. ■

Finally, we have the following consequence.

Corollary 2.17 *If $a|c$ and $b|c$ such that $gcd(a, b) = 1$, then $ab|c$.*

Proof. Suppose $a|c$ and $b|c$ such that $gcd(a, b) = 1$. It follows from Theorem 2.16 that there exists integers x and y such that $ax + by = 1$. Multiplying the both side with c, we therefore have

$$acx + bxy = c$$

Since $a|c$ and $b|c$, there exists integers r and t such that $c = ar$ and

$c = bt$, substituting these fact, we have

$$abtx + abry = c$$
$$ab(tx + ry) = c$$

This gives $ab|c$ which completes the proof. ■

2.3 Least Common Multiple (LCM)

A multiple of a number is the product of that number and an integer. For example, 12 is a multiple of 6 because $6 \times 2 = 10$, so 12 is divisible by 6 and 2. Since 12 is the smallest positive integer that is divisible by both 6 and 2, it is the least common multiple of 6 and 2. By the same concept, 12 is the least common multiple of 6 and 2 as well. Moreover, we give the formal definition for a least common multiple as follows.

Definition 2.18 *Let a and b be integers. An integer m is said to be common multiple of a and b if $a|m$ and $b|m$. Furthermore, an integer m is said to be least common multiple of a and b if satisfies the following conditions:*

1. *$a|m$ and $b|m$,*
2. *If there exists n such that $a|n$ and $b|n$, then $m|n$.*

We use $lcm(a, b) = m$ to denote the least common multiple of a and b.

Theorem 2.19 *If c is a common multiple of nonzero integers a and b, then the least common multiple $lcm(a, b)$ of a and b divides c. In other words, $lcm(a, b)|c$.*

Proof. Let c be a common multiple of nonzero integers a and b and let least common multiple $lcm(a, b) = m$. We will show that $m|c$. Suppose

$m \nmid c$. It follows from the Division Algorithm, there exist integers q and r such that

$$c = qm + r \quad 0 < r < m$$

Since c is a multiple of both a and $b, a|c$ and $b|c$. On the other hand, since $lcm(a, b) = m, a|m$ and $b|m$. Furthermore,

$$a|m \Rightarrow a|qm \Rightarrow a|(c - qm) \text{ and } a|r$$

$$b|m \Rightarrow b|qm \Rightarrow b|(c - qm) \text{ and } b|r$$

Thus, r is a multiple of both a and b such that $0 < r < m$. But this is impossible since $lcm(a, b) = m$. Hence, $lcm(a, b) = m|c$. ■

Theorem 2.20 *If* $c > 0$, *then* $lcm(ca, cb) = c \times lcm(a, b)$.

Proof. Suppose $lcm(a, b) = d$. Then $a|d$ and $b|d$. This implies $ac|dc$ and $bc|dc$. Hence, dc is a multiple of both ac and bc. It follows from Theorem 2.16 that $lcm(ac, bc)|dc$. Since $lcm(ac, bc)$ is a multiple of ac, $lcm(ac, bc)$ is a multiple of c. Suppose $lcm(ac, bc) = mc$, then $mc|dc$ which implies $m|d$. On the other hand, since $lcm(ac, bc) = mc, ac|mc$ and $bc|mc$ which implies $a|m$ and $b|m$ and it follows from Theorem 2.19 that $lcm(a, b)|m$. This gives $m|d$ and $d|m$. So we may deduce that $d = m$. In other words, $lcm(ca, cb) = c \times lcm(a, b)$. ■

Consider the following theorem as an illustration of Theorem 2.20.

Example 2.21 It is clear that $lcm(14, 18) = 126 = 2 \times 63 = 2 \times lcm(7, 9)$.

Theorem 2.22 *if* a *and* b *are positive integers, then* $gcd(a, b) \times lcm(a, b) = ab$.

Proof. Let a and b be positive integers and let $gcd(a, b) = d$, then $gcd(\frac{a}{d}, \frac{b}{d}) = 1$. This gives $lcm(\frac{a}{d}, \frac{b}{d}) = \frac{ab}{d^2}$. Multiplying the both side,

we therefore have

$$\begin{aligned} d^2 \times lcm(\frac{a}{d}, \frac{b}{d}) &= ab \\ d \times lcm(a, b) &= ab \\ gcd(a, b) \times lcm(ab) &= ab. \end{aligned}$$

■

Homework Chapter 2

1. If $gcd(a, b) = d$, then prove that $d|(ax + by)$ for any integers x and y.
2. Prove that for any integer a which is one of the form $a, a + 2$, or $a + 4$ is divided by 3.
3. If a and b are nonzero integers, then prove that

   $gcd(a, b) = gcd(-a, b) = gcd(a, -b) = gcd(-a, -b)$.
4. Let n be a positive integer and let a be any arbitrary integer. Prove that $gcd(a, a + n)|n$.
5. If $gcd(a, b) = 1$, then prove that $gcd(a^n, b^k) = 1$ for every positive integer n and k.
6. Let $gcd(a, b) = 1$ and $gcd(a, c) = 1$. Prove $gcd(a, bc) = 1$.
7. If $gcd(a, b) = 1$, then prove that $gcd(ac, b) = gcd(c, b)$
8. If a is an odd integer, prove that $24|a(a^2 - 1)$.
9. If $gcd(a, b) = 1$ and $c(a+b)$, then prove that $gcd(a, c) = gcd(b, c) = 1$.
10. Prove that $gcd(a^2, b^2) = [gcd(a, b)]^2$.

    Let a, b, c, and d be integers. Identify the following statement and determine the truth.
11. If $gcd(a, b) = gcd(a, c)$, then $lcm(a, b) = lcm(a, c)$.
12. $lcm(a, -b) = lcm(a, b)$
13. If $d|gcd(a, b)$, then $d|lcm(a, b)$.
14. If $c|(a, b)$, then $c|gcd(a, b)$.
15. $gcd(a, b)|lcm(a, b)$.

CHAPTERS 3
INTEGERS BASES

3.1 INTEGERS BASES

In this chapter, we explain some bases for integers. We know that the integer base that we use commonly is $10-$base. However, there are some bases that we have to learn.

Take a look at the following example.

Example 3.1 Recall the representation of 4.875 as follows

$$4.875 = 4.10^3 + 8.10^2 + 7.10^1 + 5.10^0.$$

Based on the Mathematical history. The ancient Babylonian used $60-$base and the Mayan tribe used $20-$base. Furthermore, computer use $2-$base or we also call it as a binary base.

Theorem 3.2 *Let b be any integer greater than 1. Then for every positive integer n can be uniquely represented as the form*

$$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0$$

where k is a nonnegative integer and a_j is an integer such that $0 \leq a_j \leq b-1$ for $j = 0, 1, 2, ..., k$ with $a_k \neq 0$.

Proof. We will use the division algorithm for the early steps. We divide n using b. Therefore, we have

$$n = bq_0 + a_0, \;\; 0 \leq a_0 \leq b-1.$$

If $q_0 \neq 0$, we divide q_0 with b, then we have

$$q_0 = bq_1 + a_1, \;\; 0 \leq a_1 \leq b-1.$$

Analogously, we continue the division processes such that we have the following equations

$$q_1 = bq_2 + a_2, \;\; 0 \leq a_2 \leq b-1.$$

$$q_2 = bq_3 + a_3, \;\; 0 \leq a_3 \leq b-1.$$

.

.

.

$$q_{k-2} = bq_{k-1} + a_{k-1}, \;\; 0 \leq a_{k-1} \leq b-1.$$

$$q_{k-1} = b.0 + ak, \;\; 0 \leq a_k \leq b-1.$$

By the division algorithm processes, we get the sequence of integers $q_0, q_1, q_2, ..., 0$ such that $n > q_0 > q_1 > q_2 \geq 0$. Substituting the equation $q_0 = bq_1 + a_1$ in the equation $n = bq_0 + a_0$, we have

$$n = b^2q_1 + ba_1 + a_0$$

The substitution process can be continuous for $q_1, q_2, ...$ Hence, we have

$$n = a_kb^k + a_{k-1}b^{k-1} + ... + b^2a_2 + ba_1 + a_0,$$

where $0 \leq a_j \leq b-1$ for $j = 0, 1, 2, ..., k$ and $a_k \neq 0$, since $a_k = q_{k-1}$ is the last quotient which is not equal to 0. The uniqueness of the representation n will be describe as follows. Assume n has two representation, that are

$$n = a_kb^k + a_{k-1}b^{k-1} + ... + b^2a_2 + ba_1 + a_0$$

$$n = c_kb^k + c_{k-1}b^{k-1} + ... + b^2c_2 + bc_1 + c_0$$

Hence,

$$(a_k - c_k)b^k + (a_{k-1} - c_{k-1})b^{k-1} + ... + b^2(a_2 - c_2) + b(a_1 - c_1) + (a_0 - c_0) = 0.$$

This equation holds if $a_j - c_j = 0$. Then $a_j = c_j$ for every $j \in \{0, 1, 2, 3, ..., k\}$. So, we can conclude that the representation of n is unique. ■

It follows from Theorem 3.2 that the integer n can be represented as

$$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0$$

where k is a nonnegative integer and a_j is an integer such that $0 \leq a_j \leq b - 1$ for $j = 0, 1, 2, ..., k$ with $a_k \neq 0$. Furthermore, the integer n can be written as $n = (a_k a_{k-1} ... a_2 a_1)_b$. This representation is called the representation of n in $b-$base.

Example 3.3 Let 5 be an integer base. Hence, the number which should be appeared to represent a number are $\{0, 1, 2, 3, 4\}$. Now, suppose an integer $n = 2.434$ in $10-$base integer. Since in the daily life, we use the $10-$base, the index identifying $10-$base is not necessarily to be written explicitly. The integer $n = 2.434$ can be represented as $n = 3.5^4 + 4.5^3 + 2.5^2 + 1.5^1 + 4.5^0$. Hence, in $5-$base number, the integer $n = 2.434$ can be written as 34.214_5.

Example 3.4 The following examples explain the conversion process from binary base to $10-$base.

i. $110110_2 = 1.2^5 + 1.2^4 + 0.2^3 + 1.2^2 + 1.2^1 + 0.2^0 = 32 + 16 + 0 + 4 + 2 + 0 = 54$

ii. $100110_2 = 1.2^5 + 0.2^4 + 0.2^3 + 1.2^2 + 1.2^1 + 0.2^0 = 32 + 0 + 0 + 4 + 2 + 0 = 38$

Example 3.5 Conversely, the following example will describe the conversion from $10-$base integer to binary base using division algorithm. Now, consider the number 116. We will be representing the number 116 into binary base. The details of the processes are described as follow.

$$116 = 2.58 + 0$$

$$58 = 2.29 + 0$$

$$29 = 2.14 + 1$$

$$14 = 2.7 + 0$$

$$7 = 2.3 + 1$$

$$3 = 2.1 + 1$$

$$1 = 2.0 + 1$$

Write the number from the bottom, we therefore have 1110100_2. Hence, $116 = 1110100_2$.

The following table explains conversion between $10-$base, binary base, $4-$base, $8-$base, and $16-$base.

Table 3.1 Conversion Table

$10-$base	binary base	$4-$base	$8-$base	$16-$base
1	1	1	1	1
2	10	2	2	2
3	11	3	3	3
4	100	10	4	4
5	101	11	5	5
6	110	12	6	6
7	111	13	7	7
8	1000	20	10	8
9	1001	21	11	9
10	1010	22	12	A
11	1011	23	13	B
12	1100	30	14	C
13	1101	31	15	D
14	1110	32	16	E
15	1111	33	17	F
16	10000	100	20	10

Remember that $8 = 2^3$. Hence, in order to convert any $8-$base number into binary base, every digit in $8-$base number will represent 3 digits in binary base. For instance, $2_8 = 010_2, 1_8 = 001_2, 4_8 = 100_2$. Moreover, every digit in $16-$base number represents 4 digits in binary base since $16 = 2^4$.

Example 3.6 The following example shows a conversion process from binary base number into $8-$base number.

1. $1010110_2 = 001.010.110_2$ (grouped into 3 digits), we have $1010110_2 = 126_8$
2. $110010100010_2 = 110.010.100.010_2 = 6242_8$

Homework Chapter 3

1. Change the following $10-$base numbers into a requested base number.

   (a). $549 = ...{}_3$

   (b). $974 = ...{}_5$

   (c). $2002 = ...{}_8$

   (d). $2019 = ...{}_4$

2. Show that if b is a non negative integer which is less than -1, then every nonzero integer can be represented as following form

   $$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0$$

   where k is a non negative integer and a_j is an integer such that $0 \leq a_j \leq |b|, j = 0, 1, 2, ..., k$ and $a_k \neq 0$.

3. Change the base of the following numbers.

   (a). $7106_8 = ...{}_2 = ...{}_4 = ...{}_{16}$.

   (b). $20021_4 = ...{}_2 = ...{}_8$.

   (c). $A3FD_16 = ...{}_4 = ...{}_2$.

   (d). $31003_9 = ...{}_3$.

   (e). $2100012_3 = ...{}_9$.

4. Change the following $2-$base and $3-$base numbers into decimal ($10-$base)!

   (a) 101001_2

   (b) 12012_3

   (c) 2100112_3

5. Calculate the result of the following operations!

(a). $101111011_2 + 1100111011_2$.

(b). $111000111_2 - 100011101_2$.

(c). $100111_2 \times 1011_2$.

(d). $1000110001_2 : 1011_2$.

6. Change the following decimal numbers into $2-$base numbers!

   (a) -6

   (b) -17

   (c) 71

7. Calculate the result of the following operations!

   (a) $2001201_3 + 100211_3$.

   (b) $2120001_3 - 2001122_3$.

   (c) $12021_3 \times 2021_3$.

   (d) $101201212_3 : 122_3$.

8. Is the integer 447836_9 divisible by 3 and 8?

9. Without performing the divisions, determine whether the integers $176, 521, 221$, and $149, 235, 678$ are divisible by 9 or 11!

10. If the integer N is represented in the base b by

$$N = a_m b^m + ... + a_2 b^2 + a_1 b + a_0$$

where $0 \leq a_k \leq b-1$ then the following condition are equivalent:

(a). $b - 1|N$.

(b). $b - 1|(a_m + ... + a_2 + a_1 + a_0)$.

CHAPTERS 4
INTEGER FACTORIZATION

One of the important concepts of the Number Theory course is the integer factorization. In number theory, integer factorization is the decomposition process of a composite number into a product of smaller integers. If these factors are further restricted to prime numbers, the process is called the prime factorization. We would like to present the importance of integer factorization by using a brief explanation from wikipedia.org.

When the numbers are sufficiently large, no efficient, non-quantum integer factorization algorithm will be used for. In 2019, Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thom and Paul Zimmermann factored a 240-digit number (RSA-240) utilizing approximately 900 core-years of computing power. The researchers estimated that a 1024-bit RSA modulus would take about 500 times as long. However, it has not been proven that no efficient algorithm exists. The presumed difficulty of this problem is at the heart of widely used algorithms in cryptography such as RSA. Many areas of mathematics and computer science have been brought to bear on the problem, including elliptic curves, algebraic number theory, and quantum computing.

Not all numbers of a given length are equally hard to factor. The hardest instances of these problems (for currently known techniques) are semiprimes, the product of two prime numbers. When they are both large, for instance more than two thousand bits long, randomly chosen, and about the same size (but not too close, for example, to avoid efficient factorization by Fermat's factorization method), even the fastest prime factorization algorithms on the fastest computers can take enough time to make the search impractical; that is, as the number of digits of the

primes being factored increases, the number of operations required to perform the factorization on any computer increases drastically.

Many cryptographic protocols are based on the difficulty of factoring large composite integers or a related problemfor example, the RSA problem. An algorithm that efficiently factors an arbitrary integer would render RSA-based public-key cryptography insecure(wikipedia.org).

4.1 Prime Number

We start from the definition of a prime number.

Definition 4.1 *A natural number p is called a prime number (or a prime) if the natural number p is greater than 1 and it cannot be formed by multiplying two smaller natural numbers. A natural number greater than 1 that is not prime is called a composite number.*

Example 4.2 Example of prime and composite numbers are given below

1. $2, 3, 5$ are prime numbers.
2. 6 is composite number since 6 can be formed by multiplying $2 \times 3 = 6$

Definition 4.3 *Every pair of two positive integers a and b is said to be co-prime if the Greatest Common Divisor $gcd(a, b) = 1$.*

Theorem 4.4 *Every positive integer $n > 1$ has a prime factor.*

Proof.
First method:

Let n be any positive integer which is greater than 1. Then n has at least one positive factor, say n itself. Hence, n has the least positive factor, say q. Then q should be a prime number. Now, assume that q is not a prime number. Then q is a composite number. Therefore, q can be

represented as $q = q_1 q_2$, where $1 < q_1, q_2 < q$. This implies q_1, q_2 are factors of n. Contrary to the statement that q is the least factor of n

Second method:

Let n be a positive number which is greater than 1. If n is a prime number, then $n|n$ which completes the proof. In case, n is a composite number, then n has positive factor other than 1 and n itself, say d_1. Hence $d_1|n$ which implies that there exists a positive n_1 such that

$$n = d_1 n_1 \text{ where } 1 < n_1 < n.$$

If n_1 is a prime number, then $n_1|n$ which states that the theorem is true. Now, if n_1 is a composite number, the n_1 has positive factor other than 1 and n_1 itself, say d_2. Thus $d_2|n_1$. This implies that there exists a positive integer n_2 such that

$$n_1 = d_2 n_2 \text{ where } 1 < n_2 < n_1.$$

If n_2 is a prime number, then $n_2|n$ which states that the theorem is true. Now, if n_2 is a composite number, the n_2 has positive factor other than 1 and n_2 itself, say d_3. Thus $d_3|n_2$. This implies that there exists a positive integer n_3 such that

$$n_2 = d_3 n_3 \text{ where } 1 < n_3 < n_2.$$

If n_2 is a prime number, then $n_3|n$ which states that the theorem is true. Now, if n_3 is a composite number, the n_3 has positive factor other than 1 and n_3 itself and we can continue to decompose such that we have the following sequence

$$n, n_1, n_2, n_3, ... \text{ where } n > n_1 > n_2 > n_3 > ... > 1$$

The decomposition described in the previous process will terminate at a prime factor, say n_k. Then we have

$$n_k|n_{k-1}, n_{k-1}|n_{k-2}, ..., n_2|n_1, n_1|n \text{ such that } n_k|n.$$

which complete the proof. ■

Theorem 4.5 *Every positive number $n > 1$ can be represented as a multiplication of prime numbers.*

Proof. Let $n > 1$ be an integer. It follows from Theorem 4.4 that there exists a prime numbers, say p_1, such that there is an integer n_2 which satisfies

$$n = p_1 n_1 \text{ where } 1 \leq n_1 < n.$$

If $n_1 = 1$, then $n = p_1$. Thus n is a prime number. If $n_1 > 1$, then it follows from Theorem 4.4 that there exists a prime number p_2 such that $p_2 | n_1$. Hence, there exists a positive integer n_2 such that

$$n_1 = p_2 n_2 \text{ where } 1 \leq n_2 < n_1.$$

If $n_2 = 1$, then $n_1 = p_2$. Thus $n = p_1 p_2$ which completes the proof. If $n_2 > 1$, then it follows from Theorem 4.4 that there exists a prime number p_3 such that $p_3 | n_2$. Hence, there exists a positive integer n_3 such that

$$n_2 = p_3 n_3 \text{ where } 1 \leq n_3 < n_2.$$

If $n_3 = 1$, then $n_2 = p_3$. Thus $n = p_1 p_2 p_3$ which completes the proof. If $n_3 > 1$, then we can continue the process and it will terminate at $n_k = 1$ which implies $n = p_1 p_2 p_3 ... p_k$. This means that $n = p_1 p_2 p_3 ... p_k$ can be represented as a multiplication of prime numbers. ■

It follows from Theorem 4.5 that every integer can be represented as a multiplication of prime numbers. It is possible to say that these prime numbers can be the same prime number. As illustration, we give the following example.

Example 4.6

1. $50 = 2.5.5 = 2.5^2$
2. $150 = 2.3.5.5 = 2.3.5^2$
3. $5544 = 2.2.2.3.3.7.11 = 2^3.3^2.7.11$

Hence, we have the following corollary.

Corollary 4.7 *Let n be an integer. Then n can be represented as a product of prime powers.*

The existence of 4.7 motivates the existence of unique factorization which will be described in the next section. On the other hand, the prime representation of any integer also helps us for finding the greatest common divisor or the least common multiple of any integers easier. The illustration will be described in the following examples.

Example 4.8 Determine the greatest common divisor and the least common multiple of the integers 216,256, and 536. We will decompose 216,256, and 536 into product of prime powers. We therefore have,

$$\begin{aligned} 216 &= 2.2.2.3.3.3 = 2^3.3^3 \\ 256 &= 2.2.2.2.2.2.2.2 = 2^8 \\ 536 &= 2.2.2.67 = 2^3.67 \end{aligned}$$

Furthermore,

$$\begin{aligned} gcd(216, 256, 536) &= 2^{min\{3,8,3\}}.3^{min\{3,0,0\}}.67^{min\{0,0,1\}} \\ &= 2^3.3^0.67^0 \\ gcd(216, 256, 536) &= 8 \\ lcm(216, 256, 536) &= 2^{max\{3,8,3\}}.3^{max\{3,0,0\}}.67^{max\{0,0,1\}} \\ &= 2^8.3^3.67^1 \\ lcm(216, 256, 536) &= 463, 104 \end{aligned}$$

One of the important concept in number theory is the prime testing. Prime testing is used to indicate whether any integer is prime. We know that prime number is very important especially in cryptography. Suppose we have to indicate whether 5,357 is a prime number or composite number. The simplest method is dividing the number 5,357 by 2,3,5, and etc. But, this method is not efficient. Thus, we give the following properties as the early concept of prime testing.

Theorem 4.9 *If n is a composite number, then n has k factors such that $1 < k \leq \sqrt{n}$.*

Proof. Since n is a composite number, there exist positive integer k and m such that

$$km = n \text{ where } 1 < k < n \text{ and } 1 < m < n$$

If k and m are greater than $\sqrt{n}$, that is, $k, m > \sqrt{n}$, then

$$n = km > \sqrt{n}\sqrt{n} = n$$

which is impossible $n > n$. Hence, one of the number k or m should not be greater than $\sqrt{n}$, say k. This gives

$$1 < k \leq \sqrt{n}$$

So, we may deduce that n has k factors where $1 < k \leq \sqrt{n}$. ■

The next theorem, we present more specific in determining whether any integer is prime or composite.

Theorem 4.10 *If a positive integer n has no prime factor p such that $1 < p \leq \sqrt{n}$, than n is a prime number.*

Proof. We suggest to the reader to prove this theorem by using indirect proof. Assume that n is a composite number, then we have the opposite of the antecedent of the Theorem 4.10. ■

4.2 Unique Factorization

In the previous section, we have studied the property of an integer stating that every integer which is greater than 1 can be divided by a prime number. This condition motivates the concept of a unique factorization of integer. We start this section by the following theorem.

Theorem 4.11 *If p is a prime number and $p|ab$, then $p|a$ or $p|b$.*

Proof. Since p is prime, for any integer a satisfies $gcd(a,p) = 1$ or $(a,p) = p$. If $gcd(a,p) = 1$ and $p|ab$, then $p|b$. Furthermore, if $(a,p) = p$, then $p|a$. So, we may infer that $p|a$ or $p|b$. ■

The Theorem 4.11 can be generalized for integers $a_1, a_2, ..., a_n$. The generalization of Theorem 4.11 is given below.

Theorem 4.12 *Let p be a prime number. If $p|a_1a_2a_3...a_n$, then $p|a_i$ for every $i \in \{1,2,3,...,n\}$.*

Proof. We will prove Theorem 4.12 by using mathematical induction.

1. $S(1) : p|a_1 \Rightarrow p|a_1$. Thus $S(1)$ is true.
2. Assume that the statement holds for

$$S(k) : p|a_1a_2...a_k \Rightarrow p|a_i, i \in \{1,2,...,k\}$$

3. We want to prove that the statement also holds for $S(k+1)$. Suppose $p|a_1a_2a_3...a_ka_{k+1}$. We can represent the number

$$a_1a_2a_3...a_ka_{k+1} = (a_1a_2a_3...a_k)a_{k+1}.$$

This implies $p|(a_1a_2a_3...a_k)a_{k+1}$. It follows from Theorem 4.11 that $p|a_1a_2a_3...a_k$ and $p|a_{k+1}$. Moreover, since $p|a_1a_2a_3...a_k$ and it follows from the assumption of $S(k)$ that $p|a_i, i \in \{1,2,...,k\}$. So, we can infer that $p|a_i, i \in \{1,2,...,k,k+1\}$ which completes the proof.

■

The unique representation using factorization of positive integer will be explained in the following theorem.

Theorem 4.13 *Every positive integer which is greater than* 1 *can be uniquely represented as a multiplication of prime numbers.*

Proof. It follows Theorem 4.5 that every positive integer which is greater than 1 can be represented as multiplication of prime numbers. Now let n be a positive integer which is greater than 1 and suppose n has two representation, that are:

$$n = p_1p_2...p_t \text{ and } n = q_1q_2...q_r$$

where p_i, q_j are prime numbers for every $i \in \{1, 2, ..., t\}$ and $j \in \{1, 2, ..., r\}$ such that $p_1 \geq p_2 \geq ... \geq p_t, q_1 \geq q_2 \geq ... \geq q_r$ and $t \geq r$.

Since

$$n = p_1p_2...p_t, p_1|n \Rightarrow p_1|q_1q_2...q_r,$$

tt follows from Theorem 4.12 that $p_1 = q_k$ for some k such that $1 \leq k \leq r$ and since $q_1 \geq q_2 \geq ... \geq q_r, p_1 \leq q_1$.

On the other hand, since

$$n = q_1q_2...q_r, q_1|n \Rightarrow q_1|p_1p_2...p_t,$$

it follows from Theorem 4.12 that $q_1 = p_m$ for some m such that $1 \leq m \leq t$. Since $p_1 \geq p_2 \geq ... \geq p_t$ and $q_1 \leq p_1, p_1 = q_1$. Using the same process, we have

$$p_1 = q_1, p_2 = q_2, ..., p_t = q_r.$$

Hence, we can infer that n has a unique factorization. ■

In number theory, the existence of prime numbers play an important role. Some theorems in Cryptography claimed that the bigger prime number used in the cryptosystem, the more secure the cryptosystem. This condition motivated us to use a big prime number. This can be happened since the number of prime numbers is infinite. Euclid had answered this question a thousands years ago by his theorem posted in his work, the **Elements**.

Theorem 4.14 ***Euclid's Theorem.*** *The number of prime numbers is infinite.*

Proof. Suppose $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, ...$ are the order of prime numbers and let p_n be the greatest prime number. Now define an integer

$$N = p_1 p_2 p_3 ... p_n + 1$$

Thus N can not be divided by the prime numbers $p_1, p_2, p_3, ..., p_n$ which implies N is a prime number or divisible by another prime greater than p_n, contrary to p_n is the greatest prime number. ■

Theorem 4.15 *Let $\{p_n\}$ be a sequence of prime numbers ordered by ascending condition, where $n \in \{1, 2, 3, ...\}$ and $p_1 = 2$. Then*

$$p_n \leq 2^{2^{n-1}}$$

Proof. We will use mathematical induction to prove the Theorem 4.15

1. $S(1) : p_1 \leq 2^{2^0}$ holds since $p_1 = 2$.
2. Assume that the statement is true for $S(k) : p_k \leq 2^{2^{k-1}}$
3. We will prove that the statement is true for $S(k+1) : p_{k+1} \leq 2^{2^k}$. Furthermore, we have

$$\begin{aligned} p_{k+1} &\leq (p_1 p_2 ... p_k) + 1 \\ p_{k+1} &\leq (2(2^2)(2^{2^2})(2^{2^3})...(2^{2^{k+1}})) + 1 \\ p_{k+1} &\leq 2^{1+2+2^2+2^3+...+2^{k+1}} + 1 \end{aligned}$$

Since $1 + 2 + 2^2 + 2^3 + ... + 2^{k+1} = 2^k - 1$, we therefore have

$$p_{k+1} \leq 2^{2^{k+1}} + 1$$

Since $2^{2^{k+1}} + 1 > 1$ for every natural number k, we have

$$\begin{aligned} p_{k+1} &\leq 2^{2^2-1} + 2^{2^{k+1}} + 1 \\ p_{k+1} &\leq 2^{2^k} \end{aligned}$$

Hence, we may infer that

$$p_n \leq 2^{2^{n-1}}$$

for every ordinal number n. ■

It follows from Theorem 4.15 that the $n+1$ prime number, that is, $p_n \leq 2^{2^n}$. So, the number of prime numbers which are less that $p_n \leq 2^{2^n}$ is at least $n+1$ prime numbers. In other words, for $n \geq 1$, then there exist $n+1$ prime numbers which are less than 2^{2^n}.

Homework Chapter 4

1. Determine the greatest common divisor and the least common multiple of the integers $54, 24, 35$, and 25!

2. Determine the canonic form of the integer 6552 and 4563. Furthermore, determine their greatest common divisor and least common multiple!

3. Give a counter example to show that the following statement is not true.
   Every positive integer can be represented as the from $p+a^2$ where p is a prime number or 1 and $a \geq 0$.

4. Prove the following statements:

   a. Every prime number of the form $3n + 1$ can be represented as the form of $6m + 1$.

   b. A prime number of the form $n^3 - 1$ is only the prime number 7.

5. Determine the prime numbers which divide 51!

6. If p and q are prime numbers such that $p \geq q \geq 5$, then show that $24|(p^2 - q^2)$!

7. If p is a prime number greater than 3. Prove that $p^2 + 2$ is a composite number.

8. Prove that if n is a composite number greater than 4, then $n|(n - 1)$!

9. If p is a prime number which is not equal to 5, prove that $p^2 - 1$ or $p^2 + 1$ is divisible by 10!.

10. Prove that if $2^n - 1$ is a prime number, then so is n!

11. Determine the prime number p such that $17p+1$ is a square number.

12. If $n \geq 1$, show that there are infinite of prime numbers of the form $(4n+1)$ and $(4n+3)$.

13. For $n > 3$, show that between the integers $n, n+2, n_4$ at least one is not a prime number.

14. Show that there is no integer of the form n^3+1 which is a prime number, except 2.

15. Show that every term of the following sequence is a composite number.

$$(n+1)!-2, (n+1)!-3, ..., (n+1)!-(n+1).$$

CHAPTERS 5
CONGRUENCE

In number theory, modular arithmetic is a system of arithmetic for integers, where numbers ”wrap around” when reaching a certain value, called the **modulus**. The first modern approach to modular arithmetic was developed by Carl Friedrich Gauss in his book *Disquisitiones Arithmeticae* which had been published in 1801. We will give a simple illustration below.

A familiar use of modular arithmetic is in the 12-hour clock, in which the day is divided into two 12-hour periods. If the time is 7:00 now, then 9 hours later it will be 4:00. Simple addition would result in 7 + 9 = 16, but clocks ”wrap around” every 12 hours. Because the hour number starts over after it reaches 12, this is arithmetic modulo 12. In terms of the definition below, 16 is **congruent** to 4 modulo 12, so ”16:00” on a 24-hour clock is displayed ”4:00” on a 12-hour clock. Hence, it is very important to us to learn the congruence relation on integer. In this chapter, we will be studying about the concept and properties of congruences and their application.

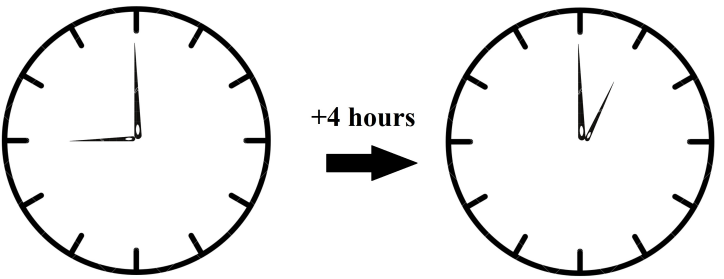

Figure 5.1 Modular Arithmetic on 12-Hour Clock

5.1 Concept and Basic Properties

Definition 5.1 *Let m be a positive integer. An integer a is said to be congruence to b modulo m if m divides $(a-b)$. The congruence relation between the integers a and b will be denoted by $a \equiv b \pmod{m}$.*

Consider the following examples.

1. $26 \equiv 2 \pmod{4}$ since $26 - 2 = 24$ is divisible by 4.
2. $12 \not\equiv 1 \pmod{3}$ since $12 - 1 = 11$ is not divisible by 3.

The following theorem is a necessary and sufficient condition for an integer to be congruent to another integer.

Theorem 5.2 *Let a, b, m are positive integers, $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = km + b$.*

Proof. Let a, b, m be positive integers. Suppose $a \equiv b \pmod{m}$. It follows from the definition of congruence that $a - b$ is divisible by m. This means $a - b = km$ for some integer k. Furthermore,

$$a - b = km \Rightarrow a = km + b.$$

Conversely, suppose there exists integer k such that $a = km + b$. This gives $a - b = km$ which means $a - b$ is divisible by m. In other words,

$$a \equiv b \pmod{m}.$$

■

Let a and m be integers such that $m > 0$. It follows from division algorithm that a can be represented as

$$a = qm + r \text{ where } 0 \leq r < m.$$

Since $0 \leq r < m$, there exist m number of integers to be congruence to r. These integers are the set

$$\{0, 1, 2, ..., m-2, m-1\}.$$

This condition is fixed by the following theorem.

Theorem 5.3 *Let m be a positive integer. Every integer is exactly congruence modulo m to one of the member $\{0, 1, 2, ..., m-1\}$.*

Definition 5.4 *If $a \equiv r \pmod{m}$ where $0 \leq r < m$, then r is called the smallest remainder of a modulo m. The set $\{0, 1, 2, ..., m-1\}$ is called the set of all smallest remainders modulo m.*

Example 5.5

1. The set of all remainders modulo 6 is $\{0, 1, 2, 3, 4, 5\}$.
2. The set of all remainders modulo 11 is $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.
3. The set of all remainders modulo 25 is $\{0, 1, 2, 3, 4, 5, ..., 23, 24\}$.

Another necessary and sufficient condition for integers to be congruence to each other is given below.

Theorem 5.6 *$a \equiv b \pmod{m}$ if and only if a and b have the same remainder if both of them are divided by m.*

Proof. Suppose $a \equiv b \pmod{m}$. Then a and b have the same remainder if a and b are divided by m. Let r be the remainder. Then $a \equiv r \pmod{m}$ and $b \equiv r \pmod{m}$ where $0 \leq r < m$. Furthermore,

$$\begin{aligned} a \equiv r \pmod{m} &\Rightarrow a = qm + r \text{ for some integer } q \\ b \equiv r \pmod{m} &\Rightarrow b = tm + r \text{ for some integer } t \end{aligned}$$

which implies a and b have the same remainder if a and b are divided by m.

Conversely, suppose a and b have the same remainder if a and b are divided by m. We therefore have

$$a = qm + r \text{ for some integer } q$$

$$b = tm + r \text{ for some integer } t.$$

Moreover, $a - b = qm - tm = (q - t)m \Rightarrow m|a - b$. In other words, $a \equiv b \pmod{m}$. ■

Definition 5.7 *The set $\{r_1, r_2, ..., r_m\}$ is called a system of the complete remainders modulo m if every r_i is congruence modulo m to a single element of $\{0, 1, 2, ..., m-1\}$, where $i \in \{1, 2, ..., m\}$.*

Theorem 5.8 *If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv b+d \pmod{m}$*

Proof. Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then $a = qm+b$ for some integer q and $c = tm + d$ for some integer t. Hence,

$$\begin{aligned} a + c &= qm + b + tm + d \\ &= (q + t)m + (b + d) \\ (a + c) - (b + d) &= (q + t)m. \end{aligned}$$

This implies $m|(a+c)-(b+d)$. In other words, $a+c \equiv b+d \pmod{m}$ ■

Theorem 5.9 *If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ax + cy \equiv bx + dy \pmod{m}$ for every integers x and y.*

Proof. Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then we have

$$a = ms + b \text{ for some integer } s \quad (1)$$
$$c = mt + d \text{ for some integer } t \quad (2).$$

Multiplying equation (1) (respectively, (2)) by x (respectively, y), then

we have

$$\begin{aligned} ax + cy &= (msx + bx) + (mty + dy) \\ ax + cy &= m(sx + ty) + (bx + dy) \\ (ax + cy) - (bx + dy) &= m(sx + ty) \end{aligned}$$

This yields

$$m|(ax + cy) - (bx + dy) \Longrightarrow ax + cy \equiv bx + dy \pmod{m}$$

■

The next theorem, we give another properties of congruences

Theorem 5.10 *If* $ac \equiv bc \pmod{m}$ *such that* $gcd(c, m) = 1$, *then* $a \equiv b \pmod{m}$.

Proof. Suppose $ac \equiv bc \pmod{m}$ then $m|ac - bc$. Hence

$$m|c(a - b)$$

It follows from $gcd(c, m) = 1$ that $m|a - b$ which gives

$$a \equiv b \pmod{m}.$$

■

In general, we have the following property

Theorem 5.11 *If* $ac \equiv bc \pmod{m}$ *such that* $gcd(c, m) = d$, *then* $a \equiv b \pmod{\frac{m}{d}}$

Proof. Suppose $ac \equiv bc \pmod{m}$ and $gcd(c, m) = d$. Then

$$ac \equiv bc \pmod{m} \Rightarrow m|ac - bc \Rightarrow m|c(a - b).$$

Since $gcd(c, m) = d$,

$$d|m, d|c \text{ and } gcd(\frac{c}{d}, \frac{m}{d}) = 1.$$

Furthermore

$$\frac{m}{d} \text{ and } \frac{c}{d} \text{ are integers}$$

because c and m are divisible by d. Since $m|c(a-b)$,

$$\frac{m}{d}|\frac{c}{d}(a-b).$$

This gives $\frac{m}{d}|(a-b)$ which implies

$$a \equiv b \pmod{\frac{m}{d}}$$

■

5.2 Application of Congruences

The divisibility tests for integers can be developed by congruences. In the following discussion let $n = \overline{a_k a_{k-1} \dots a_1 a_0}$ denotes

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

where $0 \le a_j \le 9$ for $j = 0, 1, 2, \dots, k$.

We begin with tests for divisibility by powers of 2. Note that

$$\begin{aligned}
&n \equiv \overline{a_0} \pmod 2,\\
&n \equiv \overline{a_1 a_0} \pmod{2^2},\\
&n \equiv \overline{a_2 a_1 a_0} \pmod{2^3},\\
&\ \ \vdots\\
&n \equiv \overline{a_{l-1} \dots a_1 a_0} \pmod{2^l}.
\end{aligned}$$

We have the following theorem.

Theorem 5.12 *$n = \overline{a_k a_{k-1} \dots a_1 a_0}$ is divisible by 2^l if and only if 2^l divides $\overline{a_{l-1} \dots a_1 a_0}$.*

Example 5.13 Let $n = 4188048$. We see that

$$\begin{aligned}
&2 \mid n \text{ since } 2 \mid 8,\\
&4 \mid n \text{ since } 4 \mid 48,\\
&8 \mid n \text{ since } 8 \mid 48,\\
&16 \mid n \text{ since } 16 \mid 8048,\\
&\text{but } 32 \nmid n \text{ because } 32 \nmid 88048.
\end{aligned}$$

Next, the divisibility tests for powers of 5 are analogous to those for powers of 2. We have the following theorem.

Theorem 5.14 $n = \overline{a_k a_{k-1} \ldots a_1 a_0}$ *is divisible by* 5^l *if and only if* 5^l *divides* $\overline{a_{l-1} \ldots a_1 a_0}$.

Example 5.15 Let $n = 175375$. We see that

$$\begin{aligned}
&5 \mid n \text{ since } 5 \mid 5,\\
&25 \mid n \text{ since } 25 \mid 75,\\
&125 \mid n \text{ since } 125 \mid 375,\\
&\text{but } 625 \nmid n \text{ because } 625 \nmid 5375.
\end{aligned}$$

Theorem 5.16 $10^n \equiv 1 \pmod 9$ *for* $n = 0, 1, 2, 3, \ldots$.

Proof. We will prove the theorem using mathematical induction.

1. $S(0) : 10^0 \equiv 1 \pmod 9$. Thus $S(0)$ is true.
2. Assume that the statement is true for $S(k) : 10^n \equiv 1 \pmod 9$
3. We will prove that the statement is true for $S(k+1) : 10^{n+1} \equiv 1 \pmod 9$. Since $10^{n+1} = 10.10^n$,

$$\begin{aligned}
10.10^n &\equiv 10^n \pmod 9\\
10^n &\equiv 1 \pmod 9
\end{aligned}$$

which implies

$$10^{n+1} = 10.10^n \equiv 1 \pmod 9.$$

■

Theorem 5.17 *Every integer modulo 9 is congruence to the sum of their digit.*

Proof. Let n be any integer. Then n can be represented as

$$n = \overline{d_k d_{k-1} ... d_2 d_1 d_0}$$

where $0 \leq d_i < 9, i \in \{0, 1, 2, ..., k\}$ and $d_i, i \in \{0, 1, 2, ..., k\}$ are the digit which appear. In another representation, we have

$$n = d_k.10^k + d_{k-1}.10^{k-1} + ... + d_2.10^2 + d_1.10 + d_0.10^0.$$

It follows from Theorem 5.16 that $10^n \equiv 1 \pmod 9$. Hence

$$\begin{aligned} n \equiv & d_k(1) + d_{k-1}(1) + ... + d_2(1) + d_1(1) + d_0(1) \pmod 9 \\ n \equiv & d_k + d_{k-1} + ... + d_2 + d_1 + d_0 \pmod 9 \end{aligned}$$

Thus, the integer n is congruence to the sum of its digits which completes the proof. ■

We will give some examples below which describe the implementation of the concept of congruence to solve number theory problems.

Example 5.18 Determine the remainder of the integer 35.952 if it is divided by 9.
It follows from Theorem 5.17 that

$$\begin{aligned} 35.952 &\equiv 3 + 5 + 9 + 5 + 2 \pmod 9 \\ &\equiv 24 \pmod 9 \\ 35.952 &\equiv 6 \pmod 9 \end{aligned}$$

Hence, the remainder is 6.

Example 5.19 Determine whether the integer 7.587 is divisible by 9 or not!
It follows from Theorem 5.17 that

$$\begin{aligned} 7.587 &\equiv 7+5+8+7 \pmod 9 \\ &\equiv 27 \pmod 9 \\ 7.587 &\equiv 0 \pmod 9 \end{aligned}$$

Hence, the remainder is 0. In other words, 7.587 is divisible by 9.

Example 5.20 Determine whether the integer 48.866 is divisible by 9 or not!
It follows from Theorem 5.17 that

$$\begin{aligned} 48.866 &\equiv 4+8+8+6+6 \pmod 9 \\ &\equiv 32 \pmod 9 \\ 48.866 &\equiv 5 \pmod 9 \end{aligned}$$

Hence, the remainder is 5. In other words, 48.866 is not divisible by 9.

Remark 5.21 *The following properties are important.*

1. *An integer is divisible by 2 if and only if its latest digit is divisible by 2.*
2. *An integer is divisible by 3 if and only if the sum of its digits is divisible by 3.*
3. *An integer is divisible by 4 if and only if its two latest digits are divisible by 4.*
4. *An integer is divisible by 6 if and only if it is divisible by 2 and 3.*
5. *An integer is divisible by 8 if and only if its three latest digits are divisible by 8.*

Lemma 5.22 *Let n be a natural number. Then* $10^n \equiv (-1)^n \pmod{11}$

Proof. We will prove the Lemma using mathematical induction.

1. $S(0) : 10^0 \equiv (-1)^0 \pmod{11}$. The statement $S(0)$ is true.
2. Assume the statement $S(k) : 10^k \equiv (-10)^k$ is true.
3. We will prove that the statement $S(k+1) : 10^{k+1} \equiv (-10)^{k+1}$ is true. Now assume that k is even. Then $10^k \equiv 1 \pmod{11}$. This implies

$$\begin{aligned} 10^{k+1} &\equiv 10^k.10 \pmod{11} \\ &\equiv (1)(-1) \pmod{11} \\ 10^{k+1} &\equiv -1 \pmod{11} \end{aligned}$$

   If k is even integer, then $k+1$ is an odd integer which implies $(-1)^{k+1} = -1$. Hence, $S(k+1) : 10^{k+1} \equiv (-1)^{k+1} \pmod{11}$ is true. Analogously, the same way we can prove if n is an odd integer.

Hence, $10^n \equiv (-1)^n \pmod{11}$ for every natural number n. ■

Theorem 5.23 *Let $n = \overline{a_k a_{k-1} ... a_2 a_1 a_0}$ be an integer. The integer n is divisible by 11 if and only if*

$$(a_0 + a_2 + a_4 + ...) - (a_1 + a_3 + a_5 + ...)$$

is divisible by 11.

Proof. It follows from Lemma 5.22 that $10^n \equiv (-1)^n \pmod{11}$. Let $n = \overline{a_k a_{k-1} ... a_2 a_1 a_0}$ be an integer where $0 \leq a_i \leq 9, i \in \{0, 1, ..., k\}, a_k \neq 0$. We therefore have

$$\begin{aligned} n &\equiv a_k 10^k + a_{k-1} 10^{k-1} + ... + a_2 10^2 + a_1 10 + a_0 10^0 \pmod{11} \\ &\equiv a_k (-1)^k + a_{k-1} (-1)^{k-1} + ... + a_2 (-1)^2 \\ &\quad + a_1 (-1) + a_0 (-1)^0 \pmod{11} \\ &\equiv a_k (-1)^k + a_{k-1} (-1)^{k-1} + ... + a_2 - a_1 + a_0 \pmod{11} \\ n &\equiv ((a_0 + a_2 + a_4 + ...) - (a_1 + a_3 + a_5 + ...)) \equiv \pmod{11} \end{aligned}$$

This means that the integer n is divisible by 11 if and only if

$$(a_0 + a_2 + a_4 + ...) - (a_1 + a_3 + a_5 + ...)$$

is divisible by 11. ■

Example 5.24 The integer 180.851 is divisible by 11 since $(1+8+8)-(5+0+1) = 17 - 6 = 11$ is divisible by 11.

Homework Chapter 5

1. Let a, b, c, d, m be integers. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Prove that:

   a. $ac \equiv bd \pmod{m}$

   b. $a^n \equiv b^n \pmod{m}$ for every positive integer n

2. Let a, b, m be integers and let c be a positive integer. Prove that the following conditions are equivalent:

   a. $a \equiv b \pmod{m}$

   b. $ac \equiv bc \pmod{mc}$

3. If $a \equiv b \pmod{m}$ such that $d|m$ and $d|a$, then prove that $d|b$.

4. If $a \equiv b \pmod{m}$, then prove that $gcd(a, m) = gcd(b, m)$.

5. If $a \equiv b \pmod{m}$ such that $0 \leq |b - a| < m$, then prove that $a = b$.

6. If $a \equiv b \pmod{m}$ and If $a \equiv b \pmod{n}$ such that $gcd(m, n) = 1$, then prove that If $a \equiv b \pmod{mn}$

7. If $a \equiv b \pmod{m}$ such that $n|m$, then prove that $a \equiv b \pmod{n}$.

8. Clarify the truth of the mathematics statement: if $a^2 \equiv b^2 \pmod{m}$, then $a \equiv b \pmod{m}$!

9. Determine the remainder of the integers 2^{57} and 41^{85} if they are divided by 7.

10. Determine the remainder of the integer $(1^5 + 2^5 + ... + 100^5)$ if it is divided by 4.

11. Identify whether the integers below are divisible by 9 or not.

    a. 178.531.221

b. 159.215.573

12. Identify whether the integers below whether the integers are divisible by 11 or not.

    a. 178.531.221

    b. 159.215.573

13. Let n be an integer such that the integer n can be represented as the $b-$ base form as follows

$$n = a_m b^m + a_{m-1} b^{m-1} + ... + a_1 b + a_0$$

    where $0 \leq a_i \leq b-1, i \in \{0, 1, 2, ..., m\}$. Show that the following conditions are equivalent.

    a. $(b-1)|n$

    b. $(b-1)|\sum_{i=0}^{m} a_i$

14. The following integers are disivible by 9 and 11. Determine the integer p.

    (a) $52.817 \times 3.212.146 = 169.655.p15.282$

    (b) $2.p99.561 = (3(523+p))^2$

15. Show that the following conditions are valid.

    (a) If n is an even integer, then $10^{3n} \equiv 1 \pmod{1001}$

    (b) If n is an odd integer, then $10^{3n} \equiv -1 \pmod{1001}$

CHAPTERS 6
DIOPHANTINE EQUATION

Mathematics historians have approximated the birth of Diophantus to be at about 200 AD in Alexandria, Egypt and his death at 284 AD in Alexandria as well. Diophantus is best known for his work, Arithmetica, which contains 13 books "consisting of 130 problems giving numerical solutions to determinate equations (those with a unique solution) and indeterminate equations" (Diophantus). The method he formulated for solving later became known as Diophantine analysis. From his book, Arithmetica , only 6 of the 13 books have survived. Scholars who studied his works concluded that "Diophantus was always satisfied with a rational number and did not require a whole number" (Diophantus). He did not deal with negative solutions and only required one solution to a quadratic equation, which was what most of the Arithmetica problems led to (Diophantus). Brahmagupta was the first to give the general solution of the linear Diophantine equation $ax + by = c$. He also gained fame from another book called On Polygonal Numbers. Diophantus' methods of solving problems have had both lasting effects and great benefits for the studies of algebra and number theory. In mathematics, a Diophantine equation is a polynomial equation, usually in two or more unknowns, such that only the integer solutions are sought or studied (an integer solution is such that all the unknowns take integer values). A linear Diophantine equation equates the sum of two or more monomials, each of degree 1 in one of the variables, to a constant. We start this chapter with the linear congruence.

6.1 Linear Congruence

Definition 6.1 *A congruence is said to be linear congruence if the congruence contains a variable x with degree one.*

Example 6.2 Let $a, b,$ and m be integers. The congruence $ax \equiv b \pmod{m}$ is a linear congruence, where x is a variable.

Theorem 6.3 *If $gcd(a, m) \nmid b$, then the linear congruence $ax \equiv b \pmod{m}$ has no solution.*

Proof. Assume the congruence $ax \equiv b \pmod{m}$ has a solution. Hence, $gcd(a, m)|b$. Let r be the solutions of $ax \equiv b \pmod{m}$. Then, we therefore have $ar \equiv b \pmod{m}$. This means $ar - b = km$ for an integer k. Since $gcd(a, m)|a$ and $(a, m)|km$, $(a, m)|b$. Contrary to $gcd(a, m) \nmid b$. So we can infer that the linear congruence $ax \equiv b \pmod{m}$ has no solution. ■

Example 6.4 The linear congruence $6x \equiv 5 \pmod{8}$ has no solution since $gcd(6, 8) = 2$ and $2 \nmid 5$.

Theorem 6.5 *If $gcd(a, m) = 1$ and $d|b$, then the congruence $ax \equiv b \pmod{m}$ has exactly 1 solution.*

Proof. Since $gcd(a, m) = 1$, there exist integers r and s such that $ar + ms = 1$. If the both side of the equation $ar + ms = 1$ is multiplied by b, then we therefore have

$$\begin{aligned} (ar)b + (ms)b &= b \\ a(rb) + m(sb) &= b \\ a(rb) - b &= -(sb)m \end{aligned}$$

This gives $a(rb) - b$ is divisible by m. Thus $a(rb) \equiv b \pmod{m}$. Hence, the solution of the congruence $ax \equiv b \pmod{m}$ is the smallest remainder rb modulo m. Now, we will show that the solution is unique. Sup-

pose the congruence $ax \equiv b \pmod{m}$ has two solutions, that are, r and s. Then

$$ar \equiv b \pmod{m}$$

$$as \equiv b \pmod{m} \Longrightarrow b \equiv as \pmod{m}.$$

Then, we therefore have

$$ar \equiv as \pmod{m}.$$

Since $gcd(a, m) = 1, r \equiv s \pmod{m}$. This gives $m|r - s$. In other word, since the integer r and s are the solution of the congruence $ax \equiv b \pmod{m}, 0 \leq r < m$ and $0 \leq s < m$. This implies

$$-m < r - s < m.$$

Since $m|r - s, r - s = 0$ or $r = s$. This means that the solution is unique. ■

Example 6.6 Determine the solution of the congruence $2x \equiv 1 \pmod{17}$. It follows from the congruence $18 \equiv 1 \pmod{17}$, we therefore have

$$2x \equiv 1 \pmod{17}$$
$$2x \equiv 18 \pmod{17}$$

Since $gcd(2, 17) = 1$, we have

$$x \equiv 9 \pmod{17}$$

Hence the solution of the linear congruence $2x \equiv 1 \pmod{17}$ is 9.

Theorem 6.7 *If $gcd(a, m) = d$ and $d|b$, then the congruence $ax \equiv b \pmod{m}$ has exactly d solution.*

Proof. Suppose $ax \equiv b \pmod{m}$ be a linear congruence such that $gcd(a, m) = d$ and $d|b$. We will show that the congruence $ax \equiv b$

$(\text{mod } m)$ has exactly d solution. Since $gcd(a, m) = d$, there exists a' and m' such that $a = da'$ and $m = dm'$. furthermore, since $d|b, b = db'$ for an integer b'. We therefore have,

$$da'x \equiv db' \pmod{dm'}$$

or

$$a'x \equiv b' \pmod{m}.$$

On the other hand, it follows from $gcd(a, m) = d$ that $gcd(da', dm') = d$ which implies $gcd(a', m') = 1$. It follows from Theorem 6.5 that $a'x \equiv b' \pmod{m'}$ has exactly one solution, say r. This implies that there exist d integers, that are,

$$r, r + m', r + 2m', ..., r + (d - 1)m'$$

which satisfy the congruence $ax \equiv b \pmod{m}$. We will clarify this property into three steps as follow. Every member of the set $\{r, r + m', r+2m', ..., r+(d-1)m'\}$ satisfies the congruence $ax \equiv b \pmod{m}$. Let n be any member of the set $\{r, r + m', r + 2m', ..., r + (d - 1)m'\}$. Then n can be represented as $n = r+km'$ where $k \in \{0, 1, 2, ..., d-1\}$.

1. We therefore have.

$$ax = a(r + km') = da'(r + km') = da'r + da'km'$$

Since $a'r \equiv b' \pmod{m'}$ and $m'd = m$, then

$$\begin{aligned} ax \equiv & a'rd + a'km'd \pmod{m} \\ \equiv & b'd + a'km'd \pmod{m} \\ \equiv & b'd \pmod{m} \\ ax \equiv & b \pmod{m} \ since \ b = b'd \end{aligned}$$

Hence $n = r + km'$ satisfies the congruence $ax \equiv b \pmod{m}$.

2. Since r is the solution of the congruence $a'x \equiv b' \pmod{m'}, r \geq 0$ which implies $0 \leq r + km'$. Furthermore,

$$r + km' \leq r + (d-1)m' \text{ for every } k \in \{0, 1, 2, ...\}.$$
$$r + (d-1)m' < m' + (d-1)m' = dm' = m$$

Hence, $0 \leq r + km' < m$.

3. There are no two members of the set $\{r, r+m', r+2m', ..., r+(d-1)m'\}$ which are congruence to m since the set $\{r, r+m', r+2m', ..., r+(d-1)m'\}$ is the remainders of modulo m and they are different.

These imply that the congruence $ax \equiv b \pmod{m}$ has d solution. Now let s is the other solution of the congruence $ax \equiv b \pmod{m}$. Then $as \equiv b \pmod{m}$ and $ar \equiv b \pmod{m}$. Since $gcd(a, m) = d$ and $as \equiv ar \pmod{m}$. Moreover,

$$s \equiv r \pmod{\frac{m}{d}}$$
$$s \equiv r \pmod{m'} \text{ since } m = dm'.$$

This means $s - r = tm'$ or $s = r + tm'$ for some integer t. Since s is the smallest remainder of modulo m, s should be a member of the set $\{r, r+m', r+2m', ..., r+(d-1)m'\}$. This completes the proof. ■

Example 6.8 We will find the solutions of the congruence $6x \equiv 18 \pmod{33}$. Since $gcd(6, 33) = 3$, the congruence has 3 solutions. Furthermore,

$$6x \equiv 18 \pmod{33}$$
$$2x \equiv 6 \pmod{11}$$
$$x \equiv 3 \pmod{11}$$

Hence the solutions of the congruence $6x \equiv 18 \pmod{33}$ are $3, 14$ and 25.

6.2 Linear Diophantine Equation

Definition 6.9 *Let n be a positive integer and $a_1, a_2, \ldots, a_n, b$ are integers where $a_i \neq 0, i = 1, 2, \ldots, n$. The equation*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{6.1}$$

is called a Diophantine linear equation where we require the solutions for x_i to be integers.

Example 6.10 The Diophantine equation $7x_1 + 5x_2 = 1$ has solution $x_1 = -2$ and $x_2 = 3$, but $x_1 = \frac{1}{2}$ and $x_2 = -\frac{1}{2}$ is not a solution.

Example 6.11 The Diophantine equation $3x_1 - 6x_2 = 0$ can be simplified to $x_1 = 2x_2$ (without altering the set of solutions). If we let x_2 be any integer k and $x_1 = 2k$, this forms an infinite set of solutions for this equation. It fact, every possible solution is of this form. We can write the set of solution as

$$S = \{(2k, k) : k \in \mathbb{Z}\}.$$

The main result concerning linear Diophantine equations is the following theorem.

Theorem 6.12 *The equation (6.1) is solvable if and only if*

$$\gcd(a_1, \ldots, a_n) \mid b.$$

In case of solvability, all integer solutions to (6.1) can be expressed in terms of $n - 1$ integral parameters.

Proof. Let $d = \gcd(a_1, \ldots, a_n)$. Note that if b is not divisible by d then for every integers $x_1, \ldots, x_n$, the left-hand side of (6.1) is divisible by d and the right-hand side is not. This implies (6.1) is not solvable.

If $d|b$, then we obtain the equivalent equation

$$a_1'x_1 + \cdots + a_n'x_n = b',$$

where $a_i' = a_i/d$ for $i = 1, \ldots, n$ and $b' = b/d$. Clearly, we have $\gcd(a_1', \ldots, a_n') = 1$. The rest of the proof can be completed using induction on the number n of the variable.

In the case $n = 1$, the equation has the form $x_1 = b$ or $-x_1 = b$, and thus the unique solution does not depend on any parameter. We now assume that $n \geq 2$ and that the solvability property holds for all linear equations in $n - 1$ variables. The goal is to show that the equations in n variables have a solution. Set $d_{n-1} = \gcd(a_1, \ldots, a_{n-1})$. Then any solution $(x_1, \ldots, x_n)$ satisfies the congruence

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{dn - 1},$$

which is equivalent to

$$a_nx_n \equiv b \pmod{d_n - 1}. \tag{6.2}$$

Multiplying both sides of (6.2) by $a_n^{\phi(d_{n-1})-1}$ and taking into account that $a_n^{\phi(d_{n-1})} \equiv 1 \pmod{d_{n-1}}$, we obtain

$$x_n \equiv c \pmod{d_{n-1}},$$

where $c = a_n^{\phi(d_{n-1}-1)b}$. It follows that $x_n = c + d_{n-1}t_{n-1}$ for some integer t_{n-1}. Substituting in (6.1) and rearranging yields the equation in $(n - 1)$ variables

$$a_1x_1 + \cdots + a_{n-1}x_{n-1} = b - a_nc - a_{n-1}d_{n-1}t_{n-1}.$$

It remains to show that $d_{n-1} \mid (b - a_nc - a_{n-1}d_{n-1}t_{n-1})$, which is equivalent to $a_nc \equiv b \pmod{d_n - 1}$. The last relation is true because of the choice of c. Therefore we can divide the last equation by d_{n-1}, and obtain

$$a_1'x_1 + \cdots + a_{n-1}'x_{n-1} = b', \tag{6.3}$$

where $a_i' = a_i/d_{n-1}$ for $i = 1, \ldots, n - 1$ and $b' = (b - a_nc)/d_{n-1} - a_nt_n - 1$. Because $\gcd(a_1', \ldots, a_{n-1}') = 1$, by the induction hypothesis

the Equation (6.3) is solvable for each integer t_{n-1} and its solutions can be written in terms of $n-2$ integral parameters. If we add to these solutions $x_n = c + d_{n-1}t_{n-1}$, we obtain solutions to (6.1) in terms of $n-1$ parameters. ■

Corollary 6.13 *Let a_1, a_2 be relatively prime integers. If $(\hat{x_1}, \hat{x_2})$ is a solution to the equation*

$$a_1x_1 + a_2x_2 = b$$

then all of its solutions are given by

$$x_1 = \hat{x_1} + a_2t,$$

$$x_2 = \hat{x_2} + a_1t,$$

for every integer t.

Theorem 6.14 *The Diophantus linear equation $a'x + b'y = c'$ which is derived from the equation $ax + by = c$ where $a' = a : gcd(a, b), b' = b : gcd(a, b)$ and $c' = c : gcd(a, b)$ has a solution $x = r$ and $y = s$. Then, the set of all solutions of $ax + by = c$ is $\{gcd(x, y)|x = r + b't, y = s + a't, t$ is an integer $\}$.*

Proof. Prove this theorem as exercise. ■

6.3 System of Linear Congruences

A collection of some linear congruences which forms a system is called system of linear congruences.

Based on the mathematics history, congruences were first used to calculate calendars in ancient China in the beginning of the 2^{nd} century B.C. Many historian believed that the astronomers had defined *shangyuan* as the starting point of the calendar. If the Winter Solstice

of a certain year occurred d_l days after *shangyuan* and d_2 days after the new moon, then that year was N years after *shangyuan*; hence motivated the system of congruences.

$$dN \equiv d_1 \pmod{60}$$
$$dN \equiv d_2 \pmod{m}$$

where d is the number of days in a tropical year and m is the number of days in a lunar month. On the other hand, a master Sun's Mathematical manual from China, *Sun Zi Suanjing*, raised a problem which means there are certain things whose number is unknown. A number is repeatedly divided by 3, the remainder is 2; divided by 5, the remainder is 3; and by 7, the remainder is 2. Furthermore, the question asked what will the number be?. It follows from the problem that we have the system of linear congruences as follows.

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

Sun Zi had solved the problem by giving the solution as follows

$$x \equiv 140 + 63 + 30 \equiv 233 \equiv 23 \pmod{105}.$$

We begin to explain the properties of a system of linear congruences by the following theorem.

Theorem 6.15 *A system of linear congruences* $x \equiv a_i \pmod{m}, i = 1, 2, 3, ..., k$ *where* $(m_i, m_j) = 1$ *for every* $i \neq j$ *has a solution modulo* m *such that* $m = m_1 m_2 ... m_k$ *and the solution is unique.*

Proof. We will prove the theorem by using mathematical induction.

1. It is clear that the statement $S(1) : x \equiv a_1 \pmod{m_1}$ is true since the congruence $x \equiv a_1 \pmod{m_1}$ has a solution.

2. Consider the system of linear congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2},$$

where $gcd(m_1, m_2) = 1$. We will show that the system of linear congruences has a solution. Since $x \equiv a_1 \pmod{m_1}, x = a_1 + k_1 m_1$ for some integer k_1. We therefore have,

$$a_1 + k_1 m_1 \equiv a_2 \pmod{m_2}$$
$$k_1 m_1 \equiv a_2 - a_1 \pmod{m_2}$$

Since $gcd(m_1, m_2) = 1$, the latest congruence, $k_1 m_1 \equiv a_2 - a_1 \pmod{m_2}$, has a solution, say t,. Then $k_1 = t + k_2 m_2$ for some integer k_2 which satisfies the latest congruence. Hence,

$$x = a_1 + k_1 m_1 = a_1 + (t + k_2 m_2) m_1$$
$$x = (a_1 + t m_1) + k_2 m_2 m_1.$$
$$\text{This means } x \equiv (a_1 + t m_1) \pmod{m_1 m_2}$$

which implies that the system of linear congruence has a solution. Now assume that $S(r-1) : x \equiv a_i \pmod{m_i}$ has a solution, where $i \in \{1, 2, 3, ..., r-1\}$, say the solution is s. Then

$$x \equiv s \pmod{m_1 m_2 m_3 ... m_{r-1}}.$$

3. We will show that $S(r) : x \equiv a_i \pmod{m_i}$ has a solution, where $i \in \{1, 2, 3, ..., r-1, r\}$. Since

$$x \equiv s \pmod{m_1 m_2 m_3 ... m_{r-1}},$$

the system of the linear congruences containing r linear congruences can be represented as follows.

$$x \equiv s \pmod{m_1 m_2 m_3 ... m_{r-1}}$$
$$x a_1 \pmod{m_r}$$

This system of linear congruences has the same solution since $gcd(m_1 m_2 m_3 ... m_{r-1}) = 1$ since m_i and m_j are relatively prime for every $i \neq j$, and $i, j \in \{1, 2, 3, ..., r-1\}$.

Moreover, we will show that the solution is unique. Suppose that the system of linear congruences $x \equiv a_i \pmod{m}, i = 1, 2, 3, ..., k$ where $(m_i, m_j) = 1$ for every $i \neq j$ has two solutions modulo m, say r and s. We therefore have.

$$\begin{aligned} r &\equiv a_i \pmod{m_i} \\ s &\equiv a_i \pmod{m_i} \end{aligned}$$

Hence,

$$r - s \equiv 0 \pmod{m_i}$$

It means that $m_i|(r - s)$ for every $i \in \{1, 2, 3, ..., k\}$. In other words, $r - s$ is a common multiple of $m_i, m_2, ..., m_k$. Since $gcd(m_i, m_j) = 1$ for every $i \neq j, (m_1 m_2 ... m_k)|(r - s)$. Remember that r and s are the solution of the system of linear congruences, the integers r and s are the smallest remainder modulo $(m_1 m_2 ... m_k)$ such that

$$-(m_1 m_2 ... m_k) < r - s < (m_1 m_2 ... m_k).$$

Since r and s is common multiples of $m_1, m_2, ...m_k$ and for every $i \neq j, gcd(m_i, m_j) = 1$. Hence, we can infer that

$$r - s = 0 \text{ or } r = s.$$

In other words, the system of linear congruences has a unique solution. ■

Example 6.16 We will find the solution of the following system of linear congruence.

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 1 \pmod{3} \end{aligned}$$

In order to solve the problem easier, we give the following hint. Now consider the system of linear congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \quad \vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

such that $gcd(m_1, m_2, ..., m_k) = 1$. Define

$$M_i = \frac{\prod_{i=1}^{k} m_i}{m_i}$$

and s_i is the solution of the linear congruence $M_i x \equiv 1 \pmod{m_i}, i \in \{1, 2, ..., k\}$. Then

$$s = \sum_{i=1}^{k} a_i s_i M_i$$

satisfies the system of linear congruences. Thus, the solution is

$$x \equiv s \pmod{\prod_{i=1}^{k} m_i}.$$

Implement this method to solve this example. It follows from the problem explained in this example that

$$\begin{aligned} a_1 &= 3 \quad m_1 = 4 \\ a_2 &= 4 \quad m_2 = 5 \\ a_3 &= 1 \quad m_3 = 3. \end{aligned}$$

We therefore have,

$M_1 = 5.3 = 15$, which implies $15x \equiv 1 \pmod 4$ or $x \equiv 3 \pmod 4$
$M_2 = 4.3 = 12$, which implies $12x \equiv 1 \pmod 5$ or $x \equiv 2 \pmod 5$
$M_3 = 4.5 = 20$, which implies $20x \equiv 1 \pmod 3$ or $x \equiv 2 \pmod 3$

Thus

$$\begin{aligned} s &= \sum_{i=1}^{3} a_i s_i M_i \\ &= 3.3.15 + 4.3.12 + 1.3.20 \\ &= 135 + 144 + 60 \\ s &= 339 \end{aligned}$$

So, the solution of the system of linear congruences can be represented as

$$\begin{aligned} x &\equiv 339 \pmod{4.5.3} \\ &\equiv 339 \pmod{60} \\ x &\equiv 39 \pmod{60}. \end{aligned}$$

In the previous material, we have learned to solve a system of linear congruence with one variable. Moreover, we will describe some properties of a system of linear congruences with multiple variable.

Theorem 6.17 *Let m be a natural number and $\gcd(\Delta, m) = 1$ such that $\Delta = ad - bc$. Then the system of linear congruence*

$$\begin{aligned} ax + by &\equiv e \pmod{m} \\ cx + dy &\equiv f \pmod{m} \end{aligned}$$

has a solution, say (x, y) where

$$\begin{aligned} x &= \Delta^{-1}(de - bf) \pmod{m} \\ y &= \Delta^{-1}(af - ce) \pmod{m} \end{aligned}$$

and Δ^{-1} is the inverse of Δ modulo m.

Proof. We multiply the congruence $ax + by \equiv e \pmod{m}$ with integer d and the congruence $cx + dy \equiv f \pmod{m}$ with the integer b, we therefore have

$$\begin{aligned} adx + bdy &\equiv de \pmod{m} \\ bcx + bdy &\equiv bf \pmod{m} \end{aligned}$$

Thus,

$$(ad - bc)x \equiv (de - bf) \pmod{m},$$

and since $\Delta = ad - bc$, where Δ is the determinant of the representation matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\Delta x \equiv (de - bf) \pmod{m}.$$

Furthermore, since $gcd(\Delta, m) = 1, \Delta$ has an inverse modulo m, say Δ^{-1}. Hence,

$$x \equiv \Delta^{-1}(de - bf) \pmod{m}.$$

Using the same method to eliminate the x variable, we multiply the congruence $ax + by \equiv e \pmod{m}$ with integer c and the congruence $cx + dy \equiv f \pmod{m}$ with the integer a, we therefore have

$$\begin{aligned} acx + bcy &\equiv ce \pmod{m} \\ acx + ady &\equiv af \pmod{m} \end{aligned}$$

Thus

$$\begin{aligned} (ad - bc)y &\equiv (af - ce) \pmod{m} \\ \Delta y &\equiv (af - ce) \pmod{m} \end{aligned}$$

Since $gcd(\Delta, m) = 1$, we therefore have

$$y \equiv \Delta^{-1}(af - ce) \pmod{m}.$$

This implies that (x, y) is the solution of the system of multivariable linear congruences, where

$$x \equiv \Delta^{-1}(de - bf) \pmod{m}$$

$$y \equiv \Delta^{-1}(af - ce) \pmod{m},$$

which completes the proof. ■

Definition 6.18 *Let $A = (a_{ij})$ and $B = (b_{ij})$ be $n \times k$ matrices such that their entries are integers. The matrix A is congruence to the matrix B modulo m (it is denoted by $A \equiv B \pmod{m}$) if the entry $a_{ij} \equiv b_{ij} \pmod{m}$ for every $i \in \{1, 2, .., n\}, j \in \{1, 2, ..., k\}$.*

Example 6.19 The matrix

$$\begin{pmatrix} 15 & 3 \\ 8 & 12 \end{pmatrix} \equiv \begin{pmatrix} 4 & 3 \\ 8 & 1 \end{pmatrix} \pmod{11}$$

since

$$\begin{aligned} 15 &\equiv 4 \pmod{11} \\ 3 &\equiv 3 \pmod{11} \\ 8 &\equiv 8 \pmod{11} \\ 12 &\equiv 1 \pmod{11}. \end{aligned}$$

Theorem 6.20 *Let $A = (a_{ij}), B = (b_{ij})$ be $n \times k$ matrices, let $C = (c_{ij})$ be a $k \times p$ matrix, and let $D = (d_{ij})$ be a $t \times p$ matrix such that their entries are integers. Then, we have*

$$\begin{aligned} AC &\equiv BC \pmod{m} \\ DA &\equiv DB \pmod{m} \end{aligned}$$

Proof. It is clear. ■

Matrix is a useful tool that can be used to solve a system of linear congruences especially for a multivariable linear congruences. Consider the following example.

Example 6.21 The following system of linear congruences.

$$\begin{aligned} x + 4y &\equiv 5 \pmod{13} \\ 2x + 5y &\equiv 7 \pmod{13} \end{aligned}$$

can be represented as

$$\begin{pmatrix} 1 & 4 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 7 \end{pmatrix} \pmod{13}$$

Definition 6.22 *Let A be an $n \times n$ matrix and its entries are integers such that $AA^{-1} = A^{-1}A \equiv I \pmod{m}$, where I is the $n \times n$ identity matrix. The matrix A^{-1} is called the inverse of A modulo m.*

Theorem 6.23 *Let*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be a matrix, where a, b, c, d are integers such that $det(A) = \Delta = ad - bc$ is prime relative to a positive integer m. Then

$$A^{-1} = \Delta^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

is the inverse of A modulo m.

Proof. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be a matrix such that its entries are integers. Then

$$AA^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Delta^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Analogously, we can see that $A^{-1}A = I$. ■

Theorem 6.24 *If A is a square matrix such that $\Delta = detA \neq 0$, then $Aadj(A) = (det(A))I$.*

Proof. Prove this theorem as exercise. ■

Theorem 6.25 *If A is a square matrix and its entries are integers and let m be a positive integer such that $gcd(\Delta, m) = 1$, then the inverse of A modulo m is*

$$A^{-1} = \Delta^{-1} adj(A)$$

Proof. Let A be a square matrix and its entries are integers and let m be a positive integer such that $gcd(\Delta, m) = 1$, where $\Delta = det(A)$. Then Δ^{-1} exists. Thus $Aadj(A) = \Delta I$. We therefore have

$$A\Delta^{-1}adj(A) \equiv \Delta\Delta^{-1}I \equiv I \pmod{m}$$
$$\Delta^{-1}adj(A)A \equiv \Delta\Delta^{-1}I \equiv I \pmod{m}$$

These show that $A^{-1} = \Delta^{-1}adj(A)$. ■

Example 6.26 We will solve the following system of linear congruences three variables.

$$2x_1 + 3x_2 + 2x_3 \equiv 3 \pmod{11}$$
$$4x_1 - 5x_2 + 5x_3 \equiv -7 \pmod{11}$$
$$-3x_1 + 7x_2 - 2x_3 \equiv 5 \pmod{11}$$

We therefore have the following representation matrix.

$$\begin{pmatrix} 2 & 3 & 2 \\ 4 & -5 & 5 \\ -3 & 7 & -2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ -7 \\ 5 \end{pmatrix} \pmod{11}$$

Furthermore, we will represented the inverse of the entries with the respect of addition modulo 11. We have the following condition.

$$\begin{pmatrix} 2 & 3 & 2 \\ 4 & 6 & 5 \\ 8 & 7 & 9 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix} \pmod{11}$$

The inverse of the matrix

$$\begin{pmatrix} 2 & 3 & 2 \\ 4 & 6 & 5 \\ 8 & 7 & 9 \end{pmatrix} \pmod{11}$$ is the following matrix

$$\begin{pmatrix} 3 & 2 & 8 \\ 7 & 9 & 3 \\ 9 & 1 & 0 \end{pmatrix}.$$

This gives

$$\begin{aligned} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} &\equiv \begin{pmatrix} 3 & 2 & 8 \\ 7 & 9 & 3 \\ 9 & 1 & 0 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix} \pmod{11} \\ &\equiv \begin{pmatrix} 57 \\ 72 \\ 31 \end{pmatrix} \pmod{11} \\ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} &\equiv \begin{pmatrix} 2 \\ 6 \\ 9 \end{pmatrix} \pmod{11} \end{aligned}$$

Homework Chapter 6

1. Let $9x \equiv k \pmod{m}$ where k be an element of the set of all remainders of module 12. Determine the integer k such that.

   a. The congruence has no solution.

   b. The congruence has solutions.

2. Find the solution of the congruence $4x \equiv 6 \pmod{18}$.

3. Determine how many the number of the solutions of the following congruences.

   a. $3x \equiv 6 \pmod{15}$

   b. $6x \equiv 11 \pmod{15}$

   c. $3x \equiv 6 \pmod{24}$

   d. $3x \equiv 1 \pmod{23}$

4. Find the integers x and y which are the solutions of the following equation.

   (a) $2x + by = 18$

   (b) $6x + 15y = 51$

5. Determine the smallest positive integer $a > 2$ such that $2|a, 3|a+1, 4|a+2, 5|a+3, 6|a+4$.

6. Mr.Bob opened his store in the early morning. He provides duck eggs and chicken eggs in his store. The price of duck egg is Rp 2.900,00 per grain and the price of chicken egg is Rp 1.800,00 per grain. How many eggs which are successfully sold if Mr. Bob received Rp 28.900,00 for the total sales.

7. If $a \equiv b \pmod{m}$, the prove that $a \equiv b \pmod{2m}$ or $a \equiv b+m \pmod{2m}$.

8. Determine the solution of the system of linear congruences as follows:

$$x + 2y \equiv 1 \pmod 5$$
$$2x + y \equiv 1 \pmod 5$$

9. Determine the matrix A such that the entries of A are the members of the set of all remainders of modulo 5. Suppose

$$A \equiv \begin{pmatrix} 2 & 4 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 4 & 2 \\ 0 & 1 \end{pmatrix} \pmod 5$$

10. Let A and B be $n \times n$ square matrices such that the entries of the both matrices are integers. Show that if $A \equiv B \pmod m$, then $A^k \equiv B^k \pmod m$ for every positive integer k.

11. Show that the matrix

$$A = \begin{pmatrix} 4 & 11 \\ 1 & 22 \end{pmatrix}$$

satisfies the congruence $A^2 \equiv I \pmod m$ where I is the 2×2 identity matrix, that is,

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

12. Determine the inverse modulo 7 of the following matrices.

$$A = \begin{pmatrix} 0 & 2 \\ 4 & 1 \end{pmatrix}$$

$$B = \begin{pmatrix} 1 & 2 \\ 5 & 1 \end{pmatrix}$$

$$C = \begin{pmatrix} 3 & 3 \\ 4 & 6 \end{pmatrix}$$

13. Determine the inverse modulo 7 of the following matrices.

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 5 \\ 1 & 4 & 6 \end{pmatrix}$$

14. Determine the solution of the following system of linear congruence.

$$\begin{aligned} x + y &\equiv 1 \pmod 7 \\ x + z &\equiv 3 \pmod 7 \\ y + z &\equiv 2 \pmod 7 \end{aligned}$$

15. Determine the solution of the following system of linear congruence.

$$\begin{aligned} x + 2y + 3z &\equiv 1 \pmod{11} \\ x + 2y + 5z &\equiv 1 \pmod{11} \\ y + 4y + 6z &\equiv 1 \pmod{11} \end{aligned}$$

CHAPTERS 7
FERMAT AND WILSON THEOREM

7.1 Fermat Theorem

Pierre de Fermat was born in Beaumont-de-Lomagne between 31 October and 6 December 1607. He was a French lawyer at the Parlement of Toulouse, France. He was also a mathematician. He has many contributions in the development of number theory. Fermat's original statement was

Tout nombre premier mesure infailliblement une des puissances -1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous-multiple du nombre premier donné -1; et, après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question.

which was interpreted in English as:

Every prime number $[p]$ divides necessarily one of the powers minus one of any [geometric] progression $[a, a^2, a^3, ...]$ and the exponent of this power $[t]$ divides the given prime minus one [divides $p - 1$]. After one has found the first power $[t]$ that satisfies the question, all those whose exponents are multiples of the exponent of the first one satisfy similarly the question [that is, all multiples of the first t have the same property

Based on the history of the development of number theory. The man who provided the published proof was Euler. He published the proof in his article entitled *"Theorematum Quorundam ad Numeros Primos*

Spectantium Demonstratio" in the Proceedings of the St. Petersburg Academy in 1936. On the other hand, Leibniz also gave the same proof but the draft was unpublished. In this section, we will explain the Fermat Theorem and some related properties. We start with the following theorem.

Theorem 7.1 *Let a and m be positive integers. If $gcd(a, m) = 1$, then the smallest remainders modulo m of the sequence $a, 2a, 3a, ..., (m-1)a$ are the permutation of $1, 2, 3, ..., m-1$.*

Proof. Consider the sequence $a, 2a, 3a, ..., (m-1)a$. In fact, every member of the sequence $a, 2a, 3a, ..., (m-1)a$ is not congruence to 0 modulo m. We will prove that every member of the sequence $a, 2a, 3a, ..., (m-1)a$ is exactly congruence to one of the member of $\{1, 2, 3, ..., m-1\}$. Suppose there are two terms of the sequence $a, 2a, 3a, ..., (m-1)a$ which is congruence to each other, say

$$ra \equiv sa \pmod{m} \text{ where } 1 \leq r < s < m.$$

Since $gcd(a, m) = 1$, we can cancel the integer a. We therefore have

$$r \equiv s \pmod{m}.$$

It follows from the property of ra and sa stating that ra and sa are the smallest remainders modulo m that $r = s$, contrary to the condition $1 \leq r < s < m$. In other words, every member of the sequence $a, 2a, 3a, ..., (m-1)a$ is exactly congruence to one of the member of $\{1, 2, 3, ..., m-1\}$ which completes the proof. ■

Theorem 7.2 ***Fermat Theorem.*** *If p is a prime number and $gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Let a be an integer and let p be a prime number such that $gcd(a, p) = 1$. It follows from Theorem 7.1 that the smallest remainders modulo p of the sequence $a, 2a, 3a, ..., (p-1)a$ is exactly congruence to one of the

member of $\{1, 2, 3, ..., p-1\}$ which implies the multiplication between them will be congruence to modulo p. Hence,

$$\begin{aligned} a.2a.3a...(p-1)a &\equiv 1.2.3...(p-1) \pmod{p} \\ a^{p-1}(1.2.3...(p-1)) &\equiv (p-1)! \pmod{p} \\ a^{p-1}(p-1)! &\equiv (p-1)! \pmod{p} \end{aligned}$$

We know that $gcd(p-1, p) = 1$. This gives

$$a^{p-1} \equiv 1 \pmod{p}$$

which completes the proof. ■

In general case, we have the following generalization.

Theorem 7.3 *Let $a4 =$ be an integer and let p be a prime number. Then $p^p \equiv a \pmod{p}$.*

Proof. It follows from Thorem 7.2 that

$$a^{p-1} \equiv 1 \pmod{p}$$

Multiplying the both side with the integer a, we have

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

■

Furthermore, prove the Theorem 7.3 using mathematical induction.

Example 7.4 We will use the Fermat Theorem to find the remainder of the division $5^{39} : 11$. It follows from the Fermat Theorem that $5^{10} \equiv 1 \pmod{11}$. Moreover,

$$\begin{aligned} 5^{39} &\equiv (5^1 0)^3 (5^2)^4 5 \pmod{11} \\ &\equiv 1.3^4.5 \pmod{11} \\ 5^{39}9 &\equiv \pmod{11} \end{aligned}$$

Hence, the remainder is 9.

Theorem 7.5 *If p and q are prime numbers such that $p \neq q$ and $a^p \equiv a \pmod{q}$, then*

$$a^{pq} \equiv a \pmod{pq}$$

Proof. It follows from Theorem 7.3 that $(a^q)^p \equiv a^q \pmod{p}$. Furthermore, since $a^q \equiv a \pmod{p}$, $a^{pq} \equiv a \pmod{p}$. This gives

$$p|(a^{pq} - a) \tag{7.1}$$

Analogously, we have

$$q|(a^{pq} - a) \tag{7.2}$$

It follows from the statement 7.1, the statement 7.2, and p, q are different prime numbers that $pq|(a^{pq} - a$. This means

$$a^{pq} \equiv a \pmod{pq}$$

■

7.2 Wilson Theorem

In this section, we will discuss an important theorem which was first stated by Ibn al-Haytam (c. 1000 AD) and in the 18th century, John Wilson stated the same theorem. However, Edward Waring also posted the theorem 1770. But Edward Waring and John Wilson still could not prove it. Later, in 1771, Lagrange gave his first proof.

Theorem 7.6 *Let p be a prime number and let $x^2 \equiv 1 \pmod{p}$. Then the congruence $x^2 \equiv 1 \pmod{p}$ has exactly two solutions, that are, 1 and $p - 1$.*

Proof. Let r be the solution of the congruence $x^2 \equiv 1 \pmod{p}$. Then

$$\begin{aligned} r^2 - 1 &\equiv 0 \pmod{p} \\ (r+1)(r-1) &\equiv 0 \pmod{p}. \end{aligned}$$

This gives $p|(r+1)(r-1)$. Since p is a prime number, $p|(r+1)$ or $p|(r-1)$. We therefor have

$$\begin{aligned} r+1 &\equiv 0 \pmod{p} \text{ or } r-1 \equiv 0 \pmod{p} \\ r &\equiv -1 \pmod{p} \text{ or } r \equiv 1 \pmod{p} \\ r &\equiv p-1 \pmod{p} \text{ or } r \equiv 1 \pmod{p} \end{aligned}$$

which implies that 1 and $p-1$ are the solutions. ■

Example 7.7 The solution of the congruence $x^2 \equiv 1 \pmod{11}$ are 1 and 10.

Theorem 7.8 *Let p be a prime number such that $p \neq 2$ and let a' be the solution of the congruence $ax \equiv 1 \pmod{p}$ where $a \in \{1, 2, 3, ..., p-1\}$. Then*

a. If $a \not\equiv b \pmod{p}$, then $a' \not\equiv b \pmod{p}$.

b. If $a = 1$ or $a = p-1$, then $a' \equiv a \pmod{p}$.

Proof. We know that if $a \in \{1, 2, 3, ..., p-1\}$, then $gcd(a, p) = 1$ such that $ax \equiv 1 \pmod{p}$ has exactly one solution. This means that a' exists, where $aa' \equiv 1 \pmod{p}$.

a. Suppose $a' \equiv b \pmod{p}$. Then $aa' \equiv ab' \equiv 1 \pmod{p}$. Remember that a' and b' are the solutions of the congruence $ax \equiv 1 \pmod{p}$. Furthermore,

$$\begin{aligned} aa'b \equiv ab'b \equiv b &\pmod{p} \text{ where } b \in \{1, 2, 3, ..., p-1\} \\ a \equiv b &\pmod{p} \text{ since } b'b \equiv 1 \pmod{p} \end{aligned}$$

which completes the proof.

b. If $a = 1$, that is $x \equiv 1 \pmod{p}$, then the solution is $a' = 1$ which

implies $a' \equiv a \pmod{p}$. Moreover,

$$\begin{aligned} \text{in case, } a = p-1, (p-1)x &\equiv 1 \pmod{p} \\ -x &\equiv 1 \pmod{p} \\ x &\equiv -1 \pmod{p} \\ x &\equiv p-1 \pmod{p} \\ \text{Hence, } a' &\equiv a \pmod{p}. \end{aligned}$$

■

Example 7.9 Consider the congruence $ax \equiv 1 \pmod{13}$. Now let a' be the integer such that $aa' \equiv 1 \pmod{13}$. We therefore have the following table.

Table 7.1 The Integers Satisfying $ax \equiv 1 \pmod{13}$

a	1	2	3	4	5	6	7	8	9	10	11	12
a'	1	7	9	10	8	11	2	5	3	4	6	12
aa'	1	1	1	1	1	1	1	1	1	1	1	1

Moreover, we have the following congruences

$$\begin{aligned} 1.1 &\equiv 1 \pmod{13} \\ 2.7 &\equiv 1 \pmod{13} \\ 3.9 &\equiv 1 \pmod{13} \\ 4.10 &\equiv 1 \pmod{13} \\ 5.8 &\equiv 1 \pmod{13} \\ 6.11 &\equiv 1 \pmod{13} \\ 12.12 &\equiv 1 \pmod{13} \end{aligned}$$

and

$$1.2.7.3.9.4.10.5.8.6.11 \equiv 1 \pmod{13}. \tag{7.3}$$

If the congruence 7.3 is multiplied the both side by 12, we therefore have

$$\begin{aligned} 1.2.3.4.5.6.7.8.9.10.11.12 &\equiv 10 \pmod{13} \\ 10! &\equiv 10 \pmod{13} \\ 10! &\equiv -1 \pmod{13} \end{aligned}$$

In general, we have the Wilson Theorem.

Theorem 7.10 ***(Wilson Theorem)*** *If p is a prime number, then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. Since every integer a such that $ax \equiv 1 \pmod{p}$ gives the existence of the integer a' such that $aa' \equiv 1 \pmod{p}$ where $a, a' \in \{2, 3, 4, ..., p-2, p-1\}$, there exist $\frac{1}{2}(p-3)$ couples numbers which are congruence to 1 modulo p. We therefore have

$$\begin{aligned} 2.3.4...(p-2) &\equiv 1 \pmod{p} \\ 1.2.3.4...(p-2)(p-1) &\equiv p-1 \pmod{p} \\ (p-1)! &\equiv -1 \pmod{p} \end{aligned}$$

which completes the proof. ■

Furthermore, the converse of the Wilson Theorem is also true. Hence, we have the following consequence.

Theorem 7.11 *Let p be a positive integer. The following conditions are equivalent.*

a. *p is a prime number.*

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

Proof. The statement from (a.) to (b.) has been already proven in Theorem 7.10. Conversely, suppose p is not a prime number. Then there exist positive integers $a \neq 1, p$ and b such that $p = ab$ such that $a|p$ and

$a \leq p-1$. Now, since $(p-1)! \equiv -1 \pmod{p}$ then $p|(p-1)!+1$ and $a|p, a|(p-1)!+1$. Moreover, since $a \leq p-1, a$ is one of the divisor of $(p-1)!$ which implies $a|(p-1)!$. Remember that $a|(p-1)!+1$ and $a|(p-1)$. Then $a|1$, contrary to the condition $a \neq 1$. Hence, p should be a prime number. ■

Theorem 7.12 *Let p be a prime number. Then the congruence $x^2+1 \equiv 0 \pmod{p}$ has solutions if and only if $p \equiv 1 \pmod{4}$.*

Proof. Let a be the solution of the congruence $x^2+1 \equiv 0 \pmod{p}$. Then $a^2 \equiv -1 \pmod{p}$ and $gcd(a,p) = 1$. It follows from Fermat Theorem, we therefore have

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p} \\ (a^2)^{\frac{1}{2}(p-1)} &\equiv 1 \pmod{p} \\ (a^2)^{\frac{1}{2}(p-1)} &\equiv 1 \pmod{p} \\ (-1)^{\frac{p-1}{2}} &\equiv 1 \pmod{p} \end{aligned}$$

Hence, the prime number of the form $4k+3$ does not satisfy the latest congruence above. On the other hand, the prime number 2 does not meet the requirement. So, the only possible prime numbers are the prime numbers of the form $4k+1$ which implies $p \equiv 1 \pmod{4}$. Conversely, consider the following conditions.

$$\begin{aligned} p-1 &\equiv -1 \pmod{p} \\ p-2 &\equiv -2 \pmod{p} \\ &\vdots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} \pmod{p} \end{aligned}$$

and

$$(p-1)! = 1.2.3...(p-1)$$

Then

$$(p-1)! \equiv 1.2.3...\frac{p-1}{2}.\frac{-p+1}{2}...(-2)(-1)(p-1) \pmod{p}$$
$$(p-1)! \equiv (-1)^{\frac{p-1}{2}}(1.2.3...\frac{p-1}{2})^2 \pmod{p}$$
$$(p-1)! \equiv (1.2.3...\frac{p-1}{2})^2 \pmod{p}$$

Since $p = 4k+1$ for some integer k, $(-1)^{\frac{p-1}{2}} = 1$ which implies

$$(p-1)! \equiv ((\frac{p-1}{2})!)^2.$$

It follows from Wilson Theorem that

$$-1 \equiv ((\frac{p-1}{2})!)^2.$$

This gives $((\frac{p-1}{2})!)^2$ satisfies the congruence $x^2+1 \equiv 0 \pmod{p}$. So, we may deduce that the congruence has solutions. ■

Example 7.13 We will find the solution for the congruence $x^2+1 \equiv 0 \pmod{17}$. Since the prime number 17 has the form of $4k+1$. Then the congruence $x^2+1 \equiv 0 \pmod{17}$ has solution

$$\begin{aligned}(\frac{17-1}{2})! &\equiv 8! \pmod{17} \\ &\equiv 40.320 \pmod{17} \\ (\frac{17-1}{2})! &\equiv 13 \pmod{17}\end{aligned}$$

Moreover, the integer $17-13 = 4$ is also the solution. Hence, the solution of the congruence $x^2+1 \equiv 0 \pmod{17}$ is $\{4, 13\}$.

Homework Chapter 7

1. Determine the remainder of the following integers.
   (a) $314^{159} : 7$
   (b) $314^{162} : 7$
2. Find the two latest digit of the integer 7^{355}!
3. If $gcd(a, 35) = 1$, show that $a^{12} \equiv 1 \pmod{35}$.
4. Prove that $n^2 1 \equiv n \pmod{15}$ for every integer n.
5. Prove that of q is an odd prime number, then
$$1^q + 2^q + 3^q + ... + (q-1)^q \equiv 0 \pmod{q}.$$
6. Determine the remainder of $16!$ if $16!$ is divided by $19!$
7. Let q be a prime number which is greater than 5. Prove that
$$2(q-3)! + 1 \equiv 0 \pmod{q}$$
8. Let n be an integer and q be a prime number. Show that
$$q | n^q + (q-1)! n$$
9. Let n be an integer and q be a prime number. Show that
$$q | (q-1)! n^q + n$$
10. Let q be an odd prime number. Show that $2q | (2^{2q-1} - 2)!$
11. Find the solution of the following congruences
    (a) $x^2 \equiv -1 \pmod{31}$
    (b) $x^2 \equiv -1 \pmod{47}$

12. Let q be a prime number and Let a and b are integers which are not divisible by q. Show that

$$a^q \equiv b^q \pmod{q} \Longrightarrow a \equiv b \pmod{q}$$

13. Let q be a prime number and Let a and b are integers which are not divisible by q. Show that

$$a^q \equiv b^q \pmod{q} \Longrightarrow a \equiv b \pmod{q^2}$$

14. Let q be an odd prime number. Show that

$$1^{q-1} + 2^{q-1} + 3^{q-1} + ... + (q-1)^{q-1} \equiv -1 \pmod{q}$$

15. For a prime p of the form $4k + 3$, prove that either

$$(\frac{p-1}{2})! \equiv 1 \pmod{p} \quad \text{or} \quad (\frac{p-1}{2})! \equiv -1 \pmod{p}$$

REFERENCES

[1] Burton, D. M., 1986, *Elementary Number Theory Revised Printing* , Allyn and Bacon, Inc., Boston.

[2] Hackman, P., 2007, *Elementary Number Theory*, HHH Production., Linköping.

[3] Ore, O., 1948, *Number Theory and Its History*, McGraw-Hill Book Company, Inc., New York.

[4] Rosen, K. H., 1993, *Elementary Number Theory and Its Applications, Third Edition*, Addison-Wesley Pubslishing Company., New York.

[5] Sukirman., 2006, *Pengantar Teori Bilangan*, Hanggar Kreator., Yogyakarta.

[6] wikipedia.org (Integer Factorization) https://en.wikipedia.org/wiki/Integer_factorization

[7] wikipedia.org (Modular Arithmetic) https://en.wikipedia.org/wiki/Modular_arithmetic

[8] wikipedia.org (Diphantine Equation) https://en.wikipedia.org/wiki/Diophantine_equation

[9] wikipedia.org (Diophantus) https://en.wikipedia.org/wiki/Diophantus

[10] wikipedia.org (Fermat Little Theorem) https://en.wikipedia.org/wiki/Fermat%27s_little_theorem

[11] wikipedia.org (Wilson Theorem) https://en.wikipedia.org/wiki/Wilson%27s_theorem

[12] Zerhusen A., Rakes, C., Meece, S., 1999, *Diophantine Equations*, University of Kentucky.,Kentucky.

AUTHOR BIOGRAPHY

Puguh Wahyu Prasetyo is a fulltime lecturer at Universitas Ahmad Dahlan. He was born in Blora on July 22, 1988. He was graduated bachelor degree (Mathematics Major) from Universitas Negeri Yogyakarta in 2010. He was graduated master degree (Mathematics Major) from Universitas Gadjah Mada in 2012. He was graduated doctoral degree (Mathematics Major) from Universitas Gadjah Mada in 2018. He was also an International Visiting Graduate Student at University of Toronto in 2016. He works on Abstract Algebra.

AUTHOR BIOGRAPHY

Uha Isnaini is a fulltime lecturer at the Department of Mathematics, Universitas Gadjah Mada, Indonesia. He received his bachelor and master degree from Universitas Gadjah Mada, and did his PhD at the National Institute of Education, Nanyang Technological University, Singapore. His research interests are Number Theory and Algebra.

AUTHOR BIOGRAPHY

Burhanudin Arif Nurnugroho is a lecturer at Universitas Ahmad Dahlan. He was graduated bachelor degree (Mathematics Major) from Universitas Islam Negeri Sunan Kalijaga in 2009. He was graduated master degree (Mathematics Major) from Universitas Gadjah Mada in 2012. He was graduated doctoral degree (Mathematics Major) from Universitas Gadjah Mada in 2019. He works on Functional analysis as his major field and algebra and number theory as his minor field.

AUTHOR BIOGRAPHY

Rully Charitas Indra Prahmana was born in Medan, Indonesia, on January 24, 1987. He is an Associate Professor in Mathematics Education Department at Universitas Ahmad Dahlan, Yogyakarta, Indonesia. His research interests lie in teaching and learning, pre-service mathematics teachers, Ethnomathematics, inclusion education, single-subject research, realistic mathematics education, PISA Task, and design research.

ISBN: 978-602-0737-75-1