

California State University, San Bernardino

CSUSB ScholarWorks

Theses Digitization Project

John M. Pfau Library

2008

Chinese remainder theorem and its applications

Jacquelyn Ha Lac

Follow this and additional works at: <https://scholarworks.lib.csusb.edu/etd-project>



Part of the [Algebra Commons](#)

Recommended Citation

Lac, Jacquelyn Ha, "Chinese remainder theorem and its applications" (2008). *Theses Digitization Project*. 3373.

<https://scholarworks.lib.csusb.edu/etd-project/3373>

This Thesis is brought to you for free and open access by the John M. Pfau Library at CSUSB ScholarWorks. It has been accepted for inclusion in Theses Digitization Project by an authorized administrator of CSUSB ScholarWorks. For more information, please contact scholarworks@csusb.edu.

CHINESE REMAINDER THEOREM AND ITS APPLICATIONS

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

by

Jacquelyn Ha Lac

December 2008

CHINESE REMAINDER THEOREM AND ITS APPLICATIONS

A Thesis

Presented to the

Faculty of

California State University,

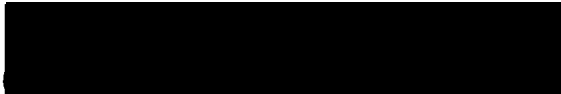
San Bernardino

by


Jacquelyn Ha Lac

December 2008

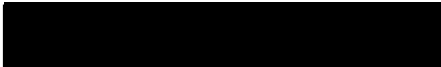
Approved by:



Dr. Laura Wallace, Committee Chair

12/3/08
Date


Dr. Joseph Chavez, Committee Member


Dr. Zahid Hasan, Committee Member


Dr. Peter Williams, Chair,
Department of Mathematics


Dr. Joseph Chavez
Graduate Coordinator,
Department of Mathematics

ABSTRACT

The Chinese Remainder Problem appeared around the first century AD in Sun Zie's book. Its uses ranged from the computation of calendars and counting soldiers to building the wall and base of a house. Later on, it became known as the Chinese Remainder Theorem involving integers and remainders under division. Over a period of time, people had expanded the theorem into abstract algebra for rings and principal ideal domains. Furthermore, the application of the Chinese Remainder Theorem can be found in computing, codes, and cryptography.

In this manuscript, the Chinese Remainder Theorem will be introduced as the original theorem dealing with integers. Then, its expansion and application into rings, principal ideal domains, and Dedekind Domains will be discussed. Finally, we will see how the theorem, as a secret-sharing scheme, takes part in the development of cryptography.

ACKNOWLEDGEMENTS

I would like to express my sincerest gratitude to Dr. Laura Wallace for her continued patience, support, and guidance in the completion of this project. I would also like to extend my appreciation to Dr. Chavez and Dr. Hasan for being on the committee reviewing this project.

Special thanks are due to my wonderful husband, Tuan Tran for his love and encouragement while I pursued my educational goals. Additionally, I would like to thank my good friends, Dilma Bonzer and Lynn Nguyen for their support.

Table of Contents

Abstract	iii
Acknowledgements	iv
1 Introduction	1
2 Foundation and Development of the Chinese Remainder Theorem	4
2.1 Historical Development	4
2.2 Basic Properties of Relatively Prime Integers	6
2.3 Chinese Remainder Theorem for Integers	9
2.4 Chinese Remainder Algorithm for Integers	10
3 Various Formulations of the Chinese Remainder Theorem	16
3.1 Rings, Ideals, and Homomorphisms	16
3.2 Chinese Remainder Theorem for Rings and Domains	20
3.3 Chinese Remainder Theorem for Polynomial Rings	24
4 Applications of the Chinese Remainder Theorem	27
4.1 Finite Sequence of Integers	27
4.2 A Characterization of Dedekind Domains	28
4.3 Cryptography Schemes	30
5 Conclusion	34
Bibliography	35

Chapter 1

Introduction

In the mid thirteenth century, a method for solving systems of linear congruences was published by the Chinese mathematician Ch'in Chiu-Shao. He wrote the *Mathematical Treatises in the Nine Sections*. This method was then called the Chinese Remainder Theorem due to the contribution of Ch'in Chiu-Shao ([Gal06]).

In an old guide book for magicians ([DPS96]), the form of the Chinese Remainder Theorem is found as a mind-reading trick to impress the audience. A magician would ask a helper to think of a number less than 60. Then the helper is asked to divide this number by 3 and tell the remainder. The process continues as the helper divides the original number by 4 and 5. Upon hearing the remainders, the magician will announce the number. For example, the number will be 23 corresponding to the remainders 2, 3, and 3, obtained by dividing by 3, 4, and 5 respectively. By the instruction of the guide book, the magician divides the numbers $40a + 45b + 36c$ by 60 where a, b, c are the three remainders. So, in the above case $40 \times 2 + 45 \times 3 + 36 \times 3 = 80 + 135 + 108 = 323 \div 60 = 5r23$. The last remainder 23 is the answer. This is a concrete example of using the Chinese Remainder Theorem with three moduli.

In arithmetic, modulo indicates a congruence relations on the integers. Two integers a and b are said to be congruent of modulo m if their difference $a - b$ is a multiple of m . Also if we divide both a and b by m , their remainders will be the same. The magician problem above starts with simple moduli of the integers; however, the congruence relation is expanded into abstract algebra with the operations on rings, domains, fields, and so on.

The Chinese Remainder Theorem began with a problem similar to that of the magician and the Chinese used its algorithm to calculate the calendar, compute the number of soldiers when marching in lines, or compute the construction of building a wall. Nowadays, we have found more uses involving the application of this theorem. In dealing with logic and mathematics, the theorem was used to prove that any finite sequence of integers can be represented in terms of two integers ([DPS96]). The property shows part of the power of the Chinese Remainder Theorem which will be proved in chapter 4.

Property: Let a_i , $0 \leq i \leq t$, be a finite sequence of nonnegative integers. Then there are integers u and v such that $(u \bmod (1 + (i + 1)v)) = a_i$, for every $i = 0, 1, \dots, t$.

Modern mathematicians also generalized the theorem into rings and integral domains which is our topic in chapter 3. Other applications that directly involve the theorem are seen in Dedekind domains and cryptography which will be discussed in chapter 4. In dealing with cryptography, the theorem itself is already a secret-sharing scheme which as mentioned above, was employed to compute the number of soldiers to prevent the enemy from such information as follows. A general asks his soldiers to stand in r_1, r_2, \dots, r_n rows in turn, and each time he counts the remainders. Finally, he computes the number of his soldiers using the Chinese Remainder Algorithm, the process of applying the Chinese Remainder Theorem. This is a secret method to calculate the number of soldiers.

Even though the theorem, originated as a puzzle, first appeared in China, the concept was also recognized in other areas of the world. There were several mathematicians exploring this idea. The work of Brahmagupta in Indian involved planar geometry, arithmetic progressions, and quadratic equations. A form of the theorem was also mentioned in his work. Even though the Chinese Remainder Theorem was just a glimpse in Fibonacci's work, we could see the substantial spread of the theorem. We will take a brief glance of how the Chinese Remainder Theorem is treated by Fibonacci.

In Fibonacci's book *Liber Abaci*, the Chinese Remainder Theorem was discussed as follows. "Let a contrived number be divided by 3, also by 5, also by 7; and ask each time what remains from each division. For each unity that remains from the division by 3, retain 70; for each unity that remains from the division by 5, retain 21; and for each unity that remains from the division by 7, retain 15. And as much as the number

surpasses 105, subtract from it 105; and what remains to you is the contrived number. Example: suppose from the division by 3 the remainder is 2; for this you retain twice 70, or 140; from which you subtract 105, and 35 remains. From the the division by 5, the remainder is 3; for which you retain three times 21, or 63, which you add to the above 35; you get 98. From the division by 7, the remainder is 4, for which you retain four times 15, or 60; which you add to the above 98, and you get 158, from which you subtract 105, and the remainder is 53, which is the contrived number. From this rule comes a pleasant game, namely if someone has learned this rule with you; if somebody else should say some number privately to him, then your companion, not interrogated, should silently divide the number for himself by 3, by 5, and by 7 according to the above-mentioned rule; the remainders from each of these divisions he says to you in order; and in this way you can know the number said to him in private.” ([DPS96])

Fibonacci’s presentation is very similar to Sun Zi’s approach in generating a method to find the mystery number. Chinese Remainder type of problems as mentioned above were also considered by other mathematicians such as Euler, Gauss, and Lagrange. Its popularity took a great part in our modern application to cryptography.

Chapter 2

Foundation and Development of the Chinese Remainder Theorem

2.1 Historical Development

In historical times, problems involving finding the number of objects, such as the numbers of baskets, blocks of bricks, or numbers of soldiers in a group under certain conditions were to compute the remainders when dividing the mystery number in different steps. One of the examples was as follow: “We have a number of things, but do not know exactly how many. If we count them by threes we have two left over. If we count them by fives we have three left over. If we count them by sevens we have two left over. How many things are there?” ([DPS96])

This problem is presented in the mathematical classic of Sun Zi, a mathematician in ancient China. Sun Zi Suanjing, Sun’s Mathematical Manual was dated approximately to the beginning of Graeco-Roman time, A.D. 100 - A.D. 500. The oldest Chinese mathematical classic is Chou Pei Suanjing. This book recorded mathematics for astronomical calculations. It was dated about 1000 B.C. The Pythagorean Theorem was used in the astronomical calculations in this book. Therefore, Sun Zi’s book is not the oldest Chinese mathematical classic; however, the Chinese Remainder Theorem appeared in it for the very first time.

The calculation of calendars in ancient China was the main source of the remainder theorem. Around A.D. 237, the Chinese astronomers defined the starting point

of the calendar as “shangyuan”, which is a moment that occurred simultaneously with the midnight of the first day of the 60 days cycle, the Winter Solstice and the new moon. The system of congruences

$$\begin{aligned}xN &= r_1 \pmod{60} \\xN &= r_2 \pmod{y}\end{aligned}$$

indicates the number of years N after *shangyuan*. So for the above system of congruences, if the Winter Solstice of a certain year occurred r_1 days after *shangyuan* and r_2 days after the new moon, then that year was N years after *shangyuan*, where x is the number of days in a tropical year and y is the number of days in a lunar month.

This example is considered the very first application of the Chinese Remainder Theorem ([DPS96]). This kind of computation was also used in building a wall or the base of a house such as the construction of the Great Wall during feudal times 475-221 B.C. It is described as follows. To construct a rectangular base for a building, there are four kinds of materials available: big cubic materials with each side 130 units long; small cubic materials with each side 110 units; city bricks that are 120 units long, 60 units wide, and 25 units deep; and “six-door” bricks that are 100 units long, 50 units wide, and 20 units deep. These four materials were used to build the base without breaking any of them into little pieces. Therefore, we end up with a system of congruences as we calculate different materials for each time a specific type of material is used. If big cubic materials are used, then 60 units base length is left, but 60 units more base width is needed. If small cubic materials are used, then 20 units based length is left, but 30 units more base width is needed. If the length of the city bricks is used, then 30 units base length is left, but 10 units more base width is needed. If the width of the city brick is used, then 30 units base length is left, but 10 units more base width is needed. If the depth of the city bricks is used, then 5 units base length is left, and 10 units base width is needed. If the length, width and depth of the six-door bricks are used, the base length has 30, 30 and 10 units left respectively, and the base width has 10, 10 and 10 units left respectively. The goal is to determine how large the base length X and base width Y are.

The above example is simplified into the following congruences where X is the material used each time and Y is the material needed:

$$\begin{aligned}X &= 60 \pmod{130} \\ &= 30 \pmod{120}\end{aligned}$$

$$\begin{aligned}
&= 20 \pmod{110} \\
&= 30 \pmod{100} \\
&= 30 \pmod{60} \\
&= 30 \pmod{50} \\
&= 5 \pmod{25} \\
&= 10 \pmod{20} \\
\text{and } Y &= 60 \pmod{130} \\
&= 10 \pmod{120} \\
&= 30 \pmod{110} \\
&= 10 \pmod{100} \\
&= 10 \pmod{60} \\
&= 10 \pmod{50} \\
&= 10 \pmod{25} \\
&= 10 \pmod{20}.
\end{aligned}$$

As mentioned in Chapter 1, this algorithm is also used to compute the number of soldiers that went out for battles. To avoid the enemy of knowing the number of soldiers he has, a general would count his soldiers in a certain way. For example, first he asks his soldiers to line up in rows of 11, then in rows of 17, 29, and 31. Respectively, each time, he is reported with remainder 8, 5, 16, and 24. Then he will calculate his soldiers in private. Since not many people know of this secret computation, the general can conceal his number of soldiers. From this example, we compile the following system of congruences with relatively prime moduli where x would be the number of soldiers:

$$\begin{aligned}
x &\equiv 8 \pmod{11}, \\
x &\equiv 5 \pmod{17}, \\
x &\equiv 16 \pmod{29}, \\
x &\equiv 24 \pmod{31}.
\end{aligned}$$

We will solve these three types of problems in the last section of this chapter.

2.2 Basic Properties of Relatively Prime Integers

Before introducing the theorem, there are several terms, lemmas, and theorems that we need to know concerning relatively prime integers.

Definition 2.1. A set of integers is said to be *pairwise relatively prime* if every pair of integers a and b in the set have no common divisor other than 1, in other words $(a, b) = 1$ where (a, b) is the greatest common divisor of a and b .

Example 2.2. The set $\{10, 7, 33, 13\}$ is pairwise relatively prime because any pair of numbers has greatest common divisor equal to 1.

$$(10, 7) = (10, 33) = (10, 13) = (7, 33) = (7, 13) = (33, 13) = 1.$$

This concept of *pairwise relatively prime* is used commonly in the Chinese Remainder Theorem. The property in the next theorem and those that follow are useful in dealing with greatest common divisors.

Theorem 2.3. *The greatest common divisor of the integers a and b , not both 0, is the least positive integer that is a linear combination of a and b .*

Proof: Let m be the least positive integer that is a linear combination of a and b . Then we have $m = ax + by$ for some integers x and y . By the Division Algorithm, there exists integers q and r such that $a = mq + r$, $0 \leq r < m$. So $r = a - mq$. Substitute m by the linear combination above, we get $r = a - (ax + by)q = (1 - xq)a - byq$. Then r is a linear combination of a and b . Since $0 \leq r < m$, and m is the least positive linear combination of a and b , we have $r = 0$. Therefore, $m \mid a$. Similarly $m \mid b$. Hence, m is a common divisor of a and b . Now let n be another divisor of a and b . For $m = ax + by$, if $n \mid a$ and $n \mid b$ then $n \mid m$, so $n \leq m$. Consequently, m is the greatest common divisor of a and b .

□

Proposition 2.4. *For any integers $a, b \in \mathbb{Z}$, $(a, b) = 1$ if and only if $ax + by = 1$ for some integers x and y .*

Proof: By Theorem 2.3, we have $(a, b) = 1$ leading to $ax + by = 1$ for any integers x and y . Conversely, suppose that $ax + by = 1$, and let $m = (a, b)$ then $m \mid a$ and $m \mid b$. So $m \mid (ax + by)$. Hence $m \mid 1$. Thus $m = 1$.

□

Lemma 2.5. *For any integers $a, b, c \in \mathbb{Z}$, $[a, b] \mid c$, where $[a, b]$ is the least common multiple of a and b , if and only if $a \mid c$ and $b \mid c$.*

Proof: Suppose $[a, b] \mid c$. Then $c = [a, b]x$ for some integer x . Also $a \mid [a, b]$, so $[a, b] = ay$ for some integer y . So, we have $c = axy$. Hence, $a \mid c$. Similarly, we obtain $b \mid c$.

Conversely, if $a \mid c$ and $b \mid c$, we try to prove that $[a, b] \mid c$. Let $[a, b] = m$. By the Division Algorithm, there exists integers q and r such that $c = mq + r, 0 \leq r < m$. We will show $r = 0$. Since $a \mid c$, $a \mid mq + r$. However, $[a, b] = m$ so $a \mid m$. Then $a \mid r$, so $r = ax$ for some x . Similarly, $r = by$ for some y . But, $r < m$ and $m = [a, b]$, hence, $r = 0$. Thus, $c = mq$, and $m \mid c$. Therefore $[a, b] \mid c$.

□

Definition 2.6. Let m be a positive integer. If a and b are integers, we say that a is congruent to b modulo m if $m \mid (a - b)$. We write $a \equiv b \pmod{m}$.

Theorem 2.7. If $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$, where $a, b, m_1, m_2, \dots, m_k \in \mathbb{Z}$ and $m_1, m_2, \dots, m_k \geq 1$, then $a \equiv b \pmod{[m_1, m_2, \dots, m_k]}$, where $[m_1, m_2, \dots, m_k]$ is the least common multiple of m_1, m_2, \dots, m_k .

Proof: Let $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$. Then $m_1 \mid (a - b), m_2 \mid (a - b), \dots, m_k \mid (a - b)$. So, by Lemma 2.5, $[m_1, m_2, \dots, m_k] \mid (a - b)$. So $a \equiv b \pmod{[m_1, m_2, \dots, m_k]}$.

□

Lemma 2.8. a. For any $a, b, c \in \mathbb{Z}$, $(a, b) = (b, c) = 1$, then $(ac, b) = 1$.

b. For any $a_1, a_2, \dots, a_n \in \mathbb{Z}$, if $(a_1, b) = (a_2, b) = \dots = (a_n, b) = 1$ then $(a_1 a_2 \dots a_n, b) = 1$.

Proof:

a. Suppose $(a, b) = 1$. Then $ax + by = 1$ for some integers x, y . Similarly $(b, c) = 1$ implies $bs + ct = 1$ for some integers s, t . Then $(ax + by)(bs + ct) = 1$, so $abxs + acxt + b^2ys + bcyt = 1$ and $acxt + b(axs + bys + cyt) = 1$. Hence $(ac, b) = 1$ by Proposition 2.4.

b. We are going to prove this part by induction.

For $n = 1$, we have $(a, b) = 1 \Rightarrow (a, b) = 1$.

Suppose $(a_1, b) = 1, (a_2, b) = 1, \dots, (a_{n+1}, b) = 1$. Then by the induction hypothesis, $(a_1 a_2 \dots a_n, b) = 1$ and $(a_{n+1}, b) = 1$. Since $a_1, a_2, \dots, a_n \in \mathbb{Z}$, then let $a_1 \cdot a_2 \cdot \dots \cdot a_n = c$. So by part a, $(c, b) = 1$ and $(a_{n+1}, b) = 1$ implies $(ca_{n+1}, b) = 1$. Thus, $(a_1 a_2 \dots a_n a_{n+1}, b) = 1$.

□

2.3 Chinese Remainder Theorem for Integers

Now that we have some basic concepts to help us in solving the Chinese Remainder puzzle given at the beginning of this chapter, we will start with our original theorem that gives the method to acquire the solution of the puzzle.

Theorem 2.9. *Let m_1, m_2, \dots, m_r be pairwise relatively prime positive integers. Then the system of congruences:*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \dots m_r$.

Proof: Let $M_k = \frac{M}{m_k} = m_1 m_2 \dots m_{k-1} m_{k+1} \dots m_r$. By Lemma 2.8, we know that $(M_k, m_k) = 1$ because $(m_j, m_k) = 1$ whenever $j \neq k$. Then $m_k x + M_k y_k = 1$ for some x, y_k . So $M_k y_k \equiv 1 \pmod{m_k}$. Hence, y_k is the inverse of $M_k \pmod{m_k}$. We form the sum:

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_r M_r y_r$$

where x would be the solution of the r congruences.

Since $m_k \mid M_j$ whenever $j \neq k$, we have $M_j \equiv 0 \pmod{m_k}$. So $a_j M_j y_j \equiv 0 \pmod{m_k}$ for $j \neq k$. Hence, from the sum we get $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$ since $M_k y_k \equiv 1 \pmod{m_k}$.

To prove that the solution is unique modulo M , we let x_1 and x_2 be two solutions to the system of r congruences. Then $x_1 \equiv x_2 \equiv a_k \pmod{m_k}$ for each k . So $m_k \mid (x_2 - x_1)$. By Theorem 2.7, $M \mid (x_2 - x_1)$. Hence, $x_1 \equiv x_2 \pmod{M}$.

□

Now, we are going to use the construction of the solution in the proof of the Chinese Remainder Theorem to solve the problem first mentioned in section 1. Let x be the unknown number of objects. Then we have the system of congruences:

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

So $M = 3 \cdot 5 \cdot 7 = 105$. Hence, $M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$, and $M_3 = \frac{105}{7} = 15$. Then $M_1 y_1 \equiv 1 \pmod{3}$ becomes $35y_1 \equiv 1 \pmod{3}$. Simplifying this congruence and solving for y_1 we get $2y_1 \equiv 1 \pmod{3}$ so that $y_1 = 2 \pmod{3}$. Similarly, $M_2 y_2 \equiv 1 \pmod{5}$ becomes $21y_2 \equiv 1 \pmod{5}$. We get $y_2 \equiv 1 \pmod{5}$. Again, $M_3 y_3 \equiv 1 \pmod{7}$ becomes $15y_3 \equiv 1 \pmod{7}$ and we get $y_3 \equiv 1 \pmod{7}$.

So $x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 140 + 63 + 30 \equiv 233 \equiv 23 \pmod{105}$. To check this, note that $23 \equiv 2 \pmod{3}$, $23 \equiv 3 \pmod{5}$, $23 \equiv 2 \pmod{7}$.

The answer to this problem was explained in a verse in Chen Dawei's book *Suanfa Tongzong*: "Three people walking together, it is rare that one be seventy. Five cherry blossom trees, twenty one branches bearing flowers, seven disciples reunite for the half-month. Taking away one hundred and five you shall know." ([DPS96]) To understand this saying, let x be the unknown number. Divide x by three (people) and multiply the remainder by $70 = 35 \cdot 2$, divide x by five (cherry blossoms) and multiply that remainder by $21 = 21 \cdot 1$. Finally, divide x by seven (disciples) and multiply the remainder by $15 = 15 \cdot 1$. Add all three results and subtract a suitable multiple of 105, i.e. find the remainder modulo 105, and you shall find x .

2.4 Chinese Remainder Algorithm for Integers

The Chinese Remainder Algorithm was generated based on Sun Zi's method to solve the original problem. By the 13th century, Quin Jiushao gave a more general method which did not restrict the moduli m_i to pairwise relatively prime numbers. His method, however, also converted the moduli into pairwise relatively prime numbers ([DPS96]). It is described as follows:

Let m_1, m_2, \dots, m_k be the moduli and $l = \text{lcm}[m_1, \dots, m_k]$, the least common multiple of m_1, \dots, m_k . We are going to find a set of integers $\alpha_1, \alpha_2, \dots, \alpha_k$ satisfying:

1. α_i divides $m_i, i = 1, 2, \dots, k$;
2. $\text{gcd}(\alpha_i, \alpha_j) = 1$ for all $j \neq i$;
3. $\alpha_1 \alpha_2 \dots \alpha_k = \text{lcm}[m_1, \dots, m_k]$.

Then the system of congruences $x = a_i \pmod{m_i}$ for $i = 1, \dots, k$ is converted into $x = a_i \pmod{\alpha_i}$ for $i = 1, \dots, k$, where the moduli α_i are pairwise relatively prime.

To find the set of integers α_i for $i = 1, \dots, k$, we need to complete the following

procedure. Consider the first case of $k = 2$:

a. Let $(m_1, m_2) = d_1$. If $(m_1/d_1, m_2) = 1$, then take $\alpha_1 = m_1/d_1$ and $\alpha_2 = m_2$.

b. If $(m_1, m_2/d_1) = 1$, then take $\alpha_1 = m_1$ and $\alpha_2 = m_2/d_2$.

c. If $(m_1, m_2/d_1) = d_2 > 1$, then calculate $d_3 = (m_1/d_2, m_2d_2/d_1)$ where d_2 divides d_1 and d_3 divides d_1/d_2 . If $d_3 = 1$, then take $\alpha_1 = m_1/d_2$ and $\alpha_2 = m_2d_2/d_1$, otherwise calculate $d_4 = (m_1/d_2d_3, m_2d_2d_3/d_1)$. Continue this process until there exists an integer s such that $d_{s+1} = 1$. Such an s exists because $d_1 > d_2 > \dots \geq 0$. Then take $\alpha_1 = \frac{m_1}{d_2d_3\dots d_s}$ and $\alpha_2 = \frac{m_2d_2d_3\dots d_s}{d_1}$. So $(\alpha_1, \alpha_2) = 1$.

For the case of k moduli, apply the above algorithm to m_k and m_{k-1} first to obtain $\alpha_k^{(1)}$, α'_{k-1} . Then we apply the same algorithm to $\alpha_k^{(1)}$ and m_{k-2} which will give us $\alpha_k^{(2)}$, α'_{k-2} . Continue this procedure and finally apply the algorithm to $\alpha_k^{(k-2)}$ and m_1 , obtaining α_k, α'_1 . Then the integers $\alpha'_1, \alpha'_2, \dots, \alpha'_{k-1}, \alpha_k$ satisfy $(\alpha_k, \alpha'_i) = 1$ for $i = 1, 2, \dots, k-1$ and $\text{lcm}[\alpha_1, \alpha_2, \dots, \alpha_k] = \text{lcm}[\alpha'_1, \alpha'_2, \dots, \alpha'_{k-1}, \alpha_k] = \alpha_k \text{lcm}[\alpha'_1, \alpha'_2, \dots, \alpha'_{k-1}]$.

So we have reduced the case of k moduli into $k-1$ moduli. If we repeat this procedure, we will obtain the required $\alpha_1, \dots, \alpha_k$.

Example 2.10. Let $m_1 = 12$ and $m_2 = 20$ which are not pairwise relatively prime. Then $\text{lcm}[12, 20] = 60$. So by the procedure of step (a), $(12, 20) = 4$. Then $(\frac{12}{4}, 20) = 1$. So let $\alpha_1 = 3$, and $\alpha_2 = 20$. Thus $(\alpha_1, \alpha_2) = 1$. Therefore, we have $\alpha_1\alpha_2 = 3 \cdot 20 = 60 = \text{lcm}[m_1, m_2]$. If we have a system of congruences given by $x = a_1 \pmod{12}$ and $x = a_2 \pmod{20}$, then it will become $x = a_1 \pmod{3}$ and $x = a_2 \pmod{20}$ where 3 and 20 are relatively prime.

Example 2.11. Let $m_1 = 312$ and $m_2 = 16$ where m_1 and m_2 are not pairwise relatively prime. Using the algorithm, let $d_1 = (m_1, m_2) = (312, 16) = 8$. Then $d_2 = (m_1, \frac{m_2}{d_1}) = (312, 2) = 2$. So $d_3 = (\frac{m_1}{d_2}, \frac{m_2d_2}{d_1}) = (156, 4) = 4$. Continuing, $d_4 = (\frac{m_1}{d_2d_3}, \frac{m_2d_2d_3}{d_1}) = (39, 16) = 1$. Since $d_4 = 1$, we take $\alpha_1 = \frac{m_1}{d_2d_3} = 39$ and $\alpha_2 = \frac{m_2d_2d_3}{d_1} = 16$. Thus, α_1 and α_2 satisfy the three conditions:

1. α_1 divides m_1 and α_2 divides m_2 ,
2. $(\alpha_1, \alpha_2) = 1$,
3. $\alpha_1\alpha_2 = 39 \cdot 16 = 624 = \text{lcm}[m_1, m_2]$.

Hence, the algorithm sets the moduli back to pairwise relatively prime.

In the calculation of the calendars application mentioned in section 1 the algorithm is used with 2 moduli.

Example 2.12. Suppose the number of days in a tropical year is 365 and the number of days in a lunar month is 30. Then $x = 365$ and $y = 30$. Let r_1 be the number of days that the Winter Solstice occurs after *shangyuan* and r_2 be the number of days that the Winter Solstice occurs after the new moon, then we have the system of congruences

$$365N = r_1 \pmod{60}$$

$$365N = r_2 \pmod{30}$$

which is converted into

$$5N = r_1 \pmod{60}$$

$$5N = r_2 \pmod{30}$$

where N is the number of years after *shangyuan*. By the Chinese Remainder Algorithm, we get $d_1 = (60, 30) = 30$. Then $d_2 = (60, 1) = 1$. So we take $\alpha_1 = 60$ and $\alpha_2 = 1$. So the new system of congruences will be

$$5N = r_1 \pmod{60}$$

$$5N = r_2 \pmod{1}.$$

We will also use the above algorithm to illustrate the example of building walls in k moduli with $k > 2$.

Example 2.13. Let X be the base length of the wall and Y be the base width. We are going to use the algorithm to set all the moduli of X and Y into pairwise relatively prime integers. Since the moduli of X and Y are the same, we apply the algorithm to X and use the new pairwise relatively prime moduli for Y as well.

Recall that

$$\begin{aligned} X &= 60 \pmod{130} \\ &= 30 \pmod{120} \\ &= 20 \pmod{110} \\ &= 30 \pmod{100} \\ &= 30 \pmod{60} \\ &= 30 \pmod{50} \\ &= 5 \pmod{25} \end{aligned}$$

$$= 10 \pmod{20}.$$

We start from the bottom up. First of all, let m_i , $i = 1, 2, \dots, 8$ be as follow:
 $m_1 = 130$, $m_2 = 120$, $m_3 = 110$, $m_4 = 100$, $m_5 = 60$, $m_6 = 50$, $m_7 = 25$, and $m_8 = 20$.
 So we start with $m_8 = 20$ and $m_7 = 25$. Then, $d_1 = (20, 25) = 5$. So $d_2 = (20, \frac{25}{5}) = 5$.
 Consequently, $d_3 = (\frac{20}{5}, \frac{25 \cdot 5}{5}) = 1$. Thus $\alpha_8^{(1)} = \frac{20}{5} = 4$ and $\alpha_7' = 25$.
 Now apply the algorithm to $\alpha_8^{(1)} = 4$ and $m_6 = 50$. Similarly, we have $d_1 = (4, 50) = 2$.
 Then $d_2 = (4, \frac{50}{2}) = 1$. So $\alpha_8^{(2)} = 4$ and $\alpha_6' = 25$.
 Continuing this process, apply the algorithm to $\alpha_8^{(2)} = 4$ and $m_5 = 60$. Then $d_1 = (4, 60) = 4$. So $d_2 = (4, \frac{60}{4}) = (4, 15) = 1$. We have $\alpha_8^{(3)} = 4$ and $\alpha_5' = 15$.
 Next, apply the procedure to $\alpha_8^{(3)} = 4$ and $m_4 = 100$. First, $d_1 = (4, 100) = 4$. Then $d_2 = (4, \frac{100}{4}) = (4, 25) = 1$. So $\alpha_8^{(4)} = 4$ and $\alpha_4' = 25$.
 Again, the next pair is $\alpha_8^{(4)} = 4$ and $m_3 = 110$. So $d_1 = (4, 110) = 2$. Then $d_2 = (4, \frac{110}{2}) = (4, 55) = 1$. Hence, $\alpha_8^{(5)} = 4$ and $\alpha_3' = 55$.
 Consequently, the next pair is $\alpha_8^{(5)} = 4$ and $m_2 = 120$. We get $d_1 = (4, 120) = 4$. Then $d_2 = (4, \frac{120}{4}) = (4, 30) = 2$. Hence, we continue to $d_3 = (\frac{4}{2}, \frac{120 \cdot 2}{4}) = (2, 60) = 2$. Thus, $d_4 = (\frac{4}{2 \cdot 2}, \frac{120 \cdot 2 \cdot 2}{4}) = (1, 120) = 1$. Therefore, $\alpha_8^{(6)} = 1$ and $\alpha_2' = 120$.
 Lastly, the pair is $\alpha_8^{(6)} = 1$ and $m_1 = 130$. Obviously, the two numbers are relatively prime, so we obtain $\alpha_8 = 1$ and $\alpha_1' = 130$. Now that we have just reduced the 8 moduli into 7 with the last one relatively prime to the rest, we have the 7 moduli in order: 130, 120, 55, 25, 15, 25, 25. Applying this procedure again we have $d_1 = (\alpha_7', \alpha_6') = (25, 25) = 25$, then $d_2 = (25, \frac{25}{25}) = 1$ So take $\beta_7^{(1)} = 25$ and $\beta_6' = 1$.
 Next, $d_1 = (25, 15) = 5$, so $d_2 = (25, \frac{15}{5}) = 1$. Hence, $\beta_7^{(2)} = 25$ and $\beta_5' = 3$.
 Again, $d_1 = (25, 25) = 25$, then $d_2 = (25, \frac{25}{25}) = 1$. Thus, take $\beta_7^{(3)} = 25$ and $\beta_4' = 1$.
 Similarly, $d_1 = (25, 55) = 5$, and $d_2 = (25, \frac{55}{5}) = 1$. Take $\beta_7^{(4)} = 25$ and $\beta_3' = 11$.
 Now we have $d_1 = (25, 120) = 5$, so $d_2 = (25, \frac{120}{5}) = 1$. Then take $\beta_7^{(5)} = 25$ and $\beta_2' = 24$.
 Last, $d_1 = (25, 130) = 5$, then $d_2 = (25, \frac{130}{5}) = 1$. Therefore $\beta_7 = 25$ and $\beta_1' = 26$.
 The new list of moduli now has become 26, 24, 11, 1, 3, 1, 25. We can see that every element is pairwise relatively prime with each other except the two moduli 26 and 24. So we will use the algorithm one more time to convert them to pairwise relatively prime.

Let $d_1 = (26, 24) = 2$, then $d_2 = (26, \frac{24}{2}) = 2$, so $d_3 = (\frac{26}{2}, \frac{24 \cdot 2}{2}) = 1$. Thus the two moduli 26 and 24 now become 13 and 12. This, however, creates another non-pairwise relatively primes which are 12 and 3. Once again, we apply the algorithm to these two moduli.

We have $d_1 = (12, 3) = 3$, then $d_2 = (12, 1) = 1$. So the two new moduli are 12 and 1.

Now we have a new system of congruences with pairwise relatively prime integers:

$$\begin{aligned}
 X &= 60 \pmod{13} = 8 \pmod{13} \\
 &= 30 \pmod{12} = 6 \pmod{12} \\
 &= 20 \pmod{11} = 9 \pmod{11} \\
 &= 30 \pmod{1} = 0 \\
 &= 30 \pmod{1} = 0 \\
 &= 30 \pmod{1} = 0 \\
 &= 5 \pmod{25} \\
 &= 10 \pmod{1} = 0.
 \end{aligned}$$

Using the Chinese Remainder Theorem, excluding all the mod 1 congruences, we obtain

$$M = 13 \cdot 12 \cdot 11 \cdot 25 = 42,900. \text{ Therefore, } M_1 = \frac{42,900}{13} = 3,300, M_2 = \frac{42,900}{12} = 3,575, \\
 M_3 = \frac{42,900}{11} = 3,900, \text{ and } M_4 = \frac{42,900}{25} = 1,716.$$

Then $3,300y_1 = 1 \pmod{13}$ becomes $11y_1 \pmod{13}$, so $y_1 = 6 \pmod{13}$. Again, $3,575y_2 = 1 \pmod{12}$, so $11y_2 = 1 \pmod{12}$, and $y_2 = 11 \pmod{12}$. Similarly, $3,900y_3 = 1 \pmod{11}$ becomes $6y_3 = 1 \pmod{11}$, so $y_3 = 2 \pmod{11}$. Finally, $1,716y_4 = 1 \pmod{25}$, so $16y_4 = 1 \pmod{25}$, and $y_4 = 11 \pmod{25}$. Hence, $x = 8 \cdot 3,300 \cdot 6 + 6 \cdot 3,575 \cdot 11 + 9 \cdot 3,900 \cdot 2 + 5 \cdot 1,716 \cdot 11 = 558,930 \pmod{42,900} = 1,230 \pmod{42,900}$. So the base length of the wall is a multiple of $1,230 \pmod{42,900}$.

To solve for the base width of the wall, we set up the system of congruences just as above with the moduli relatively prime.

$$\begin{aligned}
 Y &= 60 \pmod{13} = 8 \pmod{13} \\
 &= 10 \pmod{12} \\
 &= 30 \pmod{11} = 8 \pmod{11} \\
 &= 10 \pmod{1} = 0 \\
 &= 10 \pmod{1} = 0 \\
 &= 10 \pmod{1} = 0
 \end{aligned}$$

$$\begin{aligned}
&= 10 \pmod{25} \\
&= 10 \pmod{1} = 0.
\end{aligned}$$

So we have $Y = 8 \cdot 3,300 \cdot 6 + 10 \cdot 3,575 \cdot 11 + 8 \cdot 3,900 \cdot 2 + 10 \cdot 1,716 \cdot 11 = 802,220 \pmod{49,000} = 18,220 \pmod{49,000}$. So the base width of the wall is a multiple of $18,220 \pmod{42,900}$.

Lastly, we will solve the problem of counting the number of soldiers.

Example 2.14. As in section 1, we have a system of congruences for the number of soldiers going out to battle.

$$\begin{aligned}
x &\equiv 8 \pmod{11}, \\
x &\equiv 5 \pmod{17}, \\
x &\equiv 16 \pmod{29}, \\
x &\equiv 24 \pmod{31}.
\end{aligned}$$

Since all the moduli are already relatively prime, we use the Chinese Remainder Theorem to solve for x . We have $M = 11 \cdot 17 \cdot 29 \cdot 31 = 168,113$, so $M_1 = \frac{168,113}{11} = 15,283$, $M_2 = \frac{168,113}{17} = 9,889$, $M_3 = \frac{168,113}{29} = 5,797$, and $M_4 = \frac{168,113}{31} = 5,423$. We determine y_1 by solving the congruence $15,283y_1 = 1 \pmod{11}$, or equivalently, $4y_1 = 1 \pmod{11}$. This yields $y_1 = 3 \pmod{11}$. By solving $9,889y_2 = 1 \pmod{17}$, or equivalently, $12y_2 = 1 \pmod{17}$, we find $y_2 = 7 \pmod{17}$. Similarly, $5,797y_3 = 1 \pmod{29}$, which is equal to $26y_3 = 1 \pmod{29}$. We get $y_3 = 10 \pmod{29}$. Finally, we solve $5,423y_4 = 1 \pmod{31}$ or $29y_4 = 1 \pmod{31}$. This gives $y_4 = 16 \pmod{31}$.

Hence, we calculate the number of soldiers going out to battles by

$$\begin{aligned}
x &= 8 \cdot 15,283 \cdot 3 + 5 \cdot 9,889 \cdot 7 + 16 \cdot 5,797 \cdot 10 + 24 \cdot 5,423 \cdot 16 = 3,722,859 = 24,373 \\
&\quad \pmod{168,113}.
\end{aligned}$$

So the number of soldiers would be 24,373 for that specific battle.

Chapter 3

Various Formulations of the Chinese Remainder Theorem

3.1 Rings, Ideals, and Homomorphisms

From the original theorem dealing with integers, the Chinese Remainder Theorem is expanded into rings and domains. We now are looking at the Chinese Remainder Theorem that can be formulated for rings which have pairwise coprime ideals. Before introducing the expansion of Chinese Remainder Theorem for rings, we are going to get acquainted with a few definitions.

Definition 3.1. A *ring* R is a nonempty set with two binary operations, addition (denoted by $a + b$) and multiplication (denoted ab), such that for all a, b, c in R :

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. There is an additive identity 0 . That is, there is an element 0 in R such that $a + 0 = a$ for all a in R .
4. There is an element $-a$ in R such that $a + (-a) = 0$.
5. $a(bc) = (ab)c$.
6. $a(b + c) = ab + ac$ and $(b + c)a = ba + bc$.

A ring is *commutative* when multiplication is commutative.

A subset S of a ring R is a *subring* of R if S itself is a ring with the operations of R .

If R has a multiplicative identity, i.e. an element $1 \in R$ such that $x \cdot 1 = 1 \cdot x = x$ then

R is said to be a *ring with unity*.

Example 3.2. The set \mathbb{Z} of integers under ordinary addition and multiplication is a commutative ring with unity.

Example 3.3. The set $n\mathbb{Z}$ of integers multiples of $n \in \mathbb{Z}$ under ordinary addition and multiplication is a commutative ring without unity and also a subring of \mathbb{Z} .

Example 3.4. The set $\mathbb{R}[x]$ of all polynomials in the variable x with real coefficients under polynomial addition and multiplication is a commutative ring.

Definition 3.5. A subring I of a ring R is called an *ideal* of R if for every $r \in R$ and every $i \in I$ both ri and ir are in I .

Theorem 3.6. *Ideal Test*

A nonempty subset I of a ring R is an ideal of R if

1. $a - b \in I$ whenever $a, b \in I$.
2. ra and ar are in I whenever $a \in I$ and $r \in R$.

Proposition 3.7. Let R be a commutative ring with unity and let $a \in R$. Then the set $\langle a \rangle = \{ra \mid r \in R\}$ is an ideal of R called the *principal ideal generated by a* .

Proof: By the Ideal Test, let $ra, sa \in \langle a \rangle$ where $r, s \in R$. Then $ra - sa = (r - s)a \in \langle a \rangle$ since $r - s \in R$. Also, let $x \in R$ then $xar = xra = (xr)a \in \langle a \rangle$ since R is a commutative ring. Therefore, $\langle a \rangle$ is an ideal. □

Example 3.8. For any positive integer n , the set of multiples of n , $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\} = \langle n \rangle$ is an ideal of \mathbb{Z} .

Example 3.9. Let $\mathbb{R}[x]$ be the set of all polynomials with real coefficients and let I be the subset of all polynomials with constant term 0. Then I is an ideal of $\mathbb{R}[x]$ and $I = \langle x \rangle$.

Definition 3.10. An *integral domain* is a commutative ring R with unity and no zero divisors, i.e. if $ab = 0$ where $a, b \in R$, then $a = 0$ or $b = 0$ for all a, b .

Example 3.11. The ring of integers \mathbb{Z} is an integral domain.

Example 3.12. The ring \mathbb{Z}_p of integers modulo a prime p is an integral domain.

Definition 3.13. A *principal ideal domain* is an integral domain R in which every ideal has the form $\langle a \rangle = \{ra \mid r \in R\}$ for some a in R .

Definition 3.14. Let R be ring and let I be an ideal of R and $s, t \in R$. The set of cosets $\{r + I \mid r \in R\}$ denoted R/I is a ring under the operations $(s + I) + (t + I) = s + t + I$ and $(s + I)(t + I) = st + I$. The ring R/I is called a *factor ring*.

Example 3.15. Let \mathbb{Z} be the ring of integers. The ring $\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$ is a factor ring. For example, we have

$$(2 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 5 + 4\mathbb{Z} = 1 + 4 + 4\mathbb{Z} = 1 + 4\mathbb{Z}, \text{ and}$$

$$(2 + 4\mathbb{Z})(3 + 4\mathbb{Z}) = 6 + 4\mathbb{Z} = 2 + 4 + 4\mathbb{Z} = 2 + 4\mathbb{Z}.$$

Example 3.16. Let $R = \mathbb{R}[x]$ and $I = \langle x \rangle$. We can see that $\langle x \rangle = \{r(x) \cdot x \mid r(x) \in \mathbb{R}[x]\}$ so $\mathbb{R}[x]/\langle x \rangle = \{f(x) + \langle x \rangle \mid f(x) \in \mathbb{R}[x]\} = \{a + \langle x \rangle \mid a \in \mathbb{R}\}$ which is similar to the ring \mathbb{R} as we will verify at the end of this section.

Example 3.17. Let $R = \mathbb{R}[x]$ and $I = \langle x^2 + 1 \rangle$ be the principal ideal generated by $x^2 + 1$. Then $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ is a factor ring. We have $\mathbb{R}[x]/\langle x^2 + 1 \rangle = \{g(x) + \langle x^2 + 1 \rangle \mid g(x) \in \mathbb{R}[x]\} = \{ax + b + \langle x^2 + 1 \rangle \mid a, b \in \mathbb{R}\}$.

Definition 3.18. Let R_1, R_2, \dots, R_n be rings and I_1, I_2, \dots, I_n be ideals. Construct a new ring as follows. Let

$$R_1/I_1 \oplus R_2/I_2 \oplus \cdots \oplus R_n/I_n = \{(a_1 + I_1, a_2 + I_2, \dots, a_n + I_n) \mid a_i + I_i \in R_i/I_i\}$$

and perform component-wise addition and multiplication, that is

$$(a_1 + I_1, a_2 + I_2, \dots, a_n + I_n) + (b_1 + I_1, b_2 + I_2, \dots, b_n + I_n) = (a_1 + b_1 + I_1, a_2 + b_2 + I_2, \dots, a_n + b_n + I_n)$$

and

$$(a_1 + I_1, a_2 + I_2, \dots, a_n + I_n)(b_1 + I_1, b_2 + I_2, \dots, b_n + I_n) = (a_1 b_1 + I_1, a_2 b_2 + I_2, \dots, a_n b_n + I_n).$$

This ring is called the *direct sum* of $R_1/I_1, R_2/I_2, \dots, R_n/I_n$.

Example 3.19. Let $\mathbb{Z}/\langle 3 \rangle \oplus \mathbb{Z}/\langle 5 \rangle$ be a direct sum. Then $(1 + \langle 3 \rangle, 4 + \langle 5 \rangle) + (2 + \langle 3 \rangle, 4 + \langle 5 \rangle) = (1 + 2 + \langle 3 \rangle, 2 + 4 + \langle 5 \rangle) = (0 + \langle 3 \rangle, 1 + \langle 5 \rangle)$ and $(1 + \langle 3 \rangle, 4 + \langle 5 \rangle)(2 + \langle 3 \rangle, 4 + \langle 5 \rangle) = (1 \cdot 2 + \langle 3 \rangle, 4 \cdot 4 + \langle 5 \rangle) = (2 + \langle 3 \rangle, 1 + \langle 5 \rangle)$.

Definition 3.20. A *ring homomorphism* ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations; that is, for all a, b in R ,

$$\phi(a + b) = \phi(a) + \phi(b) \text{ and } \phi(ab) = \phi(a)\phi(b).$$

A ring homomorphism that is both one-to-one and onto is called a *ring isomorphism*.

Example 3.21. Let ϕ be the mapping from \mathbb{Z}_4 to \mathbb{Z}_{10} with $x \rightarrow 5x$. Then $\phi(x + y) = 5(x + y) = 5x + 5y = \phi(x) + \phi(y)$. Also, $\phi(xy) = 5(xy) = 5 \cdot 5(xy)$ since $5 \cdot 5 = 5$ in \mathbb{Z}_{10} . Then $\phi(xy) = 5x \cdot 5y = \phi(x)\phi(y)$. So ϕ is a homomorphism.

Theorem 3.22. *Let ϕ be a homomorphism from a ring R to a ring S . Then kernel of ϕ , $\ker \phi = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R .*

Proof: To prove this theorem, we are going to apply the *ideal test*.

1. Let $r, s \in \ker \phi$ then $\phi(r) = \phi(s) = 0$. Hence, $\phi(r) - \phi(s) = 0 = \phi(r - s)$ since ϕ is a ring homomorphism. Therefore, $r - s \in \ker \phi$.
2. Let $t \in R$ and $r \in \ker \phi$. Then $\phi(r) = 0$. Since ϕ is a ring homomorphism $\phi(tr) = \phi(t)\phi(r) = \phi(t) \cdot 0 = 0$. Hence $tr \in \ker \phi$.

From (1) and (2), $\ker \phi$ is an ideal.

□

Example 3.23. Let ϕ be the mapping from $\mathbb{Z}[x]$ onto \mathbb{Z} given by $\phi(f(x)) = f(0)$ and let $f(x), g(x) \in \mathbb{Z}[x]$. Then ϕ is a ring homomorphism since $\phi(f(x) + g(x)) = \phi((f + g)(0)) = (f + g)(0) = f(0) + g(0) = \phi(f(x)) + \phi(g(x))$, and $\phi(f(x)g(x)) = \phi(fg(0)) = (fg)(0) = f(0) \cdot g(0) = \phi(f(x)) \cdot \phi(g(x))$. Hence $\ker \phi = \{f(x) \in \mathbb{Z}[x] \mid f(0) = 0\} = \langle x \rangle$, i.e. the kernel of ϕ is the set of polynomial with 0 constant term.

Theorem 3.24. *First Isomorphism Theorem for Rings*

Let ϕ be a ring homomorphism from R to S . Then the mapping from $R/\ker \phi$ to $\phi(R)$, given by $r + \ker \phi \rightarrow \phi(r)$ is an isomorphism. In symbols, $R/\ker \phi \approx \phi(R)$.

Proof:

Let $\phi : R \rightarrow S$ be a ring homomorphism.

Let $\bar{\phi} : R/\ker \phi \rightarrow \phi(R)$ be the mapping defined by

$$\bar{\phi}(r + \ker(\phi)) = \phi(r). \text{ We will show this mapping is one-to-one, onto, and that}$$

operations are preserved.

1. The mapping $\bar{\phi}$ is well-defined.

Let $r + \ker \phi = s + \ker \phi$. Then $r - s \in \ker \phi$. So $\phi(r - s) = 0$. It follows that $\phi(r) = \phi(s)$.

Hence, $\bar{\phi}(r + \ker\phi) = \phi(r) = \phi(s) = \bar{\phi}(s + \ker\phi)$.

2. The mapping $\bar{\phi}$ is one-to-one.

Let $\bar{\phi}(r + \ker\phi) = \bar{\phi}(s + \ker\phi)$. Then $\phi(r) = \phi(s)$ which implies $\phi(r) - \phi(s) = 0$ since ϕ is a ring homomorphism. So $\phi(r - s) = 0$, then $r - s \in \ker\phi$ and $r + \ker\phi = s + \ker\phi$.

3. The mapping $\bar{\phi}$ is onto.

Let $x \in \phi(R)$. Then $x = \phi(r) = \bar{\phi}(r + \ker\phi)$ for some $r \in R$.

4. The mapping $\bar{\phi}$ preserves addition and multiplication.

We have $\bar{\phi}((r + \ker\phi) + (s + \ker\phi)) = \bar{\phi}((r + s) + \ker\phi) = \phi(r + s) = \phi(r) + \phi(s) = \bar{\phi}(r + \ker\phi) + \bar{\phi}(s + \ker\phi)$.

Also $\bar{\phi}((r + \ker\phi)(s + \ker\phi)) = \bar{\phi}((rs) + \ker\phi) = \phi(rs) = \phi(r)\phi(s) = \bar{\phi}(r + \ker\phi)\bar{\phi}(s + \ker\phi)$.

Then by 1-4, $\bar{\phi}$ is an isomorphism. Therefore, $R/\ker\phi \approx \phi(R)$.

□

Example 3.25. Let ϕ be the mapping from \mathbb{Z} to \mathbb{Z}_n given by $\phi(x) = 0x \pmod n$. Then $\ker \phi = \langle n \rangle$ so $\mathbb{Z}/\langle n \rangle \approx \mathbb{Z}_n$.

Example 3.26. Let ϕ be the mapping from $\mathbb{R}[x]$ to \mathbb{R} given by $\phi(f(x)) = f(0)$ then $\ker \phi = \langle x \rangle$. So $\mathbb{R}[x]/\langle x \rangle \approx \mathbb{R}$ where $\langle x \rangle$ is the ideal of polynomials with zero constant term.

3.2 Chinese Remainder Theorem for Rings and Domains

We now extend the notion of relatively prime integers to coprime ideals in a ring R . This will allow us to extend the Chinese Remainder Theorem to rings and integral domains.

Definition 3.27. In a commutative ring R , two ideals A and B are called *coprime* if $A + B = R$.

Note that two principal ideals $\langle a \rangle$ and $\langle b \rangle$ are coprime in the ring of integers \mathbb{Z} if and only if a and b are relatively prime. Therefore, coprime ideals are analogous to relatively prime integers.

Proposition 3.28. Let R be a commutative ring with unity

1. If $I + J = R$, then $IJ = I \cap J$
2. If I_1, I_2, \dots, I_n are coprime in pairs, then $I_1 I_2 \cdots I_n = \bigcap_{i=1}^n I_i$.

Proof:

1. Let $r \in IJ$. Then $r = ij$ where $i \in I$ and $j \in J$. So $r \in J$, and $r \in I$ since I and J are ideals. Hence $r \in I \cap J$. Therefore, $IJ \subseteq I \cap J$.

Now we have $(I + J)(I \cap J) = I(I \cap J) + J(I \cap J) = II \cap IJ + JI \cap JJ \subseteq IJ$. Since $I + J = R$ then $(I + J)(I \cap J) = (I \cap J) \subseteq IJ$. \square

2. We proceed by induction on n . The case for $n = 2$ is proven by part (1). Assume $I_1 I_2 \cdots I_{n-1} = \bigcap_{i=1}^{n-1} I_i$. Suppose $n > 2$ and $\prod_{i=1}^{n-1} I_i = \bigcap_{i=1}^{n-1} I_i$. Let $J = \prod_{i=1}^{n-1} I_i = \bigcap_{i=1}^{n-1} I_i$. Since $I_i + I_n = R$ for $1 \leq i \leq n-1$, then $x_i + y_i = 1$ for some $x_i \in I_i$ and $y_i \in I_n$. Thus $\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) \equiv 1 \pmod{I_n}$. So $I_n + J = R$. Therefore, $\prod_{i=1}^n I_i = JI_n = J \cap I_n = \bigcap_{i=1}^n I_i$.

\square

Now it is time to use the First Isomorphism Theorem for Rings to prove the Chinese Remainder Theorem for rings with two ideals.

Theorem 3.29. *The Chinese Remainder Theorem for Two Ideals*

If R is a commutative ring and I and J are proper ideals with $I + J = R$, then $R/(I \cap J)$ is isomorphic to $R/I \oplus R/J$.

Proof: We are going to use the First Isomorphism Theorem to prove this theorem. Let $\phi : R \rightarrow R/I \oplus R/J$ be the mapping defined by

$$\phi(r) = (r + I, r + J).$$

1. ϕ is a well-defined map.

Suppose there exist $r, s \in R$ and $r = s$. Then $\phi(r) = (r + I, r + J)$ and $\phi(s) = (s + I, s + J)$. Since $r = s$, we have $r + I = s + I$ and $r + J = s + J$. Therefore, $(r + I, r + J) = (s + I, s + J)$. Hence, $\phi(r) = \phi(s)$.

2. ϕ is a homomorphism.

Suppose there exist $a, b \in R$. Then $\phi(a + b) = (a + b + I, a + b + J) = (a + I + b + I, a + J + b + J) = (a + I, a + J) + (b + I, b + J) = \phi(a) + \phi(b)$. We also have $\phi(ab) = (ab + I, ab + J) = ((a + I)(b + I), (a + J)(b + J)) = (a + I, a + J)(b + I, b + J) = \phi(a)\phi(b)$.

3. ϕ is surjective.

Let $(\bar{a}, \bar{b}) \in R/I \oplus R/J$. Then $(\bar{a}, \bar{b}) = (a + I, b + J)$ for some $a, b \in R$. Since $R = I + J$, we have $a = x + y$ and $b = s + t$ for some $x, s \in I$ and $y, t \in J$. Consider $y + s$. We obtain $\phi(y + s) = (y + s + I, y + s + J) = (y + I, s + J)$ since $s \in I, y \in J$. However,

$(\bar{a}, \bar{b}) = (a + I, b + J) = (x + y + I, s + t + J) = (y + I, s + J)$ since $x \in I$ and $t \in J$. So $\phi(y + s) = (\bar{a}, \bar{b})$. Therefore ϕ is onto.

By the First Isomorphism Theorem, we now have $R/\ker\phi \approx \phi(R)$. We know that $\phi(R) = R/I \oplus R/J$, so $R/\ker\phi \approx R/I \oplus R/J$.

4. $\ker\phi = I \cap J$.

Let $r \in I \cap J$. So $r \in I$ and $r \in J$. Then $\phi(r) = (r + I, r + J) = (I, J)$. So $r \in \ker\phi \Rightarrow I \cap J \subseteq \ker\phi$.

Suppose $b \in \ker\phi$. Then $(b + I, b + J) = \phi(b) = (I, J)$. So $b \in I$ and $b \in J$. Hence $b \in I \cap J \Rightarrow \ker\phi \subseteq (I \cap J)$.

From 1-4, we have $R/(I \cap J) \approx R/I \oplus R/J$.

□

We have to make sure that the ideals I and J are coprime, in other words, $I + J = R$ so that ϕ will be surjective. If ϕ is not onto, then the mapping will not necessarily be an isomorphism. The following example illustrates how the condition of pairwise coprime is necessary.

Example 3.30. If $R = \mathbb{Z}$, $A_1 = \langle 6 \rangle$ and $A_2 = \langle 4 \rangle$ then the mapping $\phi : R/(A_1 \cap A_2) \rightarrow R/A_1 \oplus R/A_2$ is not surjective.

Proof: Since the $\gcd(6, 4) = 2$, 6 and 4 are not relatively prime. So the ideals $\langle 6 \rangle$ and $\langle 4 \rangle$ are not coprime. Since $\langle 6 \rangle + \langle 4 \rangle = \langle 2 \rangle$ so $A_1 + A_2 \neq R$ since $1 \notin \langle 2 \rangle$. Also, $\mathbb{Z}/(\langle 6 \rangle \cap \langle 4 \rangle) \approx \mathbb{Z}/\langle 2 \rangle \approx \mathbb{Z}_2$; but, $\mathbb{Z}_2 \not\cong \mathbb{Z}_4 \oplus \mathbb{Z}_6$. There are only 2 elements in \mathbb{Z}_2 but there are 24 elements in $\mathbb{Z}_4 \oplus \mathbb{Z}_6$. Hence, ϕ cannot be surjective.

□

Now, we are going to generalize the above theorem to n ideals.

Theorem 3.31. *The Chinese Remainder Theorem for n Ideals*

If R is a ring and I_1, \dots, I_n are ideals of R which are pairwise coprime, i.e. $I_i + I_j = R$ whenever $i \neq j$, and $I = \bigcap_{i=1}^n I_i$, then R/I is isomorphic to $R/I_1 \oplus R/I_2 \oplus \dots \oplus R/I_n$.

Proof: By induction, for $n = 1$, we have $R/I \approx R/I$.

Assume that I_1, \dots, I_n, I_{n+1} are ideals of R which are pairwise coprime ($I_i + I_j = R$ whenever $i \neq j$) and R/I is isomorphic to $R/I_1 \oplus R/I_2 \oplus \dots \oplus R/I_n$ where $I = \bigcap_{i=1}^n I_i$.

Then by letting $J = I_{n+1}$ and using Theorem 3.29 and Theorem 3.30, we have $R/(I \cap J) \approx R/I \oplus R/J \approx R/I_1 \oplus R/I_2 \oplus \dots \oplus R/I_n \oplus R/J$. Therefore R/I is isomorphic to $R/I_1 \oplus R/I_2 \oplus \dots \oplus R/I_{n+1}$ where $I = \bigcap_{i=1}^{n+1} I_i$.

□

Corollary 3.32. *If $m \in \mathbb{Z}$ has the prime decomposition $m = p_1^{k_1} \dots p_i^{k_i}$ by the Fundamental Theorem of Arithmetic, ($k_i > 0$, p_i distinct primes), then there is an isomorphism of rings $\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_i^{k_i}}$.*

Proof: Since all the p_i 's are distinct primes, they are pairwise coprime and $\mathbb{Z}_m \approx \mathbb{Z}/(m)$. Therefore, by Theorem 3.32 and Proposition 3.29, we can see that $\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_i^{k_i}}$

□

Now that we have looked at the Chinese Remainder Theorem for rings through the mapping of isomorphism, we are going to reformulate theorem to be analogous to the theorem for integers.

Theorem 3.33. *General Chinese Remainder Theorem for Rings*

Let I_1, \dots, I_n be ideals in a ring R such that $I_i + I_j = R$ for all $i \neq j$. If $b_1, \dots, b_n \in R$, there there exists $b \in R$ such that $b \equiv b_i \pmod{I_i}$ for $i = 1, 2, \dots, n$. Furthermore, b is uniquely determined up to congruence modulo the ideal $I_i \cap I_2 \cap \dots \cap I_n$.

Just as Theorem 3.32, the ideals are pairwise coprime; however, instead of having the factor ring R/I isomorphic to the direct sum of all factor rings, we have the case of the intersection of all ideals which also combines several moduli to a new, larger modulo.

Proof:

Since $I_1 + I_2 = R$ and $I_1 + I_3 = R$, then

$$R = R^2 = (I_1 + I_2)(I_1 + I_3) = I_1^2 + I_1 I_3 + I_2 I_1 + I_2 I_3 \subseteq I_1 + I_2 I_3 \subseteq I_1 + (I_2 \cap I_3) \subseteq R.$$

Therefore, $R = I_1 + (I_2 \cap I_3)$. Assume inductively that

$$R = I_1 + (I_2 \cap I_3 \cap \dots \cap I_{k-1}).$$

Then

$$R = R^2 = (I_1 + (I_2 \cap \dots \cap I_{k-1}))(I_1 + I_k) \subseteq I_1 + (I_2 \cap I_3 \cap \dots \cap I_k) \subseteq R$$

Therefore, $R = I_1 + (I_2 \cap \dots \cap I_k)$. Consequently, $R = I_1 + (\bigcap_{i \neq 1} I_i)$. Similarly, for each

$k = 1, 2, \dots, n$, $R = I_k + (\cap_{i \neq k} I_i)$. Consequently, for each k there exist elements $a_k \in I_k$ and $r_k \in \cap_{i \neq k} I_i$ such that $b_k = a_k + r_k$. Furthermore $r_k \equiv b_k \pmod{I_k}$ and $r_k \equiv 0 \pmod{I_i}$ for $i \neq k$.

Let $b = r_1 + r_2 + \dots + r_n$. Then $b \equiv r_i \pmod{I_i}$ and hence $b \equiv b_i \pmod{I_i}$ for every i . Finally, if $c \in R$ is such that $c \equiv b_i \pmod{I_i}$ for every i , then $b \equiv c \pmod{I_i}$ for each i , where $b - c \in I_i$ for all i . Therefore, $b - c \in \cap_{i=1}^n I_i$ and $b \equiv c \pmod{\cap_{i=1}^n I_i}$.

□

Example 3.34. Let $\langle 2 \rangle$ and $\langle 3 \rangle$ be ideals in the ring \mathbb{Z} . Then we can see that $\langle 2 \rangle + \langle 3 \rangle = \mathbb{Z}$. For any a_1 and $a_2 \in \mathbb{Z}$, there exists an $a \in \mathbb{Z}$ such that $a \equiv a_1 \pmod{2}$ and $a \equiv a_2 \pmod{3}$. Then $a \equiv m \pmod{\langle 2 \rangle \cap \langle 3 \rangle}$, or $a \equiv m \pmod{\langle 6 \rangle}$ which takes us back to the general theorem for integers, Theorem 2.9.

3.3 Chinese Remainder Theorem for Polynomial Rings

Now let's look at how the Chinese Remainder Theorem is applied to polynomial rings. There are a few terms we need to be familiar with.

Definition 3.35. A *unit* in a ring R is an invertible element of R , i.e., an element b such that there is an a in R with $ab = ba = 1_R$.

Definition 3.36. A *field* is a commutative ring with unity in which every nonzero element is a unit.

Example 3.37. For every prime p , the ring of integers modulo p , denoted \mathbb{Z}_p is a field.

Definition 3.38. Let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be *irreducible over D* if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$.

Note: Elements a and b of an integral domain D are called *associates* if $a = ub$ where u is a unit of D .

Theorem 3.39. Let $f(x)$ and $g(x)$ be irreducible polynomials over a field F . If $f(x)$ and $g(x)$ are not associates, then $F[x]/\langle f(x)g(x) \rangle$ is isomorphic to $F[x]/\langle f(x) \rangle \oplus F[x]/\langle g(x) \rangle$.

Proof: By Theorem 3.29, and the First Isomorphism Theorem, to show that $F[x]/\langle f(x)g(x) \rangle$ is isomorphic to $F[x]/\langle f(x) \rangle \oplus F[x]/\langle g(x) \rangle$, we only need to check that if $f(x)$ and $g(x)$ are not associates, then $\langle f(x)g(x) \rangle = \langle f(x) \rangle \langle g(x) \rangle = \langle f(x) \rangle \cap \langle g(x) \rangle$.

Let $r(x) \in \langle f(x)g(x) \rangle$, so $r(x) = f(x)g(x)h(x)$ for some $h(x) \in F[x]$. Then $r(x) = [f(x)h(x)]g(x)$ since F is a field. Hence, $r(x) \in \langle f(x) \rangle \cap \langle g(x) \rangle \Rightarrow \langle f(x)g(x) \rangle \subseteq \langle f(x) \rangle \cap \langle g(x) \rangle$.

Conversely, let $s(x) \in \langle f(x) \rangle \cap \langle g(x) \rangle$, so $s(x) \in \langle f(x) \rangle$ and $s(x) \in \langle g(x) \rangle$. Then, $s(x) = f(x)h(x)$ and $s(x) = g(x)r(x)$ for some $h(x), r(x) \in F[x]$. Consequently, we have $f(x)h(x) = g(x)r(x)$. Because $f(x), g(x)$ are irreducible, $\langle f(x) \rangle + \langle g(x) \rangle = F[x]$, so $f(x)u(x) + g(x)v(x) = 1$. So $s(x)f(x)u(x) + s(x)g(x)v(x) = s(x)$.

Hence, $s(x) = g(x)r(x)f(x)u(x) + f(x)h(x)g(x)v(x) = g(x)f(x)(r(x)u(x) + h(x)v(x))$ so $s(x) \in \langle f(x)g(x) \rangle$, and hence $\langle f(x) \rangle \cap \langle g(x) \rangle \subseteq \langle f(x)g(x) \rangle$.

□

Example 3.40. For every prime p , the ring of integers modulo p , denoted \mathbb{Z}_p is a field.

Definition 3.41. A *monic polynomial* is a polynomial whose leading coefficient is 1.

Definition 3.42. Let $a(x)$ and $b(x)$ be polynomials not both zero with coefficients in a field F . The *greatest common divisor* of $a(x)$ and $b(x)$ is the monic polynomial $d(x)$ of highest degree such that $d(x)$ is a divisor of $a(x)$ and $b(x)$.

Example 3.43. Let $a(x) = x^2 + 7x + 6$ and $b(x) = x^2 - 5x - 6$. Then $a(x) = (x+1)(x+6)$ and $b(x) = (x+1)(x-6)$. Hence the $\gcd(a(x), b(x)) = x + 1$.

Theorem 3.44. *General Chinese Remainder Theorem for Polynomial Rings.*

Let F be a field and let $b_1(x), \dots, b_n(x)$ be arbitrary polynomials of $F[x]$, $m_1(x), \dots, m_n(x)$ and $a_1(x), \dots, a_n(x)$ be polynomials of $F[x]$ such that

$$\begin{aligned} \gcd(m_i(x), m_j(x)) &= 1, \quad i \neq j; \\ \gcd(a_i(x), m_i(x)) &= 1, \quad i = 1, 2, \dots, n. \end{aligned}$$

Then the system of congruences

$$a_i(x)u(x) \equiv b_i(x) \pmod{m_i(x)}, \quad i = 1, 2, \dots, n$$

has exactly one solution modulo $m(x) = m_1(x)m_2(x) \cdots m_n(x)$.

Proof: Follow the proof of Theorem 3.32 and the Chinese Remainder Algorithm, we have $\gcd(a_i(x), m_i(x)) = 1$ for $1 \leq i \leq n$. We can compute a polynomial $c_i(x) \in F[x]$ such that $c_i(x)a_i(x) = 1 \pmod{m_i(x)}$ for all i . Therefore, $a_i(x)u(x) = b_i(x) \pmod{m_i(x)}$, $i = 1, 2, \dots, n$ becomes $u(x) = c_i(x)b_i(x) \pmod{m_i(x)}$ for $1 \leq i \leq n$. Using the Chinese Remainder Algorithm, we can find $M(x) = \prod_{i=1}^n m_i(x)$, then $M_1(x) = \frac{M(x)}{m_1(x)}$, $M_2(x) = \frac{M(x)}{m_2(x)}$, ..., $M_n(x) = \frac{M(x)}{m_n(x)}$. Then proceeding as the algorithm, the solution is given by: $u(x) = b_1(x)c_1(x)M_1(x)y_1(x) + b_2(x)c_2(x)M_2(x)y_2(x) + \dots + b_n(x)c_n(x)M_n(x)y_n(x) \pmod{M(x)}$, where $y_i(x)$ is the inverse of $M_i(x) \pmod{m_i(x)}$ for $i = 1, 2, \dots, n$.

Example 3.45. Let $m_1(x) = x^3 + x + 1$ and $m_2(x) = x^3 + x^2 + 1$ in $\mathbb{Z}/(2)$. Also, let $a_1 = x^2 + x + 1$ and $a_2 = x + 1$. Since m_i and a_i cannot be factored, they are relatively prime for each i . By the Euclidean Algorithm we have $(x + 1)m_1(x) + x^2a_1(x) = 1$ and $m_2(x) + x^2a_2(x) = 1$. So the inverses $c_i(x)$ of $a_i(x)$ are $c_1(x) = x^2$ and $c_2(x) = x^2$. Since $xm_1(x) + (x + 1)m_2(x) = 1$ we have a system of congruences

$$\begin{aligned} a_1(x)u(x) &= b_1(x) \pmod{m_1(x)} \\ a_2(x)u(x) &= b_2(x) \pmod{m_2(x)}. \end{aligned}$$

The solution is given by $u(x) = (x + 1)x^2m_2(x)r_1(x) + x \cdot x^2m_1(x)r_2(x) \pmod{m(x)}$, where $m(x) = m_1(x)m_2(x)$.

Chapter 4

Applications of the Chinese Remainder Theorem

4.1 Finite Sequence of Integers

As mentioned in Chapter 1, the first indication of the power of the Chinese Remainder Theorem applies to finite sequences of integers. For any finite sequence of integers, we can find another two integers to represent it. Let first look at the theorem and its proof.

Theorem 4.1. *Let a_i , $0 \leq i \leq t$, be a finite sequence of nonnegative integers. Then there are integers u and v such that $(u \bmod (1 + (i + 1)v)) = a_i$, for every $i = 0, 1, \dots, t$.*

Proof: Let a be the largest integer of the sequence a_i , $0 \leq i \leq t$, and define $v = 2a \cdot t!$ and $m_i = 1 + v(i + 1)$, $0 \leq i \leq t$. We claim that the integers m_i , $0 \leq i \leq t$ are relatively prime in pairs. By contradiction, let p be a prime number that divides both m_i and m_j , for some $i > j$. Then p divides the difference $(i + 1)m_j - (j + 1)m_i = i - j \leq t$. Since p divides m_i and v is divisible by all integers less than or equal to t , we obtain that $p = 1$, which is not a prime. So the integers m_i qualify as moduli for the Chinese Remainder Theorem. Hence, there is a number u such that

$$u \equiv a_i \pmod{m_i}, \quad i = 0, 1, \dots, t.$$

Then, $u \bmod m_i = a_i \bmod m_i$ for all $0 \leq i \leq t$. However, since $a_i < v < m_i$, we can conclude that $a_i \bmod m_i = a_i$ for $0 \leq i \leq t$. Therefore, $u \bmod m_i = a_i$ for $0 \leq i \leq t$.

□

Below is an example using a small finite sequence of integers. For this sequence, we find two integers representing each term. If we apply this theorem to larger sequence, we should still be able to find two integers representing each term in the sequence.

Example 4.2. Let $\{2, 3, 5, 6\}$ be a finite sequence with $a_0 = 2, a_1 = 3, a_2 = 5$ and $a_3 = 6$. Then by the theorem, there are integers u and v such that $u \bmod (1 + (i + 1)v) = a_i$. We will show how to find u and v . The largest integer is 6, so by the proof of the theorem we have $v = 2 \cdot 6 \cdot 3! = 72$, and: $m_0 = 1 + 72 = 73, m_1 = 1 + 144 = 145, m_2 = 1 + 216 = 217, m_3 = 1 + 288 = 289$. Then we obtain a system of congruences:

$$\begin{aligned} u &\equiv 2 \pmod{73}, \\ u &\equiv 3 \pmod{145}, \\ u &\equiv 5 \pmod{217}, \\ u &\equiv 6 \pmod{289}. \end{aligned}$$

This system of congruence has a solution. Using the Chinese Remainder Theorem, we obtain $M = 663,817,105, M_0 = 9,093,385, M_1 = 4,578,049, M_2 = 3,059,065,$ and $M_3 = 2,296,945$. Next, we get $9,093,385y_0 = 1 \pmod{73}$ which yields $y_0 = 12 \pmod{73}$; $4,578,049y_1 = 1 \pmod{145}$ which yields $y_1 = 4 \pmod{145}$, next $3,059,065y_2 = 1 \pmod{217}$ giving $y_2 = 95 \pmod{217}$, finally $2,296,945y_3 = 1 \pmod{289}$ giving $y_3 = 107 \pmod{289}$. Therefore, $u = 2 \cdot 9,093,385 \cdot 12 + 3 \cdot 4,578,049 \cdot 4 + 5 \cdot 3,059,065 \cdot 95 + 6 \cdot 2,296,945 \cdot 107 = 545,603,973 \pmod{663,817,105}$. Hence, we can represent the terms of the sequence using the two integers 72 and 545,603,973:

$$\begin{aligned} 2 &= 545,603,973 \pmod{(1 + 72 \cdot 1)}, \\ 3 &= 545,603,973 \pmod{(1 + 72 \cdot 2)}, \\ 5 &= 545,603,973 \pmod{(1 + 72 \cdot 3)}, \\ 6 &= 545,603,973 \pmod{(1 + 72 \cdot 4)}. \end{aligned}$$

4.2 A Characterization of Dedekind Domains

In number theory, the Fundamental Theorem of Arithmetic states that every natural number greater than 1 can be written as unique product of prime numbers. In abstract algebra, a Dedekind domain has a similar set up.

Definition 4.3. A *Dedekind domain* is an integral domain in which each ideal can be written as a product of a finite number of prime ideals.

Definition 4.4. Let R be a ring and I is its ideal. If there exists an *inverse ideal* $I^{-1} = \{x \in K | xi \in R\}$ where K is the quotient field of R then $II^{-1} = R$.

Proposition 4.5. *In a Dedekind domain, every nonzero prime ideal is a maximal ideal.*

Proof: Let R be a Dedekind domain and p is nonzero prime ideal and p is not maximal. Let a be another ideal of R such that $p \subset a$. Then $a^{-1}p \subset a^{-1}a = R$ so $a^{-1}p$ is an ideal of R . Since $a(a^{-1}p) = p$ then $a \subset p$ or $a^{-1}p \subset p$. If $a^{-1}p \subset p$ then $a^{-1} \subset pp^{-1} = R$ which implies that $R \subset a$ so $a = R$. On the other hand, if $a \subset p$ and by assumption, $p \subset a$ then $p = a$. Therefore p is maximal. □

Example 4.6. The ring of integers \mathbb{Z} is an example of Dedekind domain. The principal ideals of \mathbb{Z} are all generated by each integer such as $\langle 2 \rangle = \{0, \pm 2, \pm 4, \pm 6, \dots\}$. If $a \in \mathbb{Z}$, it has a unique prime decomposition; therefore $\langle a \rangle$ can be written as a product of a finite number of ideals. That is, if $a = p_1^{k_1} \cdots p_n^{k_n}$, then $\langle a \rangle = \langle p_1^{k_1} \rangle \cdots \langle p_n^{k_n} \rangle$.

A principal ideal domain is always a Dedekind domain; however, a Dedekind domain may not be a principal ideal domain. The following proposition will state the condition in which a Dedekind domain is a principal domain.

Proposition 4.7. *If a Dedekind domain R has only a finite number of nonzero prime ideals P_1, \dots, P_n , then R is a principal ideal domain.*

Proof: For each i , choose $b_i \in P_i - P_i^2$. We are going to prove that $\langle b_i \rangle = P_i$ which implies that every prime ideal is principal, hence, R is a principal ideal domain. Since R is a Dedekind domain and it has only a finite number of nonzero prime ideals $P_i, 1 \leq i \leq n$, then these prime ideals are also maximal ideals, and so $P_i + P_j = R, i \neq j$. Because R is a Dedekind domain, $b_i = I_1 I_2 \dots I_m$, where $I_i = P_j$. By the Chinese Remainder Theorem 3.32, we have $b_i \equiv i_i \pmod{P_i}$ and $b_i \equiv 1 \pmod{P_j}$. Then since $b_i \in P_i$, $\langle b_i \rangle \subseteq P_i$. So $I_1 I_2 \dots I_m \subseteq P_i$. Then $I_j = P_i$ for some j . Then we can rearrange the ideals so that $\langle b_i \rangle = P_i I_1 \dots I_{m-1}$. If $I_r = P_i$ for some r , then $\langle b_i \rangle = P_i^2 I_1 \dots I_{m-2}$, but this contradicts $b_i \notin P_i^2$. So continuing this process, we have $\langle b_i \rangle = P_i I_1 \dots I_{m-1} = P_i \cap I_1 \cap \dots \cap I_{m-1}$ where

I_1, \dots, I_{m-1} are distinct primes. Then $b_i \in I_1$ and since $b_i \equiv 1 \pmod{I_1}$, $b_i - 1 \in I_1$. So $1 \in I_1$ and hence $I_1 = R$. Therefore, $\langle b_i \rangle = P_i$.

□

4.3 Cryptography Schemes

The Chinese Remainder Theorem is applied in secret sharing, which is an important topic of cryptography. The Chinese Remainder Theorem itself is a secret sharing scheme without any modification. Let m_1, m_2, \dots, m_t be t pairwise relatively prime positive integers. Also let $m = \prod_{i=1}^t m_i$. Suppose that we have a secret which is an integer s such that $0 \leq s < m$. Let P_1, P_2, \dots, P_t be the t parties who are going to share the secret. Then P_i has the residue $s_i = s \pmod{m_i}$ as the secret that is only known to P_i . By the Chinese Remainder Theorem, the t pieces of information s_i are sufficient to determine the original s .

For the t parties, if we give out k shares, then the secret can be computed; otherwise, $k - 1$ shares will give a possible range of the secret. A (k, t) secret-sharing scheme is defined as follows. The t parties P_i share a secret s with the following conditions:

1. Each party has a share s_i about the secret s which is not known to other parties.
2. The secret s can be computed from any k shares s_i .
3. No $k - 1$ shares s_i give any information about the secret s .

We are going to look at the two secret sharing schemes; one involves the integers and the other is for polynomials.

Scheme 1

Let $m_i, i = 1, 2, \dots, t$, be t pairwise relatively prime integers no less than 2. We define

$$\min(k) = \min\{m_{i_1} m_{i_2} \cdots m_{i_k} \mid 1 \leq i_1 \leq \dots \leq i_k \leq t\},$$

$$\max(k - 1) = \max\{m_{i_1} m_{i_2} \cdots m_{i_{k-1}} \mid 1 \leq i_1 < i_2 < \dots < i_{k-1} \leq t\},$$

where $1 < k \leq t$. In other words, $\min(k)$ is the smallest product of k of the integers m_i and $\max(k - 1)$ is the greatest product of $k - 1$ of the integers m_i . Choose w to be the largest positive integer such that

- $w < \frac{\min(k)}{\max(k-1)}$; and
- $\gcd(w, m_i) = 1, i = 1, 2, \dots, t$.

Let $m = \min(k)$.

The secret is the integer s such that $0 \leq s < w$. Therefore, we assume that the secret is equally likely to be any integer between 0 and $w - 1$.

We compute the shares for t parties as follows.

Let $a \in \mathbb{Z}$ such that $0 \leq s + aw < m$, and let $s' = s + aw$. The shares are then given by $s_i = s' \bmod m_i, i = 1, 2, \dots, t$, where s_i is the share of party P_i . We are going to prove that $k - 1$ or fewer shares give no information about the secret; but any k or more shares determine the secret.

Without loss of generality, suppose s_1, s_2, \dots, s_h are known and $1 \leq h < t$. Let $M = \prod_{i=1}^h m_i$ and $M_j = \frac{M}{m_j}$ for $j = 1, 2, \dots, h$. Then $(M_j, m_j) = 1$. By Euclidean algorithm, there exist $u_j, v_j \in \mathbb{Z}$ such that $M_j u_j + m_j v_j = 1$. This can be done by solving $M_j u_j \equiv 1 \pmod{m_j}$ and $m_j v_j \equiv 1 \pmod{M_j}$. Then by the Chinese Remainder Algorithm, the system of congruences $x \equiv s_i \pmod{m_i}$ for $1 \leq i \leq h$ has a unique solution modulo M given by $x = s_1 M_1 u_1 + s_2 M_2 u_2 + \dots + s_h M_h u_h$.

Let $s'' = \sum_{j=1}^h M_j u_j s_j \pmod{M}$ where $0 \leq s'' < M$, then $s'' \equiv s_i \pmod{m_i}$. We have two cases:

Case 1:

If $h \geq k$ then $M \geq \min(k) = m > w$. By the Chinese Remainder Theorem $s'' = s'$ since $s' \equiv s_i \pmod{m_i}, s' < m \leq M$ and solutions to the system $x \equiv s_i \pmod{m_i}$ are unique modulo M . Now $s' \bmod w = (s + aw) \bmod w = s$ so the secret is given by $s = s'' \bmod w$.

Case 2:

If $h = k - 1$ then $M \leq \max[k - 1] < \frac{m}{w}$. This follows since $w < \frac{\min[k]}{\max[k - 1]}$ implies $\frac{\max[k - 1]}{\min[k]} > \frac{1}{w}$ and so $\max[k - 1] > \frac{\min[k]}{w}$. So $w < \frac{m}{M}$ since $w > 0$. Now $s' = s'' + bM$ for some b where $0 \leq s' < m$ since the solutions to the system $x \equiv s_i \pmod{m_i}$ are unique modulo M . Then $0 \leq s' < m$ implies $0 \leq s'' + bM < m$, so $-s'' \leq bM < m - s''$ which leads to $\frac{-s''}{M} \leq b < \frac{m - s''}{M}$. Therefore, $0 \leq b \leq \lfloor \frac{m - s''}{M} \rfloor$. Also, $\frac{m - s''}{M} > \frac{m - M}{M} = \frac{m}{M} - 1 > w - 1$ since $w < \frac{m}{M}$. So $s = s' \bmod w = (s'' + bm) \bmod w$ and since b ranges

from 0 to $\lfloor \frac{m-s''}{M} \rfloor$ and $w-1 \leq \lfloor \frac{m-s''}{M} \rfloor$, s takes on $0, 1, \dots, w-1$ equally likely.

Thus any $k-1$ or fewer shares give no information about secret s .

Now let's see an example to see how the secret-sharing scheme works.

Example 4.8. Let $k = 3$, $t = 4$, $m_1 = 5$, $m_2 = 7$, $m_3 = 11$, and $m_4 = 13$. Then $m = \min(k) = 5 \cdot 7 \cdot 11 = 385$, and $\max(k-1) = 11 \cdot 13 = 143$. So there exists an integer w such that $w < \frac{\min(k)}{\max(k-1)} = \frac{385}{143}$ and $\gcd(w, m_i) = 1$. We get $w = 2$. The secret s is an integer where $0 \leq s < w$. So s is either 0 or 1. Since $t = 4$, we need to compute 4 shares. We choose an a where $0 \leq s + aw < m$. Hence $0 \leq aw < m - s$ which implies $0 \leq a < \frac{m-s}{w} = \frac{385-1}{2} = 192$. Choose $a = 30$, for example. Let $s' = s + aw = s + 60$. The four shares are given by $s_i = s' \bmod m_i$. Then $s_1 = (s + 60) \bmod 5$, $s_2 = (s + 60) \bmod 7$, $s_3 = (s + 60) \bmod 11$, and $s_4 = (s + 60) \bmod 13$. As the secret keeper, we let $s = 1$ then $s_1 = 1$ and $s_2 = 5$. Then $M = m_1 m_2 = 35$, $M_1 = 7$, and $M_2 = 5$. By the Euclidean Algorithm, we get $7 \cdot (-2) + 5 \cdot 3 = 1$. Therefore, $u = 2$ and $v = 3$. Then by the Chinese Remainder Algorithm, we have $s'' = M_1 u_1 s_1 + M_2 u_2 s_2$ since $h = 2$. Then $s'' = (7 \cdot (-2) \cdot s_1 + 5 \cdot 3 \cdot s_2) \bmod 35 = (-14 + 75) \bmod 35 = 61 \bmod 35 = 26 \bmod 35$. Since $h = 3 - 1 = 2$ we have $s' = s'' + bM = 26 + 35b$ where $0 \leq b \leq \frac{385-26}{35} = 10$. It follows that $s = s' \bmod 2 = b \bmod 2$. Since $b \in [0, 10]$, s takes on 1 and 0 equally likely. Therefore, the two shares give no information about the secret.

If we have three shares, we can calculate the secret s . So for the example above, suppose we have three shares $s_1 = 1$, $s_2 = 5$, and $s_3 = 6$. Then $M = m_1 m_2 m_3 = 5 \cdot 7 \cdot 11 = 385$, so $M_1 = 77$, $M_2 = 55$, and $M_3 = 35$. Therefore, by Euclidean Algorithm we can find u_j and v_j , for $j = 1, 2, 3$ such that:

$$77u_1 + 5v_1 = 1;$$

$$55u_2 + 7v_2 = 1,$$

$$35u_3 + 11v_3 = 1.$$

Solving the three equations, we get:

$$77 \cdot (-2) + 5 \cdot 31 = 1,$$

$$55 \cdot (-1) + 7 \cdot 8 = 1,$$

$$35 \cdot 6 + 11 \cdot (-19) = 1.$$

Hence, $s'' = 77 \cdot (-2) \cdot s_1 + 55 \cdot (-1) \cdot s_2 + 35 \cdot 6 \cdot s_3 = 831 \bmod 385 = 61 \bmod 385$.

Consequently, the secret s would be $s = 61 \bmod 2 = 1 \bmod 2$. So the secret s is 1.

Scheme 2

This secret-sharing scheme is almost similar to scheme 1, but it deals with polynomials.

Let F be a finite field and $m_i(x)$, $i = 1, \dots, t$ be t pairwise relatively prime polynomials of $F[x]$ with degree greater or equal to 1. Then

$$\min[k] = \min\{\deg(m_{i_1}m_{i_2}\cdots m_{i_k}) \mid 1 \leq i_1 < \cdots < i_k < t\},$$

$$\max[k-1] = \max\{\deg(m_{i_1}m_{i_2}\cdots m_{i_{k-1}}) \mid 1 \leq i_1 < \cdots < i_{k-1} < t\},$$

where $1 < k \leq t$. Let w be the largest positive integer such that

- there is a polynomial $W(x)$ of degree w over F with $(W(x), m_i(x)) = 1$ for $i = 1, 2, \dots, t$; and
- $w \leq \frac{\min[k]}{\max[k-1]}$.

The secret is a polynomial $s(x)$ in $F[x]$ of degree less than w . The shares for t parties are computed as follows.

Choose $a(x) \in F[x]$ such that $\deg(s(x) + a(x)W(x)) < \min[k]$. Let $s'(x) = s(x) + a(x)w(x)$. The shares are then given by $s_i(x) = s'(x) \bmod m_i$, $i = 1, 2, \dots, t$. Therefore, (k, t) is a threshold scheme.

Suppose k shares $s_1(x), s_2(x), \dots, s_k(x)$ are given. Let $M(x) = \prod_{i=1}^k m_i(x)$, and $M_j(x) = \frac{M(x)}{m_j(x)}$ for $j = 1, \dots, k$. Then $M_j(x)$ and $m_j(x)$ are relatively prime. By Euclidean Algorithm, there exist two polynomials $u_j(x)$ and $v_j(x)$ in $F[x]$ such that $M_j(x)u_j(x) + m_j(x)v_j(x) = 1$. By the Chinese Remainder Algorithm, we have $s'(x) = \sum_{j=1}^k M_j(x)u_j(x)s_j(x) \bmod M(x)$. Then the secret is given by $s(x) = s'(x) \bmod W(x)$.

Chapter 5

Conclusion

In this short manuscript, we have shown some expansion and powerful applications of the Chinese Remainder Theorem. It is amazing to see how the theorem evolved from the three basic problems of calendar, wall-building, and soldier-counting. Even though the theorem, first generated as a problem, is taken credit from the Chinese scholars, it was quite well-known in other parts of the world. Many other mathematicians were also trying to solve similar problem

Here we discuss the applications of the theorem to finite sequence of integers, Dedekind domains, and briefly cryptography. However, the Chinese Remainder Theorem is widely applied in other areas such as computing, and codes. We hope readers find this topic interesting enough to pursue further research on those areas.

Bibliography

- [DPS96] C. Ding, D. Pei, and A. Salomaa. *Chinese remainder theorem, application in computing, coding, cryptography*. World Scientific Publishing Co., Singapore, 1996.
- [Gal06] Joseph A. Gallian. *Contemporary abstract algebra*. Houghton Mifflin, New York, sixth edition, 2006.
- [Hun74] Thomas W. Hungerford. *Algebra-graduate texts in mathematics*. Springer, New York, 1974.