THE NUMBER OF RING HOMOMORPHISMS FROM $\mathbb{Z}_n$ to $\mathbb{Z}_n$

BY

JORDINAH N. WEKESA

I56/CE/33030/2014

DEPT: MATHEMATICS

A Project Report Submitted in Partial Fulfillment of the Requirements for the Award of the Degree of Masters of Science (Pure Mathematics) in the School of Pure and Applied Sciences of Kenyatta University.

NOVEMBER, 2018
DECLARATION
This project is my original work and has never been published or presented by anyone in any other university or institution for any award.

Signature……………………… Date……………………………………

Name: Jordinah N. Wekesa

I56/CE/33030/2014

This project has been submitted for examination with my approval as university supervisor.

Signature……………………… Date……………………………………

Dr. Benard Kivunge

Department of Mathematics

Kenyatta University
DEDICATION

I dedicate this work with love and affection to my lovely children Cyril Wekesa and Norah Natasha.
ACKNOWLEDGEMENTS

There are groups of people whom I owe gratitude for their contribution and support which made this work a success. To start with, I thank the Almighty for His guidance throughout the study. I am particularly grateful to my supervisor Dr. Benard Kivunge for his invaluable support and contribution to this scholarly work. He spared his time and energy to prepare me for this academic endeavor.

My gratitude also goes to my parents, my father the late Stephen Wekesa and my mother Rosemary Ann Wekesa for taking me to school. Their plans, efforts and hard work have made me reach this higher level of education. They invested a lot and made me whom I am. May God bless them. In addition, I owe gratitude to my brother Dr. Wasike who paid my fees after the demise of my father. Indeed he played the role of a parent in the absence of my father.

Finally, I am grateful to my course mates Florence Ngugi, David Otwisa, Fredrick Sanya, Linah Grace, Fridah Mwendwa and staff mates Zipporah Siwatum and Simiyu Anthony who despite them being true friends, their moral support and encouragement have helped me to go through the entire program.
TABLE OF CONTENTS

DECLARATION .............................................................................................................................. ii
DEDICATION ............................................................................................................................... iii
ACKNOWLEDGEMENTS ........................................................................................................ iv
TABLE OF CONTENTS ........................................................................................................... v
LIST OF TABLES ..................................................................................................................... vii
NOTATIONS ........................................................................................................................... viii
ABSTRACT ............................................................................................................................... ix

CHAPTER ONE ......................................................................................................................... 1
INTRODUCTION ...................................................................................................................... 1
1.1 Rings .................................................................................................................................. 1
1.2 Ideals ................................................................................................................................. 3
1.3 Homomorphisms ............................................................................................................ 4
1.4 Statement of the problem ............................................................................................... 4
1.5 Objective ........................................................................................................................ 5

CHAPTER TWO ....................................................................................................................... 6
LITERATURE REVIEW ........................................................................................................... 6

CHAPTER THREE .................................................................................................................... 9
FINDING THE NUMBER OF IDEALS IN $\mathbb{Z}_n$ ................................................................... 9
3.1 Theorem .......................................................................................................................... 9
3.2 The Euler’s Phi function .............................................................................................. 9
3.3 The number of coprime numbers in $\mathbb{Z}_n$ ............................................................. 10
3.4 The number of divisors of $\mathbb{Z}_n$ ............................................................................. 10
3.5 The number of ideals in $\mathbb{Z}_n$ ................................................................................ 12
CHAPTER FOUR ................................................................. 18

RING HOMOMORPHISM ...................................................... 18

4.1 Introduction ........................................................................ 18

4.2 Theories of Isomorphism ..................................................... 19

4.3 Homomorphism $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$, $n = 1, 2, 3, 4, 5, 6, \ldots$, 40 ........................................... 22

CHAPTER FIVE ........................................................................ 39

CONCLUSION AND RECOMMENDATIONS ............................ 39

5.1 Conclusions ........................................................................ 39

5.2 Recommendations ............................................................. 40

References .............................................................................. 41
LIST OF TABLES

Table 3.4.1 Summary of the number of divisors of \( \mathbb{Z}_n \) ............................................. 11

Table 3.5.1 The relationship between number of ideals and number of divisors of \( \mathbb{Z}_n \) .......................................................................................................................... 16

Table 4.3.1: The relationship between the number of ideals in \( \mathbb{Z}_n \) and the number of homomorphisms of \( \mathbb{Z}_n \) .......................................................................................................................... 37
**NOTATIONS**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R[x]$</td>
<td>A polynomial ring</td>
</tr>
<tr>
<td>$\langle R, +, \cdot \rangle$</td>
<td>A ring</td>
</tr>
<tr>
<td>$\epsilon$</td>
<td>Element of</td>
</tr>
<tr>
<td>$\forall$</td>
<td>For all</td>
</tr>
<tr>
<td>$E(n)$</td>
<td>Idempotent elements in $\mathbb{Z}_n$</td>
</tr>
<tr>
<td>$1_R$</td>
<td>Identity in a ring $R$</td>
</tr>
<tr>
<td>$\text{Im}(\phi)$</td>
<td>Image of homomorphism $\phi$</td>
</tr>
<tr>
<td>$\mathbb{Z}$</td>
<td>Integers</td>
</tr>
<tr>
<td>$\mathbb{Z}_n$</td>
<td>Integers modulo $n$</td>
</tr>
<tr>
<td>$\cong$</td>
<td>Isomorphic</td>
</tr>
<tr>
<td>$\text{ker}(\phi)$</td>
<td>Kernel of homomorphism $\phi$</td>
</tr>
<tr>
<td>$\sigma(n)$</td>
<td>Number of idempotent elements in $\mathbb{Z}_n$</td>
</tr>
<tr>
<td>$\phi(n)$</td>
<td>Positive integers coprime to $n$</td>
</tr>
<tr>
<td>$\mathbb{R}$</td>
<td>Real numbers</td>
</tr>
<tr>
<td>$\langle n \rangle$</td>
<td>Subring generated by $n$</td>
</tr>
</tbody>
</table>
ABSTRACT

This research deals with determining the number of homomorphism \( \phi : \mathbb{Z}_n \to \mathbb{Z}_n \), an aspect that seems to have been left open for many years. Several researches on the number of ring homomorphisms have been conducted and results published except for \( \phi : \mathbb{Z}_n \to \mathbb{Z}_n \). First, we considered the number of divisors of \( \mathbb{Z}_n \) using the Euler’s phi function, which are the generators of ideals. We then determined the number of ideals in \( \mathbb{Z}_n \), as all kernels of homomorphism are ideals. We determined the number of homomorphisms \( \phi : \mathbb{Z}_n \to \mathbb{Z}_n \) by finding the elements \( m \in \mathbb{Z}_n \), such that \( m^2 \equiv m \mod n \). A particular case of determining the number of homomorphisms \( \phi_m : \mathbb{Z}_n \to \mathbb{Z}_n \), for \( n = 2, 3, 4, \ldots, 40 \) has been given, from which conclusions were drawn and presented in form of theorems. It was deduced that the number of homomorphisms \( \phi : \mathbb{Z}_n \to \mathbb{Z}_n \) from \( \mathbb{Z}_n \) to \( \mathbb{Z}_n \) is equal to the number of idempotent elements in \( \mathbb{Z}_n \).

Finally, a generalization of the formula for finding the number of homomorphisms \( \phi : \mathbb{Z}_n \to \mathbb{Z}_n \) from \( \mathbb{Z}_n \) to \( \mathbb{Z}_n \) is given by:

\[
\sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2})\sigma(p_3^{k_3})\ldots \sigma(p_m^{k_m}) = \prod_{\text{primes} \ p} \left( \frac{p^{k+1}-1}{p-1} \right) = 2^m \text{ thus there are } 2^m \text{ homomorphisms } \phi_m : \mathbb{Z}_n \to \mathbb{Z}_n \text{, where } p_1, p_2, p_3, \ldots, p_m \text{ are distinct primes and } k_1, k_2, k_3, \ldots, k_m \in \mathbb{Z}_n.
\]
CHAPTER ONE

INTRODUCTION
This chapter gives the background information of the study. To start with, it gives an introduction by defining a ring, an ideal and homomorphism. Categories of rings, ideals and homomorphisms are also given as definitions. Lastly, the statement of the problem has been stated as well as the objective of the study.

1.1 Rings

Definition 1.1.1 According to Rotman and Joseph (2006), a ring $R$ is a triple $(R, +, \cdot)$ consisting of a non-empty set $R$ together with two binary operations of addition and multiplication such that,

I. $\langle R, + \rangle$ is an abelian group.

II. Multiplication is associative i.e $\forall a, b, c \in R$, $a(bc) = (ab)c$.

III. Multiplication is distributive i.e $\forall a, b, c \in R$, $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$. The left and right distributive laws respectively.

Definition 1.1.2 A commutative ring is a ring $R$ in which $\forall a, b \in R$, $ab = ba$.

Definition 1.1.3 A division ring is a ring $R$ with identity and every non zero element is a unit. A unit is an element $r \in R$ that is invertible.
Definition 1.1.4 A field is a commutative ring with identity in which every non zero element is a unit.

Definition 1.1.5 An integral domain is a commutative ring with identity and no zero divisors.

Definition 1.1.6 A Boolean ring is a ring $R$ in which $\forall a \in R, a^2 = a$.

Definition 1.1.7 Principal Ideal ring is a ring in which every ideal is a principal ideal.

Definition 1.1.8 Principal ideal domain is a principal ideal ring which is an integral domain.

Definition 1.1.9 Let $R$ be a ring and $I$ an ideal of $R$, $R/I = \{ a + I, a \in R \}$ is a quotient ring where addition and multiplication is defined by, $(a + I) + (b + I) = (a + b) + I$, $(a + I)(b + I) = (ab) + I$.

If $R$ is commutative then, $R/I$ is commutative. If $R$ is a ring with unity, $R/I$ is a ring with unity, Musili (1994).

Definition 1.1.10

Let $R$ be a ring. If there is a least positive integer $n$ such that $na = 0, \forall a \in R$, then $R$ is said to have characteristic $n$. If no such $n$ exists, then $R$ is said to have characteristic zero.

Theorem 1.1.11

Let $R$ be a ring with identity $I$, and character $n > 0$. 
If \( \phi : \mathbb{Z} \to R \) is the map given by \( m \to ml_R \), then \( \phi \) is a homomorphism of rings with kernel \( \langle n \rangle = \{ kn \mid k \in \mathbb{Z} \} = n\mathbb{Z} \) is the least positive integer such that \( nl_R = 0 \). \( \phi \) is a homomorphism if and only if \( m^2 = m \).

If \( R \) has no zero divisors (integral domain) then \( n \) is prime.

**Definition 1.1.12** A ring \( R \) is said to be Neotherian iff \( R \) satisfies the maximum condition of an ideal or iff every ideal of \( R \) is finitely generated i.e. two sided.

**Theorem 1.1.13**

If \( f : A \to B \) has a left and right inverse \( g \) and \( h \) respectively, then, \( g = gI_R = g(fh) \)

\( (gf)h = I_A h = h \). Thus the map \( g \) is called a two sided inverse of \( f \).

### 1.2 Ideals

**Definition 1.2.1** An ideal of a ring \( R \) is a subring \( I \) such that \( \forall r \in R \) and \( a \in I \), \( ar, ra \in I \). It is a left (right) ideal if \( ra \in I (ar \in I) \) for all \( r \in R, a \in I \)

**Definition 1.2.2** A Proper ideal is an ideal \( I \neq \{0_R \} \) or \( I \neq R \). A proper ideal does not contain any unit in \( R \). If \( u \in I \) is a unit, \( uu^{-1} = 1_R \in R \) and \( \forall r \in R, 1_R r = r \in I \) which means \( I = R \).

**Definition 1.2.3** A prime ideal is an ideal \( I \) of a ring \( R \) such that, for any other ideals of \( R \), say \( J \) and \( P \), then \( JP \subseteq I \), meaning either \( J \subseteq I \) or \( P \subseteq I \). If \( a \in J \) and \( b \in P \), then, \( ab \in I, a \in I \) or \( b \in I \).

**Definition 1.2.4** Maximal ideal \( I \) of a ring \( R \) is an ideal that is not properly contained in any other ideal of \( R \). If \( J \) is another ideal of \( R \), then \( J \subseteq I \subseteq R \), \( J = I \) or \( I = J \).
**Definition 1.2.5** A principal ideal is an ideal generated by a single element.

### 1.3 Homomorphisms

**Definition 1.3.1** Let $R$ and $S$ be rings, a ring homomorphism is a mapping $\phi : R \rightarrow S$ such that $\forall r_1, r_2 \in R, \phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ and $\phi(r_1r_2) = \phi(r_1)\phi(r_2)$.

A monomorphism is a homomorphism that is injective (one to one) and its kernel $\{0_R\}$ is $\{ e \}$.

An epimorphism is a homomorphism that is surjective (onto).

An isomorphism is a bijective homomorphism (both one to one and onto).

An endomorphism is a homomorphism from a ring $R$ into a ring itself $\phi : R \rightarrow R$.

The kernel of a homomorphism $\phi : R \rightarrow S$, denoted $\ker \phi$ is the set of elements of $R$ mapped onto the identity element of $S$ by $\phi$, John (1984).

### 1.4 Statement of the problem

Finding the number of homomorphisms in rings has been a major problem over years. This is evident from the studies that have been carried out in the past. Citing an example of Samuel (2013) who studied on how to find the number of homomorphisms from $\mathbb{Z}[x] \rightarrow \mathbb{Z}_n$, his results are not very clear hence cryptic for someone to follow. This is also the case with Einstein (2004) who dealt with finding the number of homomorphisms from a finite field into a ring. Holt and Ischwied also studied this problem in 2014 and concluded that there is not a uniform answer for all pairs of fields and rings but it depends on what one wants to deduce from the homomorphism.
Despite the efforts done, there is no publication on finding the number of homomorphisms from $\mathbb{Z}_n$ into $\mathbb{Z}_n$, which should be the base of finding the number of automorphisms in the ring $\mathbb{Z}_n$.

As such, this study determines the number of homomorphisms from $\mathbb{Z}_n$ into $\mathbb{Z}_n$.

1.5 Objective

1.5.1 General objective

The objective of the study is to find the number of homomorphism $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$.

1.5.2 Specific objectives

1. Finding the number of homomorphism $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ for $n = 2, 3, 4, 5, .................. 40$.

2. Determine the values of $m \in \mathbb{Z}_n$ for which $\phi_m : \mathbb{Z}_n \to \mathbb{Z}_n$ such that $m^2 = m \mod n$. 
CHAPTER TWO
LITERATURE REVIEW

This section considers the studies that have already been done on the number of homomorphisms of given rings. It gives the studies on the number of homomorphisms from $\mathbb{Z}_m$ to $\mathbb{Z}_n$, the number of homomorphisms from a finite field to a ring and lastly the number of homomorphisms from $\mathbb{Z}[x]$ to $\mathbb{Z}_n$

According to Galian and Buskirk (1984), a ring homomorphism $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ is uniquely determined by the conditions: $m f(1) = 0$ and $f(m) = f(1)$. They stated that in order to find how many ring homomorphisms are there in $\mathbb{Z}_m$ into $\mathbb{Z}_n$, one has to count the number of elements of the set $\{ e \in \mathbb{Z}_n : e^2 = e, me = 0 \}$

If $r \equiv k \pmod{m}$ where $0 \leq k \leq m$, then $r = mt + k$ for some $t \in \mathbb{Z}$. If $f$ is a ring homomorphism $f(r) = f(mt + k)$

$er = emt + ek$. So $emt = 0$, $em = me = 0$ and $er = ek$

Again $f(r_1 r_2) = f(r_1)f(r_2)$. $er_1 r_2 = (er_1)(er_2) = e^2 r_1 r_2$ and $e = e^2$, i.e. $e$ is idempotent.

For $me = ne = 0 \pmod{n}$ and we only check for $e^2 = e$.

Example

To determine the number of homomorphisms in:

1. $f : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{28}$

We have $m = 12$, $n = 28$, $e \in \mathbb{Z}_{28}, 0 = me = 12e$ in $\mathbb{Z}_{28}$. Iff $28|12e$ iff $7|e$

So, $f(1) \in \{0,7,14,21\}$. Only 0 and 21 are idempotent in $\mathbb{Z}_{28}$. Thus there are
2 homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{28}$

Alternatively, $e \in \mathbb{Z}_{28}$ whose idempotent elements are $\{0, 1, 8, 21\}$. Thus $e \in \{0, 1, 8, 21\}$

$me = 0$. $e = \{0, 8\}$ thus there are 2 homomorphisms in $f : \mathbb{Z}_{12} \to \mathbb{Z}_{28}$.

2. $f : \mathbb{Z}_{12} \to \mathbb{Z}_{30}$

$m = 12$, $n = 30$. $e \in \mathbb{Z}_{30}$ whose idempotent elements are $\{0, 1, 6, 10, 15, 16, 21, 25\}$

$me = 0$, $e = \{0, 10, 15, 25\}$. Thus there are 4 homomorphisms in $f : \mathbb{Z}_{12} \to \mathbb{Z}_{30}$

3. $f : \mathbb{Z}_{16} \to \mathbb{Z}_{20}$

$m = 16$, $n = 20$. Idempotent elements of $\mathbb{Z}_{20}$ are $\{0, 1, 5, 16\}$, $e \in \{0, 1, 5, 16\}$

$me = 0$, $e = \{0, 5\}$. Thus there are 2 homomorphisms in $f : \mathbb{Z}_{16} \to \mathbb{Z}_{20}$

Einstein (2004) on the other hand dealt with finding the number of homomorphisms from a finite field into a ring $\mathbb{Z}_n$. He stated that the only kernels of a ring homomorphism

$\phi : F \to R$ are 0 and $F$ itself, hence there are 2 homomorphisms i.e. 0 map and the identity map. He goes on to explain that they may be less than 2 e.g. in the case where $F = F^2$ and $R$ has an odd order. He further states that they may be more than 2 e.g. in the case where $F$ alone already has a few automorphisms or $R$ contains several copies of $F$.

Holt and Ischwieb (2014) states that there can just be the trivial homomorphisms as is the case in $F^3 \to \mathbb{Z}$, or there could be many ring homomorphisms as it is the case with
They then concluded that there is not a uniform answer for all pairs of fields and rings but it depends on what one wants to get from the homomorphism.

Samuel (2013) states that, if 1 is mapped onto 1, we can evoke the fact that $\mathbb{Z}[x]$ is the free commutative ring with unity on the set $[x]$ and $x$ can be sent to anything. He cited $\mathbb{Z}[x] \rightarrow \mathbb{Z}_{12}$ as an example, where he stated that there are 12 possible homomorphisms with 1 mapped to 1. However, he says that there exists a homomorphism where 1 is not mapped to 1. The important thing is that $f(1)f(x) = f(x)$. If $f(1) = 0$, then $f(x) = 0$.

He concluded that if $f(1) = 4$, $f(x) = 8$ and if $f(1) = 9$, then $f(x) = 0, 3, 6$ or 9. Thus, there are 8 additional possible homomorphisms. To get this, he stated that one has to find the values of $y$ such that $f(1)y = y$. 

$F^2 \rightarrow \prod_{i=1}^{\infty} F^2$. 
CHAPTER THREE

FINDING THE NUMBER OF IDEALS IN $\mathbb{Z}_n$

Introduction

This chapter aims to find the number of ideals in $\mathbb{Z}_n$. To start with, we will give the number of coprime numbers in $\mathbb{Z}_n$, then the number of divisors of $\mathbb{Z}_n$, and finally the number of ideals in $\mathbb{Z}_n$ using the Euler’s phi function. We then conclude by giving the relationship between the number of ideals and the number of divisors of $\mathbb{Z}_n$.

3.1 Theorem

Let $I_\alpha = \{f(x) | f(\alpha) = 0\}$ for $\alpha \in R$, then $I_\alpha$ is an ideal of $R[x]$. 

Proof

If $f(\alpha), g(\alpha) \in I_\alpha$, $f(\alpha) = g(\alpha) = 0$, $f(\alpha) + g(\alpha) = 0 + 0 = 0$ and $f(x) + g(x) \in I_\alpha$.

For $f(x) \in I_\alpha$ and $p(x) \in R[x]$, $f(\alpha)p(\alpha) = 0p(\alpha) = 0$ so $f(\alpha)p(\alpha) \in I_\alpha$. This shows that $I_\alpha$ is an ideal in $R[x]$.

3.2 The Euler’s Phi function

The Euler’s phi function, $\phi(n)$, also called Euler’s totient function, is the number of positive integers not greater than $n$ and relatively prime to $n$. $\phi(n) = (a, n) = 1$.

i.e. $\phi(n)$ is the number of positive integers $m$ coprime to $n$ such that $1 \leq m \leq n$.

Examples

$\phi(2) = 1$. i.e. 1

$\phi(4) = 2$. i.e. 1, 3

$\phi(12) = 4$. i.e. 1, 5, 7, 11

$\phi(15) = 8$. i.e. 1, 2, 4, 7, 8, 11, 13, 14
3.3 The number of coprime numbers in $\mathbb{Z}_n$

Case 1

If $n$ is prime, then $\varphi(n) = n - 1$ e.g. $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(5) = 4$, $\varphi(7) = 6$.

Case 2

If $n = p_1^{m_1} p_2^{m_2} p_3^{m_3} \ldots p_k^{m_k}$, then,

$$\varphi(n) = n \times \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) \times \left(1 - \frac{1}{p_3}\right) \times \ldots \times \left(1 - \frac{1}{p_k}\right)$$

Examples, $\varphi(30) = 8$, $\varphi(42) = 12$, $\varphi(105) = 48$, $\varphi(165) = 80$, $\varphi(385) = 240$

Case 3

If $n$ is a prime and $k$ is a positive integer, then $\varphi(n^k) = n^k - n^{k-1}$

Examples

$$\varphi(2^3) = 2^3 - 2^{3-1} = 8 - 4 = 4$$
$$\varphi(2^4) = 2^4 - 2^{4-1} = 8$$
$$\varphi(3^2) = 3^2 - 3^{2-1} = 6$$

Case 4

If $n = mk$, where $m$ and $k$ are relatively prime, then $\varphi(n) = \varphi(m) \varphi(k)$.

Examples

$$\varphi(6) = \varphi(2) \varphi(3) = (2 - 1)(3 - 1) = 1 \times 2 = 2$$
$$\varphi(10) = \varphi(2) \varphi(5) = (2 - 1)(5 - 1) = 1 \times 4 = 4$$
$$\varphi(200) = \varphi(25) \varphi(8) = \varphi(5^2) \varphi(2^3) = (5^2 - 5^1)(2^3 - 2^{3-1}) = 20 \times 4 = 80$$

3.4 The number of divisors of $\mathbb{Z}_n$

Let $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots p_m^{k_m}$, then the number of divisors is given by

$$(k_1 + 1)(k_2 + 1)(k_3 + 1)\ldots(k_m + 1).$$
Examples

\[ \varphi(2) = \varphi(2^1) = (1 + 1) = 2 \]

\[ \varphi(6) = \varphi(2^1 \times 3^1) = (1+1)(1+1) = 2 \times 2 = 4 \]

\[ \varphi(9) = \varphi(3^2) = (2 + 1) = 3 \]

\[ \varphi(12) = \varphi(2^2 \times 3^1) = (2 + 1)(1 + 1) = 6 \]

\[ \varphi(30) = \varphi(2 \times 3 \times 5) = (1 + 1)(1+1)(1+1) = 8 \]

Table 3.4.1 Summary of the number of divisors of \( \mathbb{Z}_n \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>Formula</th>
<th>No. of Divisors</th>
<th>Divisors</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>( \varphi(2^1) = 1 + 1 )</td>
<td>2</td>
<td>1,2</td>
</tr>
<tr>
<td>3</td>
<td>( \varphi(3^1) = 1 + 1 )</td>
<td>2</td>
<td>1,3</td>
</tr>
<tr>
<td>4</td>
<td>( \varphi(2^2) = 2 + 1 )</td>
<td>3</td>
<td>1,2,4</td>
</tr>
<tr>
<td>5</td>
<td>( \varphi(5^1) = 1 + 1 )</td>
<td>2</td>
<td>1,5</td>
</tr>
<tr>
<td>6</td>
<td>( \varphi(2^1) \varphi(3^1) = (1+1)(1+1) )</td>
<td>4</td>
<td>1,2,3,6</td>
</tr>
<tr>
<td>7</td>
<td>( \varphi(7^1) = 1 + 1 )</td>
<td>2</td>
<td>1,7</td>
</tr>
<tr>
<td>8</td>
<td>( \varphi(2^3) = 3 + 1 )</td>
<td>4</td>
<td>1,2,4,8</td>
</tr>
<tr>
<td>9</td>
<td>( \varphi(3^2) = 2 + 1 )</td>
<td>3</td>
<td>1,3,9</td>
</tr>
<tr>
<td>10</td>
<td>( \varphi(2^1) \varphi(5^1) = (1+1)(1+1) )</td>
<td>4</td>
<td>1,2,5,10</td>
</tr>
<tr>
<td>11</td>
<td>( \varphi(11^1) = 1 + 1 )</td>
<td>2</td>
<td>1,11</td>
</tr>
<tr>
<td>12</td>
<td>( \varphi(2^2) \varphi(3^1) = (2 + 1)(1 + 1) )</td>
<td>6</td>
<td>1,2,3,4,6,12</td>
</tr>
<tr>
<td>( n )</td>
<td>( \varphi(p_1^{k_1}) \varphi(p_2^{k_2}) \varphi(p_3^{k_3}) \cdots \varphi(p_m^{k_m}) )</td>
<td>( (k_1 + 1)(k_2 + 1)(k_3 + 1) \cdots (k_m + 1) )</td>
<td></td>
</tr>
</tbody>
</table>
3.5 The number of ideals in \( \mathbb{Z}_n \)

This section gives the number of ideals in \( \mathbb{Z}_n \) for \( 2 \leq n \leq 20 \), using the divisors of \( n \).

\( \mathbb{Z}_2 = \{0,1\} \)

\( \langle 0 \rangle = \{0\} \)

\( \langle 1 \rangle = \{0,1\} \)

\( \mathbb{Z}_3 = \{0,1,2\} \)

\( \langle 0 \rangle = \{0\} \)

\( \langle 1 \rangle = \{0,1,2\} = \langle 2 \rangle \)

\( \mathbb{Z}_4 = \{0,1,2,3\} \)

\( \langle 0 \rangle = \{0\} \)

\( \langle 1 \rangle = \{0,1,2,3\} = \langle 3 \rangle \)

\( \langle 2 \rangle = \{0,2\} \)

\( \mathbb{Z}_5 = \{0,1,2,3,4\} \)

\( \langle 0 \rangle = \{0\} \)

\( \langle 1 \rangle = \{0,1,2,3,4\} = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle \)

\( \mathbb{Z}_6 = \{0,1,2,3,4,5\} \)

\( \langle 0 \rangle = \{0\} \)

\( \langle 1 \rangle = \{0,1,2,3,4,5\} = \langle 5 \rangle \)

\( \langle 2 \rangle = \{0,2,4\} = \langle 4 \rangle \)

\( \langle 3 \rangle = \{0,3\} \)

\( \mathbb{Z}_7 = \{0,1,2,3,4,5,6\} \)

\( \langle 0 \rangle = \{0\} \)

\( \langle 1 \rangle = \{0,1,2,3,4,5,6\} = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 6 \rangle \)
\[ \mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\} \]
\[
\langle 0 \rangle = \{0\}
\]
\[
\langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7\} = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle
\]
\[
\langle 2 \rangle = \{0, 2, 4, 6\} = \langle 6 \rangle
\]
\[
\langle 4 \rangle = \{0, 4\}
\]
\[ \mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\} \]
\[
\langle 0 \rangle = \{0\}
\]
\[
\langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8\} = \langle 2 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 8 \rangle
\]
\[
\langle 3 \rangle = \{0, 3\} = \langle 6 \rangle
\]
\[ \mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \]
\[
\langle 0 \rangle = \{0\}
\]
\[
\langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle
\]
\[
\langle 2 \rangle = \{0, 2, 4, 6, 8, 1\} = \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle
\]
\[
\langle 5 \rangle = \{0, 5\}
\]
\[ \mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \]
\[
\langle 0 \rangle = \{0\}
\]
\[
\langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 6 \rangle = \langle 7 \rangle = \langle 8 \rangle = \langle 9 \rangle = \langle 10 \rangle
\]
\[ \mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} \]
\[
\langle 0 \rangle = \{0\}
\]
\[
\langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle
\]
\[
\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\} = \langle 10 \rangle
\]
\[
\langle 3 \rangle = \{0, 3, 6, 9\} = \langle 9 \rangle
\]
\[
\langle 4 \rangle = \{0, 4, 8\} = \langle 8 \rangle
\]
\[
\langle 6 \rangle = \{0, 6\}
\]
$\mathbb{Z}_{13} = \{0,1,2,3,4,5,6,7,8,9,10,11,12\}$

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{0,1,2,3,4,5,6,7,8,9,10,11,12\} = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 6 \rangle = \langle 7 \rangle = \langle 8 \rangle = \langle 9 \rangle = \langle 10 \rangle = \langle 11 \rangle = \langle 12 \rangle$

$\mathbb{Z}_{14} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13\}$

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13\} = \langle 3 \rangle = \langle 5 \rangle = \langle 9 \rangle = \langle 11 \rangle = \langle 13 \rangle$

$\langle 2 \rangle = \{0,2,4,6,8,10,12\} = \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle = \langle 10 \rangle = \langle 12 \rangle$

$\langle 7 \rangle = \{0,7\}$

$\mathbb{Z}_{15} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14\}$

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14\} = \langle 2 \rangle = \langle 4 \rangle = \langle 7 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 14 \rangle$

$\langle 3 \rangle = \{0,3,6,9,12\} = \langle 6 \rangle = \langle 9 \rangle = \langle 12 \rangle$

$\langle 5 \rangle = \{0,5,10\} = \langle 10 \rangle$

$\mathbb{Z}_{16} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\} = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 9 \rangle = \langle 11 \rangle = \langle 13 \rangle$

$= \langle 15 \rangle$

$\langle 2 \rangle = \{0,2,4,6,8,10,12,14\} = \langle 6 \rangle = \langle 10 \rangle = \langle 14 \rangle$

$\langle 4 \rangle = \{0,4,8,12\} = \langle 12 \rangle$

$\langle 8 \rangle = \{0,8\}$
$\mathbb{Z}_{17} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}$

\[
\{0\} = \{0\}
\]

\[
\langle 1 \rangle = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\} = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 6 \rangle = \langle 7 \rangle = \langle 8 \rangle = \langle 9 \rangle = \langle 10 \rangle = \langle 11 \rangle = \langle 12 \rangle = \langle 13 \rangle = \langle 14 \rangle = \langle 15 \rangle = \langle 16 \rangle
\]

$\mathbb{Z}_{18} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17\}$

\[
\{0\} = \{0\}
\]

\[
\langle 1 \rangle = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17\} = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle
\]

\[
\langle 2 \rangle = \{0,2,4,6,8,10,12,14,16\} = \langle 4 \rangle = \langle 8 \rangle = \langle 10 \rangle = \langle 14 \rangle = \langle 16 \rangle
\]

\[
\langle 3 \rangle = \{0,3,6,9,12,15\} = \langle 15 \rangle
\]

\[
\langle 6 \rangle = \{0,6,12\} = \langle 12 \rangle
\]

\[
\langle 9 \rangle = \{0,9\}
\]

$\mathbb{Z}_{19} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18\}$

\[
\{0\} = \{0\}
\]

\[
\langle 1 \rangle = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18\} = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 6 \rangle = \langle 7 \rangle = \langle 8 \rangle = \langle 9 \rangle = \langle 10 \rangle = \langle 11 \rangle = \langle 12 \rangle = \langle 13 \rangle = \langle 14 \rangle = \langle 15 \rangle = \langle 16 \rangle = \langle 17 \rangle = \langle 18 \rangle
\]

$\mathbb{Z}_{20} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19\}$

\[
\{0\} = \{0\}
\]

\[
\langle 1 \rangle = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19\} = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle = \langle 19 \rangle
\]

\[
\langle 2 \rangle = \{0,2,4,6,8,10,12,14,16,18\} = \langle 6 \rangle = \langle 14 \rangle = \langle 18 \rangle
\]

\[
\langle 4 \rangle = \{0,4,8,12,16\} = \langle 8 \rangle = \langle 12 \rangle = \langle 16 \rangle
\]

\[
\langle 5 \rangle = \{0,5,10,15\} = \langle 15 \rangle
\]

\[
\langle 10 \rangle = \{0,10\}
\]
Table 3.5.1 The relationship between number of ideals and number of divisors of $\mathbb{Z}_n$

<table>
<thead>
<tr>
<th>$n$</th>
<th>Divisors</th>
<th>Number of Divisors</th>
<th>Ideals</th>
<th>Number of Ideals</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1,2</td>
<td>2</td>
<td>{0, 1}</td>
<td>\textbf{2}</td>
</tr>
<tr>
<td>3</td>
<td>1,3</td>
<td>2</td>
<td>{0, 1}</td>
<td>\textbf{2}</td>
</tr>
<tr>
<td>4</td>
<td>1,2,4</td>
<td>3</td>
<td>{0, 1, 2}</td>
<td>\textbf{3}</td>
</tr>
<tr>
<td>5</td>
<td>1,5</td>
<td>2</td>
<td>{0, 1}</td>
<td>\textbf{2}</td>
</tr>
<tr>
<td>6</td>
<td>1,2,3,6</td>
<td>4</td>
<td>{0, 1, 3, 6}</td>
<td>\textbf{4}</td>
</tr>
<tr>
<td>7</td>
<td>1,7</td>
<td>2</td>
<td>{0, 1}</td>
<td>\textbf{2}</td>
</tr>
<tr>
<td>8</td>
<td>1,2,4,8</td>
<td>4</td>
<td>{0, 1, 2, 4}</td>
<td>\textbf{4}</td>
</tr>
<tr>
<td>9</td>
<td>1,3,9</td>
<td>3</td>
<td>{0, 1, 3}</td>
<td>\textbf{3}</td>
</tr>
<tr>
<td>10</td>
<td>1,2,5,10</td>
<td>4</td>
<td>{0, 1, 2, 5}</td>
<td>\textbf{4}</td>
</tr>
<tr>
<td>11</td>
<td>1,11</td>
<td>2</td>
<td>{0, 1}</td>
<td>\textbf{2}</td>
</tr>
<tr>
<td>12</td>
<td>1,2,3,4,6,12</td>
<td>6</td>
<td>{0, 1, 2, 3, 4, 6}</td>
<td>\textbf{6}</td>
</tr>
<tr>
<td>13</td>
<td>1,13</td>
<td>2</td>
<td>{0, 1}</td>
<td>\textbf{2}</td>
</tr>
<tr>
<td>14</td>
<td>1,2,7,14</td>
<td>4</td>
<td>{0, 1, 2, 7}</td>
<td>\textbf{4}</td>
</tr>
<tr>
<td>15</td>
<td>1,3,5,15</td>
<td>4</td>
<td>{0, 1, 3, 5}</td>
<td>\textbf{4}</td>
</tr>
<tr>
<td>16</td>
<td>1,2,4,8,16</td>
<td>5</td>
<td>{0, 1, 2, 4, 8}</td>
<td>\textbf{5}</td>
</tr>
<tr>
<td>17</td>
<td>1,17</td>
<td>2</td>
<td>{0, 1}</td>
<td>\textbf{2}</td>
</tr>
<tr>
<td>18</td>
<td>1,2,3,6,9,18</td>
<td>6</td>
<td>{0, 1, 2, 3, 6, 9}</td>
<td>\textbf{6}</td>
</tr>
<tr>
<td>19</td>
<td>1,19</td>
<td>2</td>
<td>{0, 1}</td>
<td>\textbf{2}</td>
</tr>
<tr>
<td>20</td>
<td>1,2,4,5,10,20</td>
<td>6</td>
<td>{0, 1, 2, 4, 5, 10}</td>
<td>\textbf{6}</td>
</tr>
</tbody>
</table>
From Table 3.5.1, we observe that,

Divisors are the generators of ideals, i.e. every divisor generates an ideal.

The number of ideals is equal to number of divisors.

In general, the number of ideals in $\mathbb{Z}_n$ is obtained as follows.

If $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots \ldots p_m^{k_m}$, the number of ideals equals to

$$(k_1 + 1)(k_2 + 1)(k_3 + 1)\ldots(k_m + 1)$$
CHAPTER FOUR
RING HOMOMORPHISM

In this chapter, a detailed discussion on ring homomorphism is given. A few theorems on this topic, the kernel and image of homomorphisms will be captured. A specific case of finding the number of homomorphisms from $\phi_m: \mathbb{Z}_n \to \mathbb{Z}_n$, for $n = 2,3,4,...,40$ is given. The section ends by giving the formula for finding the number of homomorphism

$\phi_m: \mathbb{Z}_n \to \mathbb{Z}_n$, thus solving the problem of this study.

4.1 Introduction

4.1.1 Theorem

For any ring homomorphism $\phi: R \to S$, the ker $\phi$ is an ideal, Andarson (1995).

Proof

Let $r_1, r_2 \in \ker \phi$, $r \in R$, $\phi(r_1) = \phi(r_2) = 0$, $\phi(r_1 - r_2) = \phi(r_1) - \phi(r_2) = 0 - 0 = 0$ and $\phi(rr_1) = \phi(r)\phi(r_1) = \phi(r)0 = 0$. Thus $r_1 - r_2, rr_1, r, r \in \ker \phi$ and ker $\phi$ is an ideal.

4.1.2 Theorem

Faith (1981) states that, if $I$ is an ideal of $R$, then the map $\pi : R \to R/I$ denoted by $\pi(r) = r + 1$ is an epimorphism of rings with ker $\pi = 1$. 
Proof

Let \( r_1, r_2 \in R \), \( \pi: R \to R/I \), \( \pi(r_1) = r_1 + 1 \), \( \pi(r_2) = r_2 + 1 \) and \( \pi(r_1 + r_2) = \pi(r_1) + \pi(r_2) \).
\[ \pi(r_1r_2) = \pi(r_1)\pi(r_2) \]

4.1.3 Theorem

The only homomorphisms from \( \mathbb{Z} \to \mathbb{Z} \) are 0 and the identity homomorphism.

Proof

Let \( \phi: \mathbb{Z} \to \mathbb{Z} \) be a ring homomorphism. \( \phi(n) = \phi(n.1) = \phi(n)\phi(1) \forall n \in \mathbb{Z} \), meaning \( 1^2 = 1 \) (Idempotent).

Determine the idempotent elements of \( \mathbb{Z} \). Let \( m \in \mathbb{Z} \) such that \( m^2 = m \),
\[ m^2 - m = 0, \quad m(m - 1) = 0, \quad m = 0 \text{ or } m = 1. \]
\( \phi(n) \) being idempotent implies that \( \phi(1) = 0 \) or \( \phi(1) = 1 \). Thus the only homomorphisms from \( \mathbb{Z} \) to \( \mathbb{Z} \) are the zero map and the identity map, David (2010)

4.2 Theories of Isomorphism

4.2.1 The first isomorphism theorem

Let \( \phi: R \to S \) be a ring homomorphism, then, \( R/\ker{\phi} \cong \text{Im}{\phi} \), Thomas(1984)

Proof

We first show that \( \text{Im}{\phi} \) is a subring of \( S \).

Let \( s_1, s_2 \in \text{Im}{\phi} \). Then there exists \( r_1, r_2 \in R \) such that \( s_1 = \phi(r_1) \), \( s_2 = \phi(r_2) \). Then
\[ s_1 - s_2 = \phi(r_1) - \phi(r_2) = \phi(r_1 - r_2) \in \text{Im}{\phi} \text{ and } \text{Im}{\phi} \text{ is a subring of } S. \]
Define \( \pi : R / \ker \phi \to \text{Im} \phi \) by \( \pi(r + \ker \phi) = \phi(r) \). We show that \( \pi \) is well defined, a ring homomorphism and onto.

Let \( \phi(I + r) = \phi(r) \forall r \in R \). Let \( r_1 \) and \( r_2 \) be representation of the same cosets of \( I \), so that \( x_2 = (x_1 + r_1) \) for some \( r_1 \in I \), then \( \phi(x_2) = \phi(x_1 + r_1) = \phi(x_1) + \phi(r_1) = \phi(x_1) \).

Thus, \( \phi(1 + x_1) = \phi(1 + x_2) \) is well defined. We also show that \( \phi \) is a homomorphism.

\[
\phi(1 + (x + y)) = \phi(x + y) = \phi(x) + \phi(y) = \phi(1 + x)\phi(1 + y),
\]

\[
\phi(1 + xy) = \phi(xy) = \phi(x)\phi(y) = \phi(1 + x)\phi(1 + y),
\]

\( \phi \) is onto \( \text{Im} \phi \) since \( s \in \text{Im} \phi \).

\[ S = \phi(x) = \phi(1 + x) \]

Suppose, \( \phi(1 + x) = \phi(1 + y) \), then, \( \phi(x) = \phi(y)\phi(x) - \phi(y) = \phi(x - y) = 0 \). Thus \( \phi(x - y) \in \ker \phi \) and \( x, y \) represent the same coset of \( \ker \phi \).

4.2.2 The second isomorphism theorem

Let \( I \) be an ideal of \( R \). There is one to one correspondence between the set of subrings of \( R \) which contain \( I \) and the set of subrings of \( R / I \). Under this correspondence, ideals of \( R \) containing \( I \) corresponds to ideals of \( R / I \).

Proof

Let \( S \) be a subring of \( R \). If \( I \subseteq S \), and \( x \in S \), then \( (1 + x) \subseteq S \). \( I \) is an ideal of \( S \) since it is closed under subtraction. i.e. if \( r_1, r_2 \in I \), then \( r_1 - r_2 \in I \). But \( I \in S \). Thus, \( (r_1 - r_2) \in S \).
Thus, $S/I$ is the set of all cosets of $I$ in $S$ and is a subring of $R/I$.

Conversely, let $T$ be a subring of $R/I$. Then $T$ is a set of cosets of $I$, the union of these sets are a subset $P$ of $R$, which is easily seen to be a subring of $R$ containing $I$.

Hence we have one to one correspondences

4.2.3 The third isomorphism theorem

Let $I$ be an ideal of $R$ and $S$ a subring of $R$. Then,

$I + S = \{r_i + s : r_i \in I, s \in S\}$, is a subring of $R$ containing $I$.

$I \cap S$ is an ideal of $S$

$S/I \cap S \cong (I + S/I)$

Proof

Let $\phi_S$ be a restriction of $\phi$ to $S, \phi : S \to R/I, S\phi = \phi_S$

Clearly $\phi$ is a homomorphism. The two conditions in the definition holds for arbitrary elements of $P$ and certainly for all elements of $S$.

$\text{Im} (\phi)$ consists of all cosets $I + S$ for which the representative is in $S$. These forms a subring of $R/I$ by the first isomorphism theorem. The union of all these cosets is the set $\{r_i + s : r_i \in I, s \in S = I + S\}$ by the second isomorphism theorem;

So $I + S$ is a subring of $R$ which contains $I$. $\text{Im}(\phi) = (I + S/I)$
Ker (φ) consists of all elements of S mapped onto zero by φ. Since ker(φ) = I,

we have ker(φ) = I ∩ S which is an ideal of S by the first isomorphism theorem.

\[ \frac{S}{\ker(\phi)} \cong \text{Im}(\phi) \] that is \[ \frac{I}{I \cap S} \cong \frac{I + S}{I} \] by the second isomorphism theorem.

4.3 Homomorphism \( \phi : \mathbb{Z}_n \to \mathbb{Z}_n \), \( n = 1, 2, 3, 4, 5, 6, \ldots, 40 \)

To find the homomorphism \( \phi : \mathbb{Z}_n \to \mathbb{Z}_n \), we determine \( \phi_m \) where \( m \in \mathbb{Z}_n \) such that

\[ m^2 = m \pmod{n} \]. In this section, a case study for \( 2 \leq n \leq 40 \) has been given.

\( \mathbb{Z}_2 \to \mathbb{Z}_2 \)

\( \phi_0(\mathbb{Z}_2) = \{0\} \quad \ker(\phi_0) = \mathbb{Z}_2 \)

\( \phi_1(\mathbb{Z}_2) = \mathbb{Z}_2 \quad \ker(\phi_1) = \{0\} \)

\( \mathbb{Z}_3 \to \mathbb{Z}_3 \)

\( \phi_0(\mathbb{Z}_3) = \{0\} \quad \ker(\phi_0) = \mathbb{Z}_3 \)

\( \phi_1(\mathbb{Z}_3) = \mathbb{Z}_3 \quad \ker(\phi_1) = \{0\} \)

\( \mathbb{Z}_4 \to \mathbb{Z}_4 \)

\( \phi_0(\mathbb{Z}_4) = \{0\} \quad \ker(\phi_0) = \mathbb{Z}_4 \)

\( \phi_1(\mathbb{Z}_4) = \mathbb{Z}_4 \quad \ker(\phi_1) = \{0\} \)

\( \mathbb{Z}_5 \to \mathbb{Z}_5 \)

\( \phi_0(\mathbb{Z}_5) = \{0\} \quad \ker(\phi_0) = \mathbb{Z}_5 \)

\( \phi_1(\mathbb{Z}_5) = \mathbb{Z}_5 \quad \ker(\phi_1) = \{0\} \)
\( \mathbb{Z}_6 \rightarrow \mathbb{Z}_6 \)

\( \phi_0(\mathbb{Z}_6) = \{0\} \quad \operatorname{ker} (\phi_0) = \mathbb{Z}_6 \)

\( \phi_1(\mathbb{Z}_6) = \mathbb{Z}_6 \quad \operatorname{ker} (\phi_1) = \{0\} \)

\( \phi_3(\mathbb{Z}_6) = \{0,3\} \quad \operatorname{ker} (\phi_3) = \{0,2,4\} \)

\( \phi_4(\mathbb{Z}_6) = \{0,2,4\} \quad \operatorname{ker} (\phi_4) = \{0,3\} \)

\( \mathbb{Z}_7 \rightarrow \mathbb{Z}_7 \)

\( \phi_0(\mathbb{Z}_7) = \{0\} \quad \operatorname{ker} (\phi_0) = \mathbb{Z}_7 \)

\( \phi_1(\mathbb{Z}_7) = \mathbb{Z}_7 \quad \operatorname{ker} (\phi_1) = \{0\} \)

\( \mathbb{Z}_8 \rightarrow \mathbb{Z}_8 \)

\( \phi_0(\mathbb{Z}_8) = \{0\} \quad \operatorname{ker} (\phi_0) = \mathbb{Z}_8 \)

\( \phi_1(\mathbb{Z}_8) = \mathbb{Z}_8 \quad \operatorname{ker} (\phi_1) = \{0\} \)

\( \mathbb{Z}_9 \rightarrow \mathbb{Z}_9 \)

\( \phi_0(\mathbb{Z}_9) = \{0\} \quad \operatorname{ker} (\phi_0) = \mathbb{Z}_9 \)

\( \phi_1(\mathbb{Z}_9) = \mathbb{Z}_9 \quad \operatorname{ker} (\phi_1) = \{0\} \)

\( \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10} \)

\( \phi_0(\mathbb{Z}_{10}) = \{0\} \quad \operatorname{ker} (\phi_0) = \mathbb{Z}_{10} \)

\( \phi_1(\mathbb{Z}_{10}) = \mathbb{Z}_{10} \quad \operatorname{ker} (\phi_1) = \{0\} \)

\( \phi_3(\mathbb{Z}_{10}) = \{0,5\} \quad \operatorname{ker} (\phi_3) = \{0,2,4,6,8\} \)

\( \phi_6(\mathbb{Z}_{10}) = \{0,2,4,6,8\} \quad \operatorname{ker} (\phi_6) = \{0,5\} \)
$\mathbb{Z}_{11} \rightarrow \mathbb{Z}_{11}$

$\phi_0(\mathbb{Z}_{11}) = \{0\}$ \hspace{1cm} $\ker(\phi_0) = \mathbb{Z}_{11}$

$\phi_1(\mathbb{Z}_{11}) = \mathbb{Z}_{11}$ \hspace{1cm} $\ker(\phi_1) = \{0\}$

$\mathbb{Z}_{12} \rightarrow \mathbb{Z}_{12}$

$\phi_0(\mathbb{Z}_{12}) = \{0\}$ \hspace{1cm} $\ker(\phi_0) = \mathbb{Z}_{12}$

$\phi_1(\mathbb{Z}_{12}) = \mathbb{Z}_{12}$ \hspace{1cm} $\ker(\phi_1) = \{0\}$

$\phi_4(\mathbb{Z}_{12}) = \{0,4,8\}$ \hspace{1cm} $\ker(\phi_4) = \{0,3,6,9\}$

$\phi_9(\mathbb{Z}_{12}) = \{0,3,6,9\}$ \hspace{1cm} $\ker(\phi_9) = \{0,4,8\}$

$\mathbb{Z}_{13} \rightarrow \mathbb{Z}_{13}$

$\phi_0(\mathbb{Z}_{13}) = \{0\}$ \hspace{1cm} $\ker(\phi_0) = \mathbb{Z}_{13}$

$\phi_1(\mathbb{Z}_{13}) = \mathbb{Z}_{13}$ \hspace{1cm} $\ker(\phi_1) = \{0\}$

$\mathbb{Z}_{14} \rightarrow \mathbb{Z}_{14}$

$\phi_0(\mathbb{Z}_{14}) = \{0\}$ \hspace{1cm} $\ker(\phi_0) = \mathbb{Z}_{14}$

$\phi_1(\mathbb{Z}_{14}) = \mathbb{Z}_{14}$ \hspace{1cm} $\ker(\phi_1) = \{0\}$

$\phi_7(\mathbb{Z}_{14}) = \{0,7\}$ \hspace{1cm} $\ker(\phi_7) = \{0,8\}$

$\phi_8(\mathbb{Z}_{14}) = \{0,8\}$ \hspace{1cm} $\ker(\phi_8) = \{0,7\}$

$\mathbb{Z}_{15} \rightarrow \mathbb{Z}_{15}$

$\phi_0(\mathbb{Z}_{15}) = \{0\}$ \hspace{1cm} $\ker(\phi_0) = \mathbb{Z}_{15}$
$\phi_1 (\mathbb{Z}_{15}) = \mathbb{Z}_{15}$ \hspace{1cm} ker (\phi_1) = \{0\}

$\phi_6 (\mathbb{Z}_{15}) = \{0, 3, 6, 9, 12\}$ \hspace{1cm} ker (\phi_6) = \{0, 5, 10\}

$\phi_{10} (\mathbb{Z}_{15}) = \{0, 8, 10\}$ \hspace{1cm} ker (\phi_{10}) = \{0, 3, 9, 12\}

$\mathbb{Z}_{16} \rightarrow \mathbb{Z}_{16}$

$\phi_0 (\mathbb{Z}_{16}) = \{0\}$ \hspace{1cm} ker (\phi_0) = \mathbb{Z}_{16}

$\phi_1 (\mathbb{Z}_{16}) = \mathbb{Z}_{16}$ \hspace{1cm} ker (\phi_1) = \{0\}

$\mathbb{Z}_{17} \rightarrow \mathbb{Z}_{17}$

$\phi_0 (\mathbb{Z}_{17}) = \{0\}$ \hspace{1cm} ker (\phi_0) = \mathbb{Z}_{17}

$\phi_1 (\mathbb{Z}_{17}) = \mathbb{Z}_{17}$ \hspace{1cm} ker (\phi_1) = \{0\}

$\mathbb{Z}_{18} \rightarrow \mathbb{Z}_{18}$

$\phi_0 (\mathbb{Z}_{18}) = \{0\}$ \hspace{1cm} ker (\phi_0) = \mathbb{Z}_{18}

$\phi_1 (\mathbb{Z}_{18}) = \mathbb{Z}_{18}$ \hspace{1cm} ker (\phi_1) = \{0\}

$\phi_9 (\mathbb{Z}_{18}) = \{0, 9\}$ \hspace{1cm} ker (\phi_9) = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}

$\phi_{10} (\mathbb{Z}_{18}) = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$ \hspace{1cm} ker (\phi_{10}) = \{0, 9\}

$\mathbb{Z}_{19} \rightarrow \mathbb{Z}_{19}$

$\phi_0 (\mathbb{Z}_{19}) = \{0\}$ \hspace{1cm} ker (\phi_0) = \mathbb{Z}_{19}

$\phi_1 (\mathbb{Z}_{19}) = \mathbb{Z}_{19}$ \hspace{1cm} ker (\phi_1) = \{0\}
\( \mathbb{Z}_{20} \to \mathbb{Z}_{20} \)

\[ \phi_0(\mathbb{Z}_{20}) = \{0\} \quad \ker(\phi_0) = \mathbb{Z}_{20} \]

\[ \phi_1(\mathbb{Z}_{20}) = \mathbb{Z}_{20} \quad \ker(\phi_1) = \{0\} \]

\[ \phi_5(\mathbb{Z}_{20}) = \{0,5,10,15\} \quad \ker(\phi_5) = \{0,4,8,12,16\} \]

\[ \phi_{16}(\mathbb{Z}_{20}) = \{0,4,8,12,16\} \quad \ker(\phi_{16}) = \{0,5,10,15\} \]

\( \mathbb{Z}_{21} \to \mathbb{Z}_{21} \)

\[ \phi_0(\mathbb{Z}_{21}) = \{0\} \quad \ker(\phi_0) = \mathbb{Z}_{21} \]

\[ \phi_1(\mathbb{Z}_{21}) = \mathbb{Z}_{21} \quad \ker(\phi_1) = \{0\} \]

\[ \phi_7(\mathbb{Z}_{21}) = \{0,7,14\} \quad \ker(\phi_7) = \{0,3,6,9,12,15,18\} \]

\[ \phi_{15}(\mathbb{Z}_{21}) = \{0,3,6,9,12,15,18\} \quad \ker(\phi_{15}) = \{0,7,14\} \]

\( \mathbb{Z}_{22} \to \mathbb{Z}_{22} \)

\[ \phi_0(\mathbb{Z}_{22}) = \{0\} \quad \ker(\phi_0) = \mathbb{Z}_{22} \]

\[ \phi_1(\mathbb{Z}_{22}) = \mathbb{Z}_{22} \quad \ker(\phi_1) = \{0\} \]

\[ \phi_{11}(\mathbb{Z}_{22}) = \{0,11\} \quad \ker(\phi_{11}) = \{0,2,4,6,8,10,12,14,16,18,20\} \]

\[ \phi_{12}(\mathbb{Z}_{22}) = \{0,2,4,6,8,10,12,14,16,18,20\} \quad \ker(\phi_{12}) = \{0,11\} \]

\( \mathbb{Z}_{23} \to \mathbb{Z}_{23} \)

\[ \phi_0(\mathbb{Z}_{23}) = \{0\} \quad \ker(\phi_0) = \mathbb{Z}_{23} \]

\[ \phi_1(\mathbb{Z}_{23}) = \mathbb{Z}_{23} \quad \ker(\phi_1) = \{0\} \]
\[ \mathbb{Z}_{24} \rightarrow \mathbb{Z}_{24} \]

\[ \phi_0 (\mathbb{Z}_{24}) = \{0\} \quad \text{ker} (\phi_0) = \mathbb{Z}_{24} \]

\[ \phi_1 (\mathbb{Z}_{24}) = \mathbb{Z}_{24} \quad \text{ker} (\phi_1) = \{0\} \]

\[ \phi_9 (\mathbb{Z}_{24}) = \{0,3,6,9,12,15,18,21\} \quad \text{ker} (\phi_9) = \{0,8,16\} \]

\[ \phi_{16} (\mathbb{Z}_{24}) = \{0,8,16\} \quad \text{ker} (\phi_{16}) = \{0,3,6,9,12,15,18,21\} \]

\[ \mathbb{Z}_{25} \rightarrow \mathbb{Z}_{25} \]

\[ \phi_0 (\mathbb{Z}_{25}) = \{0\} \quad \text{ker} (\phi_0) = \mathbb{Z}_{25} \]

\[ \phi_1 (\mathbb{Z}_{25}) = \mathbb{Z}_{25} \quad \text{ker} (\phi_1) = \{0\} \]

\[ \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26} \]

\[ \phi_0 (\mathbb{Z}_{26}) = \{0\} \quad \text{ker} (\phi_0) = \mathbb{Z}_{26} \]

\[ \phi_1 (\mathbb{Z}_{26}) = \mathbb{Z}_{26} \quad \text{ker} (\phi_1) = \{0\} \]

\[ \phi_{13} (\mathbb{Z}_{26}) = \{0,13\} \quad \text{ker} (\phi_{13}) = \{0,2,4,6,8,10,12,14,16,18,20,22,24\} \]

\[ \phi_{14} (\mathbb{Z}_{26}) = \{0,2,4,6,8,10,12,14,16,18,20,22,24\} \quad \text{ker} (\phi_{14}) = \{0,13\} \]

\[ \mathbb{Z}_{27} \rightarrow \mathbb{Z}_{27} \]

\[ \phi_0 (\mathbb{Z}_{27}) = \{0\} \quad \text{ker} (\phi_0) = \mathbb{Z}_{27} \]

\[ \phi_1 (\mathbb{Z}_{27}) = \mathbb{Z}_{27} \quad \text{ker} (\phi_1) = \{0\} \]
\[ \mathbb{Z}_{28} \to \mathbb{Z}_{28} \]

\[ \phi_0(\mathbb{Z}_{28}) = \{0\} \quad \text{ker}(\phi_0) = \mathbb{Z}_{28} \]

\[ \phi_1(\mathbb{Z}_{28}) = \mathbb{Z}_{28} \quad \text{ker}(\phi_1) = \{0\} \]

\[ \phi_8(\mathbb{Z}_{28}) = \{0,4,8,12,16,20,24\} \quad \text{ker}(\phi_8) = \{0,7,14,21\} \]

\[ \phi_{21}(\mathbb{Z}_{28}) = \{0,7,14,21\} \quad \text{ker}(\phi_{21}) = \{0,4,8,12,16,20,24\} \]

\[ \mathbb{Z}_{29} \to \mathbb{Z}_{29} \]

\[ \phi_0(\mathbb{Z}_{29}) = \{0\} \quad \text{ker}(\phi_0) = \mathbb{Z}_{29} \]

\[ \phi_1(\mathbb{Z}_{29}) = \mathbb{Z}_{29} \quad \text{ker}(\phi_1) = \{0\} \]

\[ \mathbb{Z}_{30} \to \mathbb{Z}_{30} \]

\[ \phi_0(\mathbb{Z}_{30}) = \{0\} \quad \text{ker}(\phi_0) = \mathbb{Z}_{30} \]

\[ \phi_1(\mathbb{Z}_{30}) = \mathbb{Z}_{30} \quad \text{ker}(\phi_1) = \{0\} \]

\[ \phi_6(\mathbb{Z}_{30}) = \{0,6,12,18,24\} \quad \text{ker}(\phi_6) = \{0,5,10,15,20,25\} \]

\[ \phi_{10}(\mathbb{Z}_{30}) = \{0,10,20\} \quad \text{ker}(\phi_{10}) = \{0,3,6,9,12,15,18,21,24,27\} \]

\[ \phi_{15}(\mathbb{Z}_{30}) = \{0,15\} \quad \text{ker}(\phi_{15}) = \{0,2,4,6,8,10,12,14,16,18,20,22,24,26,28\} \]

\[ \phi_{16}(\mathbb{Z}_{30}) = \{0,2,4,6,8,10,12,14,16,18,20,22,24,26,28\} \quad \text{ker}(\phi_{16}) = \{0,15\} \]

\[ \phi_{21}(\mathbb{Z}_{30}) = \{0,3,6,9,12,15,18,21,24,27\} \quad \text{ker}(\phi_{21}) = \{0,10,20\} \]

\[ \phi_{25}(\mathbb{Z}_{30}) = \{0,5,10,15,20,25\} \quad \text{ker}(\phi_{25}) = \{0,6,12,18,24\} \]
$\mathbb{Z}_{31} \to \mathbb{Z}_{31}$

$\phi_0 (\mathbb{Z}_{31}) = \{0\}$ \hspace{1cm} \text{ker (}\phi_0\text{) } = \mathbb{Z}_{31}$

$\phi_1 (\mathbb{Z}_{31}) = \mathbb{Z}_{31}$ \hspace{1cm} \text{ker (}\phi_1\text{) } = \{0\}$

$\mathbb{Z}_{32} \to \mathbb{Z}_{32}$

$\phi_0 (\mathbb{Z}_{32}) = \{0\}$ \hspace{1cm} \text{ker (}\phi_0\text{) } = \mathbb{Z}_{32}$

$\phi_1 (\mathbb{Z}_{32}) = \mathbb{Z}_{32}$ \hspace{1cm} \text{ker (}\phi_1\text{) } = \{0\}$

$\mathbb{Z}_{33} \to \mathbb{Z}_{33}$

$\phi_0 (\mathbb{Z}_{33}) = \{0\}$ \hspace{1cm} \text{ker (}\phi_0\text{) } = \mathbb{Z}_{33}$

$\phi_1 (\mathbb{Z}_{33}) = \mathbb{Z}_{33}$ \hspace{1cm} \text{ker (}\phi_1\text{) } = \{0\}$

$\phi_{12} (\mathbb{Z}_{33}) = \{0,3,6,9,12,15,18,21,24,27,30\}$ \hspace{1cm} \text{ker (}\phi_{12}\text{) } = \{0,11,22\}$

$\phi_{22} (\mathbb{Z}_{33}) = \{0,11,22\}$ \hspace{1cm} \text{ker (}\phi_{22}\text{) } = \{0,3,6,9,12,15,18,21,24,27,30\}$

$\mathbb{Z}_{34} \to \mathbb{Z}_{34}$

$\phi_0 (\mathbb{Z}_{34}) = \{0\}$ \hspace{1cm} \text{ker (}\phi_0\text{) } = \mathbb{Z}_{34}$

$\phi_1 (\mathbb{Z}_{34}) = \mathbb{Z}_{34}$ \hspace{1cm} \text{ker (}\phi_1\text{) } = \{0\}$

$\phi_{17} (\mathbb{Z}_{34}) = \{0,17\}$

\text{ker (}\phi_{17}\text{) } = \{0,2,4,6,8,10,12,14,16,18,20,22,24,26,28,30,32\}$

$\phi_{18} (\mathbb{Z}_{34}) = \{0,2,4,6,8,10,12,14,16,18,20,22,24,26,28,30,32\}$

\text{ker (}\phi_{18}\text{) } = \{0,17\}$
\[ \mathbb{Z}_{35} \to \mathbb{Z}_{35} \]

\[ \phi_0 (\mathbb{Z}_{35}) = \{ 0 \} \quad \text{ker} (\phi_0) = \mathbb{Z}_{35} \]
\[ \phi_1 (\mathbb{Z}_{35}) = \mathbb{Z}_{35} \quad \text{ker} (\phi_1) = \{ 0 \} \]
\[ \phi_{15} (\mathbb{Z}_{35}) = \{ 0,5,10,15,20,25,30 \} \quad \text{ker} (\phi_{15}) = \{ 0,7,14,21,28 \} \]
\[ \phi_{21} (\mathbb{Z}_{35}) = \{ 0,7,14,21,28 \} \quad \text{ker} (\phi_{21}) = \{ 0,5,10,15,20,25,30 \} \]

\[ \mathbb{Z}_{36} \to \mathbb{Z}_{36} \]

\[ \phi_0 (\mathbb{Z}_{36}) = \{ 0 \} \quad \text{ker} (\phi_0) = \mathbb{Z}_{36} \]
\[ \phi_1 (\mathbb{Z}_{36}) = \mathbb{Z}_{36} \quad \text{ker} (\phi_1) = \{ 0 \} \]
\[ \phi_9 (\mathbb{Z}_{36}) = \{ 0,9,18,27 \} \quad \text{ker} (\phi_9) = \{ 0,4,8,12,16,20,24,28,32 \} \]
\[ \phi_{28} (\mathbb{Z}_{36}) = \{ 0,4,8,12,16,20,24,28,32 \} \quad \text{ker} (\phi_{28}) = \{ 0,9,18,27 \} \]

\[ \mathbb{Z}_{37} \to \mathbb{Z}_{37} \]

\[ \phi_0 (\mathbb{Z}_{37}) = \{ 0 \} \quad \text{ker} (\phi_0) = \mathbb{Z}_{37} \]
\[ \phi_1 (\mathbb{Z}_{37}) = \mathbb{Z}_{37} \quad \text{ker} (\phi_1) = \{ 0 \} \]

\[ \mathbb{Z}_{38} \to \mathbb{Z}_{38} \]

\[ \phi_0 (\mathbb{Z}_{38}) = \{ 0 \} \quad \text{ker} (\phi_0) = \mathbb{Z}_{38} \]
\[ \phi_1 (\mathbb{Z}_{38}) = \mathbb{Z}_{38} \quad \text{ker} (\phi_1) = \{ 0 \} \]
\[ \phi_{19} (\mathbb{Z}_{38}) = \{ 0,19 \} \quad \text{ker} (\phi_{19}) = \{ 0,2,4,6,8,10,12,14,16,18,20,22,24,26,28,30,32,34,36 \} \]
\[ \phi_{20} (\mathbb{Z}_{38}) = \{ 0,2,4,6,8,10,12,14,16,18,20,22,24,26,28,30,34,36 \} \]
\[ \ker (\phi_{20}) = \{0, 9, 18, 27\} \]

\[ \mathbb{Z}_{39} \rightarrow \mathbb{Z}_{39} \]

\[ \phi_0 (\mathbb{Z}_{39}) = \{0\} \quad \text{ker (} \phi_0 \text{) = } \mathbb{Z}_{39} \]

\[ \phi_1 (\mathbb{Z}_{39}) = \mathbb{Z}_{39} \quad \text{ker (} \phi_1 \text{) = } \{0\} \]

\[ \phi_{13} (\mathbb{Z}_{39}) = \{0, 13, 26\} \quad \text{ker (} \phi_{13} \text{) = } \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36\} \]

\[ \phi_{27} (\mathbb{Z}_{39}) = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36\} \quad \text{ker (} \phi_{27} \text{) = } \{0, 13, 17\} \]

\[ \mathbb{Z}_{40} \rightarrow \mathbb{Z}_{40} \]

\[ \phi_0 (\mathbb{Z}_{40}) = \{0\} \quad \text{ker (} \phi_0 \text{) = } \mathbb{Z}_{40} \]

\[ \phi_1 (\mathbb{Z}_{40}) = \mathbb{Z}_{40} \quad \text{ker (} \phi_1 \text{) = } \{0\} \]

\[ \phi_{16} (\mathbb{Z}_{40}) = \{0, 8, 16, 24, 32\} \quad \text{ker (} \phi_{16} \text{) = } \{0, 5, 10, 15, 20, 25, 30, 35\} \]

\[ \phi_{25} (\mathbb{Z}_{40}) = \{0, 5, 15, 20, 25, 30, 35\} \quad \text{ker (} \phi_{25} \text{) = } \{0, 8, 16, 24, 32\} \]

From the above, it’s deduced that a ring homomorphism \( \phi_m : \mathbb{Z}_n \rightarrow \mathbb{Z}_n \) is generated by the elements of the set \( \{ m \in \mathbb{Z}_n : m^2 = m \pmod{n} \} \). Therefore the number of homomorphisms \( \phi_m : \mathbb{Z}_n \rightarrow \mathbb{Z}_n \) is uniquely determined by simply counting idempotent elements \( (E(n)) \) in \( \mathbb{Z}_n \), for the number of homomorphisms \( \phi_m : \mathbb{Z}_n \rightarrow \mathbb{Z}_n \) is equal to the number of idempotents \( (\sigma(n)) \) in \( \mathbb{Z}_n \). i.e. \( E(n) = \{ m \in \mathbb{Z}_n : m^{2^{\lambda+1}} = m \pmod{n}, \lambda \in \mathbb{Z}_n \} \) and \( \sigma(n) = |E(n)| \)
4.3.1 Theorem

If \( n = p^k \), the only homomorphism \( \phi_m : \mathbb{Z}_n \to \mathbb{Z}_n \) are the trivial homomorphism \( \phi_0 \) and \( \phi_1 \), \( p \) is a prime

Proof

Let \( m \in \mathbb{Z}_n \) such that \( m^2 = m \) (mod \( n \)). Then \( m^2 - m = 0, \ m(m-1) = 0, \ m = 0, \ m-1 = 0, \ m = 1 \) m and \( (m-1) \) are relatively prime. Hence either \( p^k | m \) or \( p^k | (m-1) \).

Since \( 0 < m < p^k = n, \ p^k \) does not divide \( m \) and \( p^k \) does not divide \( (m-1) \).

\( E(n) = \{0,1\}, \ \sigma(n) = 2 \), meaning there are 2 homomorphisms from \( \mathbb{Z}_n \) to \( \mathbb{Z}_n \) when \( n = p^k \) i.e. \( \phi_0 \) and \( \phi_1 \) are the only homomorphism

4.3.2 Theorem

If \( n = p_1^{k_1} p_2^{k_2} \), where \( p_1 \) and \( p_2 \) are distinct primes, then there are \( 2^2 = 4 \) homomorphisms

\( \phi_m : \mathbb{Z}_n \to \mathbb{Z}_n \) namely, \( \phi_{(0,0)}, \phi_{(0,1)}, \phi_{(1,0)}, \phi_{(1,1)} \).
Proof

Let \( n = p_1^{k_1} p_2^{k_2} \), for all \( p_1, p_2 \) prime and \( k_1, k_2 \in \mathbb{Z}_n \),

\[
E(n) = E(p_1^{k_1})E(p_2^{k_2}) = \{0,1\} \times \{0,1\} \cong \{0,0,0,0,1,1,1,1\} \mod{p_1^{k_1}, \mod{p_2^{k_2}}}
\]

\[
E(21)\times E(21) = \{0,1\} \times \{0,1\} \cong \{0,0,0,0,1,1,1,1\} \mod{2, \mod{5}}
\]

\[
\sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) = 2 \times 2 = 2^2 = 4.
\]

Thus, there are 4 homomorphisms

i.e. \( \phi_{0,0}, \phi_{0,1}, \phi_{1,0}, \phi_{1,1} \).

Example 4.3.2.1

In \( \phi_m: \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}, \) \( 10 = 2 \times 5 \).

\[
E(10) = E(2)E(5) = \{0,1\} \times \{0,1\} \cong \{0,0,0,0,1,1,1,1\} \mod{2, \mod{5}}
\]

\[
\sigma(10) = \sigma(2)\sigma(5) = 2 \times 2 = 2^2 = 4.
\]

meaning there are 4 homomorphisms namely;

(0,0) Corresponding to 0, (1,1) corresponding to 1, (0,1) corresponding to 6 and
(1,0) Corresponding to 5, thus \( \phi_0, \phi_1, \phi_5 \) and \( \phi_6 \) are the homomorphism from \( \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10} \)

This agrees with the number of homomorphisms in section 4.3.

Example 4.3.2.2

In \( \phi_m: \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{12}, \) \( 12 = 2^2 \times 3 \).

\[
E(12) = E(2^2)E(3) = \{0,1\} \times \{0,1\} \cong \{0,0,0,0,1,1,1,1\} \mod{4, \mod{3}}
\]

\[
\sigma(12) = \sigma(2^2)\sigma(3) = 2 \times 2 = 2^2 = 4.
\]

meaning there are 4 homomorphisms namely;

(0,0) Corresponding to 0, (1,1) corresponding to 1, (0,1) corresponding to 4 and
(1,0) Corresponding to 9, thus $\phi_0$, $\phi_1$, $\phi_4$ and $\phi_9$ are the homomorphisms from $\mathbb{Z}_{12} \rightarrow \mathbb{Z}_{12}$

4.3.3 Theorem

If $n = p_1^{k_1} p_2^{k_2} p_3^{k_3}$, then there are $2^3$ homomorphisms $\phi_m : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$

Proof

Let $n = p_1^{k_1} p_2^{k_2} p_3^{k_3}$, where $p_1, p_2, p_3$ are distinct prime numbers and $k_1, k_2, k_3 \in \mathbb{Z}_n$

$E(n) = E(p_1^{k_1})E(p_2^{k_2})E(p_3^{k_3})$

$= \{0,1\} \times \{0,1\} \times \{0,1\}$

$\cong \{(0,0,0),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1),(mod \ p_1^{k_1}, mod \ p_2^{k_2}, mod \ p_3^{k_3})\}$

$\sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2})\sigma(p_3^{k_3}) = 2 \times 2 \times 2 = 2^3$. Thus, there are $2^3 = 8$ homomorphisms.

Example 4.3.3.1

In $\phi_m : \mathbb{Z}_{30} \rightarrow \mathbb{Z}_{30}$, $30 = 2 \times 3 \times 5$

$E(30) = E(2)E(3)E(5) = \{0,1\} \times \{0,1\} \times \{0,1\}$

$\cong (0,0,0),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1) (mod \ 2, mod \ 3, mod \ 5)$

$\sigma(30) = \sigma(2)\sigma(3)\sigma(5) = 2 \times 2 \times 2 = 2^3 = 8$, thus there are $2^3 = 8$ homomorphisms

from $\mathbb{Z}_{30} \rightarrow \mathbb{Z}_{30}$ namely: $\phi_0, \phi_1, \phi_6, \phi_10, \phi_{15}, \phi_{16}, \phi_{21}, \phi_{25}$, where $(0,0,0)$ corresponding to 0, $(1,1,1)$ corresponding to 1, $(0,0,1)$ corresponding to 6, $(0,1,0)$ corresponding to 10.
(0,1,1) corresponding to 16, (1,0,0) corresponding to 15, (1,0,1) corresponding to 21 and lastly (1,1,0) corresponding to 25.

Example 4.3.3.2

In $\phi_m: \mathbb{Z}_{60} \rightarrow \mathbb{Z}_{60}$, $60 = 2^2 \times 3 \times 5$

$E(60) = E(2^2)E(3)E(5) = \{0,1\} \times \{0,1\} \times \{0,1\}$

$\cong \{0,0,0\}, \{0,1,0\}, \{1,0,0\}, \{1,0,1\}, \{1,1,0\}, \{1,1,1\} \pmod{4, 3, 5}$

$\sigma(60) = \sigma(2^2)\sigma(3)\sigma(5) = 2 \times 2 \times 2 = 2^3 = 8$, thus there are $2^3 = 8$ homomorphisms from $\mathbb{Z}_{60} \rightarrow \mathbb{Z}_{60}$ namely, $\phi_0, \phi_1, \phi_{16}, \phi_{21}, \phi_{36}, \phi_{40}, \phi_{45}$, where (0,0,0) corresponds to 0, (1,1,1) corresponds to 1, (0,0,1) corresponds to 36, (0,1,0) corresponds to 40, (0,1,1) corresponds to 16, (1,0,0) corresponds to 45, (1,0,1) corresponds to 21 and lastly (1,1,0) corresponds to 25.

4.3.4 Theorem

In general, there are $2^m$ homomorphisms $\phi_m: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ where

$n = \prod_{i=1}^{m} p_i^{k_i}, p_1, p_2, p_3, ..., p_m$ are distinct primes and

$k_1, k_2, k_3, ..., k_m \in \mathbb{Z}_n$.

Proof

Let $n = \prod_{i=1}^{m} p_i^{k_i}, p_1, p_2, p_3, ..., p_m$ are distinct primes and

$k_1, k_2, k_3, ..., k_m \in \mathbb{Z}_n$. 
$$E(n) = E(p_1^{k_1})E(p_2^{k_2})E(p_3^{k_3})\cdots E(p_m^{k_m}) = \{0,1\} \times \{0,1\} \times \cdots \times \{0,1\}$$

$$\cong \{(0,0,\ldots,0),(0,0,\ldots,1),\ldots,(1,0,\ldots,0),(1,1,\ldots,1)\mod p_1^{k_1}, \mod p_2^{k_2}, \ldots, \mod p_m^{k_m}\}$$

$$\sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2})\sigma(p_3^{k_3})\cdots\sigma(p_m^{k_m}) = \mathcal{4}\times\mathcal{4}\times\mathcal{2}\times\mathcal{2}\times\mathcal{2} = 2^m$$

Thus there are $2^m$ homomorphisms $\phi_m : \mathbb{Z}_n \to \mathbb{Z}_n$.

### 4.3.5 Theorem

$\phi_1 : \mathbb{Z}_n \to \mathbb{Z}_n$ is the only monomorphism.

**Proof**

By contradiction, let $\phi_m : \mathbb{Z}_n \to \mathbb{Z}_n$ be another ring homomorphism and

$$a, b, c, d, x, y, z \in \mathbb{Z}_m$$

$$\phi_m(\mathbb{Z}_n) = \{0, m, x, y\}, \ker(\phi_m) \in \{0, m, x, y\} \neq \{e\}.$$ Thus a contradiction hence $\phi_1$ is the only monomorphism.
Table 4.3.1: The relationship between the number of ideals in \( \mathbb{Z}_n \) and the number of homomorphisms of \( \mathbb{Z}_n \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>Number of ideals</th>
<th>Number of homomorphisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>15</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>16</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>18</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>19</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>20</td>
<td>6</td>
<td>4</td>
</tr>
</tbody>
</table>
From Table 4.3.1, we deduce that,

When $n$ is prime, the number of homomorphism equals the number of ideals. Each ideal is a kernel of homomorphism. The same applies when $n = p_1^{k_1}p_2^{k_2}$, $k_1 = k_2$, $p_1 \neq p_2$.

When $n = p_1^{k_1}p_2^{k_2}$, where $k_1 > 1$ or $k_2 > 1$, then the number of homomorphisms is not equal to the number of ideals. Not all ideals are the kernels of homomorphism which is the case when $n = p^k$ where $k > 1$. 
CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

In this chapter, a generalization on finding the number of homomorphisms $\phi_m : \mathbb{Z}_n \to \mathbb{Z}_n$ for different values of $n$ has been drawn. Finally, recommendations have also been given.

5.1 Conclusions

Based on the study, the following has been observed,

If $n$ is prime, there are only 2 homomorphism i.e. the trivial homomorphism $\phi_0$ and $\phi_1$.

If $n = p^k$, $\forall k > 1$, then it has 2 homomorphism $\phi_0$ and $\phi_1$.

If $n = p_1^{k_1} p_2^{k_2}$, then it has 4 i.e. $2^2$ homomorphism. Here $n$ can be expressed as a product of 2 prime numbers each having 2 homomorphisms hence $2 \times 2 = 2^2 = 4$.

If $n = p_1^{k_1} p_2^{k_2} p_3^{k_3}$, then it has 8 i.e. $2^3$ homomorphism

In general, if $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots p_m^{k_m}$ then it has $2^m$ homomorphism as $n$ can be expressed as a product of $m$ prime numbers, $\forall k_1, k_2, k_3, \ldots, k_m \geq 1$ and $p_1, p_2, p_3, \ldots, p_m$ are prime numbers.
5.2 Recommendations

In this project, the number of homomorphism from \( \mathbb{Z}_n \) to \( \mathbb{Z}_n \) has been determined and general formulas given for different values of \( n \). More research is encouraged to build and extend the idea. Citing an example from Table 4.3.1 which gives the relationship between ideals in \( \mathbb{Z}_n \) and the number of homomorphisms \( \phi_m : \mathbb{Z}_n \to \mathbb{Z}_n \), further research is encouraged to establish characteristics of \( n \) where not all the ideals are the kernels of homomorphism hence derive a formula for the same.
References
Anderson (1995), A first course in abstract algebra, marlow, Boston

David Guichard, Patrick Keef et al (2010), An introduction to higher mathematics, Whitman College

Derik H. (2014), Number of homomorphism from a finite field into a ring, Math stack exchange, 79.4237


Galian J. A and Van Baskirk J. V (1984), The number of homomorphism from $\mathbb{Z}_m$ into $\mathbb{Z}_n$, AMM, 91(1984), 196-197

Hagen Van Einstein (2004), Number of homomorphism from a finite field into a ring, MSE 23.38

John B. F. (1984), A first course in abstract Algebra (2nded), Addison, U.S.A.

Matt Samuel (2013), Number of homomorphisms from $\mathbb{Z}[x] \rightarrow \mathbb{Z}_n$, pacific journal of mathematics, MSE vol. 2

