On The Number of Ring Homomorphisms Over Certain Rings

by

Sultan Amin Issa Kowkas

Supervisor

Dr. Mohammad Saleh

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science

in Mathematics

At

Birzeit University

December 16, 2014

Birzeit, Palestine

The Thesis committee for Sultan Amin Issa Kowkas

Certifies that this is the approved version of the following thesis:

On The Number of Ring Homomorphisms

Over Certain Rings

Thesis Committee

Supervisor: Mohammad Saleh	**Date**
Khalid Altachman	**Date**
Naeem Alkoumi	**Date**

Dedication

To the Sun of Islam that will never set
To the Prophet Muhammad (pbuh) who is inevitably eminent

To the soul of my father, whose memory is forever persistent

To my mother, whose prayers are my permanent assistant
To my family: wife and kids who are my main potent

Acknowledgements

All praise, gratitude and thanks are due to Allah, the most gracious and most merciful, for all the graces that he gave me, and foremost for the greatest Grace of being a Muslim and of being a follower of the Prophet Mohammad (May Allah's Peace and Praying be Upon Him).

My sincere gratitude and appreciations are to my supervisor, Dr. Mohammad Saleh, for his continuous support, great guidance and endless help.

I would also like to thank my family: my wife, my daughters: Basmaleh, Tasnim, and my son Issa for their love, patience and support.

Contents

0.1 Notations

Symbol	Definition
$\mathbb{N}$	The natural numbers $\{1, 2, 3, \ldots\}$
$\mathbb{Z}$	The ring of integers
$\mathbb{Z}_n$	The ring of integers modulo n
$\mathbb{Z}[i]$	The ring of Gaussian integers, $i^2 + 1 = 0$
$\mathbb{Z}[\rho]$	The ring of Eisenstein integers, $\rho^2 + \rho + 1 = 0$
ϕ	A group/ring homomorphism
$\ker \phi$	The kernel of the homomorphism ϕ
Φ	Euler's phi function
$\overline{\omega}$	The *conjugate* of the number ω
$N(\omega)$	The norm of the element ω, $N(\omega) = \omega \cdot \overline{\omega}$
$\mathcal{N}$	The number of ring homomorphisms
$\mathcal{N}(\phi : R \to S)$	The number of ring homomorphisms from S into R
$Rem(m)_n$	The remainder upon dividing m by n
$N_{p^k}(m_1, m_2, \ldots, m_r)$	The number of elements of the set $\{m_1, m_2, \ldots, m_r\}$ that are divisible by p^k
$\omega(n)$	The number of distinct prime factors of n in a ring
$A \cong B$	The group/ring A is *isomorphic* to the group/ring B
θ	An algebraic integer
$(\ \cdot\ )$	*Parentheses*: References within the text of the thesis
$[\ \cdot\ ]$	*Brackets*: Referred to *Main References* list [3.2], page 121
$\{\ \cdot\ \}$	*Braces*: References for *footnotes*

Abstract

The problem of finding the number of ring homomorphisms between rings of certain properties has been studied only few times. This thesis discusses the number of ring homomorphisms over algebraic integers; starting with the rings of Gaussian integers ($\mathbb{Z}_m[i]$ modulo m),where $i^2 = 1$. Over the ring of Eisenstein integers ($\mathbb{Z}_m[\rho]$ modulo m), where $\rho^2+\rho+1 = 0$, and over rings of some algebraic integers θ, $\mathbb{Z}_m[\theta]$ for an algebraic integer θ with minimal polynomial $p(x) = x^2 + ux + v$ whose absolute radicand, ($|u^2 - 4v| = m$), is a prime integer and $\mathbb{Z}[\theta]$ is a UFD. Among the results that have been found by previous researchers, in this thesis we give some generalizations to the problem. The new "original" results, corollaries and theorems, have been marked with an asterisk (*).

بسم الله الرحمن الرحيم

مُلخَّصِ الرِسالة:

الحمدُ للهِ الواحدِ الأحدْ، الفْردِ الصَمَدْ، عَدَدَاً ً يفوقُ كُلَّ عَدَدْ، والصلاةُ والسَّلامُ على سَيِّدِنا مُحَمَّدْ، خَيْرِ خَلْقِهِ أَبَدْ، ما تلى العَددُ عَدَدْ، وكُلَما نورُ الشمسِ اتَّقَدْ.

إنَّ البحثَ حولَ عددِ التَشاكُلات بين حَلقاتِ الأعدادِ لمْ يخضعْ للدراسةِ إلّا على يدِ بعضِ الباحثينَ مُؤخراً ً. فتهدفُ هذهِ الدراسةُ لبحثِ عددِ التَشاكُلات بينَ حلقاتِ الأعدادِ الجبريّة. حيثُ أنَّ عددَ هذهِ التَشاكُلات يلعبُ دوراً ً هامّاً ً في مجالَيِّ الجبرِ المُجَرَّدِ ونظريَّةِ الأعدادِ الجبْرِيَّة.

تقومُ هذهِ الدراسةِ بعرضِ بعضِ النظرياتِ التي تبحثُ حولَ عددِ التَشاكُلات بينَ الحلقاتِ التالية:

الأعدادِ الصحيحة ($\mathbb{Z}$) وحلقاتِ الأعداد الصحيحة قياس n ($\mathbb{Z}_n$ ، $n \ni \mathbb{Z}$)

بين حلقاتِ أعدادِ "غاوس" (Rings of Gaussian Integers $\mathbb{Z}[i]$)

وحلقاتِها قياس m (Rings of Gaussian Integers module m $\mathbb{Z}_m[i]$ ، $m \ni \mathbb{Z}$)

بين حلقاتِ أعدادِ "آيزنشتاين" (Rings of Eisenstein Integers $\mathbb{Z}[\rho]$)

وحلقاتِها قياس m (Rings of Eisenstein Integers module $\mathbb{Z}_m[\rho]$ ، $m \ni \mathbb{Z}$) حيثُ ρ يُحقق:

$$0 = 1 + \rho + \rho^2$$

وبين حلقاتِ الأعدادِ الجبريَّةِ على العددِ الجبريّ θ (Rings of Algebraic Integers $\mathbb{Z}[\theta]$)

وحلقاتِها على العدد الجبريّ θ قياس m (Rings of Algebraic Integers module m $\mathbb{Z}_m[\theta]$ ، $m \ni \mathbb{Z}$) حيثُ العددِ الجبريِّ θ لهُ كثيرةُ الحُدودِ الصُغْرى : $ن(س) = س^2 + ب س + جـ$

بشرط أنَّ : $|ب^2 - 4 جـ| = m =$ عدداً ً أوليَّاً ً، و ($\mathbb{Z}[\theta]$) هو نِطاقُ وحيدُ التحليل (UFD).

نُقَدِّمْ الأساسيَّات منَ الجبرِ المُجرَّدِ ونظريَّةِ الأعدادِ في الوحدةِ الأولى (المفاهيمُ الأساسيَّة)، حيثُ نعرضُ التعاريفَ والنظرياتِ الأساسيَّة المُستخدمة فيما بعد.

وفي الوحدةِ الثانيةِ (النتائجُ الرئيسِيَّة) فنعرضُ النظريّاتِ (وبراهينها الكاملة) المتعلقةِ بعددِ التشاكُلات حول حلقات الأعداد بالترتيب كما ذُكِرت أعلاه. كما ونُقَدِّمُ بعضَ النتائجِ الأصيلة (الحديثة) الخاصة المتعلقة بهذه الحُقول، حيثُ أشرنا لهذه النتائج بإشارة (مُنَجَّمة – *).

تتمَثَّلُ الوحدةُ الثالثة (الخاتمة والعمل المُستقبليّ) بعرض مُلَخَّصِ الرسالة والنتائج، كما ونوصي بعرض بعض المسائل المتعلقة بموضوع الدراسة التي تستحق البحث والتي سنقوم بدراستها لاحقاً.

Introduction

The main purpose of this thesis is to study the number of ring homomorphisms over certain rings, starting with the rings of simpler structure and to gradually carry the problem to rings of a more cumbersome structure.

Firstly; we consider the number of ring homomorphisms between rings of integers $\mathbb{Z}$. We compute the number of ring homomorphisms between a product of rings of integers into the ring of integers and into a product of rings of integers for few cases up to reaching a generalization as a simple formula for each case. After that we consider the problem among rings of integers $\mod n$, $\mathbb{Z}_n$. We give few examples as illustrations.

Secondly; we consider the rings of Gaussian integers, $\mathbb{Z}[i]$, and those $\mod n$. We find the number of ring homomorphisms between these rings and between products of these rings giving certain generalizations supported by few examples.

After that we consider the rings of Eisenstein integers, $\mathbb{Z}[\rho]$ and $\mathbb{Z}_n[\rho]$. We reach some generalizations concerning the number of ring homomorphisms between these rings.

Finally; we consider rings of algebraic integers, $\mathbb{Z}[\theta]$, $\mathbb{Z}_m[\theta]$ where θ has the minimal polynomial $p(x) = x^2+ux+v$ with $|u^2-4v|$ a prime and $\mathbb{Z}_{m_i}[\theta]$'s are unique factorization domains. We demonstrate the proofs of each case reaching few original generalizations, namely:

$$\mathcal{N}\big(\phi : \mathbb{Z}[\theta] \times \mathbb{Z}[\theta] \times \mathbb{Z}[\theta] \to \mathbb{Z}_k[\theta]\big), \quad \mathcal{N}\big(\overbrace{\mathbb{Z}[\theta] \times \cdots \times \mathbb{Z}[\theta]}^{n-times} \to \mathbb{Z}_k[\theta]\big)$$

$$\mathcal{N}\big(\phi : \mathbb{Z}_n[\theta] \times \mathbb{Z}_l[\theta] \times \mathbb{Z}_i[\theta] \to \mathbb{Z}_k[\theta]\big), \quad \mathcal{N}\big(\phi : \mathbb{Z}_{n_1}[\theta] \times \mathbb{Z}_{n_2}[\theta] \times \cdots \times \mathbb{Z}_{n_r}[\theta] \to \mathbb{Z}_k[\theta]\big)$$

Outline of the chapters:

Chapter One: ***Basic Concepts***: illustrates introductory material, including basic definitions, facts and theorems in Abstract Algebra and Algebraic Number Theory that form the building blocks of thesis.

Chapter Two: ***Main Results***: illustrates the main results (theorems) concerning the problem of finding the number of ring homomorphisms among the rings mentioned above. The original results are marked with an asterisk (*).

Chapter Three: ***Conclusions and Future Work***: we give a summary of the thesis and the main results that were achieved. We raise some important problems that could be sought in the future.

Chapter 1

Basic Concepts

This chapter covers the main basic concepts, definitions and theorems from abstract algebra, number theory and algebraic number theory that are used in the theorems and their proofs in the main results. The proofs of theorems, lemmas and corollaries in this chapter can be found in the references as specified.

1.1 Groups

Definition 1.1. ***External Direct Product/Sum***

Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. Then, the external direct product of the groups $G_1, G_2, \ldots, G_n$ is:

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_2, g_2, \ldots, g_n) \ : \ g_i \in G_i\} \qquad with$$

$$(g_1, g_2, \ldots, g_n)(g_1^{'}, g_2^{'}, \ldots, g_n^{'}) = (g_1 g_1^{'}, g_2 g_2^{'}, \ldots, g_n g_n^{'})$$

where the product in each $g_i g_i^{'}$ is according to the operation of the the group G_i

Definition 1.2. ***Group Homomorphism***

A homomorphism ϕ from a group G to a group $G^{'}$ is a mapping from G into $G^{'}$ that preserves the group operation. i.e. $\phi(ab) = \phi(a)\phi(b)$

Definition 1.3. ***Kernel of a Homomorphism***

Let ϕ: $G \to G^{'}$ be a group homomorphism over the groups G and $G^{'}$ with identity elements e and $e^{'}$ respectively. then the kernel of $\phi = \ker\phi = \{a \in G : \ \phi(a) = e^{'}\}$

Definition 1.4. ***Group Isomorphism***

Let ϕ be a one-to-one mapping (function) from a group G onto a group $G^{'}$. Then ϕ is called a group isomorphism from G onto $G^{'}$ if ϕ preserves the group operation. That is:
$\forall \quad a, b \in G, \quad \phi(a) * \phi(b) = \phi(a * b)$. *If there is an isomorphism from G onto $G^{'}$, then G and $G^{'}$ are said to be isomorphic and we write: $G \approx G^{'}$.*

1.2 Rings

Definition 1.5. ***A commutative ring:*** *A commutative ring R is a ring whose multiplication operation is commutative.*

Definition 1.6. ***A ring with unity:*** *A ring that has a multiplicative identity is called a ring with unity.*

Note: All rings considered in this thesis are commutative rings with unity.

Definition 1.7. ***The Ring of Direct Sum****: Let $R_1, R_2, \ldots, R_n$ be rings. Then the ring: $R = \bigoplus \sum_{i=1}^{n} R_i = \{(a_1, a_2, \ldots, a_n) | a_i \in R_i\}$ where the addition and multiplication are performed component wise.*

Definition 1.8. ***Ideal***

A subring I of a ring R is called an Ideal if it is closed under multiplication by the elements of R, i.e. $\forall\ a \in I$ and $\forall\ r \in R$, $ar \in I$ and $ra \in I$.

1.2.1 Ring Homomorphisms

Definition 1.9. ***Ring Homomorphism*** *A ring homomorphism ϕ from a ring R to a ring $R^{'}$ is a mapping from R into $R^{'}$ that preserves the two ring operations: i.e. $\forall\ a, b \in R$: $\phi(a + b) = \phi(a) + \phi(b) \quad$ and $\quad \phi(ab) = \phi(a)\phi(b)$*

A *one-to-one* and *onto* ring homomorphism is an *Isomorphism.*

1.2.2 Some Definitions

Definition 1.10. ***Zero Divisor***

A nonzero element a in a commutative ring R is called a zero divisor if there is a nonzero element $b \in R$ such that $ab = 0$.

Definition 1.11. ***Integral Domain***

An Integral Domain is a commutative ring with unity that has no zero-divisors.

Definition 1.12. ***Units***

An element a in a ring R with unity is called a unit if it has a multiplicative inverse, i.e. if $\exists a^{-1} \in R$ such that $a \cdot a^{-1} = 1$.

Definition 1.13. ***Irreducibles****:*

Let R be a ring. An element $a \in R$ that is not a unit is called an irreducible element in R if $a = bc$ then either b or c is a unit.

Definition 1.14. ***Primes****:*

Let R be a ring. An element $a \in R$ that is not a unit is called a prime in R if $a \mid bc$ implies that either $a \mid b$ or $a \mid c$.

Remark 1.1. *Let R be an Integral Domain. Then every prime element $p \in R$ is irreducible.*

Note that the converse is not true in general.

Definition 1.15. ***Quotient Rings****:*

Let R be a ring, and $I \lhd R$, then the quotient ring, $R/I = (r + I) = \{r + i : \ r \in R, i \in I\}$.

Remark 1.2.

The operations of the ring R/I are defined as:

$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$ *and* $(r_1 + I)(r_2 + I) = (r_1 r_2) + I$.

If R is a commutative ring with unity 1, then so is the ring R/I whose identity is $(1 + I)$.

Definition 1.16. ***The Ring of Integers Mod*** n**,** $\mathbb{Z}_n$*:*

The ring of integers modulo n, $n \in \mathbb{Z}$ is the set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ under the operations of addition and multiplication (modulo n).

Remark 1.3. *If p is a prime integer, then $\mathbb{Z}_p$ is an integral domain.*

This is clear since p is a prime integer, then by Fermat's little theorem, every nonzero element $a \in \mathbb{Z}_p$ has a multiplicative inverse. (And by the finiteness of $\mathbb{Z}_p$, it's also a field).

Definition 1.17. ***The Quotient Ring*** $\mathbb{Z}/n\mathbb{Z}$

The quotient ring $\mathbb{Z}/n\mathbb{Z} = \{k + n\mathbb{Z} : k = 0, 1, 2, \ldots, n-1\}$ with the operations of addition and multiplication defined by:

$$\begin{aligned} (x + n\mathbb{Z}) + (y + n\mathbb{Z}) &= (x + y) + n\mathbb{Z} \\ (x + n\mathbb{Z}) \cdot (y + n\mathbb{Z}) &= (x \cdot y) + n\mathbb{Z} \end{aligned}$$

Theorem 1.1. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

Definition 1.18. ***Unique Factorization Domain - UFD -****:*

An Integral Domain R is called a unique factorization domain (UFD) if nonzero element $a \in R$ that is not a unit, can be written uniquely (up to associates and order of multiplication) of irreducible elements of R; i.e. $a = \pi \prod_{i=1}^{i=n} p_i$ where π is a unit.

Remark 1.4. *Let R be a UFD, then every irreducible element in R is prime in R.*

Proof. Let the ring R be a UFD and let $a \in R$ be an irreducible element in R. Suppose that $a \mid xy$ for some $x, y \in R$. Then $xy = ap$ for some $p \in R$. Since R is a UFD, then we can factor each of x and y as a product of irreducible elements in R. But, by the unique factorization property, a is an associate of an irreducible factor of either x or y, suppose $a = cd$ for some $d \mid x$. Then $x = d \cdot p_1 p_2 \cdots p_k = ca \cdot p_1 p_2 \cdot p_k \Rightarrow a \mid x$ □

Definition 1.19. ***Idempotent Elements:***

Let R be a ring. An element $a \in R$ is called an idempotent element of R if $a^2 = a$.

Remark 1.5. *The only idempotent elements in an Integral Domain are* 0 *and* 1

1.3 Fields

Definition 1.20. ***Field*** *A field is a commutative ring with unity in which every element is a unit.*

Theorem 1.2. *A finite integral domain is a field.*

Theorem 1.3. *Any finite field F has p^n elements, where p is a prime, $n \in \mathbb{Z}^+$.*

Definition 1.21. *Let F be a subfield of a field K, then K is called a field extension of F denoted by K/F. Furthermore; the degree of the field extension K/F is $[K/F]$ is the dimension of K as a vector space over F.*

1.4 Some Number Theory

1.4.1 Some preliminaries

Definition 1.22. ***Euler's Phi Function*** *Let $n \in \mathbb{Z}^+$, then Euler's Phi Function, denoted by $\Phi(n)$ is defined as the number of positive integers less than n and that are relatively prime to n. If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \in \mathbb{Z}^+$, then:*

$$\Phi(n) = n \cdot \prod_{i=1}^{i=r} \left(1 - \frac{1}{p_i}\right)$$

Lemma 1.1.

$$\sum_{d|n} \Phi(d) = \sum_{d|n} \Phi\left(\frac{n}{d}\right) = n \tag{1.1}$$

where $\Phi(n)$ is Euler's phi function

Proof. The first equality comes from the fact that an arbitrary divisor of n may also be written in the form $\left(\frac{n}{d}\right)$.

For the second equality:

Let: $1 \leqslant m \leqslant n$, and $gcd(m,n) = d$, then $gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$ and $1 \leqslant \frac{m}{d} \leqslant \frac{n}{d}$ then this sets up a bijection between those m, $1 \leqslant m \leqslant n-1$ for which $gcd(m,n) = d$ and the invertible classes modulo $\left(\frac{n}{d}\right)$, i.e. their number is $\Phi\left(\frac{n}{d}\right)$.

Furthermore; the only m of $1 \leqslant m \leqslant n$ with $gcd(m,n) = n$ is $m = n$ and hence $\Phi\left(\frac{m}{n}\right) = \Phi(1)$ by definition and hence, summing over all possible values of d we get the desired result. □

Definition 1.23. ***Bézout's Identity*** *For all* $m, n \in \mathbb{Z} \setminus \{0\}$, *with* $\gcd(m,n) = d$; *there exist* x, *and* $y \in \mathbb{Z}$ *such that:* $xm + yn = d$.

Remark 1.6. *As a result of Bézout's Identity, we get that; for any two relatively prime integers* m *and* n: *there exist* x *and* $y \in \mathbb{Z}$ *such that:* $mx + ny = 1$.

Lemma 1.2. *Let* m, n, $u \in \mathbb{Z}$ *and suppose that* $u \mid mn$ *with* $gcd(m,u) = 1$, *then* $u \mid n$.

1.4.2 Congruences

Definition 1.24. ***Linear Congruence:*** *Let* $z_1, z_2 \in \mathbb{Z}$ *and* $0 \neq n \in \mathbb{Z}$, *then* $n \mid (z_1 - z_2)$ *is written in terms of the linear congruence:* $z_1 \equiv z_2 \mod n$.

Lemma 1.3. *Let* $m, n, a, b \in \mathbb{Z}$ *with* $\gcd(m,n) = 1$ *such that;* $an \equiv bn \mod m$ *then:*

$$a \equiv b \mod m$$

Theorem 1.4 ([14], pages 192-193)**.** ***Law of quadratic reciprocity*** *Let* p *and* q *be two distinct primes, then:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{(p-1)}{2}\right)\left(\frac{(q-1)}{2}\right)}$$

We'll consider the number of solutions to certain types of quadratic congruence:

Lemma 1.4 ([15], exercise 2.2.8, page 63)**.** *Let* p *be an odd prime integer, then the congruence:* $x^2 \equiv 1 \mod p^\alpha$ *has only two solutions:* $x \equiv 1 \mod p^\alpha$ *and* $x \equiv -1 \mod p^\alpha$.

Proof. Let $x^2 \equiv 1 \mod p^\alpha$, then $p^\alpha \mid (x^2 - 1) \Rightarrow p^\alpha \mid (x-1)(x+1)$. So, we have two cases:

Case 1. If the gcd $\Big(p^\alpha, (x-1)\Big) > 1$ then $p \mid (x-1)$ since the only divisors of p^α are powers of p. And since p is an odd prime, $p > 2$, then $p \nmid (x+1) \Rightarrow \gcd\Big(p^\alpha, (x+1)\Big) = 1$. Then by *lemma* (1.2), page 8, we see that:

$$p^\alpha \mid (x-1)(x+1) \Rightarrow p^\alpha \mid (x-1). \text{ i.e. } x \equiv 1 \mod p^\alpha.$$

Case 2. If the gcd $\Big(p^\alpha, (x-1)\Big) = 1$, then, by *lemma* (1.2), we see that:

$$p^\alpha \mid (x-1)(x+1) \Rightarrow p^\alpha \mid (x+1) \Rightarrow x \equiv -1 \mod p^\alpha$$

□

Lemma 1.5 ([15], exercise 2.2.9, page 63)**.** *Concerning the quadratic congruence:* $x^2 \equiv 1 \mod 2^k$

$$\textit{Its number of solutions} \begin{cases} \textit{for } k = 1 & \textit{is } \underline{\textit{one}} \textit{ solution} \\ \textit{for } k = 2 & \textit{is } \underline{\textit{two}} \textit{ solutions} \\ \textit{for } k \geq 3 & \textit{is precisely the } \underline{\textit{four}} \textit{ solutions:} \\ & 1,\ 2^{k-1}-1,\ 2^{k-1}+1,\ -1 \end{cases}$$

Proof.

1. For $k = 1$; $x^2 \equiv 1 \mod 2$, but we have that $\forall\ x \in \mathbb{Z}$,
   then either $x \equiv 0 \mod 2$, or $x \equiv 1 \mod 2$,
   then squaring both of these congruences gives us:

$$\left.\begin{array}{l} x \equiv 0 \mod 2 \Rightarrow\ x^2 \equiv 0 \mod 2 \\ x \equiv 1 \mod 2 \Rightarrow\ x^2 \equiv 1 \mod 2 \end{array}\right\} \Rightarrow \quad x^2 \equiv 1 \mod 2 \quad \text{if and only if} \quad x \equiv 1 \mod 2$$

2. For $k = 2$; $x^2 \equiv 1 \mod 2^2 \iff x^2 \equiv 1 \mod 4$:

But, we know that $\forall\, x \in \mathbb{Z}; \quad x \equiv 0, \quad 1, \quad 2 \quad \text{or} \quad 3 \mod 4,$

Then, squaring each of these congruences, we get:

$$\begin{aligned} x \equiv 0 \mod 4 &\Rightarrow x^2 \equiv 0 \mod 4 \\ x \equiv 1 \mod 4 &\Rightarrow x^2 \equiv 1 \mod 4 \\ x \equiv 2 \mod 4 &\Rightarrow x^2 \equiv 0 \mod 4 \\ x \equiv 3 \mod 4 &\Rightarrow x^2 \equiv 1 \mod 4 \end{aligned}$$

Which implies that: $x^2 \equiv 1 \mod 4 \Rightarrow x \equiv 1 \mod 4$ or $x \equiv 3 \mod 4$.

3. For $k \geq 3$, $x^2 \equiv 1 \mod 2^k \Rightarrow 2^k \mid (x^2 - 1) \iff 2^k \mid (x-1)(x+1)$.

   Here we have three cases to consider:

   Case 1. When the $\gcd\Big(2^k, (x+1)\Big) = 1$, then by *lemma* (1.2), we have:

   $$2^k \setminus (x-1) \quad \Rightarrow \quad x \equiv 1 \mod 2^k$$

   Case 2. When the $\gcd\Big(2^k, (x-1)\Big) = 1$, then by the same *lemma* (1.2) we have:

   $$2^k \mid (x+1) \quad \Rightarrow \quad x \equiv -1 \mod 2^k$$

   Case 3. When the $\gcd\Big(2^k, (x-1)\Big) > 1$ and the $gcd\Big(2^k, (x+1)\Big) > 1$; note that the only divisors of 2^k are powers of $2 \Rightarrow 2 \mid (x+1)$ and $2 \mid (x-1)$. And

   $$2^k \,\Big|\, (x+1)(x-1) \;\Rightarrow\; 2^{k-2} \,\Big|\, \left(\frac{(x+1)}{2}\right)\left(\frac{(x-1)}{2}\right) \tag{1.2}$$

   Note that equation 2.2 is well defined since $k > 2$.

   Now, since $\frac{(x+1)}{2} = \frac{(x-1)}{2} + 1$, then:

   either $\gcd\Big(2^{k-2}, \frac{(x+1)}{2}\Big) = 1 \quad$ or $\quad \gcd\Big(2^{k-2}, \frac{(x-1)}{2}\Big) = 1$ depending on

whether $\frac{(x-1)}{2}$ is even or odd. Then, by *lemma* (1.2) we have:

$$2^{k-2} \left| \left(\tfrac{(x+1)}{2}\right) \quad \text{or} \quad 2^{k-2} \right| \left(\tfrac{(x-1)}{2}\right) \quad \Rightarrow \quad 2^{k-1} \left| (x+1) \right. \quad \text{or} \quad 2^{k-1} \left| (x-1) \right.$$

And this leaves us with four possible congruences of x modulo 2^k; two of which have already been considered ($x \equiv 1 \mod 2^k$ and $x \equiv -1 \mod 2^k$). And the other two possibilities are:

$$x \equiv 2^{k-1} - 1 \mod 2^k \quad \text{and} \quad x \equiv 2^{k-1} + 1 \mod 2^k.$$

Hence; $x^2 \equiv 1 \mod 2^k$ has 4 solutions for $k \geq 3$; namely:

$$1, \quad 2^{k-1} - 1, \quad 2^{k-1} + 1, \quad \textit{and} \quad -1 \tag{1.3}$$

□

As a direct consequence of the last lemma, we consider the following two results:

Corollary 1.1. *The solutions to the quadratic congruence* $x^2 \equiv a \mod 2^k$, *for* $k \geq 3$ *are:*

$$a, \quad 2^{k-1} - a, \quad 2^{k-1} + a, \quad \textit{and} \quad -a$$

Proof. Suppose $x \equiv x_0 \mod 2^k \quad \Rightarrow \quad x^2 \equiv x_0^2 \mod 2^k$ which implies:

$$2^k \left| (x^2 - x_0^2) \right. \quad \Longleftrightarrow \quad 2^k \left| (x + x_0)(x + x_0) \right.$$

where we have three cases:

Case 1. If $\gcd\left(2^k, (x + x_0)\right) = 1, \Rightarrow 2^k \left| (x - x_0) \right. \Rightarrow x \equiv x_0 \mod 2^k$.

Case 2. If $\gcd\left(2^k, (x - x_0)\right) = 1, \Rightarrow 2^k \left| (x + x_0) \right. \Rightarrow x \equiv -x_0 \mod 2^k$.

Case 3. If $\gcd\Big(2^k,(x-x_0)\Big) > 1 \quad$ and $\quad \gcd\Big(2^k,(x+x_0)\Big) > 1$; since the only divisors of 2^k are powers of 2, then this $\Big($along with the fact that $2^k \;\Big|\; (x+x_0)(x-x_0)\Big)$ implies:

$$2^{k-2} \;\Big|\; \left(\frac{(x+x_0)}{2}\right)\left(\frac{(x-x_0)}{2}\right) \tag{1.4}$$

Note that equation 2.4 is well defined since $k > 2$. Also, $\frac{(x+x_0)}{2} = \frac{(x-x_0+2x_0)}{2} = \frac{(x-x_0)}{2} + x_0$ then either $\gcd\Big(2^{k-2}, \frac{(x+x_0)}{2}\Big) = 1 \quad$ or $\quad \gcd\Big(2^{k-2}, \frac{(x-x_0)}{2}\Big) = 1$ depending on whether $\Big(\frac{(x-x_0)}{2}\Big)$ is even or odd. Then, by *lemma* (1.2) we have:

$$2^{k-2} \;\Big|\; \Big(\tfrac{(x+x_0)}{2}\Big) \quad \text{or} \quad 2^{k-2} \;\Big|\; \Big(\tfrac{(x-x_0)}{2}\Big) \quad \Rightarrow \quad 2^{k-1} \;\Big|\; (x+x_0) \quad \text{or} \quad 2^{k-1} \;\Big|\; (x-x_0)$$

And this leaves us with four possible congruences of x modulo 2^k; two of which are:

$$\Big(x \equiv x_0 \mod 2^k \quad \textit{and} \quad x \equiv -x_0 \mod 2^k\Big)$$

And the other two possibilities are:

$$x \equiv 2^{k-1} - x_0 \mod 2^k \quad \text{and} \quad x \equiv 2^{k-1} + x_0 \mod 2^k.$$

Hence; $\quad x^2 \equiv a \mod 2^k \quad$ has $\quad$ 4 solutions for $k \geq 3$; namely:

$$a, \quad 2^{k-1} - a, \quad 2^{k-1} + a, \quad \textit{and} \quad -a$$

□

Lemma 1.6. *Let* $k, a \in \mathbb{Z}$ *with* $\gcd(k,a) = 1$ *and* a *is an odd integer.*
Concerning the solutions to $x^2 \equiv a \mod 2^k$.

Solution 1.1. *The solutions to* $x^2 \equiv a \mod 2^k$ *are:*

Case 1. For $k = 1$, $(x^2 \equiv a \mod 2)$ *has one solution, namely:* $x \equiv 1 \mod 2$

Case 2. For $k = 2$, $(x^2 \equiv a \mod 4)$ *has a solution if and only if* $a \equiv 1 \mod 4$, *and these solutions are:* $x \equiv 1 \mod 4 \quad$ *and* $\quad x \equiv 3 \mod 4$ *Note that; for any odd integer*

$m = 2n + 1$, $m^2 = 4n^2 + 4n + 1$, *i.e.* $m^2 \equiv 1 \mod 4$ *(For an odd integer* m*, its square value is congruent to* 1 *modulo* 4.

So, for $x^2 \equiv a \mod 4$ *to have a solution, then* $a = 4l + 1$*. Therefore, for that* $a = 4l + 1$, $x^2 \equiv 1$, *or* $\equiv 9(\mod 4)$, *i.e.* $x \equiv 1 \mod 4$ *or* $x \equiv 3 \mod 4$.

Case 3. For $k \geq 3$, $(x^2 \equiv a \mod 2^k)$ *has four unique solutions if* $a \equiv 1 \mod 8$ *and no solutions otherwise.*

Theorem 1.5. ***The Chinese Remainder Theorem*** *([12], Chapter 5)*

Let $m \in \mathbb{Z}$ *such that* $m = n_1 n_2 \cdots n_r$ *where the* n_i*'s* $\in \mathbb{Z}$ *are pairwise relatively prime; then:*

$\mathbb{Z}_m \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r}$

1.5 Special Rings

1.5.1 The Ring Of Gaussian Integers $\mathbb{Z}[i]$

The set of Gaussian integers: $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$

$\mathbb{Z}[i]$ is a ring under the operations: addition and multiplication defined by:

$(a + bi) + (c + di) = (a + c) + (b + d)i$ and $(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$.

Remark 1.7. $\mathbb{Z}[i]$ *is an integral domain*

Definition 1.25. ***The Conjugate of*** z

Let $z_1 = x + yi \in \mathbb{Z}[i]$*, then the conjugate of* z_1, $\overline{z_1}$, *is* $\overline{z_1} = x - yi$.

Definition 1.26. ***The Norm Function***

The norm of an element $z = (x + yi) \in \mathbb{Z}[i]$ *is defined as* $N(z)$*:*

$N(z) = z \cdot \overline{z} = (x + yi) \cdot (x - yi) = x^2 + y^2$

Note that $\forall z \in \mathbb{Z}[i]$, $N(z) \geq 0$.

Lemma 1.7. *([13], Ch.12, page 235) Over* $\mathbb{Z}[i]$*, the norm function,* N*, is multiplicative: i.e. For* $u, v \in \mathbb{Z}[i]$, $N(uv) = N(u)Nv$

Proof.

Let $z_1 = (x + yi), z_2 = (u + vi) \in \mathbb{Z}[i]$, then:

$$N(z_1) \cdot N(z_2) = (x^2 + y^2)(u^2 + v^2) = \underline{x^2u^2} + \underline{\underline{x^2v^2}} + \underline{\underline{y^2u^2}} + \underline{y^2v^2} =$$
$$= \underline{x^2u^2 + y^2v^2 - 2(xu)(yv)} + \underline{\underline{x^2v^2 + y^2u^2 + 2(xv)(yu)}} =$$
$$= (xu - yv)^2 + (xv + yu)^2 = N(z_1 \cdot z_2)$$ □

Corollary 1.2 ([18], proposition 3.4.1, page 50)**.** *The only units in* $\mathbb{Z}[i]$ *are:* $\pm 1, \pm i$

Proof. Firsly, every element in $\{1, -1, i, -i\}$ is a unit since; 1 and -1 are their own inverses, and i and $-i$ are the inverses of each other.

On the other hand, suppose $z_1 \in \mathbb{Z}[i]$ is a unit, and let $z_1^{-1} = z_2$; i.e. $z_1 z_2 = 1$.

Then, taking the norm of both sides of the last equation, and using the multiplicative property, we get: $N(z_1 z_2) = N(z_1)N(z_2) = N(1) = 1$ Recall that N is a nonnegative integer, then the only possible solution is that $N = \pm 1$, but $N \geq 0 \rightarrow N = 1$, i.e. $x^2 + y^2 = 1$ whose only integral solutions are ($a = \pm 1$, and $b = 0$) or ($a = 0$, and $b = \pm 1$) which yields: $z_1 = \pm 1$, and $z_1 = \pm i$. □

Theorem 1.6 ([13], Ch.12, page 235)**.** *Let* $z_1, z_2 \in \mathbb{Z}[i]$*. If* $z_1 \mid z_2$ *then* $N(z_1) \mid N(z_2)$

Proof. Let $z_1, z_2 \in \mathbb{Z}[i]$ such that $z_1 \mid z_2$, then $z_2 = z_1 \cdot w$ for some $w \in \mathbb{Z}[i]$, then:

$N(z_2) = N(z_1 w) = N(z_1)N(w) \Rightarrow N(z_1) \mid N(z_2)$ □

Corollary 1.3. $\forall z \in \mathbb{Z}[i]$ $N(z)$ *is even if and only if* z *is a multiple of* $(1 + i)$*.*

Proof. Let $z = w \cdot (1 + i)$ for any $w \in \mathbb{Z}[i]$. since $N(1 + i) = 1^2 + 1^2 = 2$,

then $N(z) = N(w) \cdot N(1 + i) = 2 \cdot N(w)$, hence, it's even.

Conversely; Let $z = x + yi$ has an even norm. Then $N(z) = x^2 + y^2 \equiv 0 \mod 2$. By considering cases; first, note that if only one of x or y is an odd integer and the other is even, then $x^2 + y^2$ is an odd integer too. W.L.O.G. suppose x is even, say $(2m)$, and y is odd, say $(2n+1)$. Then: $x^2 + y^2 = (2m)^2 + (2n+1)^2 = 4m^2 + 4n^2 + 4n + 1 = 2(2m^2 + 2n^2 + 2n) + 1$ which is odd.

Now, assume x and y are both even, say $x = 2m$ and $y = 2n$. Then:

$x^2 + y^2 = 4m^2 + 4n^2 = 2(2m^2 + 2n^2)$

On the other hand, if x and y are both odd, say $x = 2m + 1$ and $y = 2n + 1$: Then:

$x^2 + y^2 = (2m+1)^2 + (2n+1)^2 = 4m^2 + 4m + 1 + 4n^2 + 4n + 1 = 2(2m^2 + 2n^2 + 2m + 2n + 1)$

Deducing: $x \equiv y \mod 2$; $\Rightarrow x - y \equiv 0 \mod 2$ and $x + y = (x - y) + 2y \equiv 2y \equiv 0 \mod 2$.

$$x + yi = \left(\frac{(x+y)+(x-y)}{2}\right) + \left(\frac{(x+y)-(x-y)}{2}\right) i = (1+i)\left(\frac{(x+y)}{2} + \frac{(y-x)}{2} i\right)$$

□

Theorem 1.7 ([18], lemma 3.4.2, page 50)**.** *Let $z \in \mathbb{Z}[i]$, then if $N(z)$ is prime in $\mathbb{Z}$ then z is prime in $\mathbb{Z}[i]$, but the converse is not true in general.*

Proof. Let $z = uv \in \mathbb{Z}[i]$ be of a prime norm $p \in \mathbb{Z}^+$. Then, $p = N(z) = N(u)N(v) \Rightarrow$ either $N(u) = 1$ or $N(v) = 1$, i.e. either u or v is a unit. So z is a prime element in $\mathbb{Z}[i]$.
The converse is not true in general, for example, 3 is a prime in $\mathbb{Z}$ but $N(3) = 9$. □

Lemma 1.8.

Let $0 \neq z \in \mathbb{Z}[i]$, then the divisors u_i of z with $N(u_i) = 1$ or $N(u_i) = N(z)$ are units or units multiple of z

Proof. Suppose $u \mid z$ with $N(u) = 1$, then $u = \pm 1$ or $u = \pm i$.
On the other hand, if $N(u) = N(z)$ Then, since $z = uv \Rightarrow N(z) = N(u)N(v) = N(z)N(v)$ $\Rightarrow N(v) = 1$ and so: $v = \pm 1$ or $v = \pm i$. Thus, $v = \pm z$ or $v = \pm iz$. Hence, $u = \pm z$ or $u = \pm iz$. □

Theorem 1.8. ***Unique Factorization****([13], Ch.12, Theorem 215, page 238) Every $z \in \mathbb{Z}[i]$ with a norm $N(z) > 1$ can be written uniquely as a product of primes in $\mathbb{Z}[i]$.*

Proof. we shall prove this theorem by *Strong* induction on $N(z)$:
Let $z \in \mathbb{Z}[i]$ such that $N(z) > 1$.
Suppose that $N(z) = 2$ which means that $z = 1 \pm i$ or $z = -1 \pm i$. Then, by *Theorem* (1.7), z is a prime in $\mathbb{Z}[i]$.
Now, suppose that $\forall\ \underline{z} \in \mathbb{Z}[i]$ with $1 < N(z) < k$ $\underline{z}$ is a product of primes in $\mathbb{Z}[i]$. Then:
If there isn't any Gaussian integer with $N(z) = n$, then there is nothing to prove.

So, suppose there is a $z \in \mathbb{Z}[i]$ such that $N(z) = n$. If n is a prime, then we're done. If not, that is, if n is a composite integer, then write z as a non-trivial factorization: $z = uv$ with $N(u)$, $N(v) < N(z) = n$, and by our inductive hypothesis, u and v are each a product of primes in $\mathbb{Z}[i]$. Hence, $z = uv$ is a product of primes.

Now, to prove uniqueness: If z is a prime, then it's clearly unique. And if $N(z) = 2$, then, as we have seen above that such a z is prime. Proceeding by induction on z:

Now, for the cases $N(z) \geq 3$: assume that every $z \in \mathbb{Z}[i]$ with $1 < N(z) < n$, z has a unique factorization of primes in $\mathbb{Z}[i]$.

So, let z has a norm $N(z) = n$ and assume that z has two factorizations:

$$z = u_1 u_2 \cdots u_k = v_1 v_2 \cdots v_l \tag{1.5}$$

Now, since u_1 is a prime and $u_1 \mid z \Rightarrow u_1 \mid v_1 v_2 \cdots v_l$. And since the v_i's are all primes, then $u_1 \mid v_j$ for some j. Reordering, we may write $u_1 \mid v_{j_1}$, but u_1 and v_{j_1} are primes, then $u_1 = \varepsilon v_{j_1}$ for some unit $\varepsilon \in \{\pm 1, \pm i\}$. Then the factorization equation (1.5) will become:

$$z = \varepsilon v_{j_1} u_2 \cdots u_k = v_{j_1} v_2 \cdots v_l \tag{1.6}$$

Cancelling v_{j1} from both sides leads:

$$z_1 = \varepsilon u_2 u_3 \cdots u_k = v_2 v_3 \cdots v_l \tag{1.7}$$

$$Note, \quad N(z_1) = \left(\frac{N(z)}{N(v_{j_1})} \right) < N(z)$$

Now, note that since ε is a unit, then εu_2 is a prime, and equation (2.8) gives us two prime factorizations for z_1, and by our inductive hypothesis, z_1 has a unique prime factorization with $k-1$ primes on the left and $l-1$ ones on the right. Therefore, $k - 1 = l - 1 \Rightarrow k = l$ along with some reordering, we get $u_i = \varepsilon v_{j_i}$. And therefore the factorization of z is unique. Note that, *Remark* (1.7) on page 13 implies that $\mathbb{Z}[i]$ is a UFD. □

As a direct consequence of this theorem, we get the following corollary:

Corollary 1.4. *Let $w \in \mathbb{Z}[i]$ be a prime. Then $uv \equiv 0 \mod w$ if and only if $u \equiv 0 \mod w$ or $v \equiv 0 \mod w$.*

Theorem 1.9 ([18], Theorem 3.4.3, page 51)**.** *Every prime $p \in \mathbb{Z}^+$ is a composite integer in $\mathbb{Z}[i]$ if and only if it is a sum of two squares.*

Proof. Let $p \in \mathbb{Z}^+$ be a prime that is composite in $\mathbb{Z}[i]$, say $p = uv$ for some non-units u, $v \in \mathbb{Z}[i]$. Then, $N(p) = p^2 = N(u)N(v) \Rightarrow N(u) = p$, letting $u = x + yi$, then $p = N(u) = x^2 + y^2$. Conversely; Let p be a prime in $\mathbb{Z}^+$ that is a sum of two squares, say, $p = x^2 + y^2$, then $p = (x + yi)(x - yi)$ is a composition of p in $\mathbb{Z}[i]$. □

Theorem 1.10 ([18], ch.3)**.** *Let $p \in \mathbb{Z}^+$ be a prime integer such that $p \equiv 3 \mod 4$, then p is not a sum of two squares and it would also be prime in $\mathbb{Z}[i]$.*

Proof. First of all, let $x \in \mathbb{Z}$, then x is either even or odd. If x is even, then $x = 2k$ for some $k \in \mathbb{Z}^+ \Rightarrow x^2 = 4k^2 \equiv 0 \mod 4$.
If x is odd, then $x = 2k+1$ for some $k \in \mathbb{Z}^+$ then $x^2 = (2k+1)^2 = 4k^2+4k+1 \equiv 1 \mod 4$. So, the square of an integer is either 0 or 1 $\mod 4$. Now, adding any two squares ($\mod 4$): $(0 + 0 = 0)$, $(1 + 0 = 1)$, $(1 + 1 = 2)$ ($\mod 4$). In each case we never get 3 $\mod 4$, so any prime $p \in \mathbb{Z}^+$ that is not congruent to 3 modulo 4 cannot be a sum of two squares.
Moreover, in view of *theorem* (1.9), if a regular prime p is not a sum of two squares, then it cannot be composite in $\mathbb{Z}[i]$ and hence it is prime in $\mathbb{Z}[i]$. □

Note, 2 is a special case, since $2 = (1+i)(1-i)$ but $(1+i) = i(1-i)$ and $(1-i) = -i(1+i)$. That is, the factors of 2 are each a unit multiple of each other. and so $2 = -i(1 + i)^2$.

Theorem 1.11 ([18], ch.3)**.** *Let $p \in \mathbb{Z}^+$ be a prime integer; then the following are equivalent:*

(1) $p = 2$ or $p \equiv 1 \mod 4$.

(2) The congruence equation: $x^2 \equiv -1 \mod 4$ has a solution.

(3) $p = x^2 + y^2$ for some x, $y \in \mathbb{Z}$.

Proof. To show (1) $\Rightarrow$ (2): If $p = 2$, then every odd integer satisfies the congruence $x^2 \equiv -1 \mod 2$.

Now Let p be an odd prime in $\mathbb{Z}^+$ such that $p \equiv 1 \mod 4$: Consider the polynomial factorization:

$$W^{p-1} - 1 = \left(W^{\left(\frac{(p-1)}{2}\right)} - 1\right)\left(W^{\left(\frac{(p-1)}{2}\right)} + 1\right) \tag{1.8}$$

where the coefficients are taken modulo p. Counting the number of roots of these polynomials, keeping in mind that the number of roots of any polynomial of degree k is less or equal to k.

The left hand side of (2.9) has the nonzero integers $\mod p$ as roots, which are $(p-1)$ in number by Fermat's little theorem.

While on the right hand side, the first polynomial, $\left(W^{\left(\frac{(p-1)}{2}\right)} - 1\right)$ is of degree $(p-1)/2$ and so the number of its roots is at most $(p-1)/2$ ($\mod p$). And this implies that the second polynomial, $\left(W^{\left(\frac{(p-1)}{2}\right)} + 1\right)$ must have some roots ($\mod p$), say r. That is: r satisfying the congruence equation: $r^{\left(\frac{(p-1)}{2}\right)} \equiv -1 \mod p$.

Now, $p \equiv 1 \mod 4$ by hypothesis assumption, so $p = 4m + 1$ for some $m \in \mathbb{Z}$. So, $\left(\frac{(p-1)}{2}\right) = 2m$ (an even integer) and so, $r^{\left(\frac{(p-1)}{2}\right)} \equiv -1 \mod p \Leftrightarrow (r^m)^2 \equiv -1 \mod p$ proving (2).

Now, to show (2) $\Rightarrow$ (3): Suppose for some $x \in \mathbb{Z}$ satisfies $x^2 \equiv -1 \mod p$, this implies that $p \mid (x^2 + 1)$ (in $\mathbb{Z}$), and so (in $\mathbb{Z}[i]$):

$$p \mid (x + i)(x - i) \tag{1.9}$$

Claim: p is a composite integer in $\mathbb{Z}[i]$. For, if not: letting p be a Gaussian prime. Then, by equation (2.10), $p \mid (x + i)$ or $p \mid (x - i)$. Which implies $(x \pm i) = p(a + bi) \Rightarrow pb = \pm 1$ which is impossible. Hence p is composite in $\mathbb{Z}[i]$ and therefore p is a sum of two squares by *theorem* (1.9).

We have already proven that (3) $\Rightarrow$ (1) above. $\square$

Theorem 1.12. *([18], Theorem 3.4.11, page 54) Let u be a prime in $\mathbb{Z}[i]$, then u is a unit multiple of one of the following:*

(i) $(1+i)$

(ii) v *or* $\overline{v}$ *with* $N(v) = p$, *where* p *is a prime in* $\mathbb{Z}$ *and* $p \equiv 1 \mod 4$

(iii) p *where* p *is a prime in* $\mathbb{Z}^+$ *and* $p \equiv 3 \mod 4$

Note that the norm of the primes in part (i) and (ii) are also primes in $\mathbb{Z}^+$. But the norms of the primes in part (iii) are of the form p^2 where p is a prime in $\mathbb{Z}^+$ and $p \equiv 3 \mod 4$. Also note that if $u \in \mathbb{Z}[i]$ is a prime, then $N(u) = p$ or $= p^2$ where p is a prime in $\mathbb{Z}^+$ and $u \mid p$. Moreover, note that if $u \in \mathbb{Z}[i]$ is a prime such that $u \neq (1+i)$ or $u \neq \alpha \cdot (1+i)$ where α is a unit, then $N(u)$ is an odd integer. So, if $u \in \mathbb{Z}[i]$ such that $N(u)$ is even, then u is divisible by $(1+i)$.

Lemma 1.9 ([9], Theorem 1, page 604)**.** *If $a \in \mathbb{Z}^+$ such that $a > 1$, then $\mathbb{Z}[i]/\langle a \rangle \cong \mathbb{Z}_a[i]$*

Proof. Define $\phi : \mathbb{Z}[i] \to \mathbb{Z}_a[i]$ by $\phi(x+yi) = [x]_a + [y]_a i$, where $[\ \cdot\ ]_a$ represents the equivalence class modulo a.

Note that ϕ is a surjective ring homomorphism; since $\phi(a) = [a]_a = [0]_a$ so $a \in \ker(\phi)$ and hence $\langle a \rangle \subseteq \ker(\phi)$. On the other hand:

if $\phi(x+yi) = 0$, then both x and y are congruent to $0 \mod a$, so $x = ax'$ and $y = ay'$ for some x', $y' \in \mathbb{Z}$.

$\Rightarrow x + yi = ax' + ay'i = a(x' + y'i) \in \langle a \rangle$.

$\Rightarrow \ker(\phi) = \langle a \rangle$ and by the First Isomorphism Theorem for rings, we have:

$$\mathbb{Z}[i]/\langle a \rangle \cong \mathbb{Z}_a[i]. \qquad \square$$

Corollary 1.5. $\mathbb{Z}[i]/\langle (1+i)^n \rangle \cong \mathbb{Z}_{2^{n/2}}[i]$

Proof. Note that since $(1+i)^2 = 2i$, then the ideal $\langle (1+i)^n \rangle$ can be written as:

$\langle (1+i)^n \rangle = \langle (2i)^{n/2} \rangle = \langle 2^{n/2} \rangle$,

Therefore, by *Lemma* (1.9) above: $\mathbb{Z}[i]/\langle (1+i)^n \rangle = \mathbb{Z}[i]/\langle 2^{n/2} \rangle \cong \mathbb{Z}_{2^{n/2}}[i]$. $\square$

1.5.2 The Ring of Eisenstein Integers $\mathbb{Z}[\rho]$

Definition 1.27. *The ring of Eisenstein integers;* $\mathbb{Z}[\rho] = \{x+y\rho : x, y \in \mathbb{Z},\ \ \rho^2+\rho+1 = 0\}$

Note that $\rho = e^{\frac{2}{3}\pi i} = \frac{1}{2}\left(-1 + i\sqrt{3}\right)$, so ρ satisfies $\rho^2 + \rho + 1 = 0$.

The three cubic roots of unity are: 1, ρ and ρ^2, and the ring $\mathbb{Z}[\rho]$ is the ring of algebraic integers in the quadratic extension $\mathbb{Q}(\sqrt{-3})$ of $\mathbb{Q}$.

The elements of $\mathbb{Z}[\rho]$ are complex numbers of the form $u = a + b\rho$ with a, $b \in \mathbb{Z}$.

Let $u = a + b\rho \in \mathbb{Z}[\rho]$ and the complex conjugate of u is $\overline{u} = a + b\rho^2$.

Definition 1.28. *For each* $u = a + b\rho \in \mathbb{Z}[\rho]$*, the* ***Norm*** *is defined by:*

$$N(u) = u \cdot \overline{u} = (a + b\rho) \cdot (a + b\rho^2) = a^2 + b^2 - ab = \left(a - \frac{1}{2}b\right) + \frac{3}{4}b^2 \geq 0 \qquad (1.10)$$

Lemma 1.10. *Over* $\mathbb{Z}[\rho]$*, the norm function is multiplicative:*

i.e. For $u, v \in \mathbb{Z}[\rho]$*,* $N(uv) = N(u)N(v)$*.*

Proof. Let $u = a + b\rho, v = c + d\rho \in \mathbb{Z}[\rho]$, then:

$N(u) = a^2 + b^2 - ab$ and $N(v) = c^2 + d^2 - cd$.

Now, $uv = (a + b\rho)(c + d\rho) = ac + ad\rho + bc\rho + bd\rho^2$, but $\rho^2 = -1 - \rho$, so:

$$\begin{aligned} N(u)N(v) &= (a^2 + b^2 - ab)(c^2 + d^2 - cd) \\ &= a^2c^2 + a^2d^2 - a^2cd \\ &+ b^2c^2 + b^2d^2 - b^2cd \\ &- abc^2 - abd^2 + abcd \end{aligned}$$

On the other hand, $uv = (ac - bd) + (ad + bc - bd)\rho$ and so:

$$\begin{aligned}
N(uv) &= (ac-bd)^2 + (ad+bc-bd)^2 - (ac-bd)(ad+bc-bd) \\
&= a^2c^2 + b^2d^2 - 2abcd + a^2d^2 + b^2c^2 \\
&+ 2abcd + b^2d^2 - 2abd^2 - 2b^2cd - a^2cd \\
&- abc^2 + abcd + abd^2 + b^2cd - b^2d^2 \\
&= a^2c^2 + a^2d^2 - a^2cd \\
&+ b^2c^2 + b^2d^2 - b^2cd \\
&- abc^2 - abd^2 + abcd \\
&= (a^2 + b^2 - ab)(c^2 + d^2 - cd) \\
&= N(u)N(v)
\end{aligned}$$

□

Lemma 1.11. $\mathbb{Z}[\rho]$ *is an* ***Integral Domain****.*

Proof. Let $a, b \in \mathbb{Z}[\rho]$ and suppose that $0 \notin \{a, b\}$ and $ab = 0$.

Let $a = x_1 + x_2\rho$, $b = y_1 + y_2\rho$, where x_1, x_2, y_1, y_2 are nonzero integers (by assumption of the non-zero-ness of a and b). Then we have:

$0 = ab = (x_1 + x_2\rho)(y_1 + y_2\rho) = x_1y_1 + x_1y_2\rho + x_2y_1\rho + x_2y_2\rho^2 \neq 0$ since non of the four terms on the right hand side is equivalent to zero. Therefore, $\mathbb{Z}$ is an Integral Domain. □

Proposition 1.1. $\mathbb{Z}[\rho]$ *is an* ***Euclidean Domain****.*

Proof.

Let N denote the norm on $\mathbb{Q}$. Let u and v be two elements of $\mathbb{Z}[\rho]$ with $u \neq 0$. Then $\frac{u}{v} = \frac{u\overline{v}}{v\overline{v}}$. But $v\overline{v} = N(v)$ is a positive integer. Also, $u\overline{v}$ lies in $\mathbb{Z}[\rho]$ since both u and $\overline{v}$ are elements of $\mathbb{Z}[\rho]$ and $\mathbb{Z}[\rho]$ is a ring. So, $\frac{u}{v} = \frac{u\overline{v}}{v\overline{v}} = r + sw$ for some r, $s \in \mathbb{Q}$.

Now, choose m, $n \in \mathbb{Z}$ such that $|r - m| \leq \frac{1}{2}$ and $|s - n| \leq \frac{1}{2}$ and set $z = m + nw$ then $z \in \mathbb{Z}[\rho]$ and

$$N\Big(\frac{u}{v} - z\Big) = (r-m)^2 - (r-m)(s-n) + (r-n)^2$$

$$\leq \left(\frac{1}{2}\right)^2 + \frac{1}{2}\cdot\frac{1}{2} + \left(\frac{1}{2}\right)^2 = \frac{3}{4} < 1$$

Now, set $\tau = u - zv$ then $\tau \in \mathbb{Z}[\rho]$ and either $\tau = 0$ or:

$$N(\tau) = N\left(v\left(\frac{u}{v} - z\right)\right) = N(v)\cdot N\left(\frac{u}{v} - z\right) \leq \frac{3}{4} \times N(v) < N(v)$$

So, the norm N makes $\mathbb{Z}[\rho]$ into an Euclidean Domain. □

Remark 1.8. *Since the ring $\mathbb{Z}[\rho]$ with the norm described above is an Euclidean Domain, ED then it is a PID and hence a UFD.*

Lemma 1.12. *([13], Ch.12, sec. 12.9, page 241-242) Let $\varepsilon \in \mathbb{Z}[\rho]$, then ε is a unit if and only if $N(\varepsilon) = 1$. Moreover, the only units in $\mathbb{Z}[\rho]$ are $\{\pm 1, \pm\rho, \pm\rho^2\}$.*

Definition 1.29.

Let u, $v \in \mathbb{Z}[\rho]$. Then u and v are associates if there exists a unit ε such that $u = \varepsilon v$

Note that if $u \in \mathbb{Z}[\rho]$ then the associates of u are:

$$u, \quad -u \quad , \quad \rho u \quad , \quad -\rho u \quad , \quad \rho^2 u \quad , \quad -\rho^2 u$$

Definition 1.30.

Let $u \in \mathbb{Z}[\rho]$, then u is called a prime in $\mathbb{Z}[\rho]$ if u is not a unit and whenever $u|vw$ implies that $u|v$ or $u|w$.

Theorem 1.13. ***Classification of Eisenstein primes*** *([7], Theorem 8, page 65)*
The primes of $\mathbb{Z}[\rho]$ are (up to multiplication by a unit):

1. *Rational primes $p \in \mathbb{Z}$ such that $p = 2$ or $p \equiv 5 \mod 6$.*
2. *The Eisensteinen integers, $u = x + y\rho$ with $(x^2 + y^2 - xy) = p$ where p is a rational prime in $\mathbb{Z}$ and $p \equiv 1 \mod 6$.*
3. *The number $\lambda = 1 - \rho$.*

Proposition 1.2. *Let $u \in \mathbb{Z}[\rho]$ with $N(u) = p$ for some prime $p \in \mathbb{Z}$, then u is a prime in $\mathbb{Z}[\rho]$.*

Proof. Let $u \in \mathbb{Z}[\rho]$ with $N(u) = p$ for some prime $p \in \mathbb{Z}$. And suppose u is not a prime in $\mathbb{Z}[\rho]$, then, since $\mathbb{Z}[\rho]$ is an Euclidean Domain, then u is reducible in $\mathbb{Z}[\rho]$. Hence $u = wv$ for some w, $v \in \mathbb{Z}[\rho]$ with $N(w) > 1$ and $N(v) > 1$. But note that $p = N(u) = N(w)N(v)$ which cannot be true since p is a rational prime. Hence, u is a prime in $\mathbb{Z}[\rho]$. □

Lemma 1.13. *An analogue to Lemma (1.9), page 19, For any $n \in \mathbb{Z}$, $\mathbb{Z}[\rho]/\langle n \rangle \cong \mathbb{Z}_n[\rho]$*

Proof. Let $r \in \mathbb{Z}$, and let $[r]_n$ denote the equivalence class (mod n) in $\mathbb{Z}$. Consider the mapping:

$$\psi : \mathbb{Z}[\rho] \to \mathbb{Z}_n[\rho] \qquad defined \quad by :$$

$$\psi\left(r + s\rho\right) = [r]_r + [s]_n\rho.$$

ψ is a surjective ring homomorphism, and the Kernel $\ker\psi = \langle n \rangle$, and by The First Isomorphism Theorem for rings, we have $\mathbb{Z}[\rho]/\langle n \rangle \cong \mathbb{Z}_n[\rho]$ □

Definition 1.31. *Let u be a prime in $\mathbb{Z}[\rho]$, then u is called primary if $u \equiv 2 \mod 3$. Which means that if $u = x + y\rho$ is a complex prime, then $x \equiv 2 \mod 3$ and $y \equiv 0 \mod 3$*

Lemma 1.14. *Every prime u in $\mathbb{Z}[\rho]$ divides a rational prime.*

Proof. First of all, note that every Eisensteinen integer w divides its norm in $\mathbb{Z}[\rho]$, for $N(w) = w \cdot \overline{w}$.

Now, let u be a prime in $\mathbb{Z}[\rho]$, then u divides a rational integer, namely its own norm. Let the prime factorization of the norm of u, $N(u)$, in $\mathbb{Z}$ be:

$N(u) = u \cdot \overline{u} = p_1p_2 \cdots p_k \Rightarrow u \mid p_1p_2 \cdots p_k$, but u is a prime in $\mathbb{Z}[\rho]$; hence, by Euclid's Lemma in $\mathbb{Z}$, u divides one of the (prime) factors on the right hand side. □

Proposition 1.3. *For any prime element $u \in \mathbb{Z}[\rho]$, $\mathbb{Z}[\rho]/\langle u\mathbb{Z}[\rho] \rangle$ is a finite field with $N(u)$ elements.*

Proof. Firstly, we'll show that $\mathbb{Z}[\rho]/\langle u\mathbb{Z}[\rho]\rangle$ is a field:

Claim: $\mathbb{Z}[\rho]/\langle u\mathbb{Z}[\rho]\rangle$ is an Integral Domain.

Proof: Let $\alpha, \beta \in \mathbb{Z}[\rho]/\langle u\mathbb{Z}[\rho]\rangle$ be nonzero elements, and assume that $\alpha\beta = 0$.

Write $\alpha = A_1 + uA_2, \beta = B_1 + uB_2$ for some $A_1, A_2, B_1, B_2 \in \mathbb{Z}[\rho]$, with (according to our assumption) $A_1 \neq 0$, $B_1 \neq 0$. Then:

$\alpha\beta = (A_1 + uA_2)(B_1 + uB_2) = A_1B_1 + uC$ where $C = A_1B_2 + A_2B_1 + uA_2B_2$.

Obviously, $\alpha\beta \neq 0$ in $\mathbb{Z}[\rho]/\langle u\mathbb{Z}[\rho]\rangle$ since $A_1B_1 \neq 0$ (for $A_1, B_1 \in \mathbb{Z}[\rho]$ which is an Integral Domain by *Lemma* (1.11). ■

Now, let $v \in \mathbb{Z}[\rho]$ be any element such that $v \not\equiv 0 \mod u$. Since $\mathbb{Z}[\rho]$ is an Euclidean Domain, then there exist α, $\beta \in \mathbb{Z}[\rho]$ such that: $\alpha v + \beta u = 1$, which implies that $\alpha v \equiv 1 \mod u$, therefore, every nonzero element of $\mathbb{Z}[\rho]/\langle u\mathbb{Z}[\rho]\rangle$ is a unit, and thus $\mathbb{Z}[\rho]/\langle u\mathbb{Z}[\rho]\rangle$ is a field. Now, in order to show that $\mathbb{Z}[\rho]/\langle u\mathbb{Z}[\rho]\rangle$ is a finite field of $N(u)$ elements; we have three cases to consider:

(i) $u = p$, where p is a prime such that $p \equiv 2 \mod 3$.

Claim: The set $S = \{x + y\rho | x, y \in \mathbb{Z}, 0 \leq x, y < p\}$ forms a complete set of representatives ($\mod p$).

Proof: Let $\alpha = a + b\rho \in \mathbb{Z}[\rho]$, then $a = mp + x$, $b = np + y$ for some $m, x, n, y \in \mathbb{Z}$ with $0 \leq x, y < p$ and $\alpha \equiv (x + y\rho) \mod p$. So, suppose $x + y\rho \equiv x' + y'\rho \mod p$ with $0 \leq x, y, x', y' < p$. Thus: $\left(\left(\frac{(x-x')}{p}\right) + \left(\frac{(y-y')}{p}\right)\rho\right) \in \mathbb{Z}[\rho]$; which implies that $\left(\frac{(x-x')}{p}\right) \in \mathbb{Z}$ and $\left(\frac{(y-y')}{p}\right) \in \mathbb{Z}$ which can be true only if $(x-x') = 0$ and $(y-y') = 0$ $\Rightarrow x = x'$, $y = y'$. And this in turn implies that the set S above forms a complete set of representatives $\mod p$ ■

Hence the number of elements of $\left(\mathbb{Z}[\rho]/\langle u\mathbb{Z}[\rho]\rangle\right)$ is $p^2 = N(p)$.

(ii) u is a prime in $\mathbb{Z}[\rho]$ with $N(u) = u\overline{u} = q$, where q is a prime in $\mathbb{Z}$ such that $q \equiv 1 \mod 3$.

Claim: The set $T = \{0, 1, 2, \ldots, q-1\}$ forms a complete set of representatives $\mod u$.

Proof: Let $u = x + y\rho$, then $q = N(u) = x^2 + y^2 - xy$. Note that $q \mid y$ since if not, then

$q \mid u$ and $q \mid \overline{u}$ implying that q is a unit in $\mathbb{Z}[\rho]$ which is absurd.

Now, let $\alpha = a + b\rho$, then there exist some $z \in \mathbb{Z}$ such that $zy \equiv b \mod q$, and hence $\alpha - zu \equiv a - zx \mod q$, $\Rightarrow \alpha \equiv -zx \mod u$. This means that every element of $\mathbb{Z}[\rho]$ is congruent to a rational integer modulo u. And for each $k \in \mathbb{Z}$, $k = qc + d$ for some $c, d \in \mathbb{Z}$ with $0 \leq d < q$. Therefore, $k \equiv d \mod q$, hence $k \equiv d \mod u$. Thus, every element of $\mathbb{Z}[\rho]$ is congruent to an element of $T \mod u$.

Now, assume $d \equiv d' \mod u$ with $d, d' \in \mathbb{Z}$ and $0 \leq d, d' < q$ which gives us $d - d' = uv$ for some $v \in \mathbb{Z}[\rho]$, and $(d - d')^2 = qN(v)$ implying that $q \mid (d - d') \Leftrightarrow d \equiv d' \mod q$ yielding: $d = d'$. Thus T, as given above, forms a complete set of representatives mod u. ■

Therefore; the number of elements of $\left(\mathbb{Z}[\rho]/\langle u\mathbb{Z}[\rho]\rangle\right)$ is $q = N(u)$.

(iii) $u = 1 - \rho$, then $N(u) = N(1 - \rho) = 1^2 + (-1)^2 - 1(-1) = 3$.

Claim: The set $U = \{0, 1, 2\}$ forms a complete set of representatives mod u.

Proof: Let $\alpha = a + b\rho$, then $\alpha + bu = (a + b\rho) + b(1 - \rho) = a + b\rho + b - b\rho = a + b$. Thus, $\alpha + bu = a + b$, hence $\alpha \equiv (a + b) \mod u$ and therefore, every element of $\mathbb{Z}[\rho]$ is congruent to a rational integer mod u. Thus, for each $k \in \mathbb{Z}$, $k = 3c + d$ for some $c, d \in \mathbb{Z}$ with $0 \leq d < 3$. Hence $k \equiv d \mod 3$ and so $k \equiv d \mod u$ implying that every element of $\mathbb{Z}[\rho]$ is congruent to an element of $U = \{0, 1, 2\}$.

Now, suppose that $d \equiv d' \mod u$ with $d, d' \in \mathbb{Z}$ and $0 \leq d, d' < 3$, then $d - d' = uv$ for some $v \in \mathbb{Z}[\rho]$, and $(d - d')^2 = 3N(v)$ implying that $3 \mid (d - d') \Leftrightarrow d \equiv d' \mod 3$ and hence $d = d'$. Hence, U, as given above, forms a complete set of representatives mod u. ■

Therefore, the number of elements of $\left(\mathbb{Z}[\rho]/\langle u\mathbb{Z}[\rho]\rangle\right)$ is $3 = N(u)$.

□

Conclusion 1.1. *Consequently; we conclude that:* $\mathbb{Z}[\rho]/\langle(1 - \rho)\rangle \cong \mathbb{Z}_3[\rho]$

1.5.3 Rings Of Algebraic Numbers

Definition 1.32. ***Algebraic Number***

Let $P(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$ be a polynomial (not necessarily monic) with coefficients $a_i \in \mathbb{Q}$ (The rational numbers), then $\xi \in \mathbb{C}$ is called an algebraic number if it is a root of $P(x)$, i.e. If $P(\xi) = 0$.

Definition 1.33. ***Algebraic Integers***

Let $\xi \in \mathbb{C}$, then ξ is called an algebraic integer if it is a root of a monic polynomial:

$$P(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

where $a_i \in \mathbb{Z}$ for all i and $n \in \mathbb{Z}^+$.

Theorem 1.14. *([10], Theorem 21.2, page 371) Let ξ be an algebraic number. Then there exists a unique, monic, irreducible polynomial $m(x) \in \mathbb{Q}[x]$ such that ξ is a root of, and if further ξ is a root of another polynomial $p(x)$ then $m(x)|p(x)$.*

Proof. Let $S[x] = \{m_i(x) \in \mathbb{Q}[x] : m_i(\xi) = 0, i \in \mathbb{Z}\}$, i.e. $S[x]$ is the set of all polynomials for which ξ is a root of. Then, choose $m(x) \in S[x]$ to be of minimal degree, then:
Claim: $m(x)$ is irreducible
Proof: Suppose $m(x)$, as chosen above, is not irreducible. Then it can be factored as a product of non-unit polynomials, say: $m(x) = f(x)g(x)$, with:
$0 < deg\,(f(x)), deg\,(g(x)) < deg\,(m(x))$ and since ξ is a root of $m(x)$, then:
$0 = m(\xi) = f(\xi)g(\xi)$. But $\mathbb{C}$ is an integral domain, then either $f(\xi) = 0$ or $g(\xi) = 0$ contradicting the minimality of $deg\,(m(x))$ for which ξ is a root of. Thus, $m(x)$ is irreducible. ■
For uniqueness, suppose there are two polynomials of smallest degree, call them $m_1(x), m_2(x)$ such that ξ is a root of. By division algorithm, there exist polynomials $q(x), r(x) \in \mathbb{Q}[x]$ such that $m_1(x) = q(x)m_2(x) + r(x)$, with $deg\,(r(x)) = 0$ or $deg\,(r(x)) < deg\,(m_2(x))$.
Now, $m_1(\xi) = q(\xi)m_2(\xi) + r(\xi)$ with $m_1(\xi) = 0, m_2(\xi) = 0 \Rightarrow r(\xi) = 0$ contradicting the minimality of the degree of $m_1(x)$ and $m_2(x)$ implying that $r(x) = 0$. Therefore, $m_1(x) = q(x)m_2(x)$ but $m_1(x)$ and $m_2(x)$ are of same degree, makes $deg\,(q(x)) = 0$. i.e.

$q(x)$ is a unit. Hence, $m(x)$ is unique up to associates, and so we may assume it's monic. Now, let $p(x) \in \mathbb{Q}[x]$ such that $p(\xi) = 0$. Then, by the minimality of the degree of $m(x)$, we have $deg\,(p(x)) > deg\,(m(x))$ and so, if $m(x) \nmid p(x)$ then by the irreducibility of $m(x)$, $m(x)$ and $p(x)$ are relatively prime, so $\gcd\,(m(x), p(x)) = 1$. Then, $\exists\ a(x), b(x) \in \mathbb{Q}[x]$ such that $a(x)m(x) + b(x)p(x) = 1$. And so, $\underbrace{a(\xi)m(\xi)}_{=0} + \underbrace{b(\xi)p(\xi)}_{=0} = 1$ an obvious contradiction, hence $m(x)|p(x)$. □

Definition 1.34. ***Minimal Polynomial***

Let ξ be an algebraic number, then the monic polynomial $m(x) \in \mathbb{Q}[x]$ of smallest degree such that $m(\xi) = 0$ is called the minimal polynomial of ξ.

Definition 1.35. ***The Degree of ξ***

The degree of an algebraic number, ξ over a field F with minimal polynomial $m(x)$ is the degree of $m(x)$.

Definition 1.36. ***Quadratic Fields***

Let K be a field extension of $\mathbb{Q}$ of degree 2 (i.e. $[K : \mathbb{Q}] = 2$), then this field extension is called a quadratic number field.

Definition 1.37. ***Number Field***

An extension of $\mathbb{Q}$, $\mathcal{K}$, with finite degree is called a Number Field.

Definition 1.38. ***The Ring of Integers of a Field***

Let $\mathcal{K}$ be a number field, then the set of elements $\eta \in \mathcal{K}$ such that η is a root of a monic polynomial with coefficients in $\mathbb{Z}$, denoted by $\mathcal{O}_{\mathcal{K}}$ is called the ring of integers of $\mathcal{K}$; i.e:

$$\mathcal{O}_{\mathcal{K}} = \{\eta \in \mathcal{K} :\ \ f(\eta) = 0,\ \ for\ \ some\ \ monic\ \ f(x) \in \mathbb{Z}[x]\}$$

And it's also called an "Order" of a number field.

Remark 1.9.

Let θ be an algebraic integer which is a root of a quadratic minimal polynomial, $p(x)$, where

$p(x) = x^2 + ux + v$ over $\mathbb{Z}$, then the generation (aggrigation) of all algebraic integers of the form:

$$\xi = \beta_0 + \beta_1\theta$$

where $\beta_0, \beta_1 \in \mathbb{Z}$ forms a quadratic number field, denoted by $\mathbb{Z}[\theta]$. Then we may write:

$$\begin{aligned} \theta &= \tfrac{\xi+(-\beta_0)}{\beta_1} \\ &= \tfrac{-u+\sqrt{u^2-4v}}{2} \\ &= \tfrac{-u+\sqrt{m}}{2} \qquad\qquad where \\ \sqrt{m} &= 2\theta + u \end{aligned}$$

and m is a square free integer.

Therefore, any number $\xi \in \mathbb{Z}[\theta]$ can be represented by:

$$\xi = \frac{u + \sqrt{m}}{2}$$

Hence, the fields $\mathbb{Z}[\theta]$ and $\mathbb{Z}[\sqrt{m}]$ are identical. Moreover, m is called the *radicand* of the quadratic field $\mathcal{K} = \mathbb{Z}[\sqrt{m}]$

Definition 1.39. ***Conjugate of*** ξ

The conjugate of any algebraic integer $\xi = \frac{u+\sqrt{m}}{2}$ is $\overline{\xi}$ given by:

$$\overline{\xi} = \frac{u - \sqrt{m}}{2}$$

Definition 1.40. ***Trace and Norm of an algebraic integer***

The trace and norm of any algebraic integer $\xi \in \mathcal{K}$, denoted by $Tr(\xi)$ and $N(\xi)$ respectively, are given by:

$$\begin{aligned} Tr(\xi) &= \xi + \overline{\xi} = \tfrac{u+\sqrt{m}}{2} + \tfrac{u-\sqrt{m}}{2} = u \\ \textit{and} & \\ N(\xi) &= \xi\ \overline{\xi} = \left(\tfrac{u+\sqrt{m}}{2}\right)\cdot\left(\tfrac{u-\sqrt{m}}{2}\right) = \left(\tfrac{u^2-m}{4}\right) \end{aligned} \tag{1.11}$$

Chapter 2

Main Results

This chapter presents the theorems and results concerning the number of ring homomorphisms over the rings of integers, the rings of Gaussian integers, the rings of Eisentein integers and rings of certain algebraic integers. Proofs of the results are presented in full details. The original results and theorems are marked with an asterisk (*). Several examples are given as an illustration to show how the formulas given in the theorems are excellent tools for finding the number of ring homomorphisms without having to go through all the intricate calculations.

2.1 Rings of integers

Lemma 2.1. *The number of ring homomorphisms* $\phi : \mathbb{Z} \to \mathbb{Z}$ *is* 2

Proof. Let $\phi : \mathbb{Z} \to \mathbb{Z}$ be a ring homomorphism, and let $\phi(1) = x$, then:
For any $m \in \mathbb{Z}$, $\phi(m) = \phi(m \cdot 1) = m \cdot \phi(1) = mx$. Therefore, any ring homomorphism from $\mathbb{Z}$ into $\mathbb{Z}$ is completely determined by $\phi(1)$, i.e. by the value of x. Now, since 1 is an idempotent, then so is $\phi(1)$ as well. So we need to find all idempotent elements in $\mathbb{Z}$:
$x^2 = x \;\Rightarrow\; x^2 - x = 0 \;\Leftrightarrow\; x(x-1) = 0 \;\Rightarrow\; x = 0 \text{ or } x = 1$ Therefore, $\phi(1) = 0$ or $\phi(1) = 1$. Which yields two homomorphisms:

$$\phi(m) = 0 \qquad \text{and} \qquad \phi(m) = m$$

□

Lemma 2.2. *The number of ring homomorphisms:* $\phi: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ *is* 4

Proof. Let $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be a ring homomorphism. Then, 1 is an idempotent element in $\mathbb{Z}$ then so is $\phi(1)$ an idempotent in $\mathbb{Z} \times \mathbb{Z}$. And the idempotent elements of $\mathbb{Z} \times \mathbb{Z}$ are: $(0,0)$ $(1,0)$ $(0,1)$ $(1,1)$ Also, by the property of preserving the multiplication; we have $\phi(n) = n\phi(1)$ and hence we have the following four homomorphisms:

$$\textit{where} \qquad \phi(1) = \begin{cases} (0,0) \\ (1,0) \\ (0,1) \\ (1,1) \end{cases} \qquad\qquad \textit{hence} \qquad\qquad \phi(n) = \begin{cases} (0,0) \\ (n,0) \\ (0,n) \\ (n,n) \end{cases}$$

□

Corollary * 2.1. [1] *The number of ring homomorphisms:*

$$\phi: \quad \mathbb{Z} \quad \to \quad \overbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}^{k-times} \qquad \textit{is} \qquad 2^k$$

Proof. Based on the same argument of the previous lemma;
we have for $\phi: \mathbb{Z} \to \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{k}$
$\phi(n) = n\phi(1)$ and by the idempotent-ness property; we have $\phi(1) = e_i$ where e_i is a k-tuple with 1 in its i^{th} coordinate and zeros elsewhere.

Hence, the total number of ring homomorphisms equals the number of the e_i's which equals to the total number of all possibilities of arranging (with order) the 0's and 1's in a k-tuple: which is simply 2^k. □

[1] Henceforth: every result, corollary or theorem that is marked with an asterisk , *, is **an original result**

Example 2.1. *Consider the ring homomorphisms:* $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$*:*

Since 1 *is an idempotent in* $\mathbb{Z}$ *then so is* $\phi(1)$ *in* $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$*.*

And so $\phi(1) =$ *one of the* 16 *idempotents in* $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ *and* $\phi(n) = n\phi(1)$*, and thus we have* 16 *ring homomorphisms:*

$$\phi(1) = \begin{cases} (0,0,0,0), & (1,0,0,0) \\ (0,1,0,0), & (0,0,1,0) \\ (0,0,0,1), & (1,1,0,0) \\ (1,0,1,0), & (1,0,0,1) \\ (0,1,0,1), & (0,1,1,0) \\ (0,0,1,1), & (1,1,1,0) \\ (1,1,0,1), & (1,0,1,1) \\ (0,1,1,1), & (1,1,1,1) \end{cases} \qquad \textit{hence} \qquad \phi(n) = \begin{cases} (0,0,0,0), & (n,0,0,0) \\ (0,n,0,0), & (0,0,n,0) \\ (0,0,0,n), & (n,n,0,0) \\ (n,0,n,0), & (n,0,0,n) \\ (0,n,0,n), & (0,n,n,0) \\ (0,0,n,n), & (n,n,n,0) \\ (n,n,0,n), & (n,0,n,n) \\ (0,n,n,n), & (n,n,n,n) \end{cases}$$

Solution by using the formula in the theorem.

By using the simple formula in the theorem, we have:

$$\mathcal{N}\big(\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}\big) = 2^4 = 16 \ \textit{homomorphisms}$$

Lemma 2.3. *The number of ring homomorphisms:*

$$\phi : \quad \mathbb{Z} \times \mathbb{Z} \ \to \ \mathbb{Z} \qquad\qquad\qquad \textit{is} \qquad 3$$

Proof. Note that ϕ is completely determined by its action on the idempotent elements in $\mathbb{Z} \times \mathbb{Z}$; i.e. by the values of $\phi\Big((1,0)\Big)$ and $\phi\Big((0,1)\Big)$.

Let $\phi\Big((1,0)\Big) = x_1$ and $\phi\Big((0,1)\Big) = x_2$. Then, by preserving the multiplication we have:

$$\begin{array}{rcccccl} x_1 & = & \phi\Big((1,0)\cdot(1,0)\Big) & = & \phi\Big((1,0)\Big)\cdot\phi\Big((1,0)\Big) & = & x_1^2 \\ 0 & = & \phi\Big((1,0)\cdot(0,1)\Big) & = & \phi\Big((1,0)\Big)\cdot\phi\Big((0,1)\Big) & = & x_1x_2 \\ 0 & = & \phi\Big((0,1)\cdot(1,0)\Big) & = & \phi\Big((0,1)\Big)\cdot\phi\Big((1,0)\Big) & = & x_2x_1 \\ x_2 & = & \phi\Big((0,1)\cdot(0,1)\Big) & = & \phi\Big((0,1)\Big)\cdot\phi\Big((0,1)\Big) & = & x_2^2 \end{array}$$

Therefore; from the first two equations; we have: $x_1^2 = x_1 \Rightarrow x_1 = 0$ or $x_1 = 1$ and $x_1x_2 = 0$ $\Rightarrow x_1 = 0$ or $x_2 = 0$. And so, if $x_1 = 1$ then $x_2 = 0$.

Similarly, from the last two equations; we have $x_2^2 = x_2 \Rightarrow x_2 = 0$ or $x_2 = 1$ and $x_2x_1 = 0$ $\Rightarrow x_2 = 0$ or $x_1 = 0$. And so, if $x_2 = 1$ then $x_1 = 0$.

Hence; we have three homomorphisms: One that maps everything to <u>*zero*</u> and the other two homomorphisms are determined by mapping one of the elements: $(1,0), (0,1)$ to 1 and the other one to 0. □

By a similar argument we can conclude the following generalization:

Corollary * 2.2. *The number of ring homomorphisms:*

$$\phi: \quad \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{k-times} \quad \rightarrow \quad \mathbb{Z} \qquad\qquad is \quad (k+1)$$

Proof.

For ϕ to be an isomorphism, it must map idempotent elements in $\overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{k-times}$ into idempotent elements of $\mathbb{Z}$. Thus, ϕ is completely determined on its action on the idempotents of $\overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{k-times}$ which are e_i's where e_i is the $k-tuple$ whose i^{th} component is 1 and 0's elsewhere.

Now, let $x_i = \phi(e_i)$, then for preserving the multiplication of homomorphisms, we have:

$$
\begin{array}{rclcrcl}
x_1 & = & \phi\Big(e_1 \cdot e_1\Big) & = & \phi(e_1) \cdot \phi(e_1) & = & x_1^2 \\
0 & = & \phi\Big(e_1 \cdot e_2\Big) & = & \phi(e_1) \cdot \phi(e_2) & = & x_1 x_2 \\
\vdots & & & & & & \\
0 & = & \phi\Big(e_1 \cdot e_k\Big) & = & \phi(e_1) \cdot \phi(e_k) & = & x_1 x_k \\
 & & & & & & \\
0 & = & \phi\Big(e_2 \cdot e_1\Big) & = & \phi(e_2) \cdot \phi(e_1) & = & x_2 x_1 \\
x_2 & = & \phi\Big(e_2 \cdot e_2\Big) & = & \phi(e_2) \cdot \phi(e_2) & = & x_2^2 \\
\vdots & & & & & & \\
0 & = & \phi\Big(e_2 \cdot e_k\Big) & = & \phi(e_2) \cdot \phi(e_k) & = & x_2 x_k \\
 & & & & & & \\
\vdots & & & & & & \\
0 & = & \phi\Big(e_i \cdot e_1\Big) & = & \phi(e_i) \cdot \phi(e_1) & = & x_i x_1 \\
0 & = & \phi\Big(e_i \cdot e_2\Big) & = & \phi(e_i) \cdot \phi(e_2) & = & x_i x_2 \\
\vdots & & & & & & \\
x_i & = & \phi\Big(e_i \cdot e_i\Big) & = & \phi(e_i) \cdot \phi(e_i) & = & x_i^2 \\
0 & = & \phi\Big(e_i \cdot e_{i+1}\Big) & = & \phi(e_i) \cdot \phi(e_{i+1}) & = & x_i x_{i+1} \\
\vdots & & & & & & \\
0 & = & \phi\Big(e_i \cdot e_k\Big) & = & \phi(e_i) \cdot \phi(e_k) & = & x_i x_k
\end{array}
$$

So, from the set of equations for each i, we get that:

$x_i^2 = x_i \Rightarrow x_i = 0$ or $x_i = 1$ and $x_i x_j = 0$ for $i \neq j \Rightarrow x_i = 0$ or $x_j = 0$

And if $x_i = 1$ then $x_j = 0$ for all $j \neq i$.

Therefore, we have $(k+1)$ homomorphisms; One that maps everything to 0, and the other k homomorphisms map one of the idempotent elements, e_i's, to 1 and maps the other $(k-1)$ e_j's to 0. □

Lemma 2.4. *The number of ring homomorphisms:*

$$\phi: \quad \mathbb{Z}\times\mathbb{Z} \;\to\; \mathbb{Z}\times\mathbb{Z} \qquad is \quad 9$$

Proof. Note, since any element of $\mathbb{Z}\times\mathbb{Z}$ is written in the form $(x,y) = x(1,0) + y(0,1)$, then any

ring homomorphism is completely determined by the values $\phi\Big((1,0)\Big)$ and $\phi\Big((0,1)\Big)$.

Moreover; since $(1,0)^2 = (1,0)$ and $(0,1)^2 = (0,1)$ (idempotents), then $\phi\Big((1,0)\Big)$, $\phi\Big((0,1)\Big)$ must also be idempotents in $\mathbb{Z}\times\mathbb{Z}$.

Noticing that the idempotents of $\mathbb{Z}\times\mathbb{Z}$ are: $(0,0)$, $(1,0)$, $(0,1)$ and $(1,1)$. So, $\phi\Big((1,0)\Big)$ and $\phi\Big((0,1)\Big)$ would take (temporarily speaking) any of these idempotent values.

Considering the following table:

$\phi\Big((1,0)\Big)$	$\phi\Big((0,1)\Big)$	$\phi\Big((x,y)\Big)$
$(0,0)$	$(0,0)$	$(0,0)$
$(0,0)$	$(1,0)$	$(y,0)$
$(0,0)$	$(0,1)$	$(0,y)$
$(0,0)$	$(1,1)$	(y,y)
$(1,0)$	$(0,0)$	$(x,0)$
$(1,0)$	$(1,0)$	$(\cancel{x+y},0)$
$(1,0)$	$(0,1)$	(x,y)
$(1,0)$	$(1,1)$	$(\cancel{x+y},y)$

$\phi\Big((1,0)\Big)$	$\phi\Big((0,1)\Big)$	$\phi\Big((x,y)\Big)$
$(0,1)$	$(0,0)$	$(0,x)$
$(0,1)$	$(1,0)$	(y,x)
$(0,1)$	$(0,1)$	$(0,\cancel{x+y})$
$(0,1)$	$(1,1)$	$(y,\cancel{x+y})$
$(1,1)$	$(0,0)$	(x,x)
$(1,1)$	$(1,0)$	$(\cancel{x+y},x)$
$(1,1)$	$(0,1)$	$(x,\cancel{x+y})$
$(1,1)$	$(1,1)$	$(\cancel{x+y},\cancel{x+y})$

Where we have scratched out every $(x+y)$ to preserve the idempotent-ness property; so:

For $\phi\Big((1,0)\Big) = (0,0)$ it combines with all 4 choices for $\phi\Big((0,1)\Big)$.

For $\phi\Big((1,0)\Big) = (1,0)$ it combines with only 2 choices for $\phi\Big((0,1)\Big)$, and similarly;

For $\phi\Big((1,0)\Big) = (0,1)$ it combines with only 2 choices for $\phi\Big((0,1)\Big)$.

While for $\phi\Big((1,0)\Big) = (1,1)$ it combines with only 1 choice for $\phi\Big((0,1)\Big)$.

Hence, giving us a total of $1\times 4 + 2\times 2 + 1\times 1 = 9$ choices.

Therefore; the number of ring homomorphisms is 9 homomorphisms.

Note that we could have proven this result in the following manner:

Let $\phi: \mathbb{Z}\times\mathbb{Z} \rightarrow \mathbb{Z}\times\mathbb{Z}$ be a ring homomorphism.

Then note that any element $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ can be written as:

$(x,y) = x(1,0)+y(0,1)$. Therefore, any ring homomorphisms, ϕ, is completely determined by the values of $\phi\Big((1,0)\Big)$ and $\phi\Big((0,1)\Big)$.

Moreover, since $(1,0)^2 = (1,0)$, and $(0,1)^2 = (0,1)$ then $(1,0)$ and $(0,1)$ are idempotents, and so must also $\phi\Big((1,0)\Big)$ and $\phi\Big((0,1)\Big)$ be idempotents.

Note that the idempotents elements of $\mathbb{Z}\times\mathbb{Z}$ satisfy $(a^2,b^2) = (a,b)$ which gives us that $a,b = 0$ or 1. And so the idempotent elements of $\mathbb{Z}\times\mathbb{Z}$ are:

$$(0,0) \qquad (1,0) \qquad (0,1) \qquad (1,1)$$

Now, taking all possible values of $(1,0)$ and $(0,1)$ from the list of idempotents, and keeping in mind that $(1,1)$ is an idempotent gives us that we have to choose for x,y in $\phi\Big((x,y)\Big)$ from $\{0,x,y\}$, giving us that the number of all these possibilities is:

$$(2+1)^2 = 3^2 = 9$$

□

Corollary * 2.3. *The number of ring homomorphisms:*

$$\phi: \mathbb{Z}\times\mathbb{Z} \rightarrow \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \qquad \textit{is} \qquad 27$$

Proof. Similar to the argument in the proof of *Result 1*, any ring homomorphism is completely determined by the values $\phi\Big((1,0)\Big)$ and $\phi\Big((0,1)\Big)$.

Now $(1,0)$ and $(0,1)$ are idempotents implying that $\phi\Big((1,0)\Big)$ and $\phi\Big((0,1)\Big)$ must also be idempotents in $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$. Noticing that the idempotents of $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ are:

$$(0,0,0) \qquad (1,0,0) \qquad (0,1,0) \qquad (0,0,1)$$
$$(1,1,0) \qquad (1,0,1) \qquad (0,1,1) \qquad (1,1,1)$$

Hence, $\phi\Big((1,0)\Big)$ and $\phi\Big((0,1)\Big)$ would take any of these idempotent values. But, to preserve the idempotent-ness property, we see that:

- For $\phi\Big((1,0)\Big) = (0,0,0)$ it can combine with all 8 choices of the idempotents for $\phi\Big((0,1)\Big)$.
- For $\phi\Big((1,0)\Big) \in \{(1,0,0),(0,1,0),(0,0,1)\}$ (i.e. One 1 in its coordinates), then: $\phi\Big((1,0)\Big)$ may combine with only 4 choices for $\phi\Big((0,1)\Big)$, and we have three cases of a single 1 in $\phi\Big((1,0)\Big)$'s coordinates, thus we have 3×4 choices.
- For $\phi\Big((1,0)\Big) \in \{(1,1,0),(1,0,1),(0,1,1)\}$ (i.e. Two 1's in its coordinates), then: $\phi\Big((1,0)\Big)$ may combine with only 2 choices for $\phi\Big((0,1)\Big)$, and we have three cases of a double 1 in $\phi\Big((1,0)\Big)$'s coordinates, thus we have 3×2 choices.
- Finally, for $\phi\Big((1,0)\Big) = (1,1,1)$ (Three 1's in its coordinates), $\phi\Big((1,0)\Big)$ may combine with only one idempotent value for $\phi\Big((0,1)\Big)$, namely $(0,0,0)$, and we only have one such case, so 1×1 choices.

Note that we can summarize the previous cases by using some *Combinatorics*:
For the first case, we have one case of choosing 0's out of 3 giving us $\binom{3}{0}$,
For the second case, we have two cases of selecting 1's out of 3 $\Rightarrow$ $\binom{3}{1}$,
For the third case, we have four cases of selecting two 1's out of 3 $\Rightarrow$ $\binom{3}{2}$,
For the fourth case, we have eight cases of selecting three 1's out of 3, $\Rightarrow$ $\binom{3}{3}$.
Therefore, the total number of ring homomorphisms is:

$$\binom{3}{0}2^3 + \binom{3}{1}2^2 + \binom{3}{2}2 + \binom{3}{3}2^0 \;=\; (2+1)^3 = 3^3 = 27$$

Where we have used the combinatory's identity:

$$\sum_{i=0}^{n} \binom{n}{i} \cdot 2^{3-i} = 3^n \tag{2.1}$$

□

Corollary * 2.4. *The number of ring homomorphisms:*

$$\phi: \ \mathbb{Z}\times\mathbb{Z} \ \rightarrow \ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{k-times}$$

$$is \quad 3^k$$

Proof. Similar to the argument above; any ring homomorphism is completely determined by the values $\phi\Big((1,0)\Big)$ and $\phi\Big((0,1)\Big)$.
Now $(1,0)$ and $(0,1)$ are idempotents implying that $\phi\Big((1,0)\Big)$ and $\phi\Big((0,1)\Big)$ must also be idempotents in $\overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{k-times}$.

Now, the idempotents of $\overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{k-times}$ are the " 2^k " k-tuples f_j whose coordinates are 0's and 1's only. So, we have the following cases:

- For $\underline{\phi\Big((1,0)\Big)} = (\overbrace{0,0,\cdots,0}^{k-times})$, then <u>it</u> may combine with the 2^k choices for $\phi\Big((0,1)\Big)$, giving us $1\cdot\binom{k}{0}$ choices.
- For $\underline{\phi\Big((1,0)\Big)}$ equals to an k-tuple with only one single 1 in its coordinates and zeros elsewhere. Then <u>it</u> would combine with $\binom{k}{1}$ of the values of $\phi\Big((0,1)\Big)$
  and we have 2 such cases.
- For $\underline{\phi\Big((1,0)\Big)}$ equals to an k-tuple with only two 1's in its coordinates and zeros elsewhere. Then <u>it</u> would combine with $\binom{k}{2}$ of the values of $\phi\Big((0,1)\Big)$
  and we have $2^2 = 4$ such cases.

  $\vdots$
- For $\underline{\phi\Big((1,0)\Big)}$ equals to an k-tuple with only $(k-1)$ 1's in its coordinates and zeros elsewhere. Then <u>it</u> would combine with $\binom{k}{k-1}$ of the values of $\phi\Big((0,1)\Big)$
  and we have 2^{k-1} such cases.

- For $\underline{\phi\Big((1,0)\Big)}$ equals to an k-tuple with all 1's in every coordinates. Then it would combine with $\binom{k}{k}$ of the values of $\phi\Big((0,1)\Big)$
  and we have 2^k such cases.

Therefore, the total number of ring homomorphisms is:

$$\binom{k}{0}2^k + \binom{k}{1}2^{k-1} + \binom{k}{2}2^{k-2} + \cdots + \binom{k}{k-2}2^2 + \binom{k}{k-1}2^1 + \binom{k}{k}2^0 \;\; = \;\; 3^k$$

where we have used the *identity* (2.1) □

Corollary * 2.5. *The number of ring homomorphisms:*

$$\phi: \quad \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \;\; \to \;\; \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \qquad is \quad 64$$

Proof. Similar to the argument of the proof of *Lemma* (2.4), any $(x,y,z) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ is written in the form of:

$$(x,y,z) = x(1,0,0) + y(0,1,0) + z(0,0,1)$$

And the idempotent elements of $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ are:

$$(0,0,0) \qquad (1,0,0) \qquad (0,1,0) \qquad (0,0,1) \qquad (1,1,0) \qquad (1,0,1) \qquad (0,1,1) \qquad (1,1,1)$$

Now, taking all possible values of $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$ from the list of idempotents gives us that we have to choose for x,y,z in $\phi\Big((x,y,z)\Big)$ from $\{0,x,y,z\}$. Therefore; the number of all these possibilities is:

$$(3+1)^3 = 4^3 = 64$$

□

As a direct consequence of last two results, proceeding inductively; we have the following *Corollary*:

Corollary * 2.6. *The number of ring homomorphisms over:*

$$\phi: \quad \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{k-times} \quad \rightarrow \quad \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{k-times}$$

is given by: $(k+1)^k$

Corollary * 2.7. *The number of ring homomorphisms:* $\phi: \ \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \ \rightarrow \ \mathbb{Z}$ *is* 4

Proof. Let $\phi: \ \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \ \rightarrow \ \mathbb{Z}$ be a ring homomorphism.

Note, any element of $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ is written in the form:

$$(x,y,z) = x(1,0,0) + y(0,1,0) + z(0,0,1)$$

So, any ring homomorphism is completely determined by the values of:

$$\phi\Big(1,0,0\Big) \qquad \phi\Big(0,1,0\Big) \qquad \phi\Big(0,0,1\Big)$$

And since these are idempotent elements in $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ then so are their images, and the only idempotent elements of $\mathbb{Z}$ are 0 and 1.

Consider the following table:

$\phi\Big((1,0,0)\Big)$	$\phi\Big((0,1,0)\Big)$	$\phi\Big((0,0,1)\Big)$	$\phi\Big((x,y)\Big)$
0	0	0	0
0	0	1	z
0	1	0	y
0	1	1	$(\cancel{y+z})$
1	0	0	x
1	0	1	$(\cancel{x+z})$
1	1	0	$(\cancel{x+y})$
1	1	1	$(\cancel{x+y+z})$

Where we have scratched out four choices in order to preserve the *idempotent-ness* property;

so we only have four homomorphisms; namely:

$$\phi\Big((x,y,z)\Big) = 0, \quad \phi\Big((x,y,z)\Big) = x, \quad \phi\Big((x,y,z)\Big) = y, \quad \phi\Big((x,y,z)\Big) = z$$

□

Corollary * 2.8. *The number of ring homomorphisms:*

$$\phi: \ \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \ \rightarrow \ \mathbb{Z}\times\mathbb{Z} \qquad \textit{is} \qquad 4^2 = 16$$

Proof.

Similar to the previous arguments; any element of $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ is written in the form:

$$(x,y,z) = x(1,0,0) + y(0,1,0) + z(0,0,1)$$

And so, any ring homomorphism is completely determined by the values of:

$$\phi\Big((1,0,0)\Big), \qquad \phi\Big((0,1,0)\Big), \qquad \phi\Big((0,0,1)\Big)$$

Considering the idempotent-ness property of $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$ gives us that

$\phi\Big((1,0,0)\Big)$, $\phi\Big((0,1,0)\Big)$ and $\phi\Big((0,0,1)\Big)$ would take the values of the idempotent elements

in $\mathbb{Z}\times\mathbb{Z}$ which are: $(0,0)$ $(1,0)$ $(0,1)$ $(1,1)$

So, we'll consider the following cases:

$\phi\Big((1,0,0)\Big)$	$\phi\Big((0,1,0)\Big)$	$\phi\Big((0,0,1)\Big)$	Number of choices for $\phi\Big((x,y)\Big)$
$(0,0)$	$(0,0)$	$(0,0)$, $(1,0)$, $(0,1)$, $(1,1)$	4 choices
$(0,0)$	$(1,0)$	$(0,0)$, $(0,1)$	2 choices
$(0,0)$	$(0,1)$	$(0,0)$, $(1,0)$	2 choices
$(0,0)$	$(1,1)$	$(0,0)$	1 choice
$(1,0)$	$(0,0)$	$(0,0)$, $(0,1)$	2 choices
$(1,0)$	~~$(1,0)$~~	No Choices	0 choices
$(1,0)$	$(0,1)$	$(0,0)$	1 choice
$(1,0)$	~~$(1,1)$~~	No Choices	0 choices
$(0,1)$	$(0,0)$	$(0,0)$, $(1,0)$	2 choices
$(0,1)$	$(1,0)$	$(0,0)$	1 choice
$(0,1)$	~~$(0,1)$~~	No Choices	0 choices
$(0,1)$	~~$(1,1)$~~	No Choices	0 choices
$(1,1)$	$(0,0)$	$(0,0)$	1 choice
$(1,1)$	~~$(1,0)$~~	No Choices	0 choices
$(1,1)$	~~$(0,1)$~~	No Choices	0 choices
$(1,1)$	~~$(1,1)$~~	No Choices	0 choices

So, we have a total of: $4+2+2+1+2+1+2+1+1=16$ ring homomorphisms.

Note that we can summarize the above cases by using some combinatorics [{2}]:

The total number of ring homomorphisms is:

$$\binom{2}{0}3^2+\binom{2}{1}3+\binom{2}{2}1=(3+1)^2=4^2=16$$

□

[{2}] (See [14], pages 8 - 10)

Corollary * 2.9. *The number of ring homomorphisms:*

$$\phi: \ \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \ \rightarrow \ \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \qquad is \qquad 4^3 = 64$$

Proof. By using similar argument, it's easy to see that using combinatorics simplifies the computing procedure, and we get for the total number of ring homomorphisms to be:

$$\binom{3}{0}3^3 + \binom{3}{1}3^2 + \binom{3}{2}3 + \binom{3}{3}1 = (3+1)^3 = 4^3 = 64$$

□

Corollary * 2.10. *The number of ring homomorphisms:*

$$\phi: \ \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \ \rightarrow \ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{k-times} \qquad is \qquad 4^k$$

Proof. We may use the same lengthy procedure inductively; we've already seen that the statement is true for $k = 1, 2, 3$. Assuming that the statement is true for $k = n$ for some $n \in \mathbb{Z}^+$; Then:

$$\phi: \ \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \ \rightarrow \ \overbrace{\mathbb{Z}\times\mathbb{Z}\times \ \cdots\cdots \ \times\mathbb{Z}}^{(n+1)-\text{times}}$$

$$\Leftrightarrow \phi: \ \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \ \rightarrow \ (\overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{n-\text{times}})\times\mathbb{Z}.$$

So, we have the the same number of homomorphisms for the $k = n$ case (which is 4^k homomorphisms) multiplied by the $\Big($three (nontrivial) homomorphisms plus the zero homomorphisms$\Big)$ from $(\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z})$ to the extra $\mathbb{Z}$. Hence; we have $4^n \times 4 = 4^{n+1}$ homomorphisms.
Note that we could have also used the same *Combinatorics* procedure which I have pointed out. Noticing that the total number of homomorphisms is just:

$$\binom{k}{0}3^k + \binom{k}{1}3^{k-1} + \cdots + \binom{k}{k-1}3 + \binom{k}{k}3^0 \ = \ (3+1)^k \ = \ 4^k$$

□

Corollary * 2.11. *The number of ring homomorphisms:*

$$\phi: \ \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \ \rightarrow \ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{k-times} \qquad is \qquad 5^k$$

Proof. Again; by using *Combinatorics*, we have; the total number of ring homomorphisms to be:

$$\binom{k}{0}4^k+\binom{k}{1}4^{k-1}+\cdots+\binom{k}{k-1}4+\binom{k}{k}4^0 = \ (4+1)^k \ = \ 5^k$$

□

Corollary * 2.12. *The number of ring homomorphisms:*

$$\mathcal{P}: \qquad \phi: \ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{k-times} \ \rightarrow \ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{m-times} \qquad is \qquad \Big(k+1\Big)^m$$

Proof. We'll prove the statement $\mathcal{P}$ by *double* induction:

We've already proven that $\mathcal{P}(1,m)\Rightarrow 2^m$ and $\mathcal{P}(k,1)\Rightarrow(k+1)$ by *Corollary** (2.1) (page 30) and *Corollary** (2.2) (page 32) respectively.

So, assume that: $\mathcal{P}(k,m+1)$ and $\mathcal{P}(k+1,m)$ are true for some $k, \ m \ \in \ \mathbb{Z}^+$.

We need to deduce that $\mathcal{P}(k+1,m+1)$ is also true!. That is; we assume that:

$$\mathcal{P}(k,m+1) \quad \begin{cases} \text{The number of ring homomorphisms:} \\ \phi: \ \overbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}^{k-\text{times}} \ \rightarrow \ \overbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}^{(m+1)-\text{times}} \\ \text{is} \quad (k+1)^{(m+1)} \end{cases} \tag{2.2}$$

$$\mathcal{P}(k+1,m) \quad \begin{cases} \text{The number of ring homomorphisms:} \\ \phi: \ \overbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}^{(k+1)-\text{times}} \ \rightarrow \ \overbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}^{m-\text{times}} \\ \text{is} \quad (k+2)^m \end{cases} \tag{2.3}$$

We will use *equation* (2.3): [{3}]

So, considering the statement: $\mathcal{P}(k+1, m+1)$ which deals with:

$$\mathcal{N}\left(\phi:\ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{(k+1)-\text{times}}\ \to\ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{(m+1)-\text{times}}\right)$$

$$\iff\ \mathcal{N}\left(\phi:\ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{(k+1)-\text{times}}\ \to\ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{m-\text{times}}\ \times\mathbb{Z}\right)$$

$$\text{So}\qquad \mathcal{N}\left(\phi:\ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{(k+1)-\text{times}}\ \to\ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{(m+1)-\text{times}}\right)\ =$$

$$\mathcal{N}\left(\phi:\ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{(k+1)-\text{times}}\ \to\ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{m-\text{times}}\right)\ \times\underline{\underline{(k+2)}}$$

Where the multiplication by $\underline{\underline{(k+2)}}$ comes from:

$$\text{the}\ \Big((k+1)(\text{nontrivial homomorphisms}\ \underline{\text{plus}}\ \text{the zero homomorphism}\Big)$$
$$\text{from}\ (\overbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}^{(k+1)-\text{times}})\ \text{into the extra}\ \mathbb{Z}\ \text{ring.}$$

Therefore; the total number of ring homomorphisms is:

$$\mathcal{N}\left(\phi:\ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{(k+1)-\text{times}}\ \to\ \overbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}^{(m+1)-\text{times}}\right)\ =$$

$$=\ (k+2)^m\times(k+2)$$

$$=\ (k+2)^{(m+1)}$$

□

[{3}] Note that we could have used equation (2.2) as well, but it's much easier to use equation (2.3)

Lemma 2.5. *The number of ring homomorphisms:*

$$\phi: \quad \mathbb{Z} \quad \rightarrow \quad \mathbb{Z}_n \qquad is \quad Id(n)$$

where $Id(n)$ is the number of idempotent elements in $\mathbb{Z}_n$.

Proof.

Since, for $x \in \mathbb{Z}$ we have, as noted before, that $\phi(x) = \phi(x \cdot 1) = x\phi(1)$.

So, ϕ is completely determined by its action on 1; i.e. by the value/values of $\phi(1)$. Note that:

$$\phi(x+y) = (x+y)\phi(1) = x\phi(1) + y\phi(1) = \phi(x) + \phi(y)$$

$$and \qquad \underline{\phi(xy)} = \underline{\underline{xy\phi(1)}} = \underline{\phi(x)\phi(y)} = \underline{\underline{xy\Big(\phi(1)\Big)^2}}$$

Therefore; ϕ is a ring homomorphism if and only if $\Big(\phi(1)\Big)^2 = \phi(1)$ in $\mathbb{Z}_n$

which implies that $\phi(1)$ takes all the possible values of the idempotent elements of $\mathbb{Z}_n$.

Hence, the number of ring homomorphisms from $\mathbb{Z}$ into $\mathbb{Z}_n$ is $Id(n)$ where $Id(n)$ is the number of idempotent elements of $\mathbb{Z}_n$. □

Remark 2.1.

Let $\phi : \mathbb{Z}_k \rightarrow \mathbb{Z}_k$ be a ring homomorphism. Then:

The only homomorphisms possible are those of the form: $\phi(x) = mx$ where $x \in \mathbb{Z}_k$ and $\phi(1) = m$ in $\mathbb{Z}_k$.

Theorem 2.1. *[1, Theorem 2]*

The number of ring homomorphisms:

$$\phi: \quad \mathbb{Z}_m \ \rightarrow \ \mathbb{Z}_n \qquad is \qquad 2^{\omega(n)-\omega\left(\frac{n}{\gcd(m,n)}\right)}$$

where $\omega(n)$ = the number of distinct prime divisors of n.

Proof. Let $\phi : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ be a ring homomorphism.

Then, a ring homomorphism is completely determined by its action on 1.

Moreover, since 1 is an idempotent element in $\mathbb{Z}_m$, then so is $\phi(1)$ in $\mathbb{Z}_n$.

Let $n = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ be the prime decomposition of n. Then, by the Chinese Remainder Theorem, $\mathbb{Z}_n$ is naturally ring homomorphic to the direct sum: $\mathbb{Z}_{q_1^{t_1}} \oplus \mathbb{Z}_{q_2^{t_2}} \oplus \cdots \oplus \mathbb{Z}_{q_s^{t_s}}$.

Also, we see that any ring homomorphism from $\mathbb{Z}_m$ into $\mathbb{Z}_n$ induces a ring homomorphism from $\mathbb{Z}_m$ into $\mathbb{Z}_{q_i^{t_i}}$ for $i = 1, 2, \ldots s$.

So, let $\phi(1) = a \in \mathbb{Z}_n$, then in the direct sum $a = (a_1, a_2, \cdots, a_s)$ where $a_i \in \mathbb{Z}_{q_i^{t_i}}$.

Then, each a_i is also an idempotent of $\mathbb{Z}_{q_i^{t_i}}$, hence $a_i = 0$, or 1. Which implies that there are at most 2^s ring homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$.

But note that a ring homomorphism is also a group homomorphism, which implies that the additive order of a_i also divides m.

And conversely, if $(a_1, a_2, \cdots a_s)$ is any member of the direct sum with $a_i = 0$ or 1 with the additive order of $a_i \mid m$,

then there is a ring homomorphism from $\mathbb{Z}_m$ into $\mathbb{Z}_{q_1^{t_1}} \oplus \mathbb{Z}_{q_2^{t_2}} \oplus \cdots \oplus \mathbb{Z}_{q_s^{t_s}}$ which carries 1 to $(a_1, a_2, \cdots, a_s)$. so the number of ring homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$ is simply the number of s-tuples which meet these two conditions.

Now, since the additive order of 0 is 1 and the additive order of 1 in $\mathbb{Z}_{q_i^{t_i}}$ is $q_i^{t_i}$, then we may take $a_i = 0$ or 1 when $q_i^{t_i} \mid m$, but we must take $a_i = 0$ when $q_i^{t_i} \nmid m$.

Claim: : $q_i^{t_i} \nmid m$ *if and only if* $q_i \,\Big|\, \left(\frac{n}{gcd(m,n)}\right)$

Proof: : ($\Rightarrow$): Let $n = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$,

and W.L.O.G. let $m = q_1^{T_1} q_2^{T_2} \cdots q_s^{T_s} \cdots q_l^{T_l}$ with $(T_i)'s \geq 0$,

Denote by $M_i = \min(t_i, T_i)$. So $\gcd(m,n) = q_1^{M_1} q_2^{M_2} \cdots q_s^{M_s}$.

Therefore; if $q_i^{t_i} \nmid m$, then the exponent t_i of q_i is $t_i > T_i$, $\Rightarrow M_i = T_i$, hence:

$$\left(\frac{n}{\gcd(m,n)}\right) = q_1^{t_1 - M_1} q_2^{t_2 - M_2} \cdots \underline{q_i^{t_i - T_i}} \cdots q_s^{t_s - M_s}.$$

Noting that $t_i - T_i > 0$ since $t_i > T_i$ implying that $t_i - T_i \geq 1$, (at least 1):

$$\Rightarrow \qquad q_i \,\Big|\, \left(\frac{n}{\gcd(m,n)}\right)$$

Conversely ($\Leftarrow$): Suppose that $q_i \,\Big|\, \left(\frac{n}{\gcd(m,n)}\right)$. Then:

$$since: \quad \left(\frac{n}{\gcd(m,n)}\right) = q_1^{t_1 - M_1} q_2^{t_2 - M_2} \cdots q_i^{t_i - M_i} \cdots q_l^{t_s - M_s}$$

$$and \quad q_i \,\Big|\, \left(\frac{n}{\gcd(m,n)}\right) \;\Rightarrow\; t_i - M_i \quad \text{is at least one;}$$

$$\text{i.e. } t_i > M_i, \text{ and } M_i = min(t_i, T_i) \;\Rightarrow\; M_i = T_i \;\Rightarrow\; t_i > T_i$$

$$\text{and so,} \quad q_i^{t_i} \nmid q_i^{T_i} \;\Rightarrow\; q_i^{t_i} \nmid m$$

■

Therefore, denoting by $\omega(k)$ the number of distinct prime divisors of the integer k, and therefore the number of ring homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$ is $2^{\omega(n) - \omega\left(\frac{n}{gcd(m,n)}\right)}$. □

An illustrating example is given on the next page:

Example 2.2. *Suppose we need to compute the number of ring homomorphisms:*

$$\phi : \mathbb{Z}_{20} \to \mathbb{Z}_{30}$$

First, we will solve the problem by finding these homomorphisms:
Let $\phi : \mathbb{Z}_{20} \to \mathbb{Z}_{30}$ *be a ring homomorphism: then for an* $x \in \mathbb{Z}_{30}$. *So, let* $\phi(1) = a$, *then* $\phi(x) = \phi(1 \cdot x) = x \cdot \phi(1) = ax$, *where* $a \in \mathbb{Z}_{30}$ *and the order of* a *must divide* 30 *and* 20. *That is:* $|a| \mid 30$ *and* $|a| \mid 20$. *Thus,* $|a|$ *is a common divisor of* 20 *and* 30, *so* $a \in \{1, 2, 5, 10\}$. *Now, the elements of* $\mathbb{Z}_{30}$ *that are of these orders are:*

Order	*The elements*
1	0
2	15
5	6, 12, 18, 24
10	3, 9, 21, 27

Moreover, since 1 *is an idempotent, so is* $\phi(1)$ *too, that is:* $a^2 = a$. *Computing the squares of our elements (* $\mod 30$*), we find:*
$\underline{0^2 = 0}$, $\underline{15^2 = 15}$, $\underline{6^2 = 6}$, $12^2 = 24$, $18^2 = 24$, $3^2 = 9$, $9^2 = 21$, $\underline{21^2 = 21}$ *and* $27^2 = 9$. *Therefore, the underlined elements are the idempotents, so* $a = 0, 6, 15, 21$ *and we have four ring homomorphisms:*

$$\phi(x) = 0, \quad \phi(x) = 6x, \quad \phi(x) = 15x, \quad \phi(x) = 21x$$

Solution by using the formula in the theorem. *Considering our formula above (in the theorem), we only have the following simple calculations to do:*
$m = 20, n = 30$, $\left(\frac{n}{\gcd(m,n)}\right) = \left(\frac{30}{\gcd(20,30)}\right) = \left(\frac{30}{10}\right) = 3$, $\omega(30) = 3$, $\omega(3) = 1$, *hence:*

$$\mathcal{N}(\phi : \mathbb{Z}_{20} \to \mathbb{Z}_{30}) = 2^{\omega(30)-\omega(3)} = 2^{3-1} = 2^2 = 4$$

Theorem 2.2. *[3, Theorem 1]*

The number of ring homomorphisms:

$$\phi: \quad \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} \quad \rightarrow \quad \mathbb{Z}_{p^k}$$

$$is \quad \left(1 + N_{p^k}(m_1, m_2, \cdots, m_r)\right)$$

Where $N_{p^k}(m_1, m_2, \ldots, m_r)$ is the number of elements in the set $\{m_1, m_2, \ldots, m_r\}$ that are divisible by p^k.

Proof. Let $\phi : \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} \rightarrow \mathbb{Z}_{p^k}$ be a ring homomorphism.

Let e_i be the r-tuple with 1 in the i^{th} component and 0's elsewhere. Then ϕ is completely determined by $\phi(e_1), \phi(e_2), \ldots, \phi(e_r)$.

Note that since e_i's is an idempotent element in $\mathbb{Z}_{m_i}$ for each i, then so are the $\phi(e_i)$ in $\mathbb{Z}_{p^k}$ $\forall\ i$, thus, $\phi(e_i) = 0$ or $1\ \forall i$.

Also, if $\phi(e_i) = \phi(e_j) = 1$ for some $i \neq j$. Then we have:

$0 = \phi(0) = \phi(e_i e_j) = \phi(e_i)\phi(e_j) = 1$, a contradiction.

Therefore, if ϕ is not the zero homomorphism, then $\phi(e_i) = 1$ for exactly one value i:

Claim: For that i, p^k must divide m_i

Proof: Let $\phi : \mathbb{Z}_{m_i} \rightarrow \mathbb{Z}_{p^k}$ be a natural ring homomorphism; then ϕ is surjective by definition. $\mathbb{Z}_{m_i}$ has the identity element $[1]_{m_i}$ and since ϕ is surjective, then $\phi([1]_{m_i})$ is the identity of $\mathbb{Z}_{p^k}$, so $\phi([1]_{m_i}) = [1]_{p^k}$, but:

$[0]_{p^k} = \phi([0]_{m_i}) = \phi(m_i[1]_{m_i}) = m_i\phi([1]_{m_i}) = m_i[1]_{p^k} = [m_i]_{p^k}$.

which implies $p^k \mid m_i$. ■

Hence, for each i, p^k must divide m_i, so the number of ring homomorphisms:

$\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ into $\mathbb{Z}_{p^k}$ is $1 + N_{p^k}(m_1, m_2, \cdots, m_r)$. □

Example 2.3.

Suppose we want to compute the number of ring homomorphisms: $\phi : \mathbb{Z}_{12} \times \mathbb{Z}_6 \to \mathbb{Z}_{2^2}$.

Note that ϕ *is completely determined by its action on* $(1,0)$ *and* $(0,1)$*:*

Let $\phi\big((0,1)\big) = a$*, then since* $6(0,1) = (0,0)$ *in* $\mathbb{Z}_{12} \times \mathbb{Z}_6$ *then* $6a = 0$ *in* $\mathbb{Z}_4$*, and therefore* $a = 0$ *or* $a = 2$.

The first value; $a = 0$ *gives us the first nontrivial homomorphism* $\phi\big((x,y)\big) = x(\mod 4)$.

The second value; $a = 2$ *gives us* $\phi\big((x,y)\big) = x + 2y$*, but this wouldn't be a ring homomorphism, and so, only the first possibility would be allowed.*

Therefore, we have two ring homomorphisms, namely:

$$\phi\big((x,y)\big) = 0, \quad \phi\big((x,y)\big) = x$$

Solution by using the formula in the theorem.

Let's compute the number of ring homomorphisms by using the formula in the theorem:

The number of elements in the set $\{12, 6\}$ *that are divisible by* $2^2 = 4$ *is* 1 *(namely,* 12*),*

i.e. $N_{2^2}(12,6) = 1$.

Hence the number of ring homomorphisms is $1 + N_{2^2}(12,6) = 1 + 1 = 2$*. We see that this is a much easier way to compute the number of ring homomorphisms than actually finding those homomorphisms.*

As a direct consequence of the last theorem, we get:

Theorem 2.3. *[3, Theorem 2]*

The number of ring homomorphisms:

$$\phi : \quad \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} \quad \to \quad \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_s^{k_s}}$$

is

$$\prod_{i=1}^{s} \Big(1 + N_{p^{k_i}}(m_1, m_2, \cdots, m_r)\Big)$$

2.2 Rings of Gaussian integers

Lemma 2.6. *For $i^2+1=0$, The number of ring homomorphisms:*

$$\phi : \mathbb{Z}[i] \quad \to \quad \mathbb{Z} \qquad\qquad is \qquad 1$$

Proof. Let $\phi :\ \mathbb{Z}[i] \to \mathbb{Z}$ be a ring homomorphism.

Any element in $\mathbb{Z}[i]$ is of the form $(x+yi)$ and for any $x \in \mathbb{Z}$, $\phi(x) = \phi(x \cdot 1) = x\phi(1)$, and $\phi(x+iy) = x\phi(1) + y\phi(i)$. So, any ring homomorphism is completely determined by the values of $\phi(1)$ and $\phi(i)$. Now, since 1 is an idempotent in $\mathbb{Z}$ ($1^2 = 1$), then so is $\phi(1)$. And the only idempotent elements in $\mathbb{Z}$ are 0 and 1. Then; $\phi(1) = 1$, or $\phi(1) = 0$: Note that $\phi(1)$ cannot be 1. Since, if it were, $\phi(1) = 1$; then we have:

$0 = \phi\Big(x + (-x)\Big) = \phi(x) + \phi(-x) \Rightarrow \phi(-x) = -\phi(x)$, and considering $\phi(i)$:

We have $-1 = -\phi(1) = \phi(-1) = \phi(i^2) = \Big(\phi(i)\Big)^2 \Rightarrow \Big(\phi(i)\Big)^2 = -1$, which would imply that $\phi(i)$ takes imaginary values in $\mathbb{Z}$, an absurd. Therefore, the only ring homomorphisms from $\mathbb{Z}[i]$ into $\mathbb{Z}$ is the zero (trivial) homomorphism: $\phi(x+iy) = 0$. □

Lemma 2.7. *The number of ring homomorphisms:*

$$\phi : \mathbb{Z}[i] \quad \to \quad \mathbb{Z}[i] \qquad\qquad is \qquad 3$$

Proof. Let $\phi :\ \mathbb{Z}[i] \ \to \ \mathbb{Z}[i]$ be a ring homomorphism.

Similar to the argument above: we have $\phi(1) = 1$ or 0.

If $\phi(1) = 0$ then we have the trivial homomorphism.

If $\phi(1) = 1$, then $\phi(x) = x\phi(1)$ and $0 = \phi\Big(x+(-x)\Big) = \phi(x)+\phi(-x)$ and so $\phi(-x) = -\phi(x)$

Thus; $-1 = -\phi(1) = \phi(-1) = \phi(i^2) = \Big(\phi(i)\Big)^2 \Rightarrow \phi(i) = \pm i$.

and so $\phi(x+iy) = x\phi(1) + y\phi(i) = x \pm yi$. Therefore; the only ring homomorphisms are:

$$\phi(x+yi) = x+yi \qquad \phi(x+yi) = x-yi \qquad \phi(x+yi) = 0$$

□

Theorem 2.4. *[2, Theorem 1]*

For $i^2 + 1 = 0$, The number of ring homomorphisms:

$$\phi : \mathbb{Z}[i] \quad \rightarrow \quad \mathbb{Z}[i]/\langle n \rangle$$

$$is \quad c_n \cdot 3^{\omega(n)}$$

Where $\omega(n)$ is the number of distinct prime factors of n in $\mathbb{Z}[i]$ and where:

$$c_n = \begin{cases} 1 & \text{if } 4 \nmid n; \\ \frac{5}{3} & \text{if } 4 \mid n \text{ but } 8 \nmid n; \\ 3 & \text{if } 8 \mid n \end{cases}$$

Proof. Let $\phi : \mathbb{Z}[i] \rightarrow \mathbb{Z}[i]/\langle n \rangle$ be a ring homomorphism.

Then, ϕ is completely determined by its action on 1 and i.

Let $\phi(1) = a$, and $\phi(i) = b$. Now, since $1^2 = 1$, $1 \cdot i = i$, and $i^2 = -1$; then in $\mathbb{Z}[i]/\langle n \rangle$:

$$\begin{aligned} 1^2 = 1 \quad &\Rightarrow \quad a^2 = a \\ 1 \cdot i = i \quad &\Rightarrow \quad a \cdot b = b \\ i^2 = -1 \quad &\Rightarrow \quad b^2 = -a \end{aligned}$$

Let the prime decomposition of n be: $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then by the Chinese Remainder Theorem, we have:

$$\mathbb{Z}[i]/\langle n \rangle \;\cong\; \mathbb{Z}[i]/\langle p_1^{k_1} \rangle \;\oplus\; \mathbb{Z}[i]/\langle p_2^{k_2} \rangle \;\oplus\; \cdots \;\mathbb{Z}[i]/\langle p_r^{k_r} \rangle$$

But a homomorphism from $\mathbb{Z}[i] \rightarrow \mathbb{Z}[i]/\langle n \rangle$ induces a homomorphism from $\mathbb{Z}[i]$ into $\mathbb{Z}[i]/\langle p_j^{k_j} \rangle$ for all j.

In the direct sum; let $a = (a_1, a_2, \ldots, a_r)$, and $b = (b_1, b_2, \ldots, b_r)$, then:

$$a_j^2 \equiv a_j \mod p_j^{k_j} \quad \Leftrightarrow \quad p_j^{k_j} \mid (a_j^2 - a_j) \quad \Leftrightarrow \quad p_j^{k_j} \mid a_j(a_j - 1)$$

But $\mathbb{Z}[i]$ is a UFD (by theorem (1.8), page 15) with a_j and $(a_j - 1)$ are relatively prime, which implies that either $p_j^{k_j} \mid a_j$ or $p_j^{k_j} \mid (a_j - 1)$.
Thus, either $a_j = 0,$ or $a_j = 1$.

$$\begin{aligned} If\ \ a_j = 0 \quad then \quad b_j = a_j \cdot b_j = 0 \quad &\Rightarrow \quad b_j = 0 \\ If\ \ a_j = 1 \quad then \quad b_j^2 = -a_j = -1 \quad &\Rightarrow \quad b_j^2 + 1 = 0 \end{aligned}$$

Therefore; $(b_j + i)(b_j - i) = 0$ in $\mathbb{Z}[i]/\langle p_j^{k_j} \rangle$, which implies $p_j^{k_j} \mid (b_j + i)(b_j - i)$
Now, if $p_j \neq 1 + i$, then since the only prime divisors of $2i$ is $(1 + i)$ (up to associates), then p_j cannot divide both factors: $(b_j + i)$ and $(b_j - i)$; and therefore:

$$p_j^{k_j} \mid (b_j + i) \quad or \quad p_j^{k_j} \mid (b_j - i) \quad \Rightarrow \quad b_j = \pm i$$

Now, consider the case when $p_j = 1 + i$:
Note that since $(1 + i)^2 = 2i$, then $(1 + i)$ can divide both factors; but since n is an integer, and since $|1 + i| = \sqrt{2}$, then the exponent, k_j, of p_j $(= 1 + i)$ must be an even integer, say $k_j = 2t$.
Then we have to consider three cases:

Case 1. $k_j = 2$, Then by *Corollary* (1.5) ,page 19, we have:

$$\mathbb{Z}[i]/\langle p_j^2 \rangle \ = \ \mathbb{Z}[i]/\langle 2i \rangle \ \cong \ \mathbb{Z}[i]/\langle 2^{2/2} \rangle \ = \ \mathbb{Z}[i]/\langle 2 \rangle$$

And hence we have two possibilities for b_j.

Case 2. For $k_j = 4$, by the same *Corollary* (1.5), we have:

$$\mathbb{Z}[i]\Big/\Big\langle p_j^4\Big|_{p_j=1+i}\Big\rangle \ \cong \ \mathbb{Z}[i]/\langle 2^{4/2} \rangle \ = \ \mathbb{Z}[i]/\langle 2^2 \rangle \ = \ \mathbb{Z}[i]/\langle 4 \rangle.$$

And the number of possibilities for b_j is 4.

Case 3. For $k_j \geq 6$, note that $p_j^2 = 2i$, so if p_j^2 divides $(b_j + i)$;

i.e. if $2i \mid b_j + i$; $\Rightarrow b_j + i = 2mi$ for some $m \in \mathbb{Z}$, hence:

$$b_j = 2mi - i \;\Rightarrow\; b_j - i \;=\; 2mi - 2i \;=\; 2i(m-1) \;\Rightarrow\; (p_j^2 = 2i) \mid (b_j - i)$$

$$So, \quad if \quad p_j^2 \mid (b_j + i) \qquad \Rightarrow \qquad p_j^2 \mid (b_j - i)$$

Similarly; if $p_j^2 \mid (b_j - i)$, then $\exists\ l \in \mathbb{Z}$ such that $b_j - i = 2li$, and so:

$$b_j = 2li + i \quad \Rightarrow \quad b_j + i \;=\; 2li + 2i \;=\; 2i(l+1) \quad \Rightarrow \quad p_j^2 \mid b_j + i$$

Therefore $p_j^2 = (1+i)^2$ divides one factor if and only if it divides the other.
But $(1+i)^3 = 2i(1+i) = (2i-2)$ which cannot divide both factors for:
if $\Big((1+i)^3 = (2i-2)\Big)\Big|(b_j + i)$, then:

$$\begin{aligned} & b_j + i &=& \ (2i-2)m \\ \Rightarrow \quad & b_j &=& \ (2i-2)m - i \\ \Rightarrow \quad & b_j &=& \ 2mi - 2m - i = i(2m-1) - 2m \\ \Rightarrow \quad & b_j - i &=& \ 2i(m-1) - 2m \end{aligned}$$

And $(1+i)^3 \nmid \big(2i(m-1) - 2m\big)$ [4] , i.e. $(1+i)^3 \nmid (b_j - i)$, So $(1+i)^3$ cannot divide both factors, $b_j + i$, $b_j - i$, hence $(1+i)^{k_j - 2}$ must divide one of the factors.
Now, $(1+i)^{k_j-2} = (1+i)^{2t-2} = (1+i)^{2(t-1)} = \big((1+i)^2\big)^{t-1} = (2i)^{t-1} = 2^{t-1}$ (up to associates). Note that the set $2^{t-1}(r+si)$ has 4 elements in $\mathbb{Z}[i]/\langle 2^{2t/2}\rangle$ and:

$$\mathbb{Z}[i]/\langle 2^{2t/2}\rangle = \mathbb{Z}[i]/\langle 2^t\rangle \cong \mathbb{Z}[i]/\langle p_j^{k_j}\rangle \tag{2.4}$$

which gives $2 \times 4 = 8$ possibilities for the values of b_j. So we determined the necessary and sufficient conditions for the existence of a ring homomorphisms from $\mathbb{Z}[i]$ into $\mathbb{Z}[i]/\langle n\rangle$.

[4] In view of *Theorem* (1.6), page 14, $N\big((1+i)^3\big) = 8 \nmid 4\big(\underbrace{2m^2 - 2m + 1}_{an\ \ odd\ \ number}\big) = N\big(2i(m-1) - 2m\big)$

Conversely; If $(a_1, a_2, \ldots, a_r)$ and $(b_1, b_2, \ldots, b_r)$ are any elements of the direct sum which satisfy the above conditions, then the number of ring homomorphisms from $\mathbb{Z}[i]$ into $\mathbb{Z}[i]/\langle n\rangle$ is as claimed. □

Example 2.4. *The ring homomorphisms from:* $\mathbb{Z}[i] \to \mathbb{Z}[i]/\langle 3\rangle$*:*

First, we solve the problem by actually finding the ring homomorphisms:

Let $\phi : \mathbb{Z}[i] \to \mathbb{Z}[i]/\langle 3\rangle$ *be a ring homomorphism, then:*

Since $(x + iy) = x(1) + y(i)$*, then* $\phi(x + iy) = x\phi(1) + y\phi(i)$*, and so* ϕ *is completely determined by its action on* 1 *and* i*.*

Let $\phi(1) = a$ *and* $\phi(i) = b$*, so* $\phi(x + iy) = ax + by$

$1^2 = 1 \Rightarrow a^2 = a \Rightarrow a = 0$ *or* $a = 1$*.*

$i^2 = -1 \Rightarrow b^2 = -a \Rightarrow b = 0$ *or* $b = \pm i$*, i.e. in* $\mathbb{Z}_3[i]$*,* $b = i, 2i$

If $a = 0$ *then* $b = 0$ *and we have the zero homomorphism:* $\phi(x + iy) = 0$*.*

If $a = 1$ *and* $b = i$*, then* $\phi(x + iy) = x + iy$

If $a = 1$ *and* $b = 2i$*, then* $\phi(x + iy) = x + 2iy$*, which is a ring homomorphism since:*

Let $\alpha = x + iy$*,* $\beta = u + iv$*, then:* $\phi(\alpha) = x + 2iy$ *and* $\phi(\beta) = u + 2iv$ *and:*

$\alpha \cdot \beta = (xu - yv) + i(xv + yu)$,

$\phi(\alpha \cdot \beta) = (xu\underline{-yv}) + 2i(xv + yu) = (xu\underline{+2yv}) + 2i(xv + yu)$

$\phi(\alpha) \cdot \phi(\beta) = (x + 2iy)(u + 2iv) = (xu\underline{\underline{-4yv}}) + 2i(xv + yu)$

$= (xu\underline{\underline{+2yv}}) + 2i(xv + yu) = \phi(\alpha \cdot \beta)$

Therefore, we have $\mathcal{N}\Big(\phi : \mathbb{Z}[i] \to \mathbb{Z}[i]/\langle 3\rangle\Big) = 3$*, namely:*

$$\phi(x + iy) = 0, \qquad \phi(x + iy) = x + iy, \qquad \phi(x + iy) = x + 2iy$$

Solution by using the formula in the theorem.

Let's consider the same problem using the formula in the theorem:

Note, $4 \nmid 3$ *(*$4 \nmid n$*) and we have the first case of* c_n*: thus,* $c_n = 1$*.*

$\omega(3) = 1$ *(3 is a prime in* $\mathbb{Z}[i]$*) Therefore:*

$$\mathcal{N}\Big(\phi : \mathbb{Z}[i] \to \mathbb{Z}[i]/\langle 3\rangle\Big) = 1 \times 3^{\omega(3)} = 1 \times 3^1 = 3$$

Theorem 2.5. *[2, Theorem 2]*

The number of ring homomorphisms:

$$\phi : Z[i]/\langle m\rangle \quad \rightarrow \quad Z[i]/\langle n\rangle$$

$$is \quad c_n \cdot 3^{\omega(n)-\omega\left(\frac{n}{\gcd(m,n)}\right)}$$

where $\omega(k)$ is the number of distinct prime factors of k in $Z[i]$ and c_n is:

$$c_n = \begin{cases} 1 & \text{if } 4 \nmid n, \text{ or } 2 \mid \left(\frac{n}{\gcd(m,n)}\right); \\ \frac{5}{3} & \text{if } 2 \nmid \left(\frac{n}{\gcd(m,n)}\right) \text{ and } 4 \mid n \text{ but } 8 \nmid n; \\ 3 & \text{if } 8 \mid n \text{ and } 2 \nmid \left(\frac{n}{\gcd(m,n)}\right) \end{cases}$$

Proof.

Note that we still have the same conditions as in the previous theorem's proof, but moreover:

$$Let \quad \phi : \mathbb{Z}[i]/\langle m\rangle \rightarrow \mathbb{Z}[i]/\langle n\rangle$$

be a ring homomorphism, and let the prime decomposition of $n \in \mathbb{Z}[i]/\langle n\rangle$ be:

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

Let $\phi(1) = a = (a_1, a_2, \ldots, a_r) \in \mathbb{Z}[i]/\langle n\rangle$. Then:
When $a_j = 1 \in \mathbb{Z}[i]/\langle p_j^{k_j}\rangle$, then $ma_j = m = 0$ in $\mathbb{Z}[i]/\langle p_j^{k_j}\rangle$ because $m \cdot 1 = 0$ in $\mathbb{Z}[i]/\langle m\rangle$
So, whenever $p_j^{k_j}$ doesn't divide m, then only the trivial homomorphism for that component of the direct product is possible, hence, reducing the exponent of 3 or 5. □

Example 2.5.

Consider the number of ring homomorphisms: $\phi : \mathbb{Z}[i]/\langle 3\rangle \to \mathbb{Z}[i]/\langle 6\rangle$*:*

Solving the problem by finding the ring homomorphisms:

For an $\alpha \in \mathbb{Z}[i]/\langle 3\rangle$, $\alpha = a(1) + b(i)$, *so* ϕ *is determined by the values of* $\phi(1)$ *and* $\phi(i)$. *So, let* $e = \phi(1)$ *and* $f = \phi(i)$, *we have the following conditions to satisfy:*

$e^2 = e$, $ef = f$, $f^2 = -e$ *with* $3e = 0$,*and as an idempotent,* $e \in \{0, 1, 3, 4\}$.

For $e = 0 \Rightarrow f = 0$ *giving us the zero homomorphism:* $(e, f) = (0, 0)$.

For $e = 1$ *and* $e = 3$ *are not acceptable since* $3e \neq 0$ *in either case.*

For $e = 4 \Rightarrow f^2 = -4$, *and so* $f = \pm i$ *giving us* $(e, f) = (4, 2i)$ *and* $(4, -2i)$.

Therefore, we have the following 3 *ring homomorphisms:*

$$\phi(x + iy) = 0 \qquad \phi(x + iy) = 4x + 2iy \qquad \phi(x + iy) = 4x - 2iy$$

Solution by using the formula in the theorem.

Solving the problem using the formula in the theorem.

We have $m = 3$ *and* $n = 6$, *and* $4 \nmid 6$ *giving us the first case of* c_n *which is* $c_n = 1$.

Note, even thought 2 *is not a Gaussian prime and it factors as* $2 = (1 + i)(1 - i)$, *but actually, the number of distinct prime factors of* 2 *is one since* $(1 + i)$ *and* $(1 - i)$ *are the same Gaussian prime (for* $1 + i = i(1 - i)$*). Hence, we have,the number of prime divisors of* 6 *is* 2 *in* $\mathbb{Z}[i]$, *and that of* 2 *is* 1, *thus:*

$\omega(6) = 2$, *and* $\omega\left(\frac{6}{\gcd(3,6)}\right) = \omega\left(\frac{6}{3}\right) = \omega(2) = 1$.

Hence, $\mathcal{N}\big(\phi : \mathbb{Z}[i]/\langle 3\rangle \to \mathbb{Z}[i]/\langle 6\rangle\big) = c_n \cdot 3^{\omega(6) - \omega\left(\frac{6}{\gcd(3,6)}\right)} = 1 \cdot 3^{\omega(6) - \omega(2)} = 3^{2-1} = 3$.

Theorem 2.6. *[4, Theorem 1]*

The number of ring homomorphisms:

$$\phi : \mathbb{Z}_m[i] \times \mathbb{Z}_n[i] \quad \rightarrow \quad \mathbb{Z}_k[i]$$

$$is \quad c_n \cdot 5^{\omega(k)-\omega\left(\frac{k}{\gcd(m,n,k)}\right)} \cdot 3^{2\omega\left(\frac{k}{\gcd(m,n,k)}\right)-\omega\left(\frac{k}{\gcd(m,k)}\right)-\omega\left(\frac{k}{\gcd(n,k)}\right)}$$

where $\omega(s)$ is the number of distinct prime factors of s in $Z[i]$ and:

$$c_n = \begin{cases} 1 & \text{if either } 4 \nmid k \text{ or } \left(4 \mid k,\ \left(2 \middle| \left(\frac{k}{\gcd(m,k)}\right)\right) \text{ and } \left(2 \middle| \left(\frac{k}{\gcd(n,k)}\right)\right)\right) \\ \frac{5}{3} & \text{if } 4 \mid k,\ 8 \nmid k \text{ and } \left(4 \mid n \text{ or } 4 \mid m \text{ but not both}\right) \\ \frac{9}{5} & \text{if } 4 \mid k,\ 8 \nmid k \text{ and } 2 \not\middle| \left(\frac{k}{\gcd(m,n,k)}\right) \\ 3 & \text{if } 8 \mid k \text{ and } \left(8 \mid n \text{ or } 8 \mid m \text{ but not both}\right) \\ \frac{17}{5} & \text{if } 8 \mid k \text{ and } 2 \not\middle| \left(\frac{k}{\gcd(m,n,k)}\right) \end{cases}$$

Proof.

$$Let \qquad \phi \ : \ \mathbb{Z}_m[i] \ \times \ \mathbb{Z}_n[i] \quad \rightarrow \quad \mathbb{Z}_k[i]$$

be a ring homomorphism; then any ring homomorphism is completely determined by its action on $(1,0),(0,1),(i,0)$ and $(0,i)$.

Let the the prime decomposition of k be: $\quad k = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$.

Then, by the Chinese Remainder Theorem:

$$\mathbb{Z}_k[i] \ \cong \ \mathbb{Z}_{p_1^{r_1}}[i] \ \times \ \mathbb{Z}_{p_2^{r_2}}[i] \ \times \ \cdots \ \times \ \mathbb{Z}_{p_t^{r_t}}[i]$$

For $\phi((1,0))$ and $\phi((0,1))$:

Let $\ \phi((1,0)) = u \mod k \qquad$ and $\qquad \phi((0,1)) = v \mod k$, then:

Let $\phi((s,t)) = (us + vt) \mod k$

$$\begin{aligned}
&\textit{but} && 0 = \phi\Big((0,0)\Big) = \phi\Big((m,0)\Big) = m\phi\Big((1,0)\Big) = mu, && \textit{so} \quad u = 0 \quad \textit{or} \quad u = m \\
&\textit{and} && u = \phi\Big((1,0)\Big) = \phi\Big((1,0)^2\Big) = \Big(\phi\Big((1,0)\Big)\Big)^2 = u^2, && \textit{so} \quad u = 0 \quad \textit{or} \quad u = 1 \\
&\textit{Similarly} && 0 = \phi\Big((0,0)\Big) = \phi\Big((0,n)\Big) = n\phi\Big((0,1)\Big) = nv, && \textit{so} \quad v = 0 \quad \textit{or} \quad v = n \\
&\textit{And} && v = \phi\Big((0,1)\Big) = \phi\Big((0,1)^2\Big) = \Big(\phi\Big((0,1)\Big)\Big)^2 = v^2, && \textit{so} \quad v = 0 \quad \textit{or} \quad v = 1
\end{aligned}$$

Therefore; $\phi\left((1,0)\right)$ and $\phi\left((0,1)\right)$ in $\mathbb{Z}_{p_j^{r_j}}[i]$ each is equal to 0 or 1 $\forall j$.

And since ϕ sends idempotent elements into idempotent elements, then any ring homomorphism is completely determined by its action on $(i,0)$ and $(0,i)$:

So let $a = \phi\left((i,0)\right)$ and $b = \phi\left((0,i)\right)$. Thus, the ring homomorphism is completely determined by its action on the values of a, b.

Moreover, the order of a must divide $gcd(m,k)$ and the order of b must divide $gcd(n,k)$.

Suppose $p_j \neq 1+i$ then we have three cases to consider:

Case 1. If $p_j^{r_j} \mid gcd(m,n)$ then:

$$\begin{aligned}
(i,0)^2 &= (-1,0) = -1(1,0) \quad \Rightarrow \quad a_j^2 = -u \\
(i,0)\cdot(0,i) &= (mu,nv) \quad \Rightarrow \quad a_j \cdot b_j = 0 \\
(0,i)^2 &= (0,-1) = -1(0,1) \quad \Rightarrow \quad b_j^2 = -v
\end{aligned}$$

But $u = 0, 1$, and $v = 0, 1$. Thus, for $u, v \neq 0$, $a_j^2 = -1$ and $b_j^2 = -1$.

Therefore, $p_j^{r_j} \mid (a_j + i)(a_j - i)$ and $p_j^{r_j} \mid (b_j + i)(b_j - i)$.

$\Rightarrow a_j = 0, i$ or $-i$ and $b_j = 0, i$ or $-i$.

Now, $k = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ and by the Chinese Remainder Theorem:

$\mathbb{Z}_k[i] \cong \mathbb{Z}_{p_1^{r_1}}[i] \times \mathbb{Z}_{p_2^{r_2}}[i] \times \cdots \times \mathbb{Z}_{p_t^{r_t}}[i]$; so a homomorphism from $\mathbb{Z}_m[i] \times \mathbb{Z}_n[i]$ into $\mathbb{Z}_k[i]$ induces a homomorphism from $\mathbb{Z}_m[i] \times \mathbb{Z}_n[i]$ into $\mathbb{Z}_{p_j^{r_j}}[i]$ $\forall j$.

Now, since $(i,0)^2 = -i(i,0)$, then $a_j^2 \equiv -ia_j \mod p_j^{r_j} \Rightarrow p_j^{r_j} \mid a_j(a_j + i)$, and

since $\mathbb{Z}_m[i] \times \mathbb{Z}_n[i]$ is a UFD, then a_j and $(a_j + i)$ are relatively prime; therefore, either $p_j^{r_j} \mid a_j$ or $p_j^{r_j} \mid (a_j + i)$; $\Rightarrow \Big(a_j = 0 \text{ or } a_j = -i\Big) \in \mathbb{Z}_{p_j^{r_j}}[i]$

Therefore, in $\mathbb{Z}_{p_j^{r_j}}[i]$ $\Big(a_j = 0 \text{ or } a_j = -i\Big)$ along with $\big(b_j = 0,\ i,\ -i\big)$ giving us:

$(0,0)$	$(0,i)$	$(0,-i)$
$(-i,0)$	$(-i,i)$	$(-i,-i)$

Similarly, $(0,i)^2 = -i(0,i) \Rightarrow b_j^2 = -ib_j \mod p_j^{r_j} \Rightarrow p_j^{r_j} \mid b_j(b_j + i)$

$\Rightarrow \Big(b_j = 0, \text{ or } b_j = -i\Big) \in \mathbb{Z}_{p_j^{r_j}}[i]$

Therefore, in $\mathbb{Z}_{p_j^{r_j}}[i]$ $\Big(b_j = 0 \text{ or } b_j = -i\Big)$ along with $\big(a_j = 0,\ i,\ -i\big)$ giving us:

$(0,0)$	$(i,0)$	$(-i,0)$
$(0,-i)$	$(i,-i)$	$(-i,-i)$

but $a_j b_j = 0 \mod p_j^{r_j} \Rightarrow$ we have 5 choices as described in the following table:

$(0,0)$	$(0,-i)$	$(-i,0)$	~~$(-i,-i)$~~
$(0,i)$	$(i,0)$	~~$(-i,i)$~~	~~$(i,-i)$~~

Also, note that the number of primes p_j such that $p_j^{r_j} \mid \gcd(m,n,k)$ is:

$$\omega(k) - \omega\left(\tfrac{k}{\gcd(m,n,k)}\right)$$

Case 2. If $p_j^{r_j} \mid m$ but $p_j^{r_j} \nmid n$, then we have:

$$a_j = 0, \quad i, \quad \text{or} \quad -i \quad \text{and} \quad b_j = 0 \quad \Rightarrow \quad \text{we have} \quad 3 \quad \text{choices}$$

And noting that the number of primes p_j such that $p_j^{r_j} \mid m$ but $p_j^{r_j} \nmid n$ is:

$$\omega\left(\tfrac{k}{\gcd(m,n,k)}\right) - \omega\left(\tfrac{k}{\gcd(m,k)}\right)$$

Case 3. If $p_j^{r_j} \mid n$ but $p_j^{r_j} \nmid m$, then we have:

$$a_j = 0, \quad \text{and} \quad b_j = 0, \quad i, \quad \text{or} \quad -i \quad \Rightarrow \quad \text{we have} \quad 3 \quad \text{choices}$$

Also, the number of primes p_j such that $p_j^{r_j} \mid n$ but $p_j^{r_j} \nmid m$ is:

$$\omega\left(\tfrac{k}{\gcd(m,n,k)}\right) - \omega\left(\tfrac{k}{\gcd(n,k)}\right)$$

When $p_j = 1 + i$, complication arise: since $(1+i)^2 = 2i \Rightarrow (1+i)$ can divide both factors of $\big((a_j + i), (a_j - i)\big)$, and $\big((b_j - i), (b_j + i)\big)$. And $|1 + i| = \sqrt{2} \Rightarrow r_j$, the exponent of p_j, must be an even integer, and so, we have to consider three cases:

Case 1. $r_j = 2$, $\Rightarrow p_j^{r_j} = 2i$, and by *equation* (2.4),page 54, we have: $\mathbb{Z}_{p_j^{r_j}}[i] \cong \mathbb{Z}_2[i]$.
so if $2 \mid \gcd(m,n)$ then: Let $\phi\big((i,0)\big) = ui \mod 2$ and $\phi\big((0,i)\big) = vi \mod 2$.
So $\phi\big((s,t)\big) = (us+vt) \mod 2$, then:

$$\begin{aligned} 0 &= \phi\big((0,0)\big) = \phi\big((2i,0)\big) = 2\phi\big((i,0)\big) = 2iu \Rightarrow u = 0 \text{ or } 1 \\ 0 &= \phi\big((0,0)\big) = \phi\big((0,2i)\big) = 2\phi\big((0,i)\big) = 2iv \Rightarrow v = 0 \text{ or } 1 \end{aligned}$$

and thus we have three choices.

Case 2. $r_j = 4$, then we have:

$$\mathbb{Z}_{p_j^{r_j}}[i] \cong \mathbb{Z}_4[i]$$

If $4 \mid \gcd(m,n)$, then $\phi\big((s,t)\big) = us+vt \mod 4$, and noting that:

$$\begin{aligned} 0 &= \phi\big((0,0)\big) = \phi\big((4i,0)\big) = 4\phi\big((i,0)\big) = 4iu \Rightarrow u = 0,\ 1,\ 2 \text{ or } 3 \\ 0 &= \phi\big((0,0)\big) = \phi\big((0,4i)\big) = 4\phi\big((0,i)\big) = 4iv \Rightarrow v = 0,\ 1,\ 2 \text{ or } 3 \end{aligned}$$

Therefore, we have 9 choices.

If $4 \mid m$ or $4 \mid n$; but not both, then we have either $u = 0,1,2,3$, and $v = 0$, or vise versa: $v = 0,1,2,3$, and $u = 0$ giving us 5 choices.

If $4 \nmid m$ and $4 \nmid n \Rightarrow u = v = 0 \Rightarrow$ one choice.

Case 3. If $r_j \geq 6$:

If $8 \mid \gcd(m,n)$, then similar to the explanation in *Case* 2, a_j and b_j would have 8 choices each, giving us $2 \times 8 + 1 = 17$ choices.

If $8 \mid m$ or $8 \mid n$ but not both, $\Rightarrow 9$ choices.

And if $8 \nmid m$ and $8 \nmid n$, then we have only one choice, and hence, completing the proof.

□

Example 2.6.

Concerning the number of ring homomorphisms $\phi : \mathbb{Z}_3[i] \times \mathbb{Z}_4[i] \to \mathbb{Z}_6[i]$

ϕ *is determined by its action on the generators* $\Big((1,0),(0,1),(i,0),(0,i)\Big)$ *of* $\mathbb{Z}_3[i] \times \mathbb{Z}_4[i]$ *(as being a group homomorphism) along with the additional ring-homomorphism conditions on the images of those generators.*

So, let $x = \phi\big((1,0)\big), y = \phi\big((0,1)\big), u = \phi\big((i,0)\big), v = \phi\big(0,i)\big)$*, then:*

$x = u = 0,\ 2,\ 4,\ 2i,\ 4i,\ 2+2i,\ 2+4i,\ 4+2i,\ 4+4i$ *and* $y = v = 0,\ 3,\ 3i,\ 3+3i.$

But ϕ *being a ring homomorphism requires that* x *and* y *to be idempotents and* $x \cdot y = 0$*,* $u \cdot v = 0$*,* $u^2 = -x$*,* $v^2 = -y$*. Combining these conditions we get that:*

$x = 0,\ 4$*;* $y = 0,\ 3$*;* $u = 0,\ 4,\ 4i$*;* $v = 0,\ 3,\ 3i$*;*

For $\alpha = a + bi$ *and* $\beta = c + di$*, we have the following* 9 *ring homomorphism:*

$\phi((1,0))$	$\phi((0,1))$	$\phi((i,0))$	$\phi((0,i))$
0	0	0	0
0	3	0	3
0	3	0	$3i$
4	0	$4i$	0
4	3	$4i$	3
4	3	$4i$	$3i$
4	0	4	0
4	3	4	3
4	3	4	$3i$

$$\text{So } \phi\Big(\alpha,\beta\Big) = \begin{cases} 0 \\ (3c+3d) \\ (3c)+(3d)i \\ (4a)+(4b)i \\ (4a+3c+3d)+(4b)i \\ (4a+3c)+(4b+3d)i \\ (4a+4b) \\ (4a+4b+3c+3d) \\ (4a+4b+3c)+(3d)i \end{cases}$$

Solution by using the formula in the theorem. *We have:*

$m = 3, n = 4, k = 6$*, first of all, note that* $4 \nmid 6$*, thus* $c_n = 1$*. Then, the* ω*'s:*

$$\Big(\tfrac{k}{\gcd(m,n,k)}\Big) = \Big(\tfrac{6}{\gcd(3,4,6)}\Big) = \big(\tfrac{6}{1}\big) = 6, \quad \Big(\tfrac{k}{\gcd(m,k)}\Big) = \Big(\tfrac{6}{\gcd(3,6)}\Big) = \big(\tfrac{6}{3}\big) = 2$$

$$\Big(\tfrac{k}{\gcd(n,k)}\Big) = \Big(\tfrac{6}{\gcd(4,6)}\Big) = \big(\tfrac{6}{2}\big) = 3, \qquad \textit{Thus } \omega(6) = 2,\ \omega(3) = 1,\ \omega(2) = 1$$

and the number of ring homomorphisms $\phi : \mathbb{Z}_3[i] \times \mathbb{Z}_4[i] \to \mathbb{Z}_6[i]$ *is:*

$$\mathcal{N} = c_n \cdot 5^{\omega(k)-\omega\left(\frac{k}{\gcd(m,n,k)}\right)} \cdot 3^{2\omega\left(\frac{k}{\gcd(m,n,k)}\right)-\omega\left(\frac{k}{\gcd(m,k)}\right)-\omega\left(\frac{k}{\gcd(n,k)}\right)}$$

$$= 1 \cdot 5^{\omega(6)-\omega(6)} \cdot 3^{2\omega(6)-\omega(2)-\omega(3)} = 1 \cdot 5^0 \cdot 3^{2\cdot 2-1-1} = 3^2 = 9$$

Theorem 2.7. *[6, Theorem 1]*

The number of ring homomorphisms:

$$\phi : \mathbb{Z}_{m_1}[i] \times \cdots \times \mathbb{Z}_{m_r}[i] \quad \to \quad \mathbb{Z}_{p^k}[i]$$

$$is \qquad C_k$$

$$where \quad C_k = \begin{cases} 1 + 2N_{p^k} & if \quad p^k = 2 \quad or \quad p \equiv 3 \mod 4 \\ 1 + 4N_{p^k} & if \quad p^k = 4 \\ 1 + 6N_{p^k} & if \quad p^k = 2^k, \quad k \geq 3 \\ 1 + 8N_{p^k} & if \quad p \equiv 1 \mod 4 \end{cases}$$

Where N_{p^k} *is the number of elements in the set:* $\{m_1, m_2, \ldots, m_r\}$ *that are divisible by* p^k.

Proof.

Let $\phi : \mathbb{Z}_{m_1}[i] \times \cdots \times \mathbb{Z}_{m_r}[i] \to \mathbb{Z}_{p^k}[i]$ be a ring homomorphism.

Let $e_1, e_2, \ldots, e_r$ be the $r - tuples$ such that each e_j has 1 in the j^{th} component and 0 elsewhere.

Let $f_1, f_2, \ldots, f_r$ be the $r - tuples$ such that each f_j has i in the j^{th} component and 0 eslewhere.

Then ϕ is completely determined by the values of $\phi(e_j)$ and $\phi(f_j)$ for $j = 1, 2, \ldots, r$.

Note that since each e_j is an idempotent element in $\mathbb{Z}_{m_j}[i]$, then so is $\phi(e_j)$ in $\mathbb{Z}_{p^k}[i]$.

$$And \ if \quad \phi(e_i) \neq 0, \quad \phi(e_j) \neq 0 \qquad for \qquad i \neq j$$
$$then \qquad 0 = \phi(0) = \quad \phi(e_i e_j) = \quad \phi(e_i)\phi(e_j) \quad \neq 0 \quad which \ is \ a \ contradiction$$

And hence for a nonzero homomorphism ϕ, we have $\phi(e_i) \neq 0$ for exactly one value i, and for that i, p^k must divide m_i. Moreover:

$$f_i \cdot f_i = -e_i \qquad \Rightarrow \qquad \phi(f_i) \cdot \phi(f_i) = -\phi(e_i)$$

$$e_i \cdot f_i = f_i \qquad \Rightarrow \qquad \phi(e_i) \cdot \phi(f_i) = \phi(f_i)$$

$$\phi(e_i) \ \textit{is an idempotent} \quad \Rightarrow \quad \big(\phi(e_i)\big)^2 = \phi(e_i) \mod p^k$$

$$\textit{Therefore} \qquad \phi(e_i)\Big(\phi(e_i) - 1\Big) = 0 \mod p^k$$

Then, we will consider the following cases:

Case 1. $p^k = 2$ or $p \equiv 3 \mod 4$, So we have:

$$\begin{gathered} x^2 \equiv x \mod 2 \\ x^2 \equiv x \mod p \equiv 3 \mod 4 \end{gathered} \tag{2.5}$$

Then, equation (3.2) has a solution if and only if $x = 0$ or 1;

$$\textit{But} \qquad \phi(e_i) \neq 0 \qquad \Rightarrow \qquad \phi(e_i) = 1$$

$$\textit{So} \qquad \phi(e_i) = 1 \qquad \Rightarrow \quad \big(\phi(f_i)\big)^2 = -\phi(e_i) = -1$$

Moreover, as for the generator of $\mathbb{Z}_{p^k}[i]$, $(1 - i)$, we have $|1 - i| = \sqrt{2}$ and so:

$$\big(\phi(f_i)\big)^2 = -1 \quad \Rightarrow \quad \underline{\phi(f_i) = \pm i} \quad if \quad p^k \nmid 4$$

which gives us <u>two choices</u> for this case $(p^k = 2 \ \text{ or } \ p \equiv 3 \mod 4)$.

Case 2. $p^k = 4$: We have $\big(\phi(e_i)\big)^2 = \phi(e_i) \mod 4$.

Then, by *Lemma 1.6*, *Case* (2) (pages 12-13), we get:

$\Big((\phi(e_i))^2 \equiv \phi(e_i) \mod 4 \Big)$ has a solution if and only if:

$$\phi(e_i) \equiv 1 \mod 4 \qquad or \qquad \phi(e_i) \equiv 3 \mod 4$$

$$So,\ modulo\ 4, \quad \Big(\phi(f_i)\Big)^2 = -\phi(e_i) = \begin{cases} -1 & \Rightarrow \ \phi(f_i) = \pm i \\ -3 & \Rightarrow \ \phi(f_i) = \pm\sqrt{3}i \end{cases}$$

Therefore $\phi(f_i)$ has 4 possibilities (for $p^k = 2$).

Case 3. $p^k = 2^k$: and for $k \geq 3$, we have:

$$\big(\phi(f_i)\big)^2 = -\phi\big(e_i\big) \equiv -1 \mod 2^k \Rightarrow \big(\phi(f_i)\big)^2 \equiv -1 \mod 2^k$$

Then we have either one of the following two cases:

$$\big(\phi(f_i)\big)^2 \ = \ -1 \quad \Rightarrow \quad \phi(f_i) = \pm i$$

And by *equation* (1.3), page 11, we have:

$$\phi(f_i) = 2^{n-1} + bi, \qquad where \qquad b = 1, \quad -1, \quad 2^{n-1}+1, \quad 2^{n-1}-1.$$

Hence, $\phi(f_i)$ has 6 possibilities.

Case 4. For $p \equiv 1 \mod 4$:

$$Now \quad \big(\phi(f_i)\big)^2 = -\phi(e_i), \qquad \phi(f_i) \cdot \phi(e_i) = \phi(f_i) :$$

$$For \quad \phi(e_i) = 1 \quad \Rightarrow \quad \big(\phi(f_i)\big)^2 \equiv -1 \mod p \quad \Rightarrow \quad \phi(f_i) = \pm i$$

Since $\Big(x^2 \equiv -1 \mod p\Big)$ has a solution if and only if $\Big(p \equiv 1 \mod 4\Big)$;

And the number of solutions to the quadratic congruence is:

$$1 + \left(\frac{-1}{p}\right) = 2 \quad for \quad p \equiv 1 \mod 4$$

Therefore, $\Big(\big(\phi(f_i)\big)^2 \equiv -1 \mod p\Big)$ has two solutions for $p \equiv 1 \mod 4$;
So, taking into considerations the *associates* of each solution ξ_j, for $j = 1, 2$:

$$\xi_j, \quad -\xi_j, \quad i\xi_j, \quad -i\xi_j, \qquad j = 1, 2$$

Hence, $\phi(f_i)$ has a total of 8 possibilities.

□

Theorem 2.8. *[6, Theorem 2]*
The number of ring homomorphisms:

$$\phi : \mathbb{Z}_{m_1}[i] \times \mathbb{Z}_{m_2}[i] \times \cdots \times \mathbb{Z}_{m_r}[i] \to \mathbb{Z}_{p_1^{k_1}}[i] \times \mathbb{Z}_{p_2^{k_2}}[i] \times \cdots \times \mathbb{Z}_{p_s^{k_s}}[i]$$

$$is \qquad \prod_{i=1}^{i=s} C_k$$

Where C_k is as in theorem (2.7) (page 63).

Proof. Using the same argument as in the last theorem's proof, and taking the product of all those numbers for each case. □

2.3 Rings of Eisenstein integers

Theorem 2.9. *[2, Theorem 3]*

Let ρ be a solution of: $\rho^2 + \rho + 1 = 0$, Then, the number of ring homomorphisms:

$$\phi : \mathbb{Z}[\rho] \quad \rightarrow \quad \mathbb{Z}_n[\rho]$$

$$is \quad c_n \cdot 3^{\omega(n)}$$

where $\omega(n)$ is the number of distinct prime factors of n in $\mathbb{Z}[\rho]$ and:

$$c_n = \begin{cases} 1 & if\ 3 \nmid n; \\ \frac{4}{3} & if\ 3 \mid n\ but\ 9 \nmid n; \\ \frac{7}{3} & if\ 9 \mid n \end{cases}$$

Proof. Let $\phi : \mathbb{Z}[\rho] \rightarrow \mathbb{Z}_n[\rho]$ be a ring homomorphism.

And let $\phi(1) = a$, and $\phi(\rho) = b$, then:

$$\begin{aligned} 1^2 = 1 \quad &\Rightarrow \quad a^2 = a \\ 1 \cdot \rho = \rho \quad &\Rightarrow \quad a \cdot b = b \\ \rho^2 + \rho + 1 = 0 \quad &\Rightarrow \quad b^2 + b + a = 0 \end{aligned}$$

Let the prime-power decomposition of $n \in \mathbb{Z}[\rho]$ be: $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then:

$$\begin{aligned} a_j^2 = a_j \quad &\Rightarrow \quad a_j = 0 \quad \text{or} \quad a_j = 1 : \\ \text{If} \quad a_j = 0, \quad &\text{then} \quad b_j = a_j \cdot b_j = 0 \\ \text{If} \quad a_j = 1, \quad &\text{then} \quad b_j^2 + b_j + 1 = 0 \end{aligned}$$

$$\Rightarrow \quad (b_j - \rho)(b_j - \rho^2) = 0 \quad in \ \mathbb{Z}_{p_j^{k_j}}[\rho] \quad \Rightarrow \quad p_j^{k_j} \Big| (b_j - \rho)(b_j - \rho^2)$$

Suppose $p_j \neq (1-\rho)$, then:

$$(b_j - \rho^2) - (b_j - \rho) = \rho(1-\rho)$$

Therefore; $(1-\rho)$ is the only prime divisor of the difference of these two factors (up to associates), i.e. p_j cannot divide both factors, and thus, $\quad b_j = \rho \quad \text{or} \quad b_j = \rho^2$.

When $p_j = (1-\rho)$, then, since $(1-\rho)$ can divide both factors, and since $|1-\rho| = \sqrt{3}$, and since n is an integer, then k_j, the exponent of $p_j (= 1-\rho)$, must be an even integer. Moreover; by the *Conclusion* of *Proposition 6* (1.5.2), page 25: $\mathbb{Z}_{p_j^{k_j}}[\rho] \cong \mathbb{Z}_3[\rho]$.

$$\textit{So;} \quad a^2 = a, \quad a \cdot b = b \quad \textit{and} \quad b^2 + b + a = 0 \quad \textit{with} \quad p_j^{k_j} \mid (b_j - \rho)(b_j - \rho^2)$$

And for $k_j = 2$ and $p_j = (1-\rho)$:

$$p_j^2 = (1-\rho)^2 = 1 - 2\rho + \rho^2 = (1+\rho^2) - 2\rho = -\rho - 2\rho = -3\rho \quad \Rightarrow \quad p_j^2 = -3\rho$$

$$\textit{which shows that:} \qquad \mathbb{Z}[\rho]/\langle p_j^2 \rangle = \mathbb{Z}[\rho]/\langle (1-\rho)^2 \rangle = \mathbb{Z}[\rho]/\langle -3\rho \rangle \cong \mathbb{Z}[\rho]/\langle 3 \rangle$$

$$\begin{aligned} \textit{So,} \quad & p_j^2 = -3\rho \mid (b_j - \rho); \quad \textit{i.e.} \quad b_j \cong \rho \mod (-3\rho), \quad \textit{and} \\ & p_j^2 = -3\rho \mid (b_j - \rho^2), \quad \textit{i.e.} \quad b_j \cong \rho^2 \mod (-3\rho) \end{aligned}$$

$$\begin{aligned} & \textit{Now, if } k_j \geq 4 \quad (\textit{i.e.} k_j = 4, 6, 8, \cdots), \quad \textit{then:} \\ & p_j^4 = (1-\rho)^4 = (-3\rho)^2 = 9\rho^2, \\ & p_j^6 = (-3\rho) \cdot 9\rho^2 = -27\rho^3, \\ & p_j^8 = (-3\rho) \cdot -27\rho^3 = 81\rho^4, \\ & \quad \vdots \\ & p_j^{2t} = (1-\rho)^{2t} = (-1)^t \cdot 3^{2t}\rho^t \end{aligned}$$

Hence: $(1-\rho)^{k_j - 1} = (1-\rho)^{odd}$ divides one factor. And since $\mathbb{Z}[\rho]/\langle (1-\rho) \rangle$ has 3 elements, then $(1-\rho)^{k_j-1}$ divides 3 elements in $\mathbb{Z}[\rho]/\langle p_j^{k_j} \rangle$. Therefore, we have $(1-\rho)$ divides 3 elements and $(1-\rho)^{k_j-1}$ divides 3 elements, and so we have in total (including the zero possibility) 7 possibilities.

So, we have determined the necessary conditions for the existence of a homomorphism from $\mathbb{Z}[\rho]$ into $\mathbb{Z}_n[\rho]$.

Conversely, if $(a_1, a_2, \ldots, a_r)$ and $(b_1, b_2, \ldots, b_r)$ are the elements of the direct sum which satisfy the above conditions, then there is a homomorphism from $\mathbb{Z}[\rho]$ into $\mathbb{Z}[\rho]/\langle n\rangle$ and the number of homomorphism is as claimed. □

Example 2.7.

Considering the ring homomorphisms: $\phi : \mathbb{Z}[\rho] \to \mathbb{Z}_2[\rho]$*:*

Using the usual method of finding the ring homomorphisms: ϕ *is determined completely by its action on* 1 *and* ρ*.*

Let $\phi(1) = a$ *and* $\phi(\rho) = b$*, then* $b^2 + b + a = 0$*, and:*

$1^2 = 1 \Rightarrow a^2 = a \Rightarrow a = 0, 1.$

Now, if $a = 0$*, then* $b^2 + b = 0 \Rightarrow b = 0$ *or* $b = -1 = \rho^2 + \rho$*,*

but the second choice wouldn't preserve the ring-multiplication property, and so $b = 0$*.*

If $a = 1$*, then* $b^2 + b + 1 = 0 \Rightarrow b = \rho, \rho^2$

and thus we have three ring homomorphisms:

$$\phi(x + \rho y) = 0, \qquad \phi(x + \rho y) = x + \rho y, \qquad \phi(x + \rho y) = x + \rho^2 y$$

Solution by using the formula in the theorem. *We have:*

$n = 2$*,* $3 \nmid 2$*, so this is the first case of* c_n *on page* 67 *(*$c_n = 1$*).*

$\omega(2) = 1$ *since* 2 *is an Eisenstein prime, and:*

Thus, $\mathcal{N}\big(\phi : \mathbb{Z}[\rho] \to \mathbb{Z}_2[\rho]\big) = c_n \cdot 3^{\omega(n)} = 1 \cdot 3^{\omega(2)} = 3^1 = 3.$

Theorem 2.10. *[2, Theorem 4]*

The number of ring homomorphisms:

$$\phi : Z_m[\rho] \quad \rightarrow \quad Z_n[\rho]$$

$$is \quad c_n \cdot 3^{\omega(n)-\omega\left(\frac{n}{\gcd(m,n)}\right)}$$

where $\omega(k)$ is the number of distinct prime factors of k in $Z[\rho]$ and:

$$c_n = \begin{cases} 1 & \text{if either } 3 \nmid n, \text{ or } 3 \left| \left(\frac{n}{\gcd(m,n)}\right) \right. \\ \frac{4}{3} & \text{if } 3 \nmid \left(\frac{n}{\gcd(m,n)}\right) \text{ and } 3 \mid n \text{ but } 9 \nmid n; \\ \frac{7}{3} & \text{if } 3 \left| \left(\frac{n}{\gcd(m,n)}\right) \right. \text{ and } 9 \mid n \end{cases}$$

Proof.

Let $\phi : \mathbb{Z}_m[\rho] \rightarrow \mathbb{Z}_n[\rho]$ be a ring homomorphism.

And let the prime decomposition of n be: $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$.

Note that we still have the same conditions as in the previous theorem's proof, but moreover:

Letting $\phi(1) = a = (a_1, a_2, \ldots, a_r)$.

Then, whenever $a_j = 1 \in \mathbb{Z}[\rho]/\langle p_j^{k_j} \rangle$, we have:

$$ma_j = m = 0 \in \mathbb{Z}[\rho]/\langle p_j^{k_j} \rangle \quad since \quad m \cdot 1 = m = 0 \in \mathbb{Z}[\rho]/\langle m \rangle$$

So, whenever $p_j^{k_j}$ doesn't divide m, then, only the trivial homomorphism for that component of the direct product is possible, hence, reducing the exponent of 3. □

Example 2.8.

Consider the ring homomorphisms: $\phi : \mathbb{Z}_3[\rho] \to \mathbb{Z}_6[\rho]$*:*

As in the previous example, ϕ *is completely determined by its action on* 1 *and* ρ*;*

Let $e = \phi(1)$ *and* $f = \phi(\rho)$*, then we have to find* ϕ *that satisfies the following conditions:* $e^2 = e$*,* $ef = e$*,* $f^2 + f + e = 0$ *and as* e *is the image of an idempotent, we must have* $e \in \{0, 1, 3, 4\}$*, the idempotents of* $\mathbb{Z}_6[\rho]$*. Moreover, as* $3 \cdot 1 = 0$ *in* $\mathbb{Z}_3[\rho]$*, then* $3e = 0$*.*

For $e = 0$*, then* $f^2 + f + e = f^2 + f = 0 \Rightarrow f = 0$ *and so we have the zero homomorphism:* $(e, f) = (0, 0)$*.*

For $e = 1$ *or* $e = 3$*, they are not acceptable, since* $3e \neq 0$ *in either case.*

For $e = 4$*,* $f^2 + f + e = f^2 + f + 4 = 0$ *whose solution is* $f = 4, 4\rho, r\rho^2$ *giving us the homomorphisms:*

$(e, f) = (4, 4), (4, 4\rho)$ *and* $(4, 4\rho^2)$*.*

Therefore, we have four ring homomorphisms.

Solution by using the formula in the theorem. *We have:*

$m = 3$*,* $n = 6$*.* $\left(\frac{n}{\gcd(m,n)}\right) = \left(\frac{6}{\gcd(3,6)}\right) = \left(\frac{6}{3}\right) = 2$*,*

and $3 \nmid 2$*,* $3 \mid 6$ *but* $9 \nmid 6$ *which is the first case of* c_n *and therefore,* $c_n = \frac{4}{3}$

And for the ω*'s,* $\omega(n) = \omega(6) = 2$*,* $\omega\left(\frac{n}{\gcd(m,n)}\right) = \omega(2) = 1$ *Hence:*

$$\mathcal{N}\Big(\phi : Z_3[\rho] \quad \to \quad Z_6[\rho]\Big) = \frac{4}{3} \cdot 3^{2-1} = \frac{4}{3} \cdot 3 = 4.$$

Theorem 2.11. *[6, Theorem 3]*

The number of ring of ring homomorphisms:

$$\phi : \mathbb{Z}_{m_1}[\rho] \times \mathbb{Z}_{m_2}[\rho] \times \cdots \times \mathbb{Z}_{m_r}[\rho] \;\; \rightarrow \;\; \mathbb{Z}_{p^k}[\rho]$$

$$is \qquad C_k$$

$$where \quad C_k = \begin{cases} 1 + 2N_{p^k}(m_1, m_2, \ldots, m_r) & if\ p \neq 3, \quad and \quad p \equiv 3 \mod 4 \\ 1 + 3N_{p^k}(m_1, m_2, \ldots, m_r) & if\ p^k = 3 \\ 1 + 6N_{p^k}(m_1, m_2, \ldots, m_r) & if\ p^k = 3^k, \quad k \geq 2 \\ 1 + 8N_{p^k}(m_1, m_2, \ldots, m_r) & if\ p \equiv 1 \mod 4 \end{cases}$$

Where $N_{p^k}(m_1, m_2, \ldots, m_r)$ is the number of of elements in the set $\{m_1, m_2, \ldots, m_r\}$ that are divisible by p^k.

Proof.

Let $\phi : \mathbb{Z}_{m_1}[\rho] \times \mathbb{Z}_{m_2}[\rho] \times \cdots \times \mathbb{Z}_{m_r}[\rho] \;\; \rightarrow \;\; \mathbb{Z}_{p^k}[\rho]$ be a ring homomorphism.

Let $e_1, e_2, \ldots, e_r$ be the $r - tuples$ such that each e_j has 1 in the j^{th} component and 0 elsewhere.

Let $f_1, f_2, \ldots, f_r$ be the $r - tuples$ such that each f_j has ρ in the j^{th} component and 0 eslewhere.

Then ϕ is completely determined by the values of $\phi(e_j)$ and $\phi(f_j)$ for $j = 1, 2, \ldots, r$.

Since $\forall\ j$, each e_j is an idempotent in $\mathbb{Z}_{m_j}[\rho]$, then so is each $\phi(e_j)$ in $\mathbb{Z}_{p^k}[\rho]$.

$$\begin{aligned} &Also, \;\; for \;\; \phi(e_i) \neq 0, \;\; \phi(e_j) \neq 0 \quad for \;\; i \neq j \\ &\Rightarrow \quad 0 = \phi(0) = \phi(e_i \;\; e_j) = \phi(e_i) \;\; \phi(e_j) \neq 0; \qquad A \;\; contradiction. \end{aligned}$$

Hence; $\phi(e_i) \neq 0$ for exactly one value of i, and for that i, p^k must divide m_i. Moreover:

$$f_i^2 + f_i + e_i = 0 \quad \Rightarrow \quad \big(\phi(f_i)\big)^2 + \phi(f_i) + \phi(e_i) = 0$$

So, we consider the following cases:

Case 1. If $p^k \neq 3$ and $p \equiv 3 \mod 4$:

Note that, by the idempotent-ness of each $\phi(e_i)$, we have:

$$\big(\phi(e_i)\big)^2 = \phi(e_i) \quad \Rightarrow \quad \phi(e_i) = 1 \quad \Rightarrow \quad \big(\phi(f_i)\big)^2 + \phi(f_i) + 1 = 0$$

which implies that: $\phi(f_i) = \rho$ or $\phi(f_i) = \rho^2$.

But, $|1 - \rho| = \sqrt{3}$, thus, if $p^k \neq 3$, and $p \equiv 3 \mod 4$

then $\phi(f_i)$ has only two choices $(\rho,\ \rho^2)$.

Case 2. If $p^k = 3$; then:

$$\big(\phi(f_i)\big)^2 + \phi(f_i) + 1 = 0 \quad \big(\mod p^k \big)$$

$$\xleftrightarrow{\text{for } p^k = 3} \quad \big(\phi(f_i)\big)^2 + \phi(f_i) + 1 = 0 \quad (\mod 3) \tag{2.6}$$

And the solution to *equation* 3.3 is:

$$\phi(f_i) = 1, \qquad \rho, \qquad and \qquad -2\rho$$

Therefore; $\phi(f_i)$ has 3 possibilities.

Case 3. If $p^k = 3^k$, $k \geq 2$, then, as in the proof of *theorem 2.7*, (3), page 65:

Thus; $\phi(f_i)$ has 6 possibilities.

Case 4. Finally, for $p \equiv 1 \mod 4$; then, as in the proof of *theorem 2.7*, (4), pages 65 - 66:

Therefore; $\phi(f_i)$ has 8 possibilities.

□

Theorem 2.12. *[6, Theorem 4]*

Let p_i, $1 \leq i \leq s$, be primes not necessarily distinct. Then, the number of ring homomorphisms:

$$\phi: \ \mathbb{Z}_{m_1}[\rho] \times \mathbb{Z}_{m_2}[\rho] \times \cdots \times \mathbb{Z}_{m_r}[\rho] \quad \rightarrow \quad \mathbb{Z}_{p_1^{k_1}}[\rho] \times \mathbb{Z}_{p_2^{k_2}}[\rho] \times \cdots \times \mathbb{Z}_{p_s^{k_s}}[\rho]$$

$$is \quad \prod_{i=1}^{i=s} C_k$$

Where C_k is as defined in the previous theorem (Theorem, (2.11), page 72).

Proof. Using the same argument as in last theorem's proof, and taking the product of each result. □

Theorem 2.13. *[4, Theorem 2]:*

The number of ring homomorphisms:

$$\phi: \ \mathbb{Z}_m[\rho] \times \mathbb{Z}_n[\rho] \quad \rightarrow \quad \mathbb{Z}_k[\rho]$$

$$is \quad c_n \cdot 5^{\omega(k)-\omega\left(\frac{k}{\gcd(m,n,k)}\right)} \cdot 3^{2\omega\left(\frac{k}{\gcd(m,n,k)}\right)-\omega\left(\frac{k}{\gcd(m,k)}\right)-\omega\left(\frac{k}{\gcd(n,k)}\right)}$$

where $\omega(s)$ is the number of distinct prime factors of s in $\mathbb{Z}[\rho]$ and:

$$c_n = \begin{cases} 1 & \text{if either } 3 \nmid k \text{ or } \left(3 \mid k, \left(3 \middle| \left(\frac{k}{gcd(n,k)}\right)\right), \text{and} \left(3 \middle| \left(\frac{k}{gcd(m,k)}\right)\right)\right) \\ \frac{4}{3} & \text{if } 3 \mid k,\ 9 \nmid k \text{ and } 3 \not\middle| \left(\frac{k}{gcd(m,n,k)}\right) \\ \frac{7}{3} & \text{if } 9 \mid k \text{ and } \left(3 \mid n \text{ or } 3 \mid m \text{ but not both}\right) \\ \frac{13}{5} & \text{if } 9 \mid k \text{ and } 3 \not\middle| \left(\frac{k}{gcd(m,n,k)}\right) \end{cases}$$

Proof.

Any ring homomorphism from $\mathbb{Z}_m[\rho] \times \mathbb{Z}_n[\rho]$ into $\mathbb{Z}_k[\rho]$ is completely determined by its action on: $(1,0), \quad (\rho,0), \quad (0,1), \quad (0,\rho)$.

Let the prime-power decomposition of k in $\mathbb{Z}[\rho]$ be:

$$k = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$$

Then by the Chinese Remainder Theorem:

$$\mathbb{Z}_k[\rho] \cong \mathbb{Z}_{p_1^{r_1}}[\rho] \times \mathbb{Z}_{p_2^{r_2}}[\rho] \times \cdots \mathbb{Z}_{p_t^{r_t}}[\rho]$$

Let $\phi : \mathbb{Z}_m[\rho] \times \mathbb{Z}_n[\rho] \to \mathbb{Z}_k[\rho]$ be a ring homomorphism.

Then, as before, we have: $\phi((0,1)) = 0$ or 1, and $\phi((1,0)) = 0$ or 1.

$$\begin{aligned} \textit{Let} \quad \phi\big((\rho,0)\big) &= a = (a_1, a_2, \ldots, a_t) \\ \textit{and} \quad \phi\big((0,\rho)\big) &= b = (b_1, b_2, \ldots, b_t) \end{aligned}$$

And therefore, any ring homomorphism is completely determined by a and b: but the order of a must divide the $\gcd(m,k)$, and similarly, the order of b must divide the $\gcd(n,k)$.

Firstly: suppose that $p_j \neq 1 - \rho$, then we have 4 cases to consider:

Case 1. If $p_j^{r_j} \mid \gcd(m,n)$, then note that since $\phi((0,1)) = 0$ or 1, then:

$$\begin{aligned} (\rho,0)\cdot(\rho,0) = \rho^2 \quad &\Rightarrow \quad a_j^2 = a_j \\ (0,\rho)\cdot(0,\rho) = \rho^2 \quad &\Rightarrow \quad b_j^2 = b_j \\ \textit{and} \ (\rho,0)\cdot(0,\rho) = (0,0) = 0 \quad &\Rightarrow \quad a_j b_j = 0 \end{aligned}$$

Now, $a_j b_j = 0$, $a_j^2 + a_j + 1 = 0$ and $b_j^2 + b_j + 1 = 0$, so:

note that $0 = \phi\big((0,0)\big) = \phi\big((m\rho,0)\big) = m\phi\big((\rho,0)\big) = ma_j$,

and since $p_j^{r_j} \mid \gcd(m,n) \Rightarrow p_j^{r_j} \mid m \Rightarrow a_j = 0$.

But $a_j^2 + a_j + 1 = 0$ is factored out as $(a_j - \rho)(a_j - \rho^2) = 0 \Rightarrow a_j = \rho$, or $a_j = \rho^2$

hence: $a_j = 0, \quad \rho,$ or ρ^2.

Similarly; $0 = \phi\big((0,0)\big) = \phi\big((0,n\rho)\big) = n\phi\big((0,\rho)\big) = nb_j$;

and $p_j^{r_j} \mid \gcd(m,n) \Rightarrow p_j^{r_j} \mid n \Rightarrow b_j = 0$, and $b_j^2 + b_j + 1 = 0 \Rightarrow (b_j - \rho)(b_j - \rho^2) = 0$,

Hence, $b_j = 0, \quad \rho$ or ρ^2, but $a_j b_j = 0$, hence we reduce one choice, giving us 5

choices. Therefore, The number of primes, p_j, such that $p_j^{r_j} \mid \gcd(m,n,k)$ is:

$$\omega(k) - \omega\left(\frac{k}{\gcd(m,n,k)}\right)$$

Case 2. If $p_j^{r_j} \mid m$ but $p_j^{r_j} \nmid n$ then $a_j = 0$, ρ or ρ^2 and $b_j = 0$. which implies that we have 3 choices, and the number of primes p_j such that $p_j^{r_j} \mid \gcd(m,k)$ but $p_j^{r_j} \nmid n$ is:

$$\omega\left(\frac{k}{\gcd(m,n,k)}\right) - \omega\left(\frac{k}{\gcd(m,k)}\right)$$

Case 3. If $p_j^{r_j} \mid n$ but $p_j^{r_j} \nmid m$ then $a_j = 0$, $b_j = 0$, ρ or ρ^2. $\Rightarrow$ we have 3 choices too, and hence the number of primes p_j such that $p_j^{r_j} \mid \gcd(n,k)$ but $p_j^{r_j} \nmid m$ is:

$$\omega\left(\frac{k}{\gcd(m,n,k)}\right) - \omega\left(\frac{k}{\gcd(n,k)}\right)$$

Case 4. If $p_j^{r_j} \nmid m$ and $p_j^{r_j} \nmid n$, then $a_j = b_j = 0 \Rightarrow$ we only have the trivial case.

When $p_j = 1 - \rho$, complication arise, because $(1-\rho)$ can divided both factors.
And since $|1-\rho| = \sqrt{3}$, and k_j is an integer, then r_j, the exponent of p_j, must be an even integer:
For $r_j = 2$, then $p_j^{r_j} = p_j^2 = (1-\rho)^2 = -3\rho$, $\Rightarrow$ $\mathbb{Z}_{p_j^2}[\rho] \cong \mathbb{Z}_3[\rho]$, and so we have the following cases:

Case 1. If $3 \mid \gcd(m,n)$; $3 \mid m$, $\Rightarrow p_j^2 \mid m$ and $p_j^2 \mid (a_j - \rho)(a_j - \rho^2)$:
which implies that p_j^2 can divide both factors, and hence:
$a_j \equiv \rho \mod p_j^2$ has exactly one solution.
$a_j \equiv \rho^2 \mod p_j^2$ has exactly two solutions; giving a total of 3 solutions,
and similarly for b_j gives us 3 choices too.
But $a_j b_j = 0 \Rightarrow a_j = b_j = 0$ giving us a total of $1+2+3+1 = 7$ choices.

Case 2. If $3 \mid m$ or $3 \mid n$ but not both;

$a_j \equiv \rho \mod p_j^2 \Rightarrow$ one solution.

$a_j \equiv \rho^2 \mod p_j^2 \Rightarrow 2$ solutions.

and $b_j = 0 \Rightarrow$ a total of $1 + 2 + 1 = 4$ choices.

Case 3. If $3 \nmid m$, and $3 \nmid n \Rightarrow a_j = b_j = 0 \Rightarrow$ one choice.

Secondly; For an even $r_j \geq 4$ (i.e. $r_j = 4, 6, \ldots$), then we have the following cases:

Case 1. If $9 \mid \gcd(m, n)$ then we have:

$a_j \equiv \rho \mod p_j^2$ has exactly one solution.

$a_j \equiv \rho^2 \mod p_j^2$ has exactly two solutions.

$a_j \equiv \rho^l \mod p_j^2$ for $l = 2^s$, where $s \geq 2$ has exactly three solutions.

Giving us $1 + 2 + 3 = 6$ choices.

and similarly for b_j:

$b_j \equiv \rho \mod p_j^2$ has exactly one solution.

$b_j \equiv \rho^2 \mod p_j^2$ has exactly two solutions.

$b_j \equiv \rho^l \mod p_j^2$ for $l = 2^s$, where $s \geq 2$ has exactly three solutions.

Giving us another 6 $(= 1 + 2 + 3)$ choices.

But $a_j b_j = 0$ giving us a total of $6 + 6 + 1 = 13$ choices.

Case 2. If $9 \mid m$ or $9 \mid n$ but not both, then:

$c_j \equiv \rho \mod p_j^2$ has exactly one solution.

$c_j \equiv \rho^2 \mod p_j^2$ has exactly two solutions.

$c_j \equiv \rho^l \mod p_j^2$ for $l = 2^s$, where $s \geq 2$ has exactly three solutions.

where c represents either a or b for $9 \mid m$, or $9 \mid n$ respectively;

along with $a_j b_j = 0$ giving us a total of $1 + 2 + 3 + 1 = 7$ choices.

Case 3. Finally; if $9 \nmid m$, and $9 \nmid n$, then we only have the trivial case, and this finishes our proof.

□

Example 2.9.

Consider the ring homomorphisms: $\phi : \mathbb{Z}_3[\rho] \times \mathbb{Z}_4[\rho] \to \mathbb{Z}_6[\rho]$

Let $\alpha = x + y\rho \in \mathbb{Z}_3[\rho]$ *and* $\beta = u + v\rho \in \mathbb{Z}_4[\rho]$.

Then for any $(\alpha, \beta) \in (\mathbb{Z}_3[\rho] \times \mathbb{Z}_4[\rho])$, $\alpha = x(1,0) + y(\rho, 0)$ *and* $\beta = u(0,1) + v(0,\rho)$

So, any ring homomorphism, ϕ, *is completely determined by its action on* $(1,0)$, $(\rho,0)$, $(0,1)$ *and* $(0,\rho)$.

Let $e_1 = \phi(1,0)$, $e_2 = \phi(0,1)$, $f_1 = \phi(\rho,0)$, *and* $f_2 = \phi(0,\rho)$*; then we must have:*

For $i = 1, 2$; $e_i^2 = e_i$, $e_i f_i = f_i$, $e_1 e_2 = f_1 f_2 = 0$, $e_i \in \{0, 1, 3, 4\}$

along with $3e_1 = 0$ *and* $4e_2 = 0$.

For $e_1 = 0$, $e_2 = 0 \Rightarrow f_1 = f_2 = 0$ *giving us:* $(e_1, e_2, f_1, f_2) = (0, 0, 0, 0)$.

For $e_1 = 0$, $e_2 = 1$ *or* $e_2 = 4$ *are not acceptable, since* $4 \cdot e_2 \neq 0$ *in either case.*

For $e_1 = 0$, $e_2 = 3$ *is acceptable since* $4 \cdot e_2 = 4 \cdot 3 = 0$ *in* $\mathbb{Z}_6[\rho]$. *And:*

$f_2^2 + f_2 + e_2 = f^2 + f_2 + 3 = 0 \Rightarrow f_2 = 3\rho, 3\rho^2$ *giving us the following homomorphisms:*

$(e_1, e_2, f_1, f_2) = (0, 3, 0, 3\rho)$ *or* $= (0, 3, 0, 3\rho^2)$.

For $e_1 = 1$ *or* $e_1 = 3$ *are not acceptable, since* $3e_1 \neq 0$ *in either case.*

For $e_1 = 4$, $e_2 = 0 \Rightarrow f_1 = 4, 4\rho, 4\rho^2$ *and* $f_2 = 0$ *giving us:*

$(e_1, e_2, f_1, f_2) = (4, 0, 4, 0)$, $(4, 0, 4\rho, 0)$ *or* $(4, 0, 4\rho^2, 0)$.

For $e_1 = 4$, $e_2 = 3$ *give us the following homomorphisms:*

$(e_1, e_2, f_1, f_2) = (4, 3, 4, 3\rho), (4, 3, 4, 3\rho^2), (4, 3, 4\rho, 3\rho), (4, 3, 4\rho, 3\rho^2), (4, 3, 4\rho^2, 3\rho), (4, 3, 4\rho^2, 3\rho^2)$.

Therefore, we have the following twelve ring homomorphisms:

(letting $\alpha = a + b\rho$ and $\beta = c + d\rho$):

$\phi((1,0))$	$\phi((\rho,0))$	$\phi((0,1))$	$\phi((0,\rho))$	$\phi(\alpha,\beta)$
0	0	0	0	0
0	0	3	3ρ	$3c + 3d\rho$
0	0	3	$3\rho^2$	$3c + 3d\rho^2$
4	4	0	0	$4a + 4b$
4	4ρ	0	0	$4a + 4b\rho$
4	$4\rho^2$	0	0	$4a + 4b\rho^2$
4	4	3	3ρ	$(4a + 4b + 3c) + 3d\rho$
4	4	3	$3\rho^2$	$(4a + 4b + 3c) + 3d\rho^2$
4	4ρ	3	3ρ	$(4a + 3c) + (4b + 3d)\rho$
4	4ρ	3	$3\rho^2$	$(4a + 3c) + 4b\rho + 3d\rho^2$
4	$4\rho^2$	3	3ρ	$(4a + 3c) + 3d\rho + 4b\rho^2$
4	$4\rho^2$	3	$3\rho^2$	$(4a + 3c) + (4b + 3d)\rho^2$

Solution by using the formula in the theorem.

For: the ring homomorphisms $\phi : \mathbb{Z}_3[\rho] \times \mathbb{Z}_4[\rho] \to \mathbb{Z}_6[\rho]$

Here, $m = 3$, $n = 4$, *and* $k = 6$*: so,*

$3 \mid k$ *but* $9 \nmid k$ *which gives us the first case of* c_n, *and hence* $c_n = \frac{4}{3}$.

$$\left(\frac{k}{\gcd(m,n,k)}\right) = \left(\frac{6}{\gcd(3,4,6)}\right) = \left(\frac{6}{1}\right) = 6$$

$$\left(\frac{k}{\gcd(m,k)}\right) = \left(\frac{6}{\gcd(3,6)}\right) = \left(\frac{6}{3}\right) = 2$$

$$\left(\frac{k}{\gcd(n,k)}\right) = \left(\frac{6}{\gcd(4,6)}\right) = \left(\frac{6}{2}\right) = 3$$

$\omega(k) = \omega(6) = 2$, $\omega(2) = 1$ *and* $\omega(3) = 1$.

Therefore:

$$\begin{aligned}\mathcal{N}\big(\phi : \mathbb{Z}_3[\rho] \times \mathbb{Z}_4[\rho] \to \mathbb{Z}_6[\rho]\big) &= \\ &= \left(\tfrac{4}{3}\right) \cdot 5^{\omega(6)-\omega(6)} \cdot 3^{2\omega(6)-\omega(2)-\omega(3)} \\ &= \left(\tfrac{4}{3}\right) \cdot 5^{0} \cdot 3^{2(2)-1-1} = \tfrac{4}{3} \cdot 3^{2} = 12 \ \textit{homomorphisms}\end{aligned}$$

Notice the simplicity of the calculations done for the formula in the theorem compared to the complications of those calculations done by going through the regular methods of finding the ring homomorphisms.

2.4 Certain rings of algebraic numbers

Lemma 2.8.

Let $m \in \mathbb{Z}$ be any square free integer, then the number of ring homomorphisms:

$$\phi: \ \mathbb{Z}[\sqrt{m}] \quad \rightarrow \quad \mathbb{Z}[\sqrt{m}] \qquad\qquad is \qquad 3$$

Proof.

$$Let \qquad\qquad \phi : \mathbb{Z}[\sqrt{m}] \quad \rightarrow \quad \mathbb{Z}[\sqrt{m}]$$

Note: $\mathbb{Z}[\sqrt{m}] = \{x + y\sqrt{m} : \ x, y \in \mathbb{Z}\}$. Thus, any element of $\mathbb{Z}[\sqrt{m}]$ is of the form: $x + y\sqrt{m}$, and for any $x \in \mathbb{Z}$, a nonzero homomorphism $\phi(x) = x$. So, any homomorphism ϕ is completely determined by the value of $\phi(\sqrt{m})$.

Now, suppose that $\phi(\sqrt{m}) = \alpha + \beta\sqrt{m}$ for some $\alpha, \beta \in \mathbb{Z}$.

Thus, $\phi(k + l\sqrt{m}) = k + l(\alpha + \beta\sqrt{m})$.

So, let $a, b \in \mathbb{Z}[\sqrt{m}]$, so; $a = x + y\sqrt{m}, \quad b = z + u\sqrt{m}$, Then:

$$\phi(a) \cdot \phi(b) = \phi(a \cdot b) \tag{2.7}$$

The right hand side of *equation* (2.7) is:

$$\begin{aligned} \phi(a \cdot b) \ &= \ \phi\Big((x + y\sqrt{m}) \cdot (z + u\sqrt{m})\Big) \ = \ \phi\Big((xz + yum) + (xu + yz)\sqrt{m}\Big) \\ &= \ (xz + yum) + (xu + yz)(\alpha + \beta\sqrt{m}) \end{aligned} \tag{2.8}$$

And the left hand side of *equation* (2.7) is:

$$\begin{aligned}\phi(a)\cdot\phi(b) &= \phi\Big((x+y\sqrt{m})\Big)\cdot\phi\Big((z+u\sqrt{m})\Big)=\Big((x+y(\alpha+\beta\sqrt{m})\Big)\cdot\Big(z+u(\alpha+\beta\sqrt{m})\Big)\\ &= \Big(xz+xu(\alpha+\beta\sqrt{m}\Big)+yz(\alpha+\beta\sqrt{m})+yu(\alpha+\beta\sqrt{m})\\ &= \Big(xz+yu\alpha^2+yu\beta^2m+2yu\alpha\beta\sqrt{m}\Big)+(xu+zy)(\alpha+\beta\sqrt{m})\end{aligned} \tag{2.9}$$

Equating the results of both equations, 4.2, 4.3 yields:

$$(xz+yum)+\underline{\underline{(xu+yz)(\alpha+\beta\sqrt{m})}}=\Big(xz+yu\alpha^2+yu\beta^2m+2yu\alpha\beta\sqrt{m}\Big)+\underline{\underline{(xu+zy)(\alpha+\beta\sqrt{m})}}$$

Cancelling the underlined (*equal*) terms leads:

$$\begin{aligned}(\underline{xz}+yum) &= \Big(\underline{xz}+yu\alpha^2+yu\beta^2m+2yu\alpha\beta\sqrt{m}\Big)\\ \Rightarrow\qquad yu(m) &= yu(\alpha^2+\beta^2m+2\alpha\beta\sqrt{m})\end{aligned}$$

Which implies that:

$$m = \alpha^2 + \beta^2 m + 2\alpha\beta\sqrt{m} \tag{2.10}$$

And since m is a square free integer, then $\sqrt{m}\notin\mathbb{Z}$. So, the last equation would be possible only if $\alpha\beta=0\Rightarrow\alpha=0$ or $\beta=0$.

If $\beta=0$ then: $m=\alpha^2$ which is impossible since $\alpha\in\mathbb{Z}$ and m is a square free.

If $\alpha=0$ then: $m=m\beta^2\Rightarrow 1=\beta^2\Leftrightarrow\beta=\pm1$ which gives us two nonzero homomorphisms:

$$\phi(\sqrt{m})_+=\alpha+\beta\sqrt{m}\qquad\qquad and\qquad\qquad \phi(\sqrt{m})_-=\alpha-\beta\sqrt{m}$$

□

Theorem 2.14. *[5, Theorem 8] Let θ be an algebraic number over $\mathbb{Z}$ with minimal polynomial $p(x) = x^2 + ux + v$ whose absolute radicand,$(m = |u^2 - 4v|)$, is a prime integer and $\mathbb{Z}[\theta]$ is a UFD* [5] *then:*

The number of ring homomorphisms:

$$\phi : \ \mathbb{Z}[\theta] \ \rightarrow \ \mathbb{Z}_k[\theta] is \qquad c_k \cdot 3^{\omega(k)}$$

Where $\omega(k)$ is the number of prime factors of k in $\mathbb{Z}[\theta]$, and:

$$c_k = \begin{cases} 1 & if \quad m \nmid k \\ \frac{m+1}{3} & if \quad m \mid k \quad but \quad m^2 \nmid k \\ \frac{2m+1}{3} & if \quad m^2 \mid k \end{cases}$$

Proof. Let $k = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$ be the prime-power decomposition of k in $\mathbb{Z}[\theta]$, then by the Chinese Remainder Theorem:

$$\mathbb{Z}_k[\theta] \cong \mathbb{Z}_{p_1^{t_1}}[\theta] \times \cdots \times \mathbb{Z}_{p_s^{t_s}}[\theta]$$

Let ϕ be a ring homomorphism from $\mathbb{Z}[\theta]$ into $\mathbb{Z}_k[\theta]$. Then ϕ is completely determined by its action on 1 and θ.

Let $\phi(1) = a = (a_1, a_2, \ldots, a_s)$ and $\phi(\theta) = b = (b_1, b_2, \ldots, b_s)$.

Since $1^2 = 1$ (an idempotent element in $\mathbb{Z}[\theta]$), then a_j must also be an idempotent element in $\mathbb{Z}_{p_j^{t_j}}[\theta] \ \ \forall \ \ j.$ i.e. $a_j^2 = a_j$ in $\mathbb{Z}_{p_j^{t_j}}[\theta], \ \Rightarrow \ a_j = 0, \text{ or } \ a_j = 1.$

Note, $b = \phi(\theta) = \phi(1 \cdot \theta) = \phi(1) \cdot \phi(\theta) = ab, \text{ so } \ b_j = a_j b_j = 0 \ \ \text{whenever } a_j = 0.$

If $a_j = 1$, then $b_j = a_j b_j \neq 0$, (Recall: $P(x) = x^2 + ux + v$, and $|u^2 - 4v| = m$, a prime).

$$Now, \quad b_j^2 + ub_j + v = 0 \quad and \quad \theta^2 + u\theta + v = 0$$
$$\Rightarrow \quad b_j^2 - Tr(\theta) b_j + N(\theta) = 0$$

where $Tr =$ the trace $= (\theta + \overline{\theta})$ and $N(\theta) =$ the norm $= \theta\overline{\theta}$.

[5] Henceforth, when referring to θ, θ will always have the same definition as in *Theorem* 2.14

That implies:

$$b_j^2 - (\theta + \overline{\theta})b_j + \theta\overline{\theta} = 0$$
$$Hence; \quad b_j^2 - (\theta + \overline{\theta})b_j + \theta\overline{\theta} \equiv 0 \ \ in \ \ \mathbb{Z}_k[\theta]$$
$$Therefore; \quad p_j^{t_j} | (b_j - \theta)(b_j - \overline{\theta})$$

Now, If $p_j \neq \sqrt{m}$, then $p_j^{t_j}$ cannot divide both factors, then $p_j = \theta$ or $\overline{\theta}$ which gives us the following 3 choices:

$$a_j = 0 \quad b_j = 0$$
$$a_j = 1 \quad b_j = \theta$$
$$a_j = 1 \quad b_j = \overline{\theta}$$

If $p_j = \sqrt{m}$, then $p_j^{t_j}$ may divide both factors, and since $|p_j| = \sqrt{m}$, then t_j, the exponent of p_j, must be an even integer, giving us the following two cases:

Case 1. $t_j = 2$, then, $m \mid k$ but $m^2 \nmid k$, then working in $\mathbb{Z}_m[\theta]$:

$$b_j = x + y\theta, \ \ x, \ \ y \in \mathbb{Z}_m \quad and \quad b_j^2 + ub_j + v = 0$$

$$Note, \quad \theta^2 + u\theta + v = 0 \quad \Rightarrow \quad \theta = \frac{-u}{2} + \frac{1}{2}\sqrt{m} = \frac{1}{2}\left(\sqrt{m} - u\right)$$
$$so \quad \theta = \frac{1}{2}\left(\sqrt{m} - u\right)$$

So, to write b_j in the form:

$$b_j = x + y\theta \quad for \ \ some \quad y \in \mathbb{Z}_m$$
$$b_j = \tfrac{-u}{2} + \tfrac{y}{2}\sqrt{m}$$
$$\Rightarrow \quad b_j = \tfrac{-u}{2} + \underline{\tfrac{u}{2}y} + \tfrac{y}{2}\sqrt{m} - \underline{\tfrac{u}{2}y}$$
$$\Rightarrow \quad b_j = \tfrac{uy-u}{2} + y \cdot \left(\tfrac{1}{2}\left(\sqrt{m} - u\right)\right)$$
$$so, \quad b_j = \tfrac{u(y-u)}{2} + y\theta, \quad for \ \ some \quad y \in \mathbb{Z}_m$$
$$Thus, \quad b_j \ \ has \ \ m \ \ choices, \ \ and \ \ hence \ \ c_k = \tfrac{m+1}{3}$$

Case 2. If $t_j \geq 4$, then $m^2 \mid k$ which implies that:

$$p_j^{t_j} = p_j^4,\ p_j^6,\ p_j^8,\ \ldots \quad \xrightarrow{p_j = \sqrt{m}} \quad p_j^{t_j} = m^2,\ m^3,\ m^4,\ \cdots$$

so, $p_j^{t_j-1}$ divides one factor, and since $\mathbb{Z}_m[\theta]/\langle p_j \rangle$ has m elements and thus b_j has $2m$ choices; $\Rightarrow c_k = \frac{2m+1}{3}$.

□

Example 2.10. *Consider the ring homomorphisms* $\phi : \mathbb{Z}[\theta] \to \mathbb{Z}_3[\theta]$
where θ *is the algebraic number with the minimal polynomial* $p(x) = x^2 + x + 2$*:*
Here $k = 3$ *and* $m = |u^2 - 4v| = |1^2 - 4 \cdot 2| = |1 - 8| = |-7| = 7$*, a prime.*
Note, any element $\alpha \in \mathbb{Z}[\theta]$*,* $\alpha = x + y\theta = x(1) + y(\theta)$*,* $x, y \in \mathbb{Z}$*, and* $\theta = \left(\frac{-1+\sqrt{-7}}{2}\right)$.
So, any ring homomorphism is completely determined by its action on 1 *and* θ.
Let $\phi(1) = a$ *and* $\phi(\theta) = b$*, thus* $b^2 + b + 2a = 0$*, and in* $\mathbb{Z}_3[\theta]$.
Then $a^2 = a$ *and so,* $a = 0$*,* $a = 1$ *or* $a = 2$.
Note that if $a = 2$ *then* $b^2 + b + 2a = 0 \Rightarrow b^2 + b + 4 = b^2 + b + 1 = 0 \Rightarrow b = \rho$*, the Eisenstein integer, which wouldn't give us a ring homomorphism in* $\mathbb{Z}[\theta]$.
If $a = 0$ *then* $b + b = 0 \Rightarrow b = 0$ *or* $b = -1 = 2$ *(in* $\mathbb{Z}_3[\theta]$*).*
But $b = 2$ *wouldn't preserve the multiplication, and hence no ring homomorphism. Thus;* $a = 0 \Rightarrow b = 0$.
and if $a = 1$*, then* $b^2 + b + 2 = 0$ *whose only solutions are:* $b = \theta$ *and* $b = \overline{\theta}$.
Therefore, we have the following three ring homomorphisms:

$$\phi(x + y\theta) = 0, \qquad \phi(x + y\theta) = x + y\theta, \qquad \phi(x + y\theta) = x + y\overline{\theta}$$

Solution by using the formula in the theorem.
Here, $m = 7$*,* $k = 3$*, so* $m \nmid k$ *which is the first case of* c_k *on page 83. Thus,* $c_k = 1$*,* $\omega(3) = 1$*, and therefore:*

$$\mathcal{N}\big(\phi : \mathbb{Z}[\theta] \to \mathbb{Z}_3[\theta]\big) = 1 \cdot 3^{\omega(3)} = 1 \cdot 3^1 = 3 \quad \textit{homomorphisms.}$$

Theorem 2.15. *[5, Theorem 10]*

The number of ring homomorphisms:

$$\phi: \ \mathbb{Z}[\theta] \times \mathbb{Z}[\theta] \to \mathbb{Z}_k[\theta] \quad {}^{\{6\}} \qquad is \qquad c_k \cdot 5^{\omega(k)}$$

where $\omega(k)$ is the number of prime factors of k in $\mathbb{Z}[\theta]$, and:

$$c_k = \begin{cases} 1 & if \quad m \nmid k \\ \frac{2m+1}{5} & if \quad m \mid k, \quad but \quad m^2 \nmid k \\ \frac{4m+1}{5} & if \quad m^2 \mid k \end{cases}$$

Proof.

Let $\phi : \mathbb{Z}[\theta] \times \mathbb{Z}[\theta] \quad \to \quad \mathbb{Z}_k[\theta]$ be a ring homomorphism,

and let $k = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$ be the prime-power decomposition of k in $\mathbb{Z}[\theta]$.

Then ϕ is completely determined by its action on $(1,0)$, $(0,1)$, $(\theta,0)$ and $(0,\theta)$.

By Chinese Remainder Theorem: $\quad \mathbb{Z}_k[\theta] \ \cong \ \mathbb{Z}_{p_1^{t_1}}[\theta] \times \cdots \times \mathbb{Z}_{p_s^{t_s}}[\theta]$.

Note, $\phi\Big((1,0)\Big) = 0 \quad \text{or} \quad 1, \quad \text{and} \quad \phi\Big((0,1)\Big) = 0 \quad \text{or} \quad 1.$

Let $\phi\Big((\theta,0)\Big) = a = (a_1, a_2, \ldots, a_s)$ in $\mathbb{Z}_k[\theta]$, and

let $\phi\Big((0,\theta)\Big) = b = (b_1, b_2, \ldots, b_s)$ in $\mathbb{Z}_k[\theta]$.

So, ϕ is completely determined by the values of a and b. So, as in the previous theorem's proof, we have:

$$a_j = 0, \ \theta, \ or \ \overline{\theta} \qquad\qquad b_j = 0, \ \theta, \ or \ \overline{\theta}$$

{6} θ as in *theorem* 2.14, page 83

But $(\theta,0)\cdot(0,\theta)=0 \quad \Rightarrow \quad a_jb_j=0$. So the number of combinations is $2^2+1=5$ choices.
Now, If $p_j=\sqrt{m}$, then we have two cases to consider:

Case 1. If $t_j=2 \Rightarrow p_j^{t_j}=p_j^2=m$:

Thus, if $m \mid k$ but $m^2 \nmid k$, then (as in the proof of *theorem* (2.14)): a_j and b_j each has an $(m+1)$ choices, along with $a_jb_j=0 \Rightarrow (m+1)+(m+1)-1=2m+1$ choices, making the value of $c_k=\frac{2m+1}{5}$.

Case 2. If $t_j \geq 4, \Rightarrow m^2 \mid k$: then again, as in the proof of *theorem* (2.14), a_j has $(2m+1)$ choices, and b_j has $(2m+1)$ choices with $a_jb_j=0$ (reducing one) gives us the number of choices is:

$(2m+1)+(2m+1)-1=4m+1$ making $c_k=\frac{4m+1}{5}$.

□

Example 2.11.

Consider the ring homomorphisms $\phi:\mathbb{Z}[\theta]\times\mathbb{Z}[\theta]\to\mathbb{Z}_6[\theta]$

where θ *is the algebraic number with the minimal polynomial* $p(x)=x^2+x+2$*:*

Here, $k=3$*,* $u=1$*,* $v=2$*, so* $m=|u^2-4v|=|1^2-4(2)|=|1-8|=|-7|=7$*, a prime.*

Let $\alpha=x+y\theta$*,* $\beta=u+v\theta$*, we have:*

For any $(\alpha,\beta)\in\mathbb{Z}[\theta]\times\mathbb{Z}[\theta]$*,* $(\alpha,\beta)=\big(x(1,0)+y(\theta,0),u(0,1)+v(0,\theta)\big)$

So, any ring homomorphism, ϕ*, is completely determined by its action on* $(1,0),(\theta,0),(0,1),(0,\theta)$*.*

Let $a=\phi(1,0)$*,* $b=\phi(\theta,0)$*,* $c=(0,\theta)$*, and* $d=\phi(0,\theta)$*:*

Note that, to have a homomorphism, ϕ *must map idempotent elements into idempotent elements; thus:* $a^2=a$*,* $c^2=c$*, along with:* $ab=b$*,* $cd=d$ *and* $ac=bd=0$*.*

Idempotents in $\mathbb{Z}_6[\theta]$ *are:* $0,1,3,4$*, so* $a,c=0,1,3,4$*. Now to assure* $ac=0$*, we consider all the cases possible:*

For $a=0$*,* $ac=0$ *for* $c=0,1,3,4$*. Taking each case alone:*

$a=0$*,* $c=0$ *and* $b^2+b+2a=0\Rightarrow b^2+b=0\Rightarrow b=0,2,3,5$ *but to keep* $ab=b$ *would imply that only* $b=0$ *is allowed. And* $d^2+d+2c=d^2+d=0\Rightarrow d=0$*.*

So, we have the zero homomorphism: $(a,b,c,d)=(0,0,0,0)$*.*

For $a = 0$, $c = 1$, $b = 0$, $d^2 + d + 2c = d^2 + d + 2 = 0 \Rightarrow d = \theta, \overline{\theta}, 4\theta, 4\overline{\theta}$. *And note that the condition* $cd = d$ *is satisfied for the four values of* d, *and thus we have the four homomorphisms:* $(a, b, c, d) = (0, 0, 1, \theta),\ (0, 0, 1, \overline{\theta}),\ (0, 0, 1, 4\theta),\ (0, 0, 1, 4\overline{\theta})$.

For $a = 0$, $c = 3$, $b = 0$, $d^2 + d + 2c = d^2 + d + 6 = 0 \Rightarrow d = 0, 2, 3, 5$, *but in order to have* $cd = d$, *we must have* $d = 0, 3$ *only. Giving us the following two homomorphisms:*

$(a, b, c, d) = (0, 0, 3, 0),\ (0, 0, 3, 3)$.

For $a = 0$, $c = 4$, $b = 0$, $d^2 + d + 2c = d^2 + d + 2 = 0 \Rightarrow d = \theta, \overline{\theta}, 4\theta, 4\overline{\theta}$, *along with* $cd = d \Rightarrow d = 4\theta, 4\overline{\theta}$. *Thus, we have:* $(a, b, c, d) = (0, 0, 4, 4\theta),\ (0, 0, 4, 4\overline{\theta})$.

For $a = 1$, *with* $ac = 0 \Rightarrow c = 0$. $d^2 + d + 2c = d^2 + d = 0 \Rightarrow d = 0$ *only.*

And $b^2 + b + 2a = b^2 + b + 2 = 0 \Rightarrow b = \theta, \overline{\theta}, 4\theta, 4\overline{\theta}$ *and all the values of* b *satisfy* $ab = b$, *thus, we have the following four homomorphisms:*

$(a, b, c, d) = (1, \theta, 0, 0),\ (1, \overline{\theta}, 0, 0),\ (1, 4\theta, 0, 0),\ (1, 4\overline{\theta}, 0, 0)$.

For $a = 3$ *with* $ac = 0 \Rightarrow c = 0, 4$*:*

$a = 3$, $c = 0$*:* $d^2 + d + 2c = d^2 + d = 0 \Rightarrow d = 0$.

$b^2 + b + 2a = b^2 + b + 6 = b^2 + b = 0 \Rightarrow b = 0, 2, 3, 5$. *But* $ab = b$ *holds only for* $b = 0, 3$. *Thus, we have the following two homomorphisms:* $(a, b, c, d) = (3, 0, 0, 0),\ (3, 3, 0, 0)$.

For $a = 3$, $c = 4$, $b = 0, 3$, *and* $d^2 + d + 2c = d^2 + d + 2 = 0 \Rightarrow d = \theta, \overline{\theta}, 4\theta, 4\overline{\theta}$. *But* $cd = d \Rightarrow d = 4\theta, 4\overline{\theta}$. *Giving us:* $(a, b, c, d) = (3, 0, 4, 4\theta),\ (3, 0, 4, 4\overline{\theta}),\ (3, 3, 4, 4\theta),\ (3, 3, 4, 4\overline{\theta})$.

For $a = 4$ *with* $ac = 0 \Rightarrow c = 0, 3$*:*

For $a = 4$, $c = 0$, $b^2 + b + 2a = b^2 + b + 2 = 0 \Rightarrow b = \theta, \overline{\theta}, 4\theta, 4\overline{\theta}$ *along with* $ab = b$ *leaves us with* $b = 4\theta, 4\overline{\theta}$.

$d^2 + d + 2c = d^2 + d = 0 \Rightarrow d = 0, 2, 3, 5$, *and* $cd = d$ *holds only for* $d = 0$. *Thus, we have the two homomorphisms:* $(a, b, c, d) = (4, 4\theta, 0, 0),\ (4, 4\overline{\theta}, 0, 0)$.

For $a = 4$, $c = 3$, $b = 4\theta, 4\overline{\theta}$, $d^2 + d + 2c = d^2 + d + 6 = d^2 + d = 0 \Rightarrow d = 0, 2, 3, 5$. *And,* $cd = d$ *holds only for* $d = 0, 3$ *and therefore, we have the four homomorphisms:* $(a, b, c, d) = (4, 4\theta, 3, 0),\ (4, 4\theta, 3, 3),\ (4, 4\overline{\theta}, 3, 0),\ (4, 4\overline{\theta}, 3, 3)$.

Therefore, we have the following 25 *ring homomorphisms as illustrated on the next page:*

Let $\alpha = a + b\theta, \beta = c + d\theta$ *such that* $\Big(\alpha, \beta\Big) \in \mathbb{Z}[\theta] \times \mathbb{Z}[\theta]$

$\phi(1,0)$	$\phi(\theta,0)$	$\phi(0,1)$	$\phi(0,\theta)$	$\phi\big(\alpha,\beta\big)$
0	0	0	0	0
0	0	1	θ	$c + d\theta$
0	0	1	4θ	$c + 4d\theta$
0	0	1	$\overline{\theta}$	$c + d\overline{\theta}$
0	0	1	$4\overline{\theta}$	$c + 4d\overline{\theta}$
0	0	3	0	$3c$
0	0	3	3	$3c + 3d$
0	0	4	4θ	$4c + 4d\theta$
0	0	4	$4\overline{\theta}$	$4c + 4d\overline{\theta}$
1	θ	0	0	$a + b\theta$
1	$\overline{\theta}$	0	0	$a + b\overline{\theta}$
1	4θ	0	0	$a + 4b\theta$
1	$4\overline{\theta}$	0	0	$a + 4b\overline{\theta}$
3	0	0	0	$3a$
3	3	0	0	$3a + 3b$
3	0	4	4θ	$(3a + 4c)4d\theta$
3	0	4	$4\overline{\theta}$	$(3a + 4c) + 4d\overline{\theta}$
3	3	4	4θ	$(3a + 3b + 4c)4d\theta$
3	3	4	$4\overline{\theta}$	$(3a + 3b + 4c) + 4d\overline{\theta}$
4	4θ	0	0	$4a + 4b\theta$
4	$4\overline{\theta}$	0	0	$4a + 4b\overline{\theta}$
4	4θ	3	0	$(4a + 3c) + 4b\theta$
4	4θ	3	3	$(4a + 3c + 3d) + 4b\theta$
4	$4\overline{\theta}$	3	0	$(4a + 3c) + 4b\overline{\theta}$
4	$4\overline{\theta}$	3	3	$(4a + 3c + 3d) + 4b\overline{\theta}$

Solution by using the formula in the theorem.

Considering the formula in the theorem:

We have $k = 6$, $m = 7$ *so,* $m \nmid k$ *and thus we have the first case of* c_k,

so $c_k = 1$. *And* $\omega(k) = \omega(6) = 2$, *thus the number of these ring homomorphisms is:*

$$\mathcal{N} = c_k \cdot 5^{\omega(k)} = 1 \cdot 5^2 = 25 \ \textit{homomorphisms}$$

Theorem * 2.1. *The number of ring homomorphisms:*

$$\phi:\ \overbrace{\mathbb{Z}[\theta]\times\mathbb{Z}[\theta]\times\cdots\times\mathbb{Z}[\theta]}^{n-times}\ \ \rightarrow\ \ \mathbb{Z}_k[\theta]\ \ {}^{\{7\}}\qquad is$$

$$\begin{array}{llll}
1+P(n,1)\Big(2+N_1+N_2+N_3+\cdots+N_r\Big) & + & P(n,2)\sum_{i=2}^{r}\Big(N_1N_i\Lambda_{(I_1,I_i/k)}\Big) & \\
+\ P(n,2)\sum\limits_{i=3}^{r}\Big(N_2N_i\Lambda_{(I_2,I_i/k)}\Big)\ + & \cdots & +\ P(n,2)N_{r-1}N_r\Lambda_{(I_{r-1},I_r/k)} & \\
+\ P(n,3)\Big(N_1N_2N_3\prod\limits_{\substack{i,j=1,2,3\\ i\neq j}}\Lambda_{(I_i,I_j/k)}\Big)\ + & \cdots & +\ P(n,3)\Big(N_1N_2N_r\prod\limits_{\substack{i,j=1,2,r\\ i\neq j}}\Lambda_{(I_i,I_j/k)}\Big) & \\
+\ P(n,3)\Big(N_2N_3N_4\prod\limits_{\substack{i,j=2,3,4\\ i\neq j}}\Lambda_{(I_i,I_j/k)}\Big)\ + & \cdots & +\ P(n,3)\Big(N_2N_3N_r\prod\limits_{\substack{i,j=2,3,r\\ i\neq j}}\Lambda_{(I_i,I_j/k)}\Big) & \\
\cdots & \cdots & \cdots & \\
\vdots & \vdots & \vdots & \\
+\ P(n,4)\Big(N_1N_2N_3N_4\prod\limits_{\substack{i,j=1\\ i\neq j}}^{4}\Lambda_{(I_i,I_j/k)}\Big)\ + & \cdots & +\ P(n,4)\Big(N_1N_2N_3N_r\prod\limits_{\substack{i,j=1\\ i,j\neq 4\\ i\neq j}}\Lambda_{(I_i,I_j/k)}\Big) & \\
\vdots & \vdots & \vdots & \\
+\ P(n,r-1)\Big(N_1N_2\cdots N_{r-1}\prod\limits_{\substack{i,j=1\\ i\neq j}}\Lambda_{(I_i,I_j/k)}\Big)\ + & \cdots & +\ P(n,r)\Big(N_1N_2\cdots N_r\prod\limits_{\substack{i,j=1\\ i\neq j}}\Lambda_{(I_i,I_j/k)}\Big). &
\end{array}\tag{2.11}$$

Where I_i's are the "$\underline{r}$" idempotents of $\mathbb{Z}_k$,

N_i is the number of solutions, s_i, of $(x^2+ux+v\cdot I_i=0)$ such that $I_is_i=s_i$, where $P(x)=x^2+ux+v$ is the minimal polynomial of θ,

And Λ is a characteristic function, defined by:

$$\Lambda_{(a,b/k)}=\begin{cases}1 & if\quad ab=0 \mod k\\ 0 & if\quad ab\neq 0 \mod k\end{cases}\qquad and\quad P(n,s)=\frac{n!}{(n-s)!}\tag{2.12}$$

{7} θ as in *theorem* 2.14, page 83

Proof.

$$\text{Let} \qquad \phi : \overbrace{\mathbb{Z}[\theta] \times \mathbb{Z}[\theta] \times \cdots \times \mathbb{Z}[\theta]}^{n-times} \quad \rightarrow \quad \mathbb{Z}_k[\theta]$$

be a ring homomorphism;

Note that, for all $k \in \mathbb{N}$, $\mathbb{Z}_k$ has $2^{\omega(k)}$ idempotents, where $\omega(k)$ is the number of distinct prime divisors of k. So, the number of idempotents is always an even number, and $0, 1$ are always idempotents of $\mathbb{Z}_k$.

Let a_i be the n-tuple with 1 in the i^{th} coordinate and zeros elsewhere, and b_i be the n-tuple with θ in the i^{th} coordinate and zeros elsewhere. Let $e_i = \phi(a_i)$ and $f_i = \phi(b)$, then ϕ is completely determined by the values of e_i, and f_i.

Let S_I be the set of idempotents of $\mathbb{Z}_k$, then S_I has $2^{\omega(k)}$ elements, an even number.

0 is an idempotent, which would give us the zero homomorphism, the "1" in equation (2.11).

1 is also an idempotent, so one of the e_i's is 1 and the rest are zeros. But in any case; for $e_i = 1$, we have $f_i^2 + uf_i + ve_i = 0$ has two solutions; namely, θ and $\overline{\theta}$ giving us $P(n, 1)$ homomorphisms.

Now, let I_1 be another idempotent (different from 0 and 1). Then, let $e_i = I_1$ and the rest of the e_i's are zeros. Let N_1 be the number of solutions of $x^2 + ux + vI_1 = 0$ in $\mathbb{Z}_k[\theta]$ which would give us N_1 homomorphisms. But we also have the same number of homomorphisms for the $P(n, 1)$ cases. Therefore, we have $P(n, 1) \cdot N_1$ homomorphisms.

Similarly for any other idempotent I_i, we have $P(n, 1) \cdot N_i$ homomorphisms.

Now, we take the product of any two idempotents such that their product is zero, so that $e_i \cdot e_j = 0$, and here comes the role of the characteristic function Λ, and the number of arrangements of any two idempotents among the n possible values of the e_i's is $P(n, 2) = \left(\frac{n!}{(n-2)!}\right)$.

Similarly, we take the combination of any three idempotents, and then any four, etc.

Proceeding inductively, yields to the formula above (2.11). □

As a special case of *Theorem** (2.1). We have the following theorem:

Theorem * 2.2. *For any prime $p \in \mathbb{N}$, and any $k \in \mathbb{N}$ The number of ring homomorphisms:*

$$\phi : \overbrace{\mathbb{Z}[\theta] \times \mathbb{Z}[\theta] \times \cdots \times \mathbb{Z}[\theta]}^{n-times} \to \mathbb{Z}_{p^k}[\theta] \qquad is \qquad \big(1 + 2n\big)$$

Proof. The proof follows directly from the fact that for any prime $p \in \mathbb{N}$, the only idempotents of $\mathbb{Z}_{p^k}$ are 0 and 1.

0 gives us the zero homomorphism. $I_1 = 1$ and $P(n,1) = \left(\frac{n!}{(n-1)!}\right) = n$, $N_1 = 2$, since for any $e_i = 1$, we have two solutions for $f_i^2 + uf_i + ve_i = 0$, namely, θ and $\overline{\theta}$, and therefore, the number of homomorphisms is $1 + P(n,1) \cdot N_1 = 1 + 2n$. □

Example 2.12.

Consider $\phi : \mathbb{Z}[\theta] \times \mathbb{Z}[\theta] \times \mathbb{Z}[\theta] \to \mathbb{Z}_3[\theta]$,

where θ has the minimal polynomial: $P(x) = x^2 + x + 2$.

Let $e_1 = \phi(1,0,0)$, $e_2 = \phi(0,1,0)$, $e_3 = \phi(0,0,1)$, *and*

$f_1 = \phi(\theta,0,0)$, $f_2 = \phi(0,\theta,0)$, $f_3 = \phi(0,0,\theta)$, *Then, we have:*

$e_i e_j = 0$ *and* $f_i f_j = 0$ *for* $i \neq j$. $e_i^2 = e_i$, $e_i f_i = f_i$, *and* $f_i^2 + f_i + 2e_i = 0$ *for* $i = 1,2,3$.

In order to meet these conditions; we have: $e_i \in \{0,1\}$ *as idempotent elements in* $\mathbb{Z}_3[\theta]$.

$e_i = 0 \Rightarrow f_i = 0$ *and* $e_i = 1 \Rightarrow f_i \in \{\theta, \overline{\theta}\}$.

Working exactly as in example (2.11);

we get the following 7 *homomorphisms denoted by:*

$$\begin{array}{ccc} (x_1,x_2,x_3,x_4,x_5,x_6) & = & (e_1,e_2,e_3,f_1,f_2,f_3) = \\ (0,0,0,0,0,0) & , & (1,0,0,\theta,0,0) \\ (1,0,0,\overline{\theta},0,0) & , & (0,1,0,0,\theta,0) \\ (0,1,0,0,\overline{\theta},0) & , & (0,0,1,0,0,\theta) \\ (0,0,0,0,0,\overline{\theta}) & & \end{array}$$

Solution by using the formula in the theorem.

$n = 3$, *therefore;* $\mathcal{N} = \Big(1 + 2(3)\Big) = 7$ *homomorphisms.*

Example 2.13. *Consider* $\phi : \mathbb{Z}[\theta] \times \mathbb{Z}[\theta] \times \mathbb{Z}[\theta] \to \mathbb{Z}_6[\theta]$,

where θ *has the minimal polynomial* $(x^2 + x + 1)$.

Let $e_1 = \phi(1, 0, 0)$, $e_2 = \phi(0, 1, 0)$, $e_3 = \phi(0, 0, 1)$,

The idempotents of $\mathbb{Z}_6[\theta]$ *are* $\{0, 1, 3, 4\}$. $f_1 = \phi(\theta, 0, 0)$, $f_2 = \phi(0, \theta, 0)$, $f_3 = \phi(0, 0, \theta)$.

For $e_1 = e_2 = e_3 = 0 \Rightarrow f_i = 0$ *for* $i = 1, 2, 3$ *giving us the zero homomorphism:*

$(e_1, e_2, e_3, f_1, f_2, f_3) = (0, 0, 0, 0, 0, 0)$.

For $e_1 = e_2 = 0$, $e_3 = 1$, *then* $f_1 = f_2 = 0$ *and* $f_3^2 + f_3 + 1 = 0$ *has two solutions:* $\theta, \overline{\theta}$.

Giving us: $(e_1, e_2, e_3, f_1, f_2, f_3) = (0, 0, 1, 0, 0, \theta)$, $(0, 0, 1, 0, 0, \overline{\theta})$.

Similarly, for $e_1 = e_3 = 0$, $e_2 = 1$, $\Rightarrow f_i = 0$ *for* $i = 1, 3$ *and* $f_2 = \theta, \overline{\theta}$, *giving us:*

$(e_1, e_2, e_3, f_1, f_2, f_3) = (0, 1, 0, 0, \theta, 0)$, $(0, 1, 0, 0, \overline{\theta}, 0)$.

And, for $e_2 = e_3 = 0$, $e_1 = 1$, $\Rightarrow f_i = 0$ *for* $i = 2, 3$ *and* $f_1 = \theta, \overline{\theta}$, *giving us:*

$(e_1, e_2, e_3, f_1, f_2, f_3) = (1, 0, 0, \theta, 0, 0)$, $(1, 0, 0, \overline{\theta}, 0, 0)$.

Now, for $e_1 = e_2 = 0$, $e_3 = 3 \Rightarrow f_i = 0$ *for* $i = 1, 2$,

and $f_3^2 + f_3 + 3 = 0$ *has two solutions,* 3θ, $3\overline{\theta}$. *giving us:*

$(e_1, e_2, e_3, f_1, f_2, f_3) = (0, 0, 3, 0, 0, 3\theta)$, $(0, 0, 3, 0, 0, 3\overline{\theta})$.

For $e_1 = e_3 = 0$, $e_2 = 3$, $\Rightarrow f_i = 0$ *for* $i = 1, 3$ *and* $f_2 = 3\theta, 3\overline{\theta}$, *giving us:*

$(e_1, e_2, e_3, f_1, f_2, f_3) = (0, 3, 0, 0, 3\theta, 0)$, $(0, 3, 0, 0, 3\overline{\theta}, 0)$.

For $e_2 = e_3 = 0$, $e_1 = 3$, $\Rightarrow f_i = 0$ *for* $i = 2, 3$ *and* $f_1 = 3\theta, 3\overline{\theta}$, *giving us:*

$(e_1, e_2, e_3, f_1, f_2, f_3) = (3, 0, 0, 3\theta, 0, 0)$, $(3, 0, 0, 3\overline{\theta}, 0, 0)$.

For $e_1 = e_2 = 0$, $e_3 = 4 \Rightarrow f_i = 0$ *for* $i = 1, 2$,

and $f_3^2 + f_3 + 4 = 0$ *has three solutions;* 4, 4θ, $4\overline{\theta}$, *giving us:*

$(e_1, e_2, e_3, f_1, f_2, f_3) = (0, 0, 4, 0, 0, 4)$, $(0, 0, 4, 0, 0, 4\theta)$, $(0, 0, 4, 0, 0, 4\overline{\theta})$.

$e_1 = e_3 = 0$, $e_2 = 4$, $\Rightarrow f_i = 0$ *for* $i = 1, 3$ *and* $f_2 = 4, 4\theta, 4\overline{\theta}$, *giving us:*

$(e_1, e_2, e_3, f_1, f_2, f_3) = (0, 4, 0, 0, 4, 0)$, $(0, 4, 0, 0, 4\theta, 0)$, $(0, 4, 0, 0, 4\overline{\theta}, 0)$.

For $e_2 = e_3 = 0$, $e_1 = 4$, $\Rightarrow f_i = 0$ *for* $i = 2, 3$ *and* $f_1 = 4, 4\theta, 4\overline{\theta}$, *giving us:*

$(e_1, e_2, e_3, f_1, f_2, f_3) = (4, 0, 0, 4, 0, 0)$, $(4, 0, 0, 4\theta, 0, 0)$, $(4, 0, 0, 4\overline{\theta}, 0, 0)$.

Now, for $e_1 = 0$, $e_2 = 3$, $e_3 = 4 \Rightarrow f_1 = 0$, $f_2 = \theta, \overline{\theta}$, $f_3 = 4, 4\theta, \overline{\theta}$. *giving us*

$(e_1, e_2, e_3, f_1, f_2, f_3) = (0, 3, 4, 0, 3\theta, 4)$, $(0, 3, 4, 0, 3\theta, 4\theta)$, $(0, 3, 4, 0, 3\theta, 4\overline{\theta})$,

$(0, 3, 4, 0, 3\overline{\theta}, 4)$, $(0, 3, 4, 0, 3\overline{\theta}, 4\theta)$, $(0, 3, 4, 0, 3\overline{\theta}, 4\overline{\theta})$,

Similarly, for $e_1 = 0$, $e_2 = 4$, $e_3 = 3$, *gives us:*

$$(e_1, e_2, e_3, f_1, f_2, f_3) = (0, 4, 3, 0, 4, 3\theta),\ \ (0, 4, 3, 0, 4\theta, 3\theta),\ \ (0, 4, 3, 0, 4\overline{\theta}, 3\theta),$$
$$(0, 4, 3, 0, 4, 3\overline{\theta}),\ \ (0, 4, 3, 0, 4\theta, 3\overline{\theta}),\ \ (0, 4, 3, 0, 4\overline{\theta}, 3\overline{\theta}),$$

And for $e_1 = 3$, $e_2 = 0$, $e_3 = 4$, *and for* $e_1 = 4$, $e_2 = 0$, $e_3 = 3$ *gives us, respectively,:*

$$(e_1, e_2, e_3, f_1, f_2, f_3) = (3, 0, 4, 3\theta, 0, 4),\ \ (3, 0, 4, 3\theta, 0, 4\theta),\ \ (3, 0, 4, 3\theta, 0, 4\overline{\theta}),$$
$$(3, 0, 4, 3\overline{\theta}, 0, 4),\ \ (3, 0, 4, 3\overline{\theta}, 0, 4\theta),\ \ (3, 0, 4, 3\overline{\theta}, 0, 4\overline{\theta}),$$
$$(e_1, e_2, e_3, f_1, f_2, f_3) = (4, 0, 3, 4, 0, 3\theta),\ \ (4, 0, 3, 4\theta, 0, 3\theta),\ \ (4, 0, 3, 4\overline{\theta}, 0, 3\theta),$$
$$(4, 0, 3, 4, 0, 3\overline{\theta}),\ \ (3, 0, 4, 4\theta, 0, 3\overline{\theta}),\ \ (4, 0, 3, 4\overline{\theta}, 3\overline{\theta}),$$

for $e_1 = 3$, $e_2 = 4$, $e_3 = 0$, *and for* $e_1 = 4$, $e_2 = 3$, $e_3 = 0$ *gives us, respectively,:*

$$(e_1, e_2, e_3, f_1, f_2, f_3) = (3, 4, 0, 3\theta, 4, 0),\ \ (3, 4, 0, 3\theta, 4\theta, 0),\ \ (3, 4, 0, 3\theta, 4\overline{\theta}, 0),$$
$$(3, 4, 0, 3\overline{\theta}, 4, 0),\ \ (3, 4, 0, 3\overline{\theta}, 4\theta, 0),\ \ (3, 4, 0, 3\overline{\theta}, 4\overline{\theta}, 0),$$
$$(e_1, e_2, e_3, f_1, f_2, f_3) = (4, 3, 0, 4, 3\theta, 0),\ \ (4, 3, 0, 4\theta, 3\theta, 0),\ \ (4, 3, 0, 4\overline{\theta}, 3\theta, 0),$$
$$(4, 3, 0, 4, 3\overline{\theta}, 0),\ \ (4, 3, 0, 4\theta, 3\overline{\theta}, 0),\ \ (4, 3, 0, 4\overline{\theta}, 3\overline{\theta}, 0),$$

Which are 58 *homomorphisms in total.*

Solution by using the formula in the theorem. *We have,* $I_1 = 3$, $I_2 = 4$*:*
$x^2 + x + I_1 = 0$ *has two solutions and* $x^2 + x + I_2 = 0$ *has three solutions.*
Therefore, $N_1 = 2$ *and* $N_2 = 3$ *and* $\Lambda_{(I_1, I_2/k)} = \Lambda_{(3,4/6)} = 1$ *since* $3 \cdot 4 = 0$ *in* $\mathbb{Z}_6$.
Therefore, the total number of ring homomorphisms is:

$$\mathcal{N} = 1 + P(n, 1)\Big(2 + N_1 + N_2\Big) + P(n, 2)\Big(N_1 \cdot N_2 \cdot \Lambda_{(I_1, I_2/k)}\Big)$$

$$= 1 + \Big(\tfrac{3!}{(3-1)!}\Big)\Big(2 + 2 + 3\Big) + \Big(\tfrac{3!}{(3-2)!}\Big)\Big(2 \cdot 3 \cdot 1\Big)$$

$$= 1 + 3\big(7\big) + \big(\tfrac{6}{1}\big)\big(6\big) = 1 + 21 + 36 = 58 \qquad \textit{homomorphisms}$$

Example 2.14.

Consider $\phi : \mathbb{Z}[\theta]\times\mathbb{Z}[\theta]\times\mathbb{Z}[\theta]\times\mathbb{Z}[\theta] \to \mathbb{Z}_{30}[\theta]$, *with minimal polynomial* $P(x) = x^2+x+1$.

Let $e_1 = \phi(1,0,0,0)$, $e_2 = \phi(0,1,0,0)$, $e_3 = \phi(0,0,1,0)$, $e_4 = \phi(0,0,0,1)$, *and*

$f_1 = \phi(\theta,0,0,0)$, $f_2 = \phi(0,\theta,0,0)$, $f_3 = \phi(0,0,\theta,0)$, $f_4 = \phi(0,0,0,\theta)$.

The idempotents of $\mathbb{Z}_{30}$ *are* $\{0,1,6,10,15,16,21,25\}$, *hence,* $e_i \in \{0,1,6,10,15,16,21,25\}$.

For $e_1 = 0$ *gives us the zero homomorphism:*

$(e_1,e_2,e_3,e_4,f_1,f_2,f_3,f_4) = (0,0,0,0,0,0,0,0)$.

If one of the e_i*'s is* 1, *then* $f_i = \theta$ *or* $\overline{\theta}$,

and so we have $\underline{8}$ [{8}] *homomorphisms:*

$$(0,0,0,1,0,0,0,\theta) \quad (0,0,0,1,0,0,0,\overline{\theta}) \quad (0,0,1,0,0,0,\theta,0)$$
$$(0,0,1,0,0,0,\overline{\theta},0) \quad (0,1,0,0,0,\theta,0,0) \quad (0,1,0,0,0,\overline{\theta},0,0)$$
$$(1,0,0,0,\theta,0,0,0) \quad (1,0,0,0,\overline{\theta},0,0,0)$$

If one of the e_i*'s is* 6, *then* $f_i = 6\theta$ *or* $6\overline{\theta}$, *which gives* $\underline{8}$ *homomorphisms:*

$$(0,0,0,6,0,0,0,6\theta) \quad (0,0,0,6,0,0,0,6\overline{\theta}) \quad (0,0,6,0,0,0,6\theta,0)$$
$$(0,0,6,0,0,0,6\overline{\theta},0) \quad (0,6,0,0,0,6\theta,0,0) \quad (0,6,0,0,0,6\overline{\theta},0,0)$$
$$(6,0,0,0,6\theta,0,0,0) \quad (6,0,0,0,6\overline{\theta},0,0,0)$$

If one of the e_i*'s is* 10, *then* $f_i = 10, 10\theta$ *or* $10\overline{\theta}$, *giving us* $\underline{\underline{12}}$ *homomorphisms:*

$$(0,0,0,10,0,0,0,10) \quad (0,0,0,10,0,0,0,10\theta) \quad (0,0,0,10,0,0,0,10\overline{\theta})$$
$$(0,0,10,0,0,0,10,0) \quad (0,0,10,0,0,0,10\theta,0) \quad (0,0,10,0,0,0,10\overline{\theta},0)$$
$$(0,10,0,0,0,10,0,0) \quad (0,10,0,0,0,10\theta,0,0) \quad (0,10,0,0,0,10\overline{\theta},0,0)$$
$$(10,0,0,0,10,0,0,0) \quad (10,0,0,0,0,10\theta,0,0) \quad (10,0,0,0,10\overline{\theta},0,0,0)$$

[{8}] Henceforth in this example, $(x,x,x,x,x,x,x,x) = (e_1,e_2,e_3,e_4,f_1,f_2,f_3,f_4)$

If one of the e_i's is 15*, then* $f_i = 15\theta$*, or* $15\overline{\theta}$*, giving us* $\underline{\underline{8}}$ *homomorphisms:*

$$(0,0,0,15,0,0,0,15\theta) \quad (0,0,0,15,0,0,0,15\overline{\theta}) \quad (0,0,15,0,0,0,15\theta,0)$$
$$(0,0,15,0,0,0,15\overline{\theta},0) \quad (0,15,0,0,0,15\theta,0,0) \quad (0,15,0,0,0,15\overline{\theta},0,0)$$
$$(15,0,0,0,15\theta,0,0,0) \quad (15,0,0,0,15\overline{\theta},0,0,0)$$

If one of the e_i's is 16*, then* $f_i = 16, 16\theta, 16\overline{\theta}$*, giving us* 12 *homomorphisms:*

$$(0,0,0,16,0,0,0,16) \quad (0,0,0,16,0,0,0,16\theta) \quad (0,0,0,16,0,0,0,16\overline{\theta})$$
$$(0,0,16,0,0,0,16,0) \quad (0,0,16,0,0,0,16\theta,0) \quad (0,0,16,0,0,0,16\overline{\theta},0)$$
$$(0,16,0,0,0,16,0,0) \quad (0,16,0,0,0,16\theta,0,0) \quad (0,16,0,0,0,16\overline{\theta},0,0)$$
$$(16,0,0,0,16,0,0,0) \quad (16,0,0,0,0,16\theta,0,0) \quad (16,0,0,0,16\overline{\theta},0,0,0)$$

If one of the e_i's is 21*, then* $f_i = 21\theta$*, or* $21\overline{\theta}$*, giving us* $\underline{\underline{8}}$ *homomorphisms:*

$$(0,0,0,21,0,0,0,21\theta) \quad (0,0,0,21,0,0,0,21\overline{\theta}) \quad (0,0,21,0,0,0,21\theta,0)$$
$$(0,0,21,0,0,0,21\overline{\theta},0) \quad (0,21,0,0,0,21\theta,0,0) \quad (0,21,0,0,0,21\overline{\theta},0,0)$$
$$(21,0,0,0,21\theta,0,0,0) \quad (21,0,0,0,21\overline{\theta},0,0,0)$$

If one of the e_i's is 25*, then* $f_i = 25\theta$ *or* $25\overline{\theta}$*, giving us* $\underline{\underline{8}}$ *homomorphisms:*

$$(0,0,0,25,0,0,0,25\theta) \quad (0,0,0,25,0,0,0,25\overline{\theta}) \quad (0,0,25,0,0,0,25\theta,0)$$
$$(0,0,25,0,0,0,25\overline{\theta},0) \quad (0,25,0,0,0,25\theta,0,0) \quad (0,25,0,0,0,25\overline{\theta},0,0)$$
$$(25,0,0,0,25\theta,0,0,0) \quad (25,0,0,0,25\overline{\theta},0,0,0)$$

For to the e_i's to equal two of the idempotents, they have to satisfy that $e_i e_j = 0$ in $\mathbb{Z}_{30}[\theta]$, and this is satisfied only for: $\{(6,10),(6,15),(6,25),(10,15),(10,21),(15,16)\}$.

For any two of the e_i's to equal the pair $(6, 10)$, we have the following $\underline{\underline{72}}$ homomorphisms:

$(0,0,6,10,0,0,6\theta,10)$ $(0,0,6,10,0,0,6\theta,10\theta)$ $(0,0,6,10,0,0,6\theta,10\overline{\theta})$

$(0,0,6,10,0,0,6\overline{\theta},10)$ $(0,0,6,10,0,0,6\overline{\theta},10\theta)$ $(0,0,6,10,0,0,6\overline{\theta},10\overline{\theta})$

$(0,0,10,6,0,0,10,6\theta)$ $(0,0,10,6,0,0,10\theta,6\theta)$ $(0,0,10,6,0,0,10\overline{\theta},6\theta)$

$(0,0,10,6,0,0,10,6\overline{\theta})$ $(0,0,10,6,0,0,10\theta,6\overline{\theta})$ $(0,0,10,6,0,0,10\overline{\theta},6\overline{\theta})$

$(0,6,0,10,0,6\theta,0,10)$ $(0,6,0,10,0,6\theta,0,10\theta)$ $(0,6,0,10,0,6\theta,0,10\overline{\theta})$

$(0,6,0,10,0,6\overline{\theta},0,10)$ $(0,6,0,10,0,6\overline{\theta},0,10\theta)$ $(0,6,0,10,0,0,6\overline{\theta},10\overline{\theta})$

$(0,10,0,6,0,10,0,6\theta)$ $(0,10,0,6,0,10\theta,0,6\theta)$ $(0,10,0,6,0,10\overline{\theta},0,6\theta)$

$(0,10,0,6,0,10,0,6\overline{\theta})$ $(0,10,0,6,0,10\theta,0,6\overline{\theta})$ $(0,10,0,6,0,10\overline{\theta},0,6\overline{\theta})$

$(0,6,10,0,0,6\theta,10,0)$ $(0,6,10,0,0,6\theta,10\theta,0)$ $(0,6,10,0,0,6\theta,10\theta,0)$

$(0,6,10,0,0,6\overline{\theta},10,0)$ $(0,6,10,0,0,6\overline{\theta},10\theta,0)$ $(0,6,10,0,0,6\overline{\theta},10\overline{\theta},0)$

$(0,10,6,0,0,10,6\theta,0)$ $(0,10,6,0,0,10\theta,6\theta,0)$ $(0,10,6,0,0,10\overline{\theta},6\theta,0)$

$(0,10,6,0,0,10,6\overline{\theta},0)$ $(0,10,6,0,0,10\theta,6\overline{\theta},0)$ $(0,10,6,0,0,10\overline{\theta},6\overline{\theta},0)$

$(6,0,0,10,6\theta,0,0,10)$ $(6,0,0,10,6\theta,0,0,10\theta)$ $(6,0,0,10,6\theta,0,0,10\theta)$

$(6,0,0,10,6\overline{\theta},0,0,10)$ $(6,0,0,10,6\overline{\theta},0,0,10\theta)$ $(6,0,0,10,6\overline{\theta},0,0,10\overline{\theta})$

$(10,0,0,6,10,0,0,6\theta)$ $(10,0,0,6,10\theta,0,0,6\theta)$ $(10,0,0,6,10\overline{\theta},0,0,6\theta)$

$(10,0,0,6,10,0,0,6\overline{\theta})$ $(10,0,0,6,10\theta,0,0,6\overline{\theta})$ $(10,0,0,6,10\overline{\theta},0,0,6\overline{\theta})$

$(6,0,10,0,6\theta,0,10,0)$ $(6,0,10,0,6\theta,0,10\theta,0)$ $(6,0,10,0,6\theta,0,10\theta,0)$

$(6,0,10,0,6\overline{\theta},0,10,0)$ $(6,0,10,0,6\overline{\theta},0,10\theta,0)$ $(6,0,10,0,6\overline{\theta},0,10\overline{\theta},0)$

$(10,0,6,0,10,0,6\theta,0)$ $(10,0,6,0,10\theta,0,6\theta,0)$ $(10,0,6,0,10\overline{\theta},0,6\theta,0)$

$(10,0,6,0,10,0,6\overline{\theta},0)$ $(10,0,6,0,10\theta,0,6\overline{\theta},0)$ $(10,0,6,0,10\overline{\theta},0,6\overline{\theta},0)$

$(6,10,0,0,6\theta,10,0,0)$ $(6,10,0,0,6\theta,10\theta,0,0)$ $(6,10,0,0,6\theta,10\theta,0,0)$

$(6,10,0,0,6\overline{\theta},10,0,0)$ $(6,10,0,0,6\overline{\theta},10\theta,0,0)$ $(6,10,0,0,6\overline{\theta},10\overline{\theta},0,0)$

$(10,6,0,0,10,6\theta,0,0)$ $(10,6,0,0,10\theta,6\theta,0,0)$ $(10,6,0,0,10\overline{\theta},6\theta,0,0)$

$(10,6,0,0,10,6\overline{\theta},0,0)$ $(10,6,0,0,10\theta,6\overline{\theta},0,0)$ $(10,6,0,0,10\overline{\theta},6\overline{\theta},0,0)$

For any two of the e_i's to equal the pair $(6, 15)$,

we have the following $\underline{\underline{48}}$ *homomorphisms:*

$$
\begin{array}{lll}
(0,0,6,15,0,0,6\theta,15\theta) & (0,0,6,15,0,0,6\theta,15\overline{\theta}) & (0,0,6,15,0,0,6\overline{\theta},15\theta) \\
(0,0,6,15,0,0,6\overline{\theta},15\overline{\theta}) & (0,6,0,15,0,6\theta,0,15\theta) & (0,6,0,15,0,6\theta,0,15\overline{\theta}) \\
(0,6,0,15,0,6\overline{\theta},0,15\theta) & (0,6,0,15,0,6\overline{\theta},0,15\overline{\theta}) & (0,6,15,0,0,6\theta,15\theta,0) \\
(0,6,15,0,0,6\theta,15\overline{\theta},0) & (0,6,15,0,0,6\overline{\theta},15\theta,0) & (0,6,15,0,0,6\overline{\theta},15\overline{\theta},0) \\
(6,0,0,15,6\theta,0,0,15\theta) & (6,0,0,15,6\theta,0,0,15\overline{\theta}) & (6,0,0,15,6\overline{\theta},0,0,15\theta) \\
(6,0,0,15,6\overline{\theta},0,0,15\overline{\theta}) & (6,0,15,0,6\theta,0,15\theta,0) & (6,0,15,0,6\theta,0,15\overline{\theta},0) \\
(6,0,15,0,6\overline{\theta},0,15\theta,0) & (6,0,15,0,6\overline{\theta},0,15\overline{\theta},0) & (6,15,0,0,6\theta,15\theta,0,0) \\
(6,15,0,0,6\theta,15\overline{\theta},0,0) & (6,15,0,0,6\overline{\theta},15\theta,0,0) & (6,15,0,0,6\overline{\theta},15\overline{\theta},0,0) \\
(0,0,15,6,0,0,15\theta,6\theta) & (0,0,15,6,0,0,15\theta,6\overline{\theta}) & (0,0,15,6,0,0,15\overline{\theta},6\theta) \\
(0,0,15,6,0,0,15\overline{\theta},6\overline{\theta}) & (0,15,0,6,0,15\theta,0,6\theta) & (0,15,0,6,0,15\theta,0,6\overline{\theta}) \\
(0,15,0,6,0,15\overline{\theta},0,6\theta) & (0,15,0,6,0,15\overline{\theta},0,6\overline{\theta}) & (0,15,6,0,0,15\theta,6\theta,0) \\
(0,15,6,0,0,15\theta,6\overline{\theta},0) & (0,15,6,0,0,15\overline{\theta},6\theta,0) & (0,15,6,0,0,15\overline{\theta},6\overline{\theta},0) \\
(15,0,0,6,15\theta,0,0,6\theta) & (15,0,0,6,15\theta,0,0,6\overline{\theta}) & (15,0,0,6,15\overline{\theta},0,0,6\theta) \\
(15,0,0,6,15\overline{\theta},0,0,6\overline{\theta}) & (15,0,6,0,15\theta,0,6\theta,0) & (15,0,6,0,15\theta,0,6\overline{\theta},0) \\
(15,0,6,0,15\overline{\theta},0,6\theta,0) & (15,0,6,0,15\overline{\theta},0,6\overline{\theta},0) & (15,6,0,0,15\theta,6\theta,0,0) \\
(15,6,0,0,15\theta,6\overline{\theta},0,0) & (15,6,0,0,15\overline{\theta},6\theta,0,0) & (15,6,0,0,15\overline{\theta},6\overline{\theta},0,0)
\end{array}
$$

For any two of the e_i's to equal the pair $(6, 25)$,

we have the following $\underline{\underline{48}}$ homomorphisms:

$$
\begin{array}{lll}
(0,0,6,25,0,0,6\theta,25\theta) & (0,0,6,25,0,0,6\theta,25\overline{\theta}) & (0,0,6,25,0,0,6\overline{\theta},25\theta) \\
(0,0,6,25,0,0,6\overline{\theta},25\overline{\theta}) & (0,6,0,25,0,6\theta,0,25\theta) & (0,6,0,25,0,6\theta,0,25\overline{\theta}) \\
(0,6,0,25,0,6\overline{\theta},0,25\theta) & (0,6,0,25,0,6\overline{\theta},0,25\overline{\theta}) & (0,6,25,0,0,6\theta,25\theta,0) \\
(0,6,25,0,0,6\theta,25\overline{\theta},0) & (0,6,25,0,0,6\overline{\theta},25\theta,0) & (0,6,25,0,0,6\overline{\theta},25\overline{\theta},0) \\
(6,0,0,25,6\theta,0,0,25\theta) & (6,0,0,25,6\theta,0,0,25\overline{\theta}) & (6,0,0,25,6\overline{\theta},0,0,25\theta) \\
(6,0,0,25,6\overline{\theta},0,0,25\overline{\theta}) & (6,0,25,0,6\theta,0,25\theta,0) & (6,0,25,0,6\theta,0,25\overline{\theta},0) \\
(6,0,25,0,6\overline{\theta},0,25\theta,0) & (6,0,25,0,6\overline{\theta},0,25\overline{\theta},0) & (6,25,0,0,6\theta,25\theta,0,0) \\
(6,25,0,0,6\theta,25\overline{\theta},0,0) & (6,25,0,0,6\overline{\theta},25\theta,0,0) & (6,25,0,0,6\overline{\theta},25\overline{\theta},0,0) \\
(0,0,25,6,0,0,25\theta,6\theta) & (0,0,25,6,0,0,25\theta,6\overline{\theta}) & (0,0,25,6,0,0,25\overline{\theta},6\theta) \\
(0,0,25,6,0,0,25\overline{\theta},6\overline{\theta}) & (0,25,0,6,0,25\theta,0,6\theta) & (0,25,0,6,0,25\theta,0,6\overline{\theta}) \\
(0,25,0,6,0,25\overline{\theta},0,6\theta) & (0,25,0,6,0,25\overline{\theta},0,6\overline{\theta}) & (0,25,6,0,0,25\theta,6\theta,0) \\
(0,25,6,0,0,25\theta,6\overline{\theta},0) & (0,25,6,0,0,25\overline{\theta},6\theta,0) & (0,25,6,0,0,25\overline{\theta},6\overline{\theta},0) \\
(25,0,0,6,25\theta,0,0,6\theta) & (25,0,0,6,25\theta,0,0,6\overline{\theta}) & (25,0,0,6,25\overline{\theta},0,0,6\theta) \\
(25,0,0,6,25\overline{\theta},0,0,6\overline{\theta}) & (25,0,6,0,25\theta,0,6\theta,0) & (25,0,6,0,25\theta,0,6\overline{\theta},0) \\
(25,0,6,0,25\overline{\theta},0,6\theta,0) & (25,0,6,0,25\overline{\theta},0,6\overline{\theta},0) & (25,6,0,0,25\theta,6\theta,0,0) \\
(25,6,0,0,25\theta,6\overline{\theta},0,0) & (25,6,0,0,25\overline{\theta},6\theta,0,0) & (25,6,0,0,25\overline{\theta},6\overline{\theta},0,0)
\end{array}
$$

For any two of the e_i's to equal the pair $(10, 15)$, we have the following $\underline{\underline{72}}$ homomorphisms:

$(0,0,15,10,0,0,15\theta,10)$ $(0,0,15,10,0,0,15\theta,10\theta)$ $(0,0,15,10,0,0,15\theta,10\overline{\theta})$
$(0,0,15,10,0,0,15\overline{\theta},10)$ $(0,0,15,10,0,0,15\overline{\theta},10\theta)$ $(0,0,15,10,0,0,15\overline{\theta},10\overline{\theta})$
$(0,0,10,15,0,0,10,15\theta)$ $(0,0,10,15,0,0,10\theta,15\theta)$ $(0,0,10,15,0,0,10\overline{\theta},15\theta)$
$(0,0,10,15,0,0,10,15\overline{\theta})$ $(0,0,10,15,0,0,10\theta,15\overline{\theta})$ $(0,0,10,15,0,0,10\overline{\theta},15\overline{\theta})$
$(0,15,0,10,0,15\theta,0,10)$ $(0,15,0,10,0,15\theta,0,10\theta)$ $(0,15,0,10,0,15\theta,0,10\overline{\theta})$
$(0,15,0,10,0,15\overline{\theta},0,10)$ $(0,15,0,10,0,15\overline{\theta},0,10\theta)$ $(0,15,0,10,0,0,15\overline{\theta},10\overline{\theta})$
$(0,10,0,15,0,10,0,15\theta)$ $(0,10,0,15,0,10\theta,0,15\theta)$ $(0,10,0,15,0,10\overline{\theta},0,15\theta)$
$(0,10,0,15,0,10,0,15\overline{\theta})$ $(0,10,0,15,0,10\theta,0,15\overline{\theta})$ $(0,10,0,15,0,10\overline{\theta},0,15\overline{\theta})$
$(0,15,10,0,0,15\theta,10,0)$ $(0,15,10,0,0,15\theta,10\theta,0)$ $(0,15,10,0,0,15\theta,10\theta,0)$
$(0,15,10,0,0,15\overline{\theta},10,0)$ $(0,15,10,0,0,15\overline{\theta},10\theta,0)$ $(0,15,10,0,0,15\overline{\theta},10\overline{\theta},0)$
$(0,10,15,0,0,10,15\theta,0)$ $(0,10,15,0,0,10\theta,15\theta,0)$ $(0,10,15,0,0,10\overline{\theta},15\theta,0)$
$(0,10,15,0,0,10,15\overline{\theta},0)$ $(0,10,15,0,0,10\theta,15\overline{\theta},0)$ $(0,10,15,0,0,10\overline{\theta},15\overline{\theta},0)$
$(15,0,0,10,15\theta,0,0,10)$ $(15,0,0,10,15\theta,0,0,10\theta)$ $(15,0,0,10,15\theta,0,0,10\theta)$
$(15,0,0,10,15\overline{\theta},0,0,10)$ $(15,0,0,10,15\overline{\theta},0,0,10\theta)$ $(15,0,0,10,15\overline{\theta},0,0,10\overline{\theta})$
$(10,0,0,15,10,0,0,15\theta)$ $(10,0,0,15,10\theta,0,0,15\theta)$ $(10,0,0,15,10\overline{\theta},0,0,15\theta)$
$(10,0,0,15,10,0,0,15\overline{\theta})$ $(10,0,0,15,10\theta,0,0,15\overline{\theta})$ $(10,0,0,15,10\overline{\theta},0,0,15\overline{\theta})$
$(15,0,10,0,15\theta,0,10,0)$ $(15,0,10,0,15\theta,0,10\theta,0)$ $(15,0,10,0,15\theta,0,10\theta,0)$
$(15,0,10,0,15\overline{\theta},0,10,0)$ $(15,0,10,0,15\overline{\theta},0,10\theta,0)$ $(15,0,10,0,15\overline{\theta},0,10\overline{\theta},0)$
$(10,0,15,0,10,0,15\theta,0)$ $(10,0,15,0,10\theta,0,15\theta,0)$ $(10,0,15,0,10\overline{\theta},0,15\theta,0)$
$(10,0,15,0,10,0,15\overline{\theta},0)$ $(10,0,15,0,10\theta,0,15\overline{\theta},0)$ $(10,0,15,0,10\overline{\theta},0,15\overline{\theta},0)$
$(15,10,0,0,15\theta,10,0,0)$ $(15,10,0,0,15\theta,10\theta,0,0)$ $(15,10,0,0,15\theta,10\theta,0,0)$
$(15,10,0,0,15\overline{\theta},10,0,0)$ $(15,10,0,0,15\overline{\theta},10\theta,0,0)$ $(15,10,0,0,15\overline{\theta},10\overline{\theta},0,0)$
$(10,15,0,0,10,15\theta,0,0)$ $(10,15,0,0,10\theta,15\theta,0,0)$ $(10,15,0,0,10\overline{\theta},15\theta,0,0)$
$(10,15,0,0,10,15\overline{\theta},0,0)$ $(10,15,0,0,10\theta,15\overline{\theta},0,0)$ $(10,15,0,0,10\overline{\theta},15\overline{\theta},0,0)$

For $(10, 21)$, we'll get 72 homomorphisms, For $(15, 16)$, we'll get 72 homomorphisms too.

In order to have three different values of the e_i's, they must be pair-wise zero ($\mod 30$) under multiplication, and this is only possible for the triple: $\{6, 10, 15\}$; which gives us $\underline{\underline{288}}$ homomorphisms:

The first $\underline{\underline{48}}$ are the following:

$$
\begin{array}{ccc}
(0,6,10,15,0,6\theta,10,15\theta) & (0,6,10,15,0,6\theta,10,15\overline{\theta}) & (0,6,10,15,0,6\theta,10\theta,15\theta) \\
(0,6,10,15,0,6\theta,10\theta,15\overline{\theta}) & (0,6,10,15,0,6\theta,10\overline{\theta},15\theta) & (0,6,10,15,0,6\theta,10\overline{\theta},15\overline{\theta}) \\
(0,6,10,15,0,6\theta,10,15\theta) & (0,6,10,15,0,6\overline{\theta},10,15\overline{\theta}) & (0,6,10,15,0,6\overline{\theta},10\theta,15\theta) \\
(0,6,10,15,0,6\overline{\theta},10\theta,15\overline{\theta}) & (0,6,10,15,0,6\overline{\theta},10\overline{\theta},15\theta) & (0,6,10,15,0,6\overline{\theta},10\overline{\theta},15\overline{\theta}) \\
(0,6,15,10,0,6\theta,15\theta,10) & (0,6,15,10,6\theta,15\overline{\theta},10) & (0,6,15,10,0,6\theta,15\theta,10\theta) \\
(0,6,15,10,0,6\theta,15\overline{\theta},10\theta) & (0,6,15,10,6\theta,15\theta,10\overline{\theta}) & (0,6,15,10,0,6\theta,15\overline{\theta},10\overline{\theta}) \\
(0,6,15,10,0,6\theta,15\theta,10) & (0,6,15,10,0,6\overline{\theta},15\overline{\theta},10) & (0,6,15,10,0,6\overline{\theta},15\theta,10\theta) \\
(0,6,15,10,0,6\overline{\theta},15\overline{\theta},10\theta) & (0,6,15,10,0,6\overline{\theta},15\theta,10\overline{\theta}) & (0,6,15,10,0,6\overline{\theta},15\overline{\theta},10\overline{\theta}) \\
(6,0,10,15,6\theta,0,10,15\theta) & (6,0,10,15,6\theta,0,10,15\overline{\theta}) & (6,0,10,15,6\theta,0,10\theta,15\theta) \\
(6,0,10,15,6\theta,0,10\theta,15\overline{\theta}) & (6,0,10,15,6\theta,0,10\overline{\theta},15\theta) & (6,0,10,15,6\theta,0,10\overline{\theta},15\overline{\theta}) \\
(6,0,10,15,6\theta,0,10,15\theta) & (6,0,10,15,0,6\overline{\theta},10,15\overline{\theta}) & (6,0,10,15,6\overline{\theta},0,10\theta,15\theta) \\
(6,0,10,15,6\overline{\theta},0,10\theta,15\overline{\theta}) & (6,0,10,15,6\overline{\theta},0,10\overline{\theta},15\theta) & (6,0,10,15,6\overline{\theta},0,10\overline{\theta},15\overline{\theta}) \\
(6,0,15,10,6\theta,0,15\theta,10) & (6,0,15,10,6\theta,0,15\overline{\theta},10) & (6,0,15,10,6\theta,0,15\theta,10\theta) \\
(6,0,15,10,6\theta,0,15\overline{\theta},10\theta) & (6,0,15,10,6\theta,0,15\theta,10\overline{\theta}) & (6,0,15,10,6\theta,0,15\overline{\theta},10\overline{\theta}) \\
(6,0,15,10,6\theta,0,15\theta,10) & (6,0,15,10,6\overline{\theta},0,15\overline{\theta},10) & (6,0,15,10,6\overline{\theta},0,15\theta,10\theta) \\
(6,0,15,10,6\overline{\theta},0,15\overline{\theta},10\theta) & (6,0,15,10,6\overline{\theta},0,15\theta,10\overline{\theta}) & (6,0,15,10,6\overline{\theta},0,15\overline{\theta},10\overline{\theta})
\end{array}
$$

Permuting the three values $(6, 10, 15)$ produces the rest of the $\underline{\underline{240}}$,

Therefore, we have a total of:

$\big(1+8+8+12+8+12+8+8+72+48+48+72+72+72+288=737\big)$ *homomorphisms.*

Solution by using the formula in the theorem. $\phi : \mathbb{Z}[\theta] \times \mathbb{Z}[\theta] \times \mathbb{Z}[\theta] \times \mathbb{Z}[\theta] \to \mathbb{Z}_{30}[\theta]$

For $k = 30$*, the idempotents* $\{I_1 = 6, I_2 = 10, I_3 = 15, I_4 = 16, I_5 = 21, I_6 = 25\}$

$\Lambda_{(I_1,I_2/k)} = \Lambda_{(6,10/30)} = 1$, $\Lambda_{(I_1,I_3/k)} = \Lambda_{(6,15/30)} = 1$, $\Lambda_{(I_1,I_4/k)} = \Lambda_{(6,16/30)} = 0$,

$\Lambda_{(I_1,I_5/k)} = \Lambda_{(6,21/30)} = 0$, $\Lambda_{(I_1,I_6/k)} = \Lambda_{(6,25/30)} = 1$, $\Lambda_{(I_2,I_3/k)} = \Lambda_{(10,15/30)} = 1$,

$\Lambda_{(I_2,I_4/k)} = \Lambda_{(10,16/30)} = 0$, $\Lambda_{(I_2,I_5/k)} = \Lambda_{(10,21/30)} = 1$, $\Lambda_{(I_2,I_6/k)} = \Lambda_{(10,25/30)} = 0$,

$\Lambda_{(I_3,I_4/k)} = \Lambda_{(15,16/30)} = 1$, $\Lambda_{(I_3,I_5/k)} = \Lambda_{(15,21/30)} = 0$, $\Lambda_{(I_3,I_6/k)} = \Lambda_{(15,25/30)} = 0$,

$\Lambda_{(I_4,I_5/k)} = \Lambda_{(16,21/30)} = 0$, $\Lambda_{(I_4,I_6/k)} = \Lambda_{(16,25/30)} = 0$, $\Lambda_{(I_5,I_6/k)} = \Lambda_{(21,25/30)} = 0$

The number of solutions of $(x^2 + x + I_i)$*, "*N_i*" are as follows:*

$I_1 = 6$*:* $x^2 + x + 6 = 0$ *has two solutions, so* $N_1 = 2$*.*

$I_2 = 10$*:* $x^2 + x + 10 = 0$ *has three solutions, so* $N_2 = 3$*.*

$I_3 = 15$*:* $x^2 + x + 15 = 0$ *has two solutions, so* $N_3 = 2$*.*

$I_4 = 16$*:* $x^2 + x + 16 = 0$ *has three solutions, so* $N_4 = 3$*.*

$I_5 = 21$*:* $x^2 + x + 21 = 0$ *has two solutions, so* $N_5 = 2$*.*

$I_6 = 25$*:* $x^2 + x + 25 = 0$ *has two solutions, so* $N_6 = 2$*.*

$P(s, 2) = P(4, 2) = \left(\frac{4!}{(4-2)!}\right) = \left(\frac{4!}{2!}\right) = \frac{24}{2} = 12$*.*

$P(s, 3) = P(4, 3) = \left(\frac{4!}{(4-3)!}\right) = \left(\frac{4!}{1!}\right) = \frac{24}{1} = 24$*.*

Therefore the number of ring homomorphisms is:

$$
\begin{aligned}
\mathcal{N} &= 1 + n\Big(2 + N_1 + N_2 + N_3 + N_4 + N_5 + N_6\Big) \\
&+\ P(4,2)\Big(N_1N_2\Lambda_{(I_1,I_2/k)} + N_1N_3\Lambda_{(I_1,I_3/k)} + N_1N_4\Lambda_{(I_1,I_4/k)} \\
&\qquad + N_1N_5\Lambda_{(I_1,I_5/k)} + N_1N_6\Lambda_{(I_1,I_6/k)}\Big) \\
&+\ P(4,2)\Big(N_2N_3\Lambda_{(I_2,I_3/k)} + N_2N_4\Lambda_{(I_2,I_4/k)} + N_2N_5\Lambda_{(I_2,I_5/k)} + N_2N_6\Lambda_{(I_2,I_6/k)}\Big) \\
&+\ P(4,2)\Big(N_3N_4\Lambda_{(I_3,I_4/k)} + N_3N_5\Lambda_{(I_3,I_5/k)} + N_3N_6\Lambda_{(I_3,I_6/k)}\Big) \\
&+\ P(4,3)\Big(N_1N_2N_3\Lambda_{(I_1,I_2/k)} \cdot \Lambda_{(I_1,I_3/k)} \cdot \Lambda_{(I_2,I_3/k)}\Big) \\
&+\ P(4,3)\Big(N_1N_2N_4\Lambda_{(I_1,I_2/k)} \cdot \Lambda_{(I_1,I_4/k)} \cdot \Lambda_{(I_2,I_4/k)}\Big) \\
&+\ P(4,3)\Big(N_1N_2N_5\Lambda_{(I_1,I_2/k)} \cdot \Lambda_{(I_1,I_5/k)} \cdot \Lambda_{(I_2,I_5/k)}\Big) \\
&+\ P(4,3)\Big(N_1N_2N_6\Lambda_{(I_1,I_2/k)} \cdot \Lambda_{(I_1,I_6/k)} \cdot \Lambda_{(I_2,I_6/k)}\Big) \\
&+\ P(4,3)\Big(N_2N_3N_4\Lambda_{(I_2,I_3/k)} \cdot \Lambda_{(I_2,I_4/k)} \cdot \Lambda_{(I_3,I_4/k)}\Big) \\
&+\ P(4,3)\Big(N_2N_3N_5\Lambda_{(I_2,I_3/k)} \cdot \Lambda_{(I_2,I_5/k)} \cdot \Lambda_{(I_3,I_5/k)}\Big) \\
&+\ P(4,3)\Big(N_2N_3N_6\Lambda_{(I_2,I_3/k)} \cdot \Lambda_{(I_2,I_6/k)} \cdot \Lambda_{(I_3,I_6/k)}\Big) \\
&+\ P(4,3)\Big(N_3N_4N_5\Lambda_{(I_3,I_4/k)} \cdot \Lambda_{(I_3,I_5/k)} \cdot \Lambda_{(I_4,I_5/k)}\Big) \\
&+\ P(4,3)\Big(N_3N_4N_6\Lambda_{(I_3,I_4/k)} \cdot \Lambda_{(I_3,I_6/k)} \cdot \Lambda_{(I_4,I_6/k)}\Big) \\
&+\ P(4,3)\Big(N_4N_5N_6\Lambda_{(I_4,I_5/k)} \cdot \Lambda_{(I_4,I_6/k)} \cdot \Lambda_{(I_5,I_6/k)}\Big) \\
&=\ 1 + 4\Big(2 + 2 + 3 + 2 + 3 + 2 + 2\Big) \\
&+\ 12\Big(2 \cdot 3(1) + 2 \cdot 2(1) + 2 \cdot 3(0) + 2 \cdot 2(0) + 2 \cdot 2(1)\Big) \\
&+\ 12\Big(3 \cdot 2(1) + 3 \cdot 3(0) + 3 \cdot 2(1) + 3 \cdot 2(0)\Big) \\
&+\ 12\Big(2 \cdot 3(1) + 2 \cdot 2(0) + 2 \cdot 2(0)\Big) + 12\Big(3 \cdot 2(0) + 3 \cdot 2(0)\Big) + 2 \cdot 2(0) \\
&+\ 24\Big(2 \cdot 3 \cdot 2(1)(1)(1) + 2 \cdot 3 \cdot 3(1)(0)(0) + 2 \cdot 3 \cdot 2(1)(0)(1) + 2 \cdot 3 \cdot 2(1)(1)(0)\Big) \\
&+\ 24\Big(3 \cdot 2 \cdot 3)(1)(0)(1) + 3 \cdot 2 \cdot 2(1)(1)(0) + 3 \cdot 2 \cdot 2(1)(0)(0) \\
&+\ 2 \cdot 3 \cdot 2(1)(0)(0)2 \cdot 3 \cdot 2(1)(0)(0)3 \cdot 2 \cdot 2(0)(0)(0)\Big) \\
&=\ 1 + 4(16) + 12(6 + 4 + 0 + 0 + 4) + 12(6 + 0 + 6 + 0 + 6 + 0 + 0 + 0 + 0 + 0) \\
&+\ 24(12 + 0 + 0 + +0 + 0 + 0 + 0 + 0 + 0 + \ldots) \\
&=\ 1 + 64 + 168 + 144 + 72 + 288 = 737 \qquad \textit{homomorphisms}
\end{aligned}
$$

Theorem 2.16. *[5, Theorem 9]*

The number of ring homomorphisms:

$$\phi: \quad \mathbb{Z}_n[\theta] \quad \rightarrow \quad \mathbb{Z}_k[\theta] \quad {}^{\{9\}}$$

$$is$$

$$c_k \cdot 3^{\omega(k)-\omega\left(\frac{k}{\gcd(n,k)}\right)}$$

$$where \quad c_k = \begin{cases} 1 & if \quad m \nmid k \quad or \quad m \left| \left(\frac{k}{gcd(n,k)}\right)\right. \\ \frac{m+1}{3} & if \quad m \mid k, \quad m^2 \nmid k \quad and \quad m \not\left| \left(\frac{k}{gcd(n,k)}\right)\right. \\ \frac{2m+1}{3} & if \quad m^2 \mid k \quad and \quad m \not\left| \left(\frac{k}{gcd(n,k)}\right)\right. \end{cases}$$

Where $\omega(k)$ is the number of prime factors of k in $\mathbb{Z}[\theta]$.

Proof.

To determine the number of ring homomorphisms from $\mathbb{Z}_n[\theta]$ into $\mathbb{Z}_k[\theta]$, we see that we have the same conditions as in the last theorem's proof.

However, for a non zero homomorphism, when $a_j \neq 0$,then $p_j^{t_j}$ must divide n.

So when $p_j^{t_j} \nmid n$, then for that component we must reduce the number of ring homomorphisms accordingly by 1: $\Rightarrow$ instead of $\omega(k)$ we have $\omega(k) - \omega\left(\frac{k}{\gcd(n,k)}\right)$ completing the proof. $\square$

{9} θ as in *theorem* 2.14, page 83

Example 2.15.

Consider the ring homomorphisms: $\phi : \mathbb{Z}_3[\theta] \to \mathbb{Z}_6[\theta]$,

Where θ *is the algebraic number with minimal polynomial* $P(x) = x^2 + x + 1$.

That is; $\theta = \left(\frac{-1+\sqrt{-3}}{2}\right) = \rho$, *the Eisenstein number.*

Note that this is just example(2.8) which has been solved on page 71.

We've found that we have the four ring homomorphisms:

$(e, f) = (0, 0), (4, 4), (4, 4\rho)$ *and* $(4, 4\rho^2)$

Solution by using the formula in the theorem.

Here, $m = 3$, $n = 3$, $k = 6$ *and* $m \mid k$ $(3 \mid 6)$ *but* $m^2 \nmid k$ $(3^2 \nmid 6)$.

So, we have the second case of $c_k = \left(\frac{m+1}{3}\right) = \left(\frac{4}{3}\right)$.

$\left(\frac{k}{\gcd(n,k)}\right) = \left(\frac{6}{\gcd(3,6)}\right) = \frac{6}{3} = 2$, $\omega(6) = 2$, $\omega(2) = 1$,

$$\textit{and} \quad \textit{therefore} \qquad \mathcal{N}\big(\phi : \mathbb{Z}_3[\theta] \to \mathbb{Z}_6[\theta]\big) = \frac{4}{3} \cdot 3^{2-1} = \frac{4}{3} \cdot 3 = 4$$

Theorem 2.17. *[5, Theorem 11]*

The number of ring homomorphisms:

$$\phi: \ \mathbb{Z}_n[\theta] \times \mathbb{Z}_l[\theta] \to \mathbb{Z}_k[\theta] \quad {}^{\{10\}}$$

$$is$$

$$c_k \cdot 5^{\omega(k)-\omega\left(\frac{k}{gcd(n,l,k)}\right)} \cdot 3^{2\omega\left(\frac{k}{gcd(n,l,k)}\right)-\omega\left(\frac{k}{gcd(n,k)}\right)-\omega\left(\frac{k}{gcd(l,k)}\right)}$$

$$Where \quad c_k = \begin{cases} 1 & if \quad either\ m \nmid k \quad or \quad m \mid k, \quad but \quad m \nmid \left(\frac{k}{gcd(l,k)}\right),\ m \nmid \left(\frac{k}{gcd(n,k)}\right) \\ \frac{m+1}{3} & if \quad m \mid k, \quad m^2 \nmid k \quad and \quad m \mid l, \quad or \quad m \mid n \quad but \quad m \nmid gcd(n,l) \\ \frac{4m+1}{5} & if \quad m^2 \mid k \quad and \quad m \nmid \left(\frac{k}{gcd(n,l,k)}\right) \end{cases}$$

and $\omega(m)$ is the number of prime factors of m in $\mathbb{Z}[\theta]$.

Proof.

Let $k = p_1^{t_1} p_2^{t_2} \cdot p_s^{t_s}$ in $\mathbb{Z}[\theta]$, then by the Chinese Remainder Theorem:

$$\mathbb{Z}_k[\theta] \cong \mathbb{Z}_{p_1^{t_1}}[\theta] \times \mathbb{Z}_{p_2^{t_2}}[\theta] \times \cdots \times \mathbb{Z}_{p_s^{t_s}}[\theta]$$

Then ϕ is completely determined by its action on $(1,0),(0,1),(\theta,0),(0,\theta)$.

Note that, as in the previous proofs, $\phi((1,0))$ and $\phi((0,1))$ is each $= 0$ or 1.

Let $\phi((\theta,0)) = a = (a_1, a_2, \ldots, a_s)$ and $\phi((0,\theta)) = b = (b_1, b_2, \ldots, b_s)$ in $\mathbb{Z}_k[\theta]$.

Then ϕ is completely determined by the values of a and b.

Now, if $p_j \neq \sqrt{m}$, then $p_j^{t_j}$ cannot divide both factors; then $p_j = \theta$ or $\overline{\theta}$ which gives us:

$$a_j = 0, \quad \theta, \quad \overline{\theta} \qquad ; \qquad b_j = 0, \quad \theta, \quad \overline{\theta}$$

Which gives us $2^2 + 1 = 5$ possibilities.

{10} θ as in *theorem* 2.14, page 83

If $p_j = \sqrt{m}$, $p_j^{t_j}$ may divide both factors, $\Rightarrow t_j$ is even:

Case 1. For $t_j = 2$, $p_j^{t_j} = p_j^2 = m$. For $m \mid k$ but $m^2 \nmid k$:

If $m \mid l$; or if $m \mid n$ but $m \nmid \gcd(n, l)$ in $\mathbb{Z}_m[\theta]$ then:

Either $\quad a_j = 0, \quad b_j = 0, \quad \theta, \quad \overline{\theta}.$

$\Rightarrow \quad bj = x_b + y_b\theta, \quad x_b, \quad y_b \in \mathbb{Z}_m \quad \text{and} \quad b_j^2 + ub_j + v = 0.$

And similar to the proof of *theorem* (2.14), we have:

b_j has m choices, giving us that $c_k = \frac{m+1}{3}$.

Or $\quad a_j = 0, \quad \theta, \quad \overline{\theta}, b_j = 0.$

$\Rightarrow \quad a_j = x_a + y_a\theta, \quad x_a, \quad y_a \in \mathbb{Z}_m \quad \text{and} \quad a_j^2 + ua_j + v = 0.$

Similarly; a_j has m choices, giving us that $c_k = \frac{m+1}{3}$.

Case 2. For $t_j \geq 4$, so $m^2 \mid k$ and $m \nmid \frac{k}{\gcd(n,l,k)}$, then a_j has $(2m+1)$ choices and b_j has $(2m+1)$ choices, along with $a_j b_j = 0$, thus, we have $(4m+1)$ choices and $c_k = \frac{4m+1}{5}$

□

Example 2.16.

Consider the ring homomorphisms: $\phi : \mathbb{Z}_3[\theta] \times \mathbb{Z}_4[\theta] \to \mathbb{Z}_6[\theta]$,

where θ *has the minimal polynomial:* $P(x) = x^2 + x + 1$, *thus* $\theta = \left(\frac{-1+\sqrt{-3}}{2}\right) = \rho$.

Note that this is just example(2.9), where we've found twelve ring homomorphisms on page 79.

Solution by using the formula in the theorem. *Here,* $n = 3$, $l = 4$, $k = 6$, $m = 3$, $m \mid k$ $(3 \mid 6)$ *and* $m^2 \nmid k$ $(3^2 \nmid 6)$ *thus we have the second case of our* $c_k = \frac{m+1}{3} = \frac{4}{3}$ *and the solution follows identically as that on page 81.*

A more illustrating example is given on the next page:

Example 2.17. *The ring homomorphism:* $\phi : \mathbb{Z}_4[\theta] \times \mathbb{Z}_6[\theta] \to \mathbb{Z}_{12}[\theta]$,

where θ *has the minimal polynomial* $P(x) = x^2 + x + 1$.

Let $e_1 = \phi(1,0)$, $e_2 = \phi(0,1)$, $f_1 = \phi(\theta,0)$, $f_2 = \phi(0,\theta)$.

Note that $e_i \in \{0,1,4,9\}$, *the idempotents of* $\mathbb{Z}_{12}[\theta]$.

For $i = 1,2$: $e_i f_i = f_i$, $f_i^2 + f_i + e_i = 0$, $3e_1 = 6e_2 = 0$.

For $e_1 = e_2 = 0 \Rightarrow f_1 = f_2 = 0$, *giving us* $(e_1, e_2, f_1, f_2) = (0,0,0,0)$

For $e_1 = 1$, *or* $e_2 = 1$ *are both not acceptable, since* $4e_1 = 4 \neq 0$ *and* $6e_2 = 6 \neq 0$.

For $e_1 = 0$, $e_2 = 4$, *(note here,* $6e_2 = 6 \cdot 4 = 24 = 0$*)* $\Rightarrow f_2 = 4, 4\theta, 4\overline{\theta}$.

For $e_2 = 9$ *is not acceptable, for* $6e_2 = 6 \cdot 9 = 54 = 6 \neq 0$.

For $e_1 = 1$ *or* 4 *are not acceptable,* $4e_1 \neq 0$ *in either case.*

For $e_1 = 9$, *(note,* $4e_1 = 4 \cdot 9 = 36 = 0$*),* $e_2 = 0 \Rightarrow f_1 = 9\theta, 9\overline{\theta}$, $f_2 = 0$ *giving us:*

$(e_1, e_2, f_1, f_2) = (9,0,9\theta,0)$, $(9,0,9\overline{\theta},0)$.

For $e_1 = 9$, $e_2 = 4$, *(*$4e_1 = 0$, $6e_2 = 0$*); giving us:*

$(e_1, e_2, f_1, f_2) = (9,4,9\theta,4)$, $(9,4,9\theta,4\theta)$, $(9,4,9\theta,4\overline{\theta})$, $(9,4,9\overline{\theta},4)$, $(9,4,9\overline{\theta},4\theta)$, $(9,4,9\overline{\theta},4\overline{\theta})$.

Therefore, we have the following 12 *homomorphisms:*

$$(e_1, e_2, f_1, f_2) = \begin{matrix} (0,0,0,0) & (0,4,0,4) & (0,4,0,4\theta) \\ (0,4,0,4\overline{\theta}) & (9,0,9\theta,0) & (9,0,9\overline{\theta},0) \\ (9,4,9\theta,4) & (9,4,9\theta,4\theta) & (9,4,9\theta,4\overline{\theta}) \\ (9,4,9\overline{\theta},4) & (9,4,9\overline{\theta},4\theta) & (9,4,9\overline{\theta},4\overline{\theta}) \end{matrix}$$

Solution by using the formula in the theorem.

Here, $n = 4$, $l = 6$, $m = 3$, $k = 12$, $m \mid k$ *and* $m^2 \nmid k$ *with* $m \mid l$; *So,* $c_k = \frac{m+1}{3} = \frac{4}{3}$,

$\left(\frac{k}{\gcd(k,n,l)}\right) = \left(\frac{6}{\gcd(4,6,12)}\right) = \frac{12}{2} = 6$, $\left(\frac{k}{\gcd(k,n)}\right) = \left(\frac{12}{\gcd(12,4)}\right) = \frac{12}{4} = 3$,

$\left(\frac{k}{\gcd(k,l)}\right) = \left(\frac{12}{\gcd(12,6)}\right) = \frac{12}{6} = 2$.

Therefore, the number of ring homomorphisms is:

$\mathcal{N} = c_k \cdot 5^{\omega(12)-\omega(6)} \cdot 3^{2\omega(12)-\omega(3)-\omega(2)} = \frac{4}{3} \cdot 5^0 \cdot 3^{2(2)-1-1} = \frac{4}{3} \cdot 3^2 = 12$ *homomorphisms.*

Theorem * 2.3.

The number of ring homomorphisms:

$$\phi: \ \mathbb{Z}_{n_1}[\theta] \times \mathbb{Z}_{n_2}[\theta] \times \cdots \times \mathbb{Z}_{n_s}[\theta] \ \rightarrow \ \mathbb{Z}_k[\theta] \quad {}^{\{11\}} \qquad is$$

$$\begin{aligned}
&1 + \Big(M_1 + M_2 + M_3 + \cdots + M_r\Big) && + \quad \sum_{i=2}^{r} \Big(M_1 M_i \Lambda_{(I_1, I_i/k)}\Big) \\
&+ \ \sum_{i=3}^{r} \Big(M_2 M_i \Lambda_{(I_2, I_i/k)}\Big) \ + && \cdots \ + \ \Big(M_{r-1} M_r \Lambda_{(I_{r-1}, I_r/k)}\Big) \\
&+ \ \Big(M_1 M_2 M_3 \prod_{\substack{i,j=1,2,3 \\ i \neq j}} \Lambda_{(I_i, I_j/k)}\Big) \ + && \cdots \ + \ \Big(M_1 M_2 M_r \prod_{\substack{i,j=1,2,r \\ i \neq j}} \Lambda_{(I_i, I_j/k)}\Big) \\
&+ \ \Big(M_2 M_3 M_4 \prod_{\substack{i,j=2,3,4 \\ i \neq j}} \Lambda_{(I_i, I_j/k)}\Big) \ + && \cdots \ + \ \Big(M_2 M_3 M_r \prod_{\substack{i,j=2,3,r \\ i \neq j}} \Lambda_{(I_i, I_j/k)}\Big) \\
&\qquad \cdots && \cdots \qquad \cdots \\
&\qquad \vdots && \vdots \qquad \vdots \\
&+ \ \Big(N_1 N_2 N_3 N_4 \prod_{\substack{i,j=1 \\ i \neq j}}^{4} \Lambda_{(I_i, I_j/k)}\Big) \ + && \cdots \ + \ \Big(M_1 M_2 M_3 M_r \prod_{\substack{i,j=1 \\ i,j \neq 4 \\ i \neq j}} \Lambda_{(I_i, I_j/k)}\Big) \\
&\qquad \vdots && \vdots \qquad \vdots \\
&+ \ \Big(M_1 M_2 \cdots M_{r-1} \prod_{\substack{i,j=1 \\ i \neq j}} \Lambda_{(I_i, I_j/k)}\Big) \ + && \cdots \ + \ \Big(M_1 M_2 \cdots M_r \prod_{\substack{i,j=1 \\ i \neq j}} \Lambda_{(I_i, I_j/k)}\Big).
\end{aligned}$$

Where r and I_i as defined in Theorem (2.1) on page 91, and M_i is defined by:*

$$M_i = N_i \sum_{j=1}^{s} \Lambda_{(I_i, n_j/k)}$$

Where Λ is as defined in *equation* (2.12) on page 91.

{11} θ as in *theorem* 2.14, page 83

Proof.

Note that this theorem is just a generalization of *Theorem** (2.1), and the proof is identical to that of *Theorem** (2.1) with the additional condition that we must have $n_i I_j = 0$ in order to take it into account for producing a homomorphism, for $i = 1, 2, \ldots, s$ and for every idempotent I_j of the $\underline{r}$ idempotents of $\mathbb{Z}_k$. And here comes the role of defining the new parameter M_i, which is as defined, characterizes those idempotents that would be taken into account. Moreover, note that we have omitted the $P(n, i)$ coefficients from the formula since it is accounted for in the definition of M_i's. □

Example 2.18. *Consider the ring homomorphisms* $\phi : \mathbb{Z}_2[\theta] \times \mathbb{Z}_4[\theta] \times \mathbb{Z}_2[\theta] \to \mathbb{Z}_6[\theta]$
where θ *is the algebraic number with the minimal polynomial* $p(x) = x^2 + x + 2$
That is; $\theta = \left(\frac{-1+\sqrt{-7}}{2}\right)$
Let $e_1 = \phi(1, 0, 0)$, $e_2 = \phi(0, 1, 0)$, $e_3 = \phi(0, 0, 1)$,
$f_1 = \phi(\theta, 0, 0)$, $f_2 = \phi(0, \theta, 0)$, $f_3 = \phi(0, 0, \theta)$

We have to take into considerations the following conditions in searching for the ring homomorphisms:

$e_i^2 = e_i$ *and* $e_i f_i = f_i$ *with* $f_i^2 + f_i + 2e_i = 0$ *for* $i = 1, 2, 3$, *with* $e_i e_j = f_i f_j = 0$ *for* $i \neq j$.
Moreover, since $2(1) = 0$ *in* $\mathbb{Z}_2$ *and* $4(1) = 0$ *in* $\mathbb{Z}_4$ *then,*
we must also have $2e_1 = 2e_3 = 0$ *and* $4e_2 = 0$. *So, the only allowed idempotents of* $\mathbb{Z}_6[\theta]$ *are* 0 *and* 3. *Therefore;* $e_1, e_2, e_3 \in \{0, 3\}$.
Now, for $e_1 = 0 \Rightarrow e_2, e_3 \in \{0, 3\}$.
$e_1 = 0 \Rightarrow f_1 = 0$, *and if* $e_2 = 0$, *then* $f_2 = 0$.
Now, if also, $e_3 = 0$ *then* $f_3 = 0$ *giving us* $(e_1, e_2, e_3, f_1, f_2, f_3) = (0, 0, 0, 0, 0, 0)$
And if $e_3 = 3$, *then* $f_3^2 + f_3 + 2e_3 = f_3^2 + f_3 = 0 \Rightarrow f_3 = 0, 3$ *giving us that:*
$(e_1, e_2, e_3, f_1, f_2, f_3) = (0, 0, 3, 0, 0, 0)$ *and* $(0, 0, 3, 0, 0, 3)$
If $e_1 = 0$ *and* $e_2 = 3$, *then* $e_3 = 0$ *and* $f_1 = f_3 = 0$ *and* $f_2 = 0, 3$, *giving us:*
$(e_1, e_2, e_3, f_1, f_2, f_3) = (0, 3, 0, 0, 0, 0)$ *and* $(0, 3, 0, 0, 3, 0)$
If $e_1 = 3$ *then* $e_2 = e_3 = 0$ *and* $f_1 = 0, 3$, $f_2 = f_3 = 0$ *giving us:*
$(e_1, e_2, e_3, f_1, f_2, f_3) = (3, 0, 0, 0, 0, 0)$, $(3, 0, 0, 3, 0, 0)$

Therefore, we have the following seven ring homomorphisms:

Let $\alpha = a + b\theta$, $\beta = c + d\theta$, $\gamma = e + f\theta$, *then:*

$\phi(1,0,0)$	$\phi(\theta,0,0)$	$\phi(0,1,0)$	$\phi(0,\theta,0)$	$\phi(0,0,1)$	$\phi(0,0,\theta)$	$\phi(\alpha,\beta,\gamma)$
0	0	0	0	0	0	0
0	0	3	0	0	0	$3c$
0	0	3	0	0	3	$3c + 3f$
0	3	0	0	0	0	$3b$
0	3	0	0	3	0	$3b + 3e$
3	0	0	0	0	0	$3a$
3	0	0	3	0	0	$3a + 3d$

Solution by using the formula in the theorem.

Here, we have the non-one idempotents of $\mathbb{Z}_6$ *are* $\{0, I_1 = 3, I_2 = 4\}$.

$n_1 = 2$, $n_2 = 4$, $n_3 = 2$ *and* $k = 6$.

The number of solutions of $(x^2 + x + 2I_1 = x^2 + x + 6 = x^2 + x = 0)$ *is two, so* $N_1 = 2$.

The number of solutions of $(x^2 + x + 2I_2 = x^2 + x + 8 = x^2 + x + 2 = 0)$ *is two, so* $N_2 = 2$.

$\Lambda_{(I_1,n_1/k)} = \Lambda_{(3,2/6)} = 1$ *since* $3 \cdot 2 = 0$ *in* $\mathbb{Z}_6$, $\Lambda_{(I_1,n_2/k)} = \Lambda_{(3,4/6)} = 1$ *since* $3 \cdot 4 = 0$ *in* $\mathbb{Z}_6$,

$\Lambda_{(I_1,n_3/k)} = \Lambda_{(3,2/6)} = 1$, $\Lambda_{(I_2,n_1/k)} = \Lambda_{(4,2/6)} = 0$ *since* $4 \cdot 2 \neq 0$ *in* $\mathbb{Z}_6$.

$\Lambda_{(I_2,n_2/k)} = \Lambda_{(4,4/6)} = 0$ *since* $4 \cdot 4 \neq 0$ *in* $\mathbb{Z}_6$, $\Lambda_{(I_2,n_3/k)} = \Lambda_{(4,2/6)} = 0$.

And $\Lambda_{I_1,I_2/k)} = \Lambda_{(3,4/6)} = 1$ *since* $3 \cdot 4 = 0$ *in* $\mathbb{Z}_6$. *Therefore:*

$$M_1 = N_1\Big(\Lambda_{(I_1,n_1/k)} + \Lambda_{(I_1,n_2)} + \Lambda_{(I_1,n_3/k)}\Big) = 2\Big(1+1+1\Big) = 2 \cdot 3 = 6 \quad \Big\| \quad M_2 = \Big(\Lambda_{(I_2,n_1/k)} + \Lambda_{(I_2,n_2)} + \Lambda_{(I_2,n_3/k)}\Big) = \Big(0+0+0\Big) = 0$$

Therefore, the total number of ring homomorphisms is:

$$\begin{aligned}\mathcal{N} &= 1 + \Big(M_1 + M_2\Big) + \Big(M_1 M_2 \Lambda_{(I_1,I_2/k)}\Big) \\ &= 1 + \Big(6 + 0\Big) + \Big(6 \cdot 0 \cdot 0\Big) \\ &= 1 + 6 = 7 \qquad \textit{homomorphisms}\end{aligned}$$

Example 2.19. *Consider example (2.17) on page 109;* $\phi : \mathbb{Z}_4[\theta] \times \mathbb{Z}_6[\theta] \to \mathbb{Z}_{12}[\theta]$, *whose solution was based on Theorem (2.17) which is a special case of theorem* (2.3): Now,* $n_1 = 4$, $n_2 = 6$, $k = 12$, *the idempotents of* $\mathbb{Z}_{12}$ *are:* $0, 1, 4, 9$

$I_1 = 1,\ N_1 = 2, \qquad I_2 = 4,\ N_2 = 3, \qquad I_3 = 9,\ N_3 = 2l;$

$\Lambda_{(I_1,I_2/k)} = \Lambda_{(1,4/12)} = 0, \qquad \Lambda_{(I_1,I_3/k)} = \Lambda_{(1,9/12)} = 0, \qquad \Lambda_{(I_2,I_3/k)} = \Lambda_{(3,4/12)} = 1.$

$\Lambda_{(I_1,n_1/k)} = \Lambda_{(1,4/12)} = 0, \qquad \Lambda_{(I_1,n_2/k)} = \Lambda_{(1,6/12)} = 0,$

$\Lambda_{(I_2,n_1/k)} = \Lambda_{(4,4/12)} = 0, \qquad \Lambda_{(I_2,n_2/k)} = \Lambda_{(4,9/12)} = 1,$

$\Lambda_{(I_3,n_1/k)} = \Lambda_{(9,4/12)} = 1, \qquad \Lambda_{(I_3,n_2/k)} = \Lambda_{(9,9/12)} = 0,$

$$M_1 = N_1\Big(\Lambda_{(I_1,n_1/k)} + \Lambda_{(I_1,n_2/k)}\Big) = 2\Big(0+0\Big) = 0$$

$$M_2 = N_2\Big(\Lambda_{(I_2,n_1/k)} + \Lambda_{(I_2,n_2/k)}\Big) = 3\Big(0+1\Big) = 3$$

$$M_3 = N_3\Big(\Lambda_{(I_3,n_1/k)} + \Lambda_{(I_3,n_2/k)}\Big) = 2\Big(1+0\Big) = 2$$

Therefore, the number of ring homomorphisms is:

$$\mathcal{N} = 1 + \sum_{i=1}^{3}\Big(M_i\Big) + M_1M_2\Lambda_{(I_1,I_2/k)} + M_1M_3\Lambda_{(I_1,I_3/k)} + M_2M_2\Lambda_{(I_2,I_2/k)} + M_1M_2M_3\Lambda_{(I_1,I_2/k)}\Lambda_{(I_1,I_3/k)}\Lambda_{(I_2,I_3/k)}$$

$$= 1 + \big(0+3+2\big) + \big(0\cdot 3(0)\big) + \big(0\cdot 2(0)\big) + \big(3\cdot 2(1)\big) + \big(0\cdot 3\cdot 2\big)\cdot\big(0\cdot 0\cdot 1\big)$$

$$= 1+5+0+0+6+0 = 12 \quad \textit{homomorphisms,}$$

which is consistent with the solution (2.4) of page 109.

Example 2.20. *Consider* $\phi : \mathbb{Z}_6[\theta] \times \mathbb{Z}_6[\theta] \times \mathbb{Z}_6[\theta] \to \mathbb{Z}_6[\theta]$,

with θ *has the minimal polynomial* $P(x) = x^2 + x + 1$.

Let $e_1, e_2, e_3, f_1, f_2, f_3$ *be defined as in example (2.18).*

The idempotents of $\mathbb{Z}_6$ *are* $\{0, 1, 3, 4\}$. *So,* $e_i \in \{0, 1, 3, 4\}$.

Note that we must satisfy the same conditions in the previous example, in addition to that $e_i \cdot n_i = 0$, *for* $i = 1, 2, 3$, $n_i = 6$. *So, we must have* $6e_i = 0$:

For $e_i = 0 \to f_i = 0$ *giving us the zero homomorphism:*

$(e_1, e_2, e_3, e_4, f_1, f_2, f_3, f_4) = (0, 0, 0, 0, 0, 0)$ [{12}]

For $e_i = 1$, *note that* $n_i \cdot e_i = 6 \cdot 1 = 0$, *so* 1 *is acceptable,*

Now, $e_i = 1 \to f_i = \theta, \overline{\theta}$ *giving us* $\underline{\underline{8}}$ *homomorphisms:*

$$(0,0,0,1,0,0,0,\theta) \quad (0,0,0,1,0,0,0,\overline{\theta}) \quad (0,0,1,0,0,0,\theta,0)$$
$$(0,0,1,0,0,0,\overline{\theta},0) \quad (0,1,0,0,0,\theta,0,0) \quad (0,1,0,0,0,\overline{\theta},0,0)$$
$$(1,0,0,0,\theta,0,0,0) \quad (1,0,0,0,\overline{\theta},0,0,0)$$

For $e_i = 3$, $n_i \cdot e_i = 0$, 3 *is acceptable, and* $f_i = 3\theta, 3\overline{\theta}$, *giving us* $\underline{\underline{8}}$ *homomorphisms:*

$$(0,0,0,3,0,0,0,3\theta) \quad (0,0,0,3,0,0,0,3\overline{\theta}) \quad (0,0,3,0,0,0,3\theta,0)$$
$$(0,0,3,0,0,0,3\overline{\theta},0) \quad (0,3,0,0,0,3\theta,0,0) \quad (0,3,0,0,0,3\overline{\theta},0,0)$$
$$(3,0,0,0,3\theta,0,0,0) \quad (3,0,0,0,3\overline{\theta},0,0,0)$$

For $e_i = 4$, $n_i \cdot e_i = 0$, 4 *is acceptable, and* $f_i = 4, 4\theta, 4\overline{\theta}$, *giving us* $\underline{\underline{12}}$ *homomorphisms:*

$$(0,0,0,4,0,0,0,4) \quad (0,0,0,4,0,0,0,4\theta) \quad (0,0,0,4,0,0,0,4\overline{\theta})$$
$$(0,0,4,0,0,0,4,0) \quad (0,0,4,0,0,0,4\theta,0) \quad (0,0,4,0,0,0,4\overline{\theta},0)$$
$$(0,4,0,0,0,4,0,0) \quad (0,4,0,0,0,4\theta,0,0) \quad (0,4,0,0,0,4\overline{\theta},0,0)$$
$$(4,0,0,0,4,0,0,0) \quad (4,0,0,0,4\theta,0,0,0) \quad (4,0,0,0,4\overline{\theta},0,0,0)$$

[{12}] Henceforth in this example, $(x, x, x, x, x, x, x, x) = (e_1, e_2, e_3, e_4, f_1, f_2, f_3, f_4)$

For two of the e_i's to equal two of the idempotents, their product must be zero, so 3 *and* 4 *meet this condition.*

And this combination would give us $\underline{\underline{72}}$ *homomorphisms:*

$$
\begin{array}{lll}
(0,0,3,4,0,0,3\theta,4) & (0,0,3,4,0,0,3\theta,4\theta) & (0,0,3,4,0,0,3\theta,4\overline{\theta}) \\
(0,0,3,4,0,0,3\overline{\theta},4) & (0,0,3,4,0,0,3\overline{\theta},4\theta) & (0,0,3,4,0,0,3\overline{\theta},4\overline{\theta}) \\
(0,0,4,3,0,0,4,3\theta) & (0,0,4,3,0,0,4\theta,3\theta) & (0,0,4,3,0,0,4\overline{\theta},3\theta) \\
(0,0,4,3,0,0,4,3\overline{\theta}) & (0,0,4,3,0,0,4\theta,3\overline{\theta}) & (0,0,4,3,0,0,4\overline{\theta},3\overline{\theta}) \\
(0,3,0,4,0,3\theta,0,4) & (0,3,0,4,0,3\theta,0,4\theta) & (0,3,0,4,0,3\theta,0,4\overline{\theta}) \\
(0,3,0,4,0,3\overline{\theta},0,4) & (0,3,0,4,0,3\overline{\theta},0,4\theta) & (0,3,0,4,0,0,3\overline{\theta},4\overline{\theta}) \\
(0,4,0,3,0,4,0,3\theta) & (0,4,0,3,0,4\theta,0,3\theta) & (0,4,0,3,0,4\overline{\theta},0,3\theta) \\
(0,4,0,3,0,4,0,3\overline{\theta}) & (0,4,0,3,0,4\theta,0,3\overline{\theta}) & (0,4,0,3,0,4\overline{\theta},0,3\overline{\theta}) \\
(0,3,4,0,0,3\theta,4,0) & (0,3,4,0,0,3\theta,4\theta,0) & (0,3,4,0,0,3\theta,4\theta,0) \\
(0,3,4,0,0,3\overline{\theta},4,0) & (0,3,4,0,0,3\overline{\theta},4\theta,0) & (0,3,4,0,0,3\overline{\theta},4\overline{\theta},0) \\
(0,4,3,0,0,4,3\theta,0) & (0,4,3,0,0,4\theta,3\theta,0) & (0,4,3,0,0,4\overline{\theta},3\theta,0) \\
(0,4,3,0,0,4,3\overline{\theta},0) & (0,4,3,0,0,4\theta,3\overline{\theta},0) & (0,4,3,0,0,4\overline{\theta},3\overline{\theta},0) \\
(3,0,0,4,3\theta,0,0,4) & (3,0,0,4,3\theta,0,0,4\theta) & (3,0,0,4,3\theta,0,0,4\theta) \\
(3,0,0,4,3\overline{\theta},0,0,4) & (3,0,0,4,3\overline{\theta},0,0,4\theta) & (3,0,0,4,3\overline{\theta},0,0,4\overline{\theta}) \\
(4,0,0,3,4,0,0,3\theta) & (4,0,0,3,4\theta,0,0,3\theta) & (4,0,0,3,4\overline{\theta},0,0,3\theta) \\
(4,0,0,3,4,0,0,3\overline{\theta}) & (4,0,0,3,4\theta,0,0,3\overline{\theta}) & (4,0,0,3,4\overline{\theta},0,0,3\overline{\theta}) \\
(3,0,4,0,3\theta,0,4,0) & (3,0,4,0,3\theta,0,4\theta,0) & (3,0,4,0,3\theta,0,4\theta,0) \\
(3,0,4,0,3\overline{\theta},0,4,0) & (3,0,4,0,3\overline{\theta},0,4\theta,0) & (3,0,4,0,3\overline{\theta},0,4\overline{\theta},0) \\
(4,0,3,0,4,0,3\theta,0) & (4,0,3,0,4\theta,0,3\theta,0) & (4,0,3,0,4\overline{\theta},0,3\theta,0) \\
(4,0,3,0,4,0,3\overline{\theta},0) & (4,0,3,0,4\theta,0,3\overline{\theta},0) & (4,0,3,0,4\overline{\theta},0,3\overline{\theta},0) \\
(3,4,0,0,3\theta,4,0,0) & (3,4,0,0,3\theta,4\theta,0,0) & (3,4,0,0,3\theta,4\theta,0,0) \\
(3,4,0,0,3\overline{\theta},4,0,0) & (3,4,0,0,3\overline{\theta},4\theta,0,0) & (3,4,0,0,3\overline{\theta},4\overline{\theta},0,0) \\
(4,3,0,0,4,3\theta,0,0) & (4,3,0,0,4\theta,3\theta,0,0) & (4,3,0,0,4\overline{\theta},3\theta,0,0) \\
(4,3,0,0,4,3\overline{\theta},0,0) & (4,3,0,0,4\theta,3\overline{\theta},0,0) & (4,3,0,0,4\overline{\theta},3\overline{\theta},0,0)
\end{array}
$$

Therefore, we have $(1+8+8+12+72) = 101$ *homomorphisms.*

Solution by using the formula in the theorem.

Here, $n_i = k = 6$, $I_1 = 1$, $I_2 = 3$, $I_3 = 4$, $N_1 = 2$, $N_2 = 2$ *and* $N_3 = 3$.

$\Lambda_{(I_1,I_2/k)} = \Lambda_{(1,3/6)} = 0$ *since* $1 \cdot 3 \neq 0$,

$\Lambda_{(I_1,I_3/k)} = \Lambda_{(1,4/6)} = 0$ *since* $1 \cdot 4 \neq 0$,

$\Lambda_{(I_2,I_3/k)} = \Lambda_{(3,4/6)} = 1$ *since* $3 \cdot 4 = 0$,

$\Lambda_{(I_1,n_i/k)} = \Lambda_{(1,6/6)} = 1$ *since* $1 \cdot 6 = 0$,

$\Lambda_{(I_2,n_i/k)} = \Lambda_{(3,6/6)} = 1$ *since* $3 \cdot 6 = 0$,

$\Lambda_{(I_3,n_i/k)} = \Lambda_{(4,6/6)} = 1$ *since* $4 \cdot 6 = 0$,

$$M_1 = N_1\Big(\Lambda_{(I_1,n_1/k)} + \Lambda_{(I_1,n_2/k)} + \Lambda_{(I_1,n_3/k)} + \Lambda_{(I_1,n_4/k)}\Big) = 2\Big(1+1+1+1\Big) = 2(4) = 8$$
$$M_2 = N_2\Big(\Lambda_{(I_2,n_1/k)} + \Lambda_{(I_2,n_2/k)} + \Lambda_{(I_2,n_3/k)} + \Lambda_{(I_2,n_4/k)}\Big) = 3\Big(1+1+1+1\Big) = 3(4) = 12$$
$$M_3 = N_3\Big(\Lambda_{(I_3,n_1/k)} + \Lambda_{(I_3,n_2/k)} + \Lambda_{(I_3,n_3/k)} + \Lambda_{(I_3,n_4/k)}\Big) = 2\Big(1+1+1+1\Big) = 2(4) = 8$$

Therefore, the number of ring homomorphisms is:

$$\mathcal{N} = 1 + \sum_{i=1}^{3}\Big(M_i\Big) + M_1M_2\Lambda_{(I_1,I_2/k)} + M_1M_3\Lambda_{(I_1,I_3/k)} + M_2M_3\Lambda_{(I_2,I_3/k)}$$

$$= 1 + \Big(8+12+8\Big) + \Big(8\cdot 12\cdot(0)\Big) + \Big(8\cdot 8\cdot(0)\Big) + \Big(8\cdot 8\cdot(1)\Big)$$

$$= 1 + 28 + 72 = 101 \quad \textit{homomorphisms}$$

Theorem 2.18. *[4, Theorem 2]*

The number of ring homomorphisms:

$$\phi: \ \mathbb{Z}_{m_1}[\theta] \times \mathbb{Z}_{m_2}[\theta] \times \cdots \times \mathbb{Z}_{m_r}[\theta] \ \rightarrow \ \mathbb{Z}_{p^k}[\theta] \quad {}^{\{13\}}$$

$$is \quad C_k$$

$$where \quad C_k = \begin{cases} 1 + N_{p^k}(m_1, m_2, \ldots, m_r) & if \quad either \quad p^k \equiv 2 \quad or \quad p \equiv 3 \mod 4 \\ (m+1)N_{p^k}(m_1, m_2, \ldots, m_r) & if \quad p^k = 4 \\ (1+2m)N_{p^k}(m_1, m_2, \ldots, m_r) & if \quad p^k = 2^k, \quad k \geq 3 \\ 1 + 8N_{p^k}(m_1, m_2, \ldots, m_r) & if \quad p \equiv 1 \mod 4 \end{cases}$$

Proof.

Let $\phi : \mathbb{Z}_{m_1}[\theta] \times \mathbb{Z}_{m_2}[\theta] \times \cdots \times \mathbb{Z}_{m_r}[\theta] \rightarrow \mathbb{Z}_{p^k}[\theta]$ be a ring homomorphism.

Then ϕ is completely determined by its action on $\phi(e_i)$ and $\phi(f_i)$ for $i = 1, 2, \ldots, r$, where:

e_j is the r-tuple with 1 in the j^{th} component and 0 elsewhere, and

f_j is the r-tuple with θ in the j^{th} component and 0 elsewhere.

Note, since for each $j = 1$, e_j is an idempotent in $\mathbb{Z}_{m_j}[\theta]$; then so is each $\phi(e_j)$ in $\mathbb{Z}_{p^k}[\theta]$.

And for $\phi(e_j) \neq 0$, $\phi(e_j) \neq 0$ for $i \neq j$

$\Rightarrow 0 = \phi(0) = \phi(e_i e_j) = \phi(e_i)\phi(e_j) \neq 0$, a contradiction.

So, if ϕ is not the zero homomorphism, then $\phi(e_i) \neq 0$ for exactly one value of i. And for that i, p^k must divide m_i; So we just need to compute the number of idempotent elements in $\mathbb{Z}_{p^k}[\theta]$. And since the idempotent elements are $\phi(e_i)$'s, satisfying the quadratic congruence $(\phi(e_i))^2 \equiv \phi(e_i) \mod p^k$, then the number of idempotent elements in $\mathbb{Z}_{p^k}[\theta]$ depends on the number of solutions to that quadratic congruence under different cases:

{13} θ as in *theorem* 2.14, page 83

Using the results in the proof of *theorem* (2.7) (page 63); we consider the solutions of the quadratic congruence: $x^2 \equiv x \mod p^k$, and following those cases in the proof of *theorem* (2.14), we get:

(i) $p^k = 2$, or $p \equiv 3 \mod 4$, we have only one solution, so if $N_{p^k}(m_1, m_2, \ldots, m_r)$ is the number of elements in the set $\{m_1, m_2, \ldots, m_r\}$ that are divisible by p^k.

Then we have the number of idempotent elements is:

$$\Big(1 + N_{p^k}(m_1, m_2, \ldots, m_r)\Big)$$

(ii) $p^k = 4$, The number of solutions is $(m+1)$, hence the number of idempotent elements is:

$$\Big((m+1)N_{p^k}(m_1, m_2, \ldots, m_r)\Big)$$

(iii) $p^k = 2^k$, $k \geq 3$, the number of solutions is $(2m+1)$, hence the number of idempotent elements is:

$$\Big((2m+1)N_{p^k}(m_1, m_2, \ldots, m_r)\Big)$$

(iv) $p \equiv 1 \mod 4$, then we have 8 solutions for each m_i, and hence the number of idempotent elements is:

$$\Big(1 + 8N_{p^k}(m_1, m_2, \ldots, m_r)\Big)$$

□

Chapter 3

Conclusions and Future Work

3.1 Conclusions

We have considered the number of ring homomorphisms over special rings, namely:

- The ring, and rings related to the ring of Integers, $\mathbb{Z}$.
- The ring, and rings related to the ring of Gaussian integers, $\mathbb{Z}[i]$.
- The ring, and rings related to the ring of Eisenstein integers, $\mathbb{Z}[\rho]$.
- The ring, and rings related to the ring of a certain algebraic number, $\mathbb{Z}[\theta]$ where θ is an algebraic number and $\mathbb{Z}[\theta]$ is a unique factorization domain (UFD) under certain conditions.

Secondly, we were able to reach new generalizations concerning the number of ring homomorphisms over the ring of integers, $\mathbb{Z}$ and rings related to it as well as those of certain rings of an algebraic number subject to specific condtions, namely: $\mathbb{Z}[\theta]$ and its quotient rings where θ is an algebraic integer with minimal polynomial: $p(x) = x^2 + ux + v$ where $m = |u^2 - 4v|$ is a prime. These original results were marked with an asterisk (*).
We have given some examples in order to illustrate how to use the formulas given in the theorems. It's clear from the examples that these formulas are much easier to use than the regular methods of finding the ring homomorphisms.

3.2 Future Work

I think that it would be interesting to consider the number of ring homomorphisms over:

- The ring of algebraic integers $\mathbb{Z}[\theta]$ where θ is an algebraic integer whose minimal polynomial is: $P(x) = x^2 + ux + v$, where the radicand, $(u^2 - 4v) = m$, and m is a square free integer (not necessarily a prime).

- The quadratic number fields $\mathbb{Q}[\theta]$ where θ is an algebraic *number* with certain minimal quadratic polynomial (whose coefficients $\in \mathbb{Q}$) under certain conditions.

- The ring of cubic algebraic integers $\mathbb{Z}[\theta]$ where θ is an algebraic integer with simple minimal *cubic* polynomial with coefficients $\in \mathbb{Z}$.

I do believe that these problems are worth working on; for they open the way to reach wider generalizations, and hence, to have a clearer conception about algebraic number fields and their relations.

References

[1] J. A. Gallian and J. Van Buskirk, "The Number of Homomorphisms from Z_m into Z_n" *American Mathematical Monthly* 91(1984) : 196 − 197.

[2] J. A. Gallian and D. S. Jungreis, "Homomorphisms from $Z_m[i]$ into $Z_n[i]$ and $Z_m[\rho]$ into $Z_n[\rho]$, where $i^2 + 1 = 0$ and $\rho^2 + \rho + 1 = 0$" *American Mathematical Monthly* $95(1988), 247 - 299$.

[3] Mohammad Saleh and Hasan Yousef, "The Number of Ring Homomorphisms from $Z_{m_1} \oplus Z_{m_2} \oplus \cdots \oplus Z_{m_r}$ into $Z_{k_1} \oplus Z_{k_2} \oplus \cdots \oplus Z_{k_s}$", *American Mathematical Monthly* 105(1998) : 259 − 260

[4] M. Saleh, H. Yousef, and J. Abu Hlail, "The number of ring homomorphisms from $Z_n[\xi] \times Z_m[\xi]$ into $Z_k[\xi]$, An-Najah J., $2000, 47 - 53$.

[5] M. Saleh and H. Yousef, "On The Number Of Group And Ring Homomorphisms". To appear.

[6] M. Saleh and H. Yousef, "The number of ring homomorphisms from $Z_{m_1}[\beta] \times \cdots \times Z_{m_r}[\beta]$ into $Z_{k_1}[\beta] \times \cdots \times Z_{k_s}[\beta]$, $\beta = i$, OR $\beta = \rho$, WHERE $i^2 + 1 = 0, \rho^2 + \rho + 1 = 0$", FJMS, $2000, 549 - 554$.

[7] M. Misaghian, "Factor Rings and their decompositions in the Eisenstein integers Ring $\mathbb{Z}[\omega]$", *American Journal Of Mathematics* 5 No. 1 (2013): 58 − 68.

[8] O. Alkam and E. Abu Osba, "On Eisenstein Integers Modulo n", *International Mathematical Forum* 5 No. 22 (2010): 1075 − 1082.

[9] G. Dresden and W. M. Dymáček, "Finding Factors of Factor Rings over the Gaussian Integers", *The Mathematical Association Of America Monthly* 112 (August - September 2005): $602 - 611$.

[10] Gallian, J. *Contemporary Abstract Algebra* 3rd ed, D.C. Heath And Company, Toronto, 1994.

[11] Mine, J.S. *Algebraic Number Theory*, February 11, 2008, James S. Milne, Recovered January 19, 2014, jmilne.org/math/CourseNotes/ANT300.pdf.

[12] Stein, W. *Algebraic Number Theory, A Computational Approach*, November 14, 2012, William Stein, Recovered March 11, 2014, sage.math.washington.edu/books/ant/ant.pdf.

[13] Hardy, G. and Write, E., *An Introduction to the Theory of Numbers* 6th ed, Oxford University Press, Oxford, 2008.

[14] Burton, M. David, *Elementary Number Theory* 3rd ed, Wm. C. Brown Publishers, Dubuque, IA, 1994.

[15] Niven, I., Zuckerman H. and Montgomery H., *An introduction to the theory of numbers* 5th ed, John Wiley and Sons Inc., New York, NY, USA, 1991.

[16] Neukirch, J. (Translated version by Schappacher N.) *Algebraic Number Theory*, Springer, Strasbourg, France, 1999.

[17] Reid, W. Legh, *The Elements of The Theory of Algebraic Numbers.* The Macmillan company, NY, 1910. New York.

[18] Mileti, J. R., *Algebraic Number Theory*, May 11, 2012, Joseph R. Mileti, Recovered March 7, 2014, math.grinnell.edu/ miletijo/m324s12/AlgNumNotes.pdf.