2016

An Exposition of the Eisenstein Integers

Sarada Bandara
Eastern Illinois University

The Graduate School
EASTERN ILLINOIS UNIVERSITY

Thesis Maintenance and Reproduction Certificate

FOR: Graduate Candidates Completing Theses in Partial Fulfillment of the Degree
Graduate Faculty Advisors Directing the Theses

RE: Preservation, Reproduction, and Distribution of Thesis Research

---

Preserving, reproducing, and distributing thesis research is an important part of Booth Library's responsibility to provide access to scholarship. In order to further this goal, Booth Library makes all graduate theses completed as part of a degree program at Eastern Illinois University available for personal study, research, and other not-for-profit educational purposes. Under 17 U.S.C. § 108, the library may reproduce and distribute a copy without infringing on copyright; however, professional courtesy dictates that permission be requested from the author before doing so.

Your signatures affirm the following:

- The graduate candidate is the author of this thesis.
- The graduate candidate retains the copyright and intellectual property rights associated with the original research, creative activity, and intellectual or artistic content of the thesis.
- The graduate candidate certifies her/his compliance with federal copyright law (Title 17 of the U. S. Code) and her/his right to authorize reproduction and distribution of all copyrighted materials included in this thesis.
- The graduate candidate in consultation with the faculty advisor grants Booth Library the non-exclusive, perpetual right to make copies of the thesis freely and publicly available without restriction, by means of any current or successive technology, including by not limited to photocopying, microfilm, digitization, or internet.
- The graduate candidate acknowledges that by depositing her/his thesis with Booth Library, her/his work is available for viewing by the public and may be borrowed through the library's circulation and interlibrary loan departments, or accessed electronically.
- The graduate candidate waives the confidentiality provisions of the Family Educational Rights and Privacy Act (FERPA) (20 U. S. C. § 1232g; 34 CFR Part 99) with respect to the contents of the thesis and with respect to information concerning authorship of the thesis, including name and status as a student at Eastern Illinois University.

I have conferred with my graduate faculty advisor. My signature below indicates that I have read and agree with the above statements, and hereby give my permission to allow Booth Library to reproduce and distribute my thesis. My adviser's signature indicates concurrence to reproduce and distribute the thesis.

Graduate Candidate Signature

NARAYANA MUDIYANSELAGE PUSHPAMALI SARADA KUMARI BANDARA
Printed Name

MASTER OF ARTS IN MATHEMATICS
Graduate Degree Program

Faculty Adviser Signature

ALEJANDRA ALVARADO
Printed Name

May 18, 2016
Date

Please submit in duplicate.

An Exposition of the Eisenstein Integers

(TITLE)

BY

Sarada P. Bandara

THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

M.A. Mathematics

IN THE GRADUATE SCHOOL, EASTERN ILLINOIS UNIVERSITY
CHARLESTON, ILLINOIS

2016

YEAR

I HEREBY RECOMMEND THAT THIS THESIS BE ACCEPTED AS FULFILLING
THIS PART OF THE GRADUATE DEGREE CITED ABOVE

5-5-2016
THESIS COMMITTEE CHAIR — DATE

5-11-16
DEPARTMENT/SCHOOL CHAIR OR CHAIR'S DESIGNEE — DATE

May 5, 2016
THESIS COMMITTEE MEMBER — DATE

05 May 2016
THESIS COMMITTEE MEMBER — DATE

May 5, 2016
THESIS COMMITTEE MEMBER — DATE

THESIS COMMITTEE MEMBER — DATE

AN EXPOSITION OF THE EISENSTEIN INTEGERS

N.M.P.S.K.Bandara

A thesis submitted for the degree of Master of Arts

May 2016

Abstract

In this thesis, we will give a brief introduction to number theory and prime numbers. We also provide the necessary background to understand how the imaginary ring of quadratic integers behaves.

An example of said ring are complex numbers of the form $\mathbb{Z}[\omega] = \{a+b\omega \mid a, b \in \mathbb{Z}\}$ where $\omega^2 + \omega + 1 = 0$. These are known as the Eisenstein integers, which form a triangular lattice in the complex plane, in contrast with the Gaussian integers, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ which form a square lattice in the complex plane. The Gaussian moat problem, first posed by Basil Gordon in 1962 at the International Congress of Mathematicians in Stockholm [7], asks whether it is possible to "walk" from the origin to infinity using the Gaussian primes as "stepping stones" and taking steps of bounded length.

Although it has been shown that one cannot walk to infinity on the real number line, taking steps of bounded length and stepping only on the primes, the moat problem for Gaussian and Eisenstein primes remains unsolved. We will provide the necessary background for the reader, then investigate the Eisenstein moat problem.

Acknowledgments

A great many people have contributed to this work. I owe my gratitude to all those people who have made this thesis possible and because of whom my graduate experience has been one that I will cherish forever.

Foremost, I would like to express my sincere gratitude to my advisor and the graduate coordinator in the Department of Mathematics and Computer Science, Dr. Alejandra Alvarado for the continued support in my graduate study and research, especially in using Mathematica which was a new software for me. Also I am thankful for her patience, motivation, enthusiasm, and immense knowledge. Her guidance helped me in all the time of research and writing of this thesis. I have been amazingly fortunate to have an advisor who gave me the freedom to explore on my own, and at the same time the guidance to recover when my steps faltered.

I would like to thank Prof. Stan Wagon, professor of Mathematics and Computer Science, Macalester College, St. Paul, Minnesota, who supported me by providing necessary materials and sharing his valuable ideas to make this research a success.

Further, I would like to thank Dr. Andrew Mertz, assistant chair of the department of Mathematics and Computer Science who gave me valuable support in installing Mathematica.

I would like to take this opportunity to express my gratitude to all of the faculty members in the Department of Mathematics and Computer Science for their help and support.

Last but not the least, I would like to thank my family, especially my husband Amila Kulatunga, for all his sacrifices, love and encouragement given for me to reach my journey to a happy end. I am thankful for my in-laws and all my loved ones for their support and love.

Contents

List of Figures

List of Tables

1 Introduction

Number theory is the study of the set of positive whole numbers. Carl Friedrich Gauss said "mathematics is the queen of the sciences and number theory is the queen of mathematics". The subject is vast; shaped and fascinated with many properties of numbers. As the mathematician Waclaw Franciszek Sierpinski said, "The progress of our knowledge of numbers is advanced not only by what we already know about them, but also by realizing what we yet do not known about them".

The ultimate question we wish to address is whether one can walk to infinity on the Eisenstein primes by taking steps of bounded length. Other rings of integers have been investigated, see [11]. We concentrate on the Gaussian and Eisenstein integers.

2 History of Number Theory and Prime Numbers

Babylonian started using a number system with a base of 60 and was developed by Sumerians, by 2500 BCE. However, early Babylonians further developed the idea of numbers and it is believed that they recorded it on "Babylonian tablets", around 2000 BCE. It is recorded that Pythagoras learned mathematics from Babylonians as they had a highly developed idea on mathematics at that time.

Pythagoras and his colleagues are the first set of people who classified the integers as odd, even, prime and composite numbers. Pythagoras linked numbers with geometry, one of his most famous discoveries among all is the **Pythagorean theorem**. It states that in a right angle triangle, the square of the hypotenuse is equal to the sum of the squares of the other two sides. This theorem stated algebraically as $a^2 + b^2 = c^2$ for a right angle triangle known as **Pythagorean triangles** with sides of lengths a, b and c where c is the hypotenuse. Integers that satisfy the equation $a^2 + b^2 = c^2$ are known as **Pythagorean triples** (a, b, c). It was discovered a Babylonian tablet belongs to around 1700 BCE that recorded list of Pythagorean triples with large integers. This is considered as the first historical evidence of arithmetic nature [10].

Around 300 BCE Euclid wrote a collection of thirteen books known as **Euclid's elements** and three of them mainly discuss the theory of numbers. He proved there are infinitely many primes and he discussed a method of finding Pythagorean triples. Further, he developed the idea of perfect numbers which was found by Pythagoras. Euclid proved that $2^{p-1}(2^p - 1)$ is an even perfect number whenever $2^p - 1$ is prime for any prime p.

After Euclid's discoveries there had not be seen a drastic development in number theory. But in 250 CE, the Greek mathematician Diophantus published a series of thirteen books consisting of solutions to both determinate and indeterminate equations. **Diophantine equations** are polynomial equations with integral coefficients in which we only consider integer solutions.

In early 17th century Marin Mersenne studied numbers of the form $2^n - 1$ for integer n. They were subsequently called **Mersenne numbers** and primes of this form are called **Mersenne primes**. As of January 2016, 49 Mersenne primes are known and the largest known prime number, $2^{74,207,281} - 1$, is a Mersenne prime.

In the late 1700's Legendre and Gauss independently were led to conjecture the following.

Theorem 2.1 (Prime Number Theorem)**.** *When x is large, the number of primes less than x, $\pi(x)$, is approximately equal to $x/\ln(x)$. In other words,*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

Later Hadamard and de la Vallée Poussin, independently, proved the statement in 1896. In 1949 Atle Selberg and Paul Erdos fascinated number theory providing an elementary proof for the Prime Number Theorem. This is one of the focal points in number theory recently.

Among them Schnirelmann proved that there is a number M such that any number n can be written as a sum of M or fewer primes. In 1956 Chinese mathematician Yin Wen Lin was able to prove for the above result the value of M should be less than or equal to 18.

In 1994, after 358 years since Fermat wrote his famous conjecture in the margin of a copy of Arithmetica by Diophantus, **Fermat's Last Theorem** was finally proved by Andrew Wiles.

Theorem 2.2 (Fermat's Last Theorem). *The equation* $x^n+y^n = z^n$ *has no nontrivial solutions if* $n \geqslant 3$.

3 Algebra Background

A **group** $(G, *)$ is a set G together with a binary operation $*$ that satisfies the following conditions:

- $(x * y) * z = x * (y * z), \forall x, y, z \in G$;
- there exists a unique element $e \in G$, called the **identity element**, such that for all $x \in G$, $e * x = x * e = x$;
- for each $x \in G$, there exists a unique element $x^{'} \in G$, called the **inverse of** x such that $x * x^{'} = x^{'} * x = e$.

A group $(G, *)$ is called an **abelian group** if $x * y = y * x, \forall x, y \in G$.

A **ring** $(R, +, \cdot)$ is a set R with two binary operations addition and multiplication such that $\forall\, a, b, c \in R$:

- $(R, +)$ is an abelian group;
- closed under multiplication;
- associativity, $(a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot b \cdot c$;
- distributivity, $a \cdot (b + c) = a \cdot b + a \cdot c$; $(a + b) \cdot c = a \cdot c + b \cdot c$.

For any ring $(R, +, \cdot)$ with a multiplicative identity is a **ring with unity**, denoted by **1**, if for all $r \in R, r \cdot 1 = 1 \cdot r = r$. For any ring $(R, +, \cdot)$, the additive identity is known as the **zero element**, denoted by **0**. That is 0 is the additive identity if for all $r \in R, r + 0 = 0 + r = r$. Any element r in a ring R with unity is called a **unit**

if it has a multiplicative inverse in R. A unit can be described as an element which divides 1. Any ring $(R, +, \cdot)$ is called a **commutative ring** if $\forall\, a, b \in R$, $a \cdot b = b \cdot a$. Further any two **nonzero** elements $a, b \in R$ are said to be **zero divisors** if $a \cdot b = 0$. From here onwards, we will use ab for $a \cdot b$.

An **ideal** in a commutative ring R with a unity is a subset I of R such that:

- $0 \in I$;
- if $a, b \in I$ then $a + b \in I$;
- if $a \in I, r \in R$ then $ra \in I$.

If every nonzero element of a ring R has a multiplicative inverse, then R is called a **division ring**. A commutative division ring is called a **field**.

Example 3.1. The set of all integers modulo p, $\mathbb{Z}_p$, where p is a prime, is a field.

An **integral domain** is simply defined as a commutative ring with unity with no zero divisors. In an integral domain the cancellation law holds for multiplication by a nonzero element. That is, a, b, c are elements in a ring R such that $a \neq 0$, then $a \cdot b = a \cdot c$ implies $b = c$.

Example 3.2. $\mathbb{Z}[x]$, the set of polynomials with integer coefficients, is an integral domain.

Any two elements a, b in an integral domain R are said to be **associates** if $a = u \cdot b$ for some unit $u \in R$. A **nonzero**, nonunit element $a \in R$ is said to be an **irreducible** element if whenever $a = x \cdot y$, where $x, y \in R$ then x or y is a unit. In other words, a is irreducible if $x \mid a$ implies x is either a unit or an associate of a. A nonzero, nonunit element $p \in R$ is said to be a **prime** if $p \mid ab$ implies $p \mid a$ or $p \mid b$. In an integral domain every prime element is an irreducible element, but the converse is not necessarily true.

Example 3.3. 2 is an irreducible element in $\mathbb{Z}[\sqrt{-5}]$. But it is not a prime in $\mathbb{Z}[\sqrt{-5}]$ as $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$ but $2 \nmid 1 + \sqrt{-5}$ or $2 \nmid 1 - \sqrt{-5}$.

An integral domain R is said to be an **Euclidean domain** if there is a function, often called a **valuation**, $\lambda : R\backslash\{0\} \to \mathbb{Z}^+$ satisfying the following properties:

- for all nonzero $a, b \in R$, $\lambda(a) \leqslant \lambda(ab)$;
- for all $a, b \in R$ with $b \neq 0$ there exists $c, d \in R$ with the property $a = bc + d$ and either $d = 0$ or $\lambda(d) < \lambda(b)$.

Example 3.4. $\mathbb{Z}$ with the valuation $\lambda(x) = |x|$, is a Euclidean domain.

Let R be a commutative ring with unity and let $a \in R$. A subset of R of the form, $I = \{ra : r \in R\}$ is called the **principal ideal** generated by a. An integral domain R is a **principal ideal domain** (PID) if every ideal in R is a principal ideal.

Example 3.5. Two examples of principal ideal domains are $K[x]$, the ring of polynomials over the field K; and $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ the Gaussian integers.

If ring R is a principal ideal domain, then any element $p \in R$ is a prime if and only if p is irreducible.

An ideal I in a ring R is called a **maximal ideal** if $I \neq R$ and the only ideals containing I are I and R. In other words, I is a maximal ideal of a ring R if there are no other ideals contained between I and R.

An integral domain R is said to be a **unique factorization domain** (UFD) if every nonzero, nonunit element has a unique factorization as a product of irreducible elements of R up to order of factors. In particular, $\mathbb{Z}$ is a unique factorization domain.

Theorem 3.1 (The Fundamental Theorem of Arithmetic)**.** *Every integer greater than* 1 *is either a prime or can be represented as a product of primes and this product is unique up to the order of the factors.*

Further, we have the following chain of class inclusions.

$$\text{field} \subset \text{Euclidean domain} \subset \text{PID} \subset \text{UFD} \subset \text{integral domain}$$

4 Quadratic Number Fields

An **algebraic number** is a complex number α which is a root of a polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0 = 0,$$

where $a_0, a_1, a_2, ...a_{n-1}, a_n \in \mathbb{Q}$, and $a_n \neq 0$.

Example 4.1. Every rational number r is an algebraic number. Since r is a root of the polynomial $f(x) = x - r$.

In particular, if coefficients are in $\mathbb{Z}$ and $a_n = 1$, and α is a root of the polynomial, we call α an **algebraic integer**.

Example 4.2. The complex number $\frac{1}{2}(-1+i\sqrt{3})$ is an algebraic integer as it satisfies the equation $x^2 + x + 1 = 0$.

Any complex number which is not algebraic is called **transcendental**.

Example 4.3. The numbers π and e are transcendental numbers.

If F is a field containing k as a subfield, then F is called a **field extension** of k and we write it as F/k. If F is an extension of k then the F can be considered as a vector space over k. The dimension of this vector space is called the **degree of the field extension** and denoted by

$$[F : k] = \text{degree of } F \text{ over } k.$$

An **algebraic number field** is a subfield of $\mathbb{C}$, obtained by adjoining a finite number of algebraic numbers $\alpha_1, \alpha_2, ..., \alpha_n$ to $\mathbb{Q}$. This field is of the form $\mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$.

Theorem 4.1. *[1] If K is an algebraic number field, then there exists an algebraic number θ such that $K = \mathbb{Q}(\theta)$.*

Example 4.4. The algebraic number field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, is equal to $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, see [1].

In this thesis we will only consider algebraic extensions F, of $\mathbb{Q}$, of degree 2, also called a **quadratic field**. Hence F is of the form $\mathbb{Q}(\alpha)$ such that α is a root of an irreducible quadratic polynomial $x^2 + ax + b \in \mathbf{Q}[x]$.

Every quadratic field F can be written in the form $\mathbb{Q}(\sqrt{m})$, where m is a square free integer not equal to 1. Any element in $\mathbb{Q}(\sqrt{m})$ can be written in the form, $a + b\sqrt{m}$, with $a, b \in \mathbb{Q}$.

Example 4.5. $\mathbb{Q}(\sqrt{2})$ is a degree 2 field extension of $\mathbb{Q}$, with basis $\{1, \sqrt{2}\}$.

5 The Ring of Integers

It is well known that an integral domain D can be enlarged to (or embedded in) a field K such that every element in K can be expressed as a quotient (or fraction) of two elements of D. Often, K is denoted by **Frac**(D), and called the **field of fractions of** D or the **fraction field**.

Example 5.1. The fraction field of $\mathbb{Z}$ is the set of rational numbers $\mathbb{Q}$. Similarly we can define $\mathbb{Q}(i)$ as the fraction field of $\mathbb{Z}[i]$. In general the fraction field of $\mathbb{Z}[\sqrt{m}]$ is $\mathbb{Q}(\sqrt{m})$ for any integer m. On the other hand, if we ask what does the set of algebraic integers that lie in $\mathbb{Q}(\sqrt{m})$, look like, it is not necessarily $\mathbb{Z}[\sqrt{m}]$.

Theorem 5.1. *[1] Let K be a quadratic field. Let m be the unique square free integer such that $K = \mathbb{Q}(\sqrt{m})$. Then the set of algebraic integers in K is denoted by $\mathcal{O}_K$ and is given by,*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \not\equiv 1 (\text{mod } 4) \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & \text{if } m \equiv 1 (\text{mod } 4). \end{cases}$$

To distinguish between elements in $\mathcal{O}_K$ and elements in $\mathbb{Z}$, we will write "rational primes" and "rational integers" for those in $\mathbb{Z}$.

The norm of a rational integer is its absolute value. Hence we can conclude that for any integer u, $|u| = 1$ when $u = \pm 1$, the units in $\mathbb{Z}$. Further the set of integers forms a Euclidean domain with the norm function.

The **norm** of an element $\alpha \in \mathbb{Q}(\sqrt{m})$, is the product of $\alpha = a + b\sqrt{m}$ and its **conjugate** is defined by $\overline{\alpha} = a - b\sqrt{m}$, which is denoted by

$$N(\alpha) = \alpha \cdot \overline{\alpha} = a + b\sqrt{m} \cdot a - b\sqrt{m} = a^2 - b^2 m.$$

There are some important properties of the norm. Let α, β be two elements in $K = \mathbb{Q}(\sqrt{m})$, and $\mathcal{O}_K$ be its ring of integers.

- If $\alpha \in \mathcal{O}_K$, the norm function $N(\alpha)$ is a rational integer.
- $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.
- $N(\alpha) = \pm 1$ if and only if α is a unit of $\mathcal{O}_K$.
- If $N(\alpha) = \pm p$, where p is a rational prime,then α is irreducible.

Theorem 5.2. *[1] Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field with m be a square free integer. Then the unit group $U(\mathcal{O}_K)$ is given by,*

$$U(\mathcal{O}_K) = \begin{cases} \{\pm 1, \pm i\} \cong \mathbb{Z}_4 & \text{if } K = \mathbb{Q}(\sqrt{-1}) \\ \{\pm 1, \pm\omega, \pm\omega^2\} \cong \mathbb{Z}_6 & \text{if } K = \mathbb{Q}(\sqrt{-3}) \\ \pm 1 \cong \mathbb{Z}_2 & \text{otherwise} \end{cases}$$

where $\omega = \frac{-1+\sqrt{-3}}{2}$.

6 Factorization in Domains

In this section we discuss factorization in the Euclidean domains $\mathbb{Z}, \mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$.

In the ring of integers $\mathcal{O}_K$ for any quadratic field K, every integer can be uniquely expressed as a product of primes. This can be identified easily if we know the prime factors.

If we consider the ring of Gaussian integers $\mathbb{Z}[i]$, it behaves lot like $\mathbb{Z}$. Consider the integer 2, which is prime in $\mathbb{Z}$. In $\mathbb{Z}[i]$, this element is not prime since it factors into a product of primes, $2 = (1+i)(1-i)$. If $p = a^2 + b^2$ is a rational prime which can be written as a sum of two squares, then p is not irreducible as a Gaussian integer

since it can be factored as $p = (a+bi)(a-bi)$. Therefore, to consider the factorization in $\mathbb{Z}[i]$, we need to consider the norm. Factorization of Gaussian integers in $\mathbb{Z}[i]$ is not as obvious as in $\mathbb{Z}$.

Similarly, if we consider the rational prime 7, it is not prime in the Eisenstein integers $\mathbb{Z}[\omega] = \{a + b\omega | \, a, b \in \mathbb{Z}\}$, where ω was defined in theorem 5.2. The integer $7 = (3 + \omega)(2 - \omega)$ factors into a product of primes in $\mathbb{Z}[\omega]$. Eisenstein integers whose norm is a rational prime congruent to 0 or 1 modulo 3, are primes in $\mathbb{Z}[\omega]$. For example, $1 + 2\,\omega, 1 - \omega, -2 - \omega$ are such Eisenstein primes.

Further if we know $a + bi$ is a prime in $\mathbb{Z}[i]$, we can find all other primes associate with $a + bi$, as Gaussian integers have fourfold symmetry in the complex plane. But if we consider the prime $a + b\,\omega \in \mathbb{Z}[\omega]$, it's associates are not as easy to identify at a glance. We will discuss these associates in the next few sections.

7 Gaussian Integers

The ring of integers $\mathbb{Z}[i]$, in $\mathbb{C} \cong \mathbb{Q}(i)$, are known as **Gaussian integers**, first introduced by Carl Friedrich Gauss in 1832. It is the set of complex numbers of the form $a + ib$ where a, b are integers and denoted by $\mathbb{Z}[i]$. Recall for any complex number $z = a + bi$, its conjugate is defined by $\overline{z} = a - bi$. Also recall the norm of a Gaussian integer $a + bi$ is $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$. This norm can be shown to be a valuation on $\mathbb{Z}[i]$, hence $\mathbb{Z}[i]$ is an Euclidean domain, thus, a unique factorization domain.

The element $a + bi \in \mathbb{Z}[i]$ is said to be a **Gaussian prime** if it satisfies one of the following conditions:

- if $a = 0$, then b is a rational prime with $|b| \equiv 3 \pmod 4$;
- if $b = 0$, then a is a rational prime with $|a| \equiv 3 \pmod 4$;
- if both a and b are nonzero, then $N(a + bi) = a^2 + b^2 = p$ where p is a prime.

The Gaussian integers have the fourfold symmetry in the complex plane. This

implies if $a + bi$ is a Gaussian prime, then $\pm a \pm bi$ and $\pm b \pm ai$ are also Gaussian primes. Note that this is just the product of $a + bi$ with each of the four units.

A Gaussian integer γ is the **greatest common divisor** of two Gaussian integers α and β if γ divides each of them and any other common divisor of α and β divides γ [2]. In other words a greatest common divisor γ of α and β is a common divisor of α and β such that $N(\gamma)$ is largest. If the $N(\gamma)$ is 1, then α and β are relatively prime.

Theorem 7.1. *If α and β in $\mathbb{Z}[i]$ with $\beta \neq 0$, then there exist Gaussian integers q and r such that $\alpha = q \cdot \beta + r$ and $0 \leqslant N(r) < N(\beta)$.*

Example 7.1. We will show how to determine the $\gcd(24 - 9i, 3 + 3i)$ by applying the above Euclidean algorithm several times. Take $\alpha_1 = 24 - 9i$ and $\beta_1 = 3 + 3i$. Then consider the following ratio,

$$\begin{aligned}\frac{\alpha_1}{\beta_1} &= \frac{24 - 9i}{3 + 3i} \\ &= \frac{(24 - 9i)(3 - 3i)}{(3 + 3i)(3 - 3i)} \\ &= \frac{5}{2} - \frac{11}{2}i\end{aligned}$$

Take the nearest integers to the real and imaginary parts of the number above. It will not matter whether you round up or down, see [2]. Thus take 3 be the nearest integer to $\frac{5}{2}$ and 5 as the nearest integer to $\frac{11}{2}$. Then,

$$\begin{aligned}q_1 &= 3 - 5i \\ r_1 &= \alpha_1 - q_1 \cdot \beta_1 = -3i\end{aligned}$$

Next take $\alpha_2 = 3 + 3i$ and $\beta_2 = -3i$. Then,

$$\begin{aligned}\frac{\alpha_2}{\beta_2} &= \frac{3 + 3i}{-3i} = -1 + i \\ \alpha_2 &= (3 + 3i) = (-1 + i) \cdot (-3i) + 0 \\ q_2 &= -1 + i \\ r_2 &= 0\end{aligned}$$

Table 1:

α	β	q	r
$24-9i$	$3+3i$	$3-5i$	$-3i$
$3+3i$	$-3i$	$-1+i$	0

Hence $\gcd(24-9i, 3+3i) = -3i$. Had we rounded differently, the greatest common divisor of $24-9i$ and $3+3i$ would have been an associate of $-3i$. Table 1 summarizes the values of α, β, q and r at each step.

8 Eisenstein Integers

Consider the integral domain $\mathbb{Z}[\sqrt{-3}]$. Notice that it fails unique factorization, since for example,

$$4 = 2 \cdot 2 = (-1+\sqrt{-3})(-1-\sqrt{-3}).$$

If we instead consider a new element $\omega = \frac{-1+\sqrt{-3}}{2}$, it is clear that ω is not in $\mathbb{Z}[\sqrt{-3}]$, but it is in the fraction field of $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Q}(\sqrt{-3}) \simeq \mathbb{Q}(\omega)$. Notice also that ω is a cubic root of unity, in other words, a root of $x^3 - 1 = (x-1)(x^2+x+1) = 0$. The **Eisenstein integers** are the ring of integers, $\mathbb{Z}[\omega]$, in $\mathbb{Q}(\omega)$. Since $\omega^2+\omega+1 = 0$ we have $\omega^2 = -\omega - 1$ and it can be shown that ω^2 is the other root of $x^2+x+1 = 0$. In other words, $\bar{\omega} = \omega^2$, of ω. In this ring, we have,

$$4 = 2 \cdot 2 = (2 \cdot \omega)(2 \cdot \overline{\omega}) = (-1+\sqrt{-3})(-1-\sqrt{-3})$$

which is a unique factorization of 4, up to associates. We will show that the Eisenstein integers forms a unique factorization domain.

Recall the norm of $a + b\,\omega$, or the norm of $a + b\,\omega^2$, is

$$N(a+b\,\omega) = (a+b\,\omega)(a+b\,\omega^2) = a^2 + b^2 - ab.$$

If $N(a+b\,\omega) = \pm 1$ then $a+b\,\omega$ is a unit. It can be shown that the set of all units in Eisenstein integers are $\{\pm 1, \pm\omega, \pm\omega^2\}$. It can also be shown that this norm is a

valuation for the Eisenstein integers, which implies this ring is a Euclidean domain, hence a unique factorization domain.

An Eisenstein integer $a+b\,\omega$ is said to be an **Eisenstein prime** if it satisfies one of the following conditions:

- $b = 0$ and $a = p$ prime with $p \equiv 2 \pmod 3$;
- $a = 0$ and $b = p$ prime with $p \equiv 2 \pmod 3$;
- $N(a+b\,\omega) = a^2 - ab + b^2 = p$, where p is a prime such that $p = 3$ or $p \equiv 1 \pmod 3$.

Eisenstein primes are the irreducible elements in $\mathbb{Z}[\omega]$, since $\mathbb{Z}[\omega]$ is a PID. If $a + b\,\omega$ is an Eisenstein prime then so are its associates,

$$\{\pm(a + b\,\omega), \pm(b + (b - a)\,\omega), \pm((a - b) + a\,\omega)\}$$

as well as conjugates

$$\{\pm(b + a\,\omega), \pm(a + (a - b)\,\omega), \pm((b - a) + b\,\omega)\}.$$

So the primes in $\mathbb{Z}[\omega]$ are not as easily identifiable as the Gaussian and rational primes.

The largest known rational prime which is an Eisenstein prime is $19249 \cdot 2^{13018586} + 1$, the eleventh largest known rational prime found in 2013, see [4].

We are now interested in factoring Eisenstein integers. Factoring rational integers, and even Gaussian integers, is straightforward since there are only two and four units, respectively. Factoring Eisenstein integers becomes more difficult as there are six units. We begin with some preliminary results.

Theorem 8.1. *Let $\alpha \in \mathbb{Z}[\omega]$ be a prime, then $\mathbb{Z}[\omega]/\alpha\mathbb{Z}[\omega]$ is a field with $N(\alpha)$ elements.*

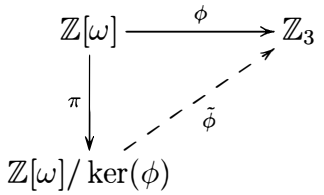
The above theorem was proved in [9] for the following two cases:

- when $N(\alpha) = p$, where $p \equiv 1 (\mathrm{mod}\ 3)$ is a prime;
- when $\alpha = p$ for a rational prime $p \equiv 2 (\mathrm{mod}\ 3)$.

Below we give the proof for the above theorem for the case $N(\alpha) = 3$.

Theorem 8.2. *If $a + b\omega \in \mathbb{Z}[\omega]$, then $a + b\omega$ is congruent to either $0, 1$ or -1 modulo $1 - \omega$.*

Proof. Consider the map $\phi : \mathbb{Z}[\omega] \to \mathbb{Z}_3$ such that, $\phi(x + y\,\omega) \equiv x + y \pmod 3$. We will use the first isomorphism theorem for rings to show that $\mathbb{Z}[\omega]/\langle 1 - \omega \rangle \mathbb{Z}[\omega] \cong \mathbb{Z}_3$.



- **ϕ is a homomorphism.**

  Take $x_1 + y_1\,\omega$, $x_2 + y_2\,\omega \in \mathbb{Z}[\omega]$.

$$\begin{aligned}
\phi((x_1 + y_1\,\omega) + (x_2 + y_2\,\omega)) &= \phi((x_1 + x_2) + (y_1 + y_2)\omega) \\
&\equiv ((x_1 + x_2) + (y_1 + y_2)) \pmod 3 \\
&\equiv ((x_1 + y_1) + (x_2 + y_2)) \pmod 3 \\
&\equiv ((x_1 + y_1) \pmod 3) + ((x_2 + y_2) \pmod 3) \\
&= \phi(x_1 + y_1\,\omega) + \phi(x_2 + y_2\,\omega)
\end{aligned}$$

$$\begin{aligned}
\phi((x_1 + y_1\,\omega) \cdot (x_2 + y_2\,\omega)) &= \phi(x_1x_2 + x_1y_2\,\omega + y_1x_2\,\omega + y_1y_2\,\omega^2) \\
&= \phi(x_1x_2 + x_1y_2\,\omega + y_1x_2\,\omega + y_1y_2\,(-1 - \omega)) \\
&= \phi[(x_1x_2 - y_1y_2) + (x_1y_2 + y_1x_2 - y_1y_2)\,)\omega] \\
&\equiv (x_1x_2 - y_1y_2) + (x_1y_2 + y_1x_2 - y_1y_2) \pmod 3 \\
&\equiv x_1x_2 + x_1y_2 + y_1x_2 - 2y_1y_2 \pmod 3 \\
&\equiv x_1x_2 + x_1y_2 + y_1x_2 + y_1y_2 \pmod 3 \\
&\equiv x_1(x_2 + y_2) + y_1(x_2 + y_2) \pmod 3 \\
&\equiv ((x_1 + y_1) \pmod 3) \cdot ((x_2 + y_2) \pmod 3) \\
&= \phi(x_1 + y_1\,\omega) \cdot \phi(x_2 + y_2\,\omega)
\end{aligned}$$

- ϕ **is surjective**.

  For any $x+y \in \mathbb{Z}_3$ there exists an element $x+y\,\omega \in \mathbb{Z}[\omega]$ such that $\phi\,(x+y\,\omega) \equiv x+y\,(\mathrm{mod}\,3)$.

- **Ker** $\phi = \langle 1-\omega \rangle$.

  Let $x+y\,\omega \in$ Ker ϕ. Then $\phi(x+y\,\omega) = x+y \equiv 0\,(\mathrm{mod}\,3)$. Hence $x+y = 3k$ for some $k \in \mathbb{Z}$. Then,

  $$\frac{x+y\,\omega}{1-\omega} = \frac{x+y\,\omega}{1-\omega}\cdot\frac{1-\omega^2}{1-\omega^2} = \frac{2x-y}{3}+\frac{x+y}{3}\,\omega = \frac{3x-(x+y)}{3}+\frac{(x+y)}{3}\,\omega = j+k\,\omega,$$

  such that k and $j = x-k$ are integers. Therefore,

  $$x+y\,\omega = (1-\omega)(j+k\,\omega).$$

  Thus, $x+y\,\omega \in \langle 1-\omega \rangle \implies$ Ker $\phi \subseteq \langle 1-\omega \rangle$

  Take any element $a+b\,\omega \in \langle 1-\omega \rangle$.

  Then there exists $c+d\,\omega \in \mathbb{Z}[\omega]$ such that $a+b\,\omega = (1-\omega)(c+d\,\omega)$.

  $$\begin{aligned}\phi(a+b\,\omega) &= \phi(1-\omega)\cdot\phi(c+d\,\omega)\\ &= (1-1)\cdot\phi(c+d\,\omega)\,(\mathrm{mod}\,3)\\ &= 0\,(\mathrm{mod}\,3)\end{aligned}$$

  $a+b\,\omega \in$ Ker ϕ. Therefore,$\langle 1-\omega \rangle \subseteq$ Ker ϕ.

  Hence Ker $\phi = \langle 1-\omega \rangle$.

We have shown that every element in $\mathbb{Z}[\omega]$ is congruent to 0, 1, or, -1 modulo $1-\omega$. □

If π is a prime in $\mathbb{Z}[\omega]$, we say that π is a **primary prime** if $\pi \equiv 2\,(\mathrm{mod}\,3)$. The last theorem in this section shows a particular way of expressing an Eisenstein integer in factored form.

Theorem 8.3. *[8] Suppose that* $N(\pi) = p \equiv 1(\mathrm{mod}\,3)$. *Among the associates of* π *exactly one is primary .*

Theorem 8.4. *For $\mu \in \mathbb{Z}[\omega]$, we can write $\mu = (-1)^a \omega^b (1-\omega)^c \prod_{i=1}^{n} \pi_i^{a_i}$, where a, b, c and a_i are nonnegative integers and π_i are primary primes.*

Proof. Let $a + b\,\omega \in \mathbb{Z}[\omega]$ be prime. Then we have the following three cases.

- If $N(a + b\,\omega) = p$, for any rational prime p with $p \equiv 1 (\mathrm{mod}\, 3)$, then $a + b\omega =$ (unit) $\cdot$ (primary prime);
- $a + b\,\omega =$ (unit) $\cdot\, p$ where $p \in \mathbb{Z}$ is prime such that $p \equiv 2\,(\mathrm{mod}\, 3)$;
- $a + b\,\omega =$ (unit) $\cdot\, (1 - \omega)$.

Since $\mathbb{Z}[\omega]$ is a UFD, any Eisenstein integer μ can be factored uniquely as follows,

$$\mu = (-1)^a \omega^b (1-\omega)^c \prod_{i=1}^{n} \pi_i^{a_i}$$

where π_i are primary primes. □

Example 8.1. With the aid of some shared functions, code was written in Mathematica to factor

$$15 + 12\omega = -\omega^2 (1-\omega)^3 (2 + 3\omega).$$

The following figures are of the Gaussian and Eisenstein primes in the complex plane, [5], [6].

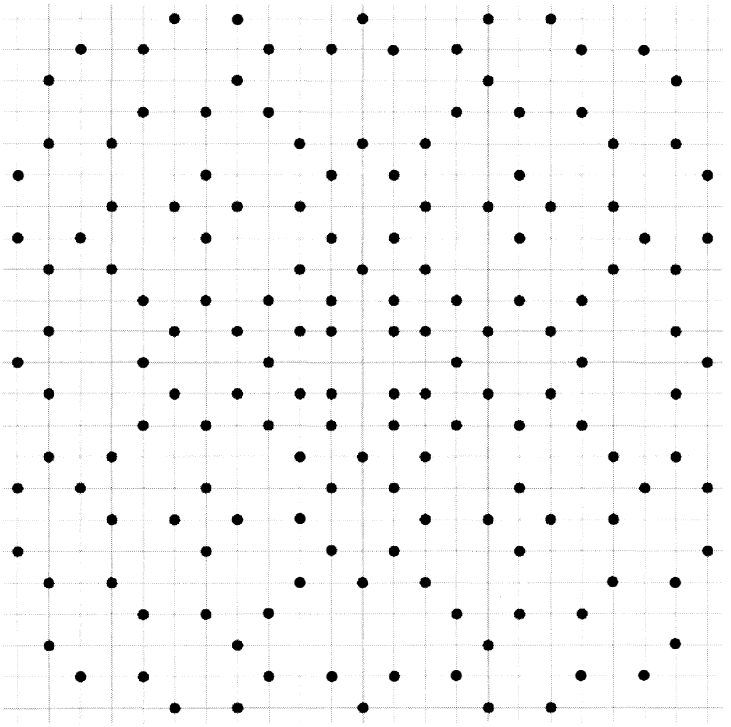


Figure 1: Gaussian Primes

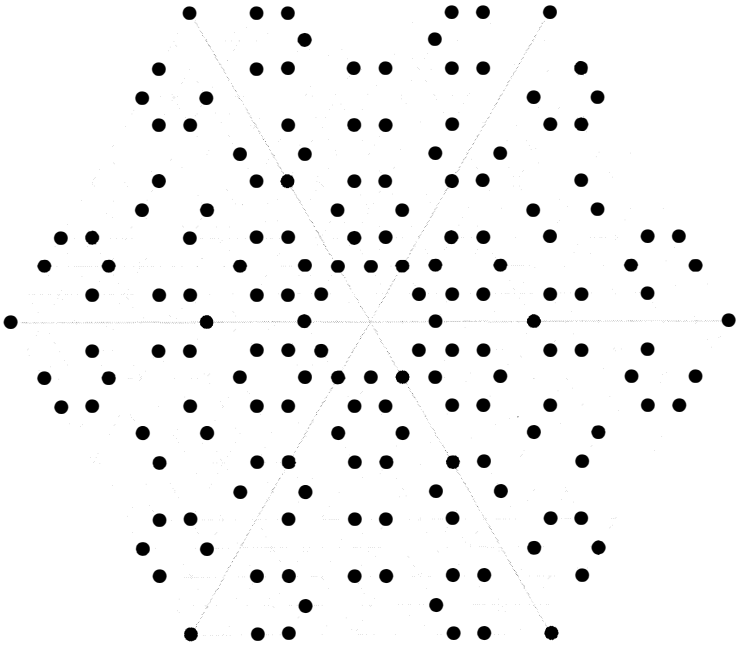


Figure 2: Eisenstein Primes

9 Prime Factorization in Quadratic Fields

A proper ideal P of an integral domain D is called a **prime ideal** if $a, b \in D$ and $a \cdot b \in P$ implies $a \in P$ and $b \in P$. Each prime ideal in $\mathcal{O}_K$ where K is an algebraic number field, is associated with a unique rational prime.

Theorem 9.1. *[1] Let K be an algebraic number field. Let P be a prime ideal of $\mathcal{O}_K$. Then there exists a unique rational prime p such that $P \mid \langle p \rangle$.*

The rational prime p is called the prime lying below P as $P \supseteq \langle p \rangle$. On the other hand, given a rational prime p, if a prime ideal P divides $\langle p \rangle$, we say P is a prime ideal lying over p.

Let I be a nonzero ideal in $\mathcal{O}_K$. We define $N(I)$, the **norm of** I, to be the number of elements in $\mathcal{O}_K/I$. It can be shown that $N(I) = |\mathcal{O}_K/I|$ is finite, as well as the multiplicative property holds.

Theorem 9.2. *[1] Let K be an algebraic number field with $[K : \mathbb{Q}] = n$. Let P be a prime ideal of $\mathcal{O}_K$. Let p be the rational prime lying below P. Then,*

$$N(P) = p^f$$

for some integer $f \in \{1, 2, ..., n\}$.

The positive integer f is called the **inertial degree of P in $\mathcal{O}_K$.** If P is a nonzero prime ideal of $\mathcal{O}_K$, then the factor ring $\mathcal{O}_K/P$ is a finite field.

Theorem 9.3. *Let K be an algebraic number field with $[K : \mathbb{Q}] = n$. Let p be a rational prime. Suppose that the principal ideal $\langle p \rangle$ factors in $\mathcal{O}_K$ in the form*

$$\langle p \rangle = P_1^{e_1} \cdot P_2^{e_2} \cdot ... \cdot P_g^{e_g}$$

where $P_1, P_2, .., P_g$ are distinct prime ideals of $\mathcal{O}_K$ and $e_1, e_2, .., e_g$ are positive integers. Suppose that f_i is the inertial degree of P_i for $i = 1, 2, ..., g$. Then,

$$e_1 f_1 + e_2 f_2 + ... + e_g f_g = n$$

[1].

The positive integer g is called the **decomposition number of p in K**; the positive integer e_i is called the **ramification index of P_i in K**. Notice that since $e_i \geq 1$ and $f_i \geq 1$, we have $n \geq g$. In other words, the principal ideal generated by a rational prime p cannot split into a product of more than n distinct prime powers.

Consider the factorization of $\langle p \rangle$ in theorem 9.3. We say:

- p **splits** completely in K, if $g = n$. This implies $e_i = f_i = 1$ for all $1 \leqslant i \leqslant g$;
- p is **inert** in K if $g = 1$, $e_1 = 1$ and $f_1 = n$;
- p is **ramified** in K if $e_i > 1$ for some $i \in \{1, 2, ..., g\}$.

Recall that we are interested in quadratic fields, $K = \mathbb{Q}(\sqrt{m})$. Let p be a rational prime. According to the Theorem 9.3 we have $n = 2$, hence $g = 1$ or 2.

- If $g = 2$ then, $e_1 f_1 + e_2 f_2 = 2$. Therefore $e_i = f_i = 1$, $i = 1, 2$. This implies p splits in K. In other words, $\langle p \rangle = P_1 P_2$, where P_1 and P_2 are distinct prime ideals and $N(P_1) = N(P_2) = p$.
- If $g = 1$ then $e_1 f_1 = 2$ and we have two cases to consider.
  - If $e_1 = 1$ and $f_1 = 2$, then p is inert in K and $\langle p \rangle = P$ is a prime ideal of $\mathcal{O}_K$, and $N(P) = p^2$.
  - If $e_1 = 2$ and $f_1 = 1$ then p ramifies in K and $\langle p \rangle = P^2$ where $N(P) = p$.

Example 9.1. Let $K = \mathbb{Q}(\omega)$. We will consider examples of three cases above.

- Recall $p = 7$ is not an Eisenstein prime since $7 = (-1 - 3\omega)(2 + 3\omega)$, a product of Eisenstein primes. Thus, $\langle 7 \rangle = P_1 P_2$ such that these two ideals are generated by the prime factors of 7.
- Recall $p = 3$ is also not an Eisenstein prime since $3 = -(1 + 2\omega)^2$, such thats $1 + 2\omega$ is an Eisenstein prime. Thus $\langle 3 \rangle = P^2$ where P is generated by $1 + 2\omega$.
- Recall $p = 5$ is not only a rational prime but an Eisenstein prime. Then $\langle 5 \rangle$ is a prime ideal.

10 Dedekind Domains

An infinite sequence of ideals $\{I_n\}_{n\in\mathbb{N}}$ in an integral domain is said to be an **infinite chain** if

$$I_1 \subseteq I_2 \subseteq .... \subseteq I_n \subseteq ....$$

The above chain is said to be **terminating ascending chain** if there exists a positive integer n_0 such that,

$$I_n = I_{n_0}$$

for all $n \geq n_0$. A chain is said to be **strictly ascending chain** if

$$I_1 \subset I_2 \subset .... \subset I_n \subset ....$$

An integral domain in which every chain of ideals terminates or which does not contain a strictly ascending chain of ideals is called a **Noetherian domain**. Further, every principal ideal domain is a Noetherian domain.

Let S be a subring of a commutative ring R with unity. An element $r \in R$ is **integral** over S, if it is the root of a monic polynomial in $R[x]$. The **integral closure of S in R**, is the set of elements in R that are integral over S. A **Dedekind domain** is an integrally closed, Noetherian domain in which every nonzero prime ideal is a maximal ideal. A field has no nontrivial proper ideals, hence every field is a Dedekind domain.

Theorem 10.1. *[1] Every principal ideal domain R is a Dedekind domain.*

Proof. Since R is a principal ideal domain, it is a Noetherian domain. Further R is a unique factorization domain, hence it is integrally closed. Each prime ideal of R is a maximal ideal. Therefore R is a Dedekind domain. □

Further, any Dedekind domain is a unique factorization domain if and only if it is a principal ideal domain.

Theorem 10.2. *[1] Let K be an algebraic number field. Let $\mathcal{O}_K$ be the ring of integers of K. Then $\mathcal{O}_K$ is a Dedekind domain.*

Proof. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. Hence it is integrally closed. Further it is a Noetherian domain and its every nonzero prime ideal are maximal ideals. Therefore $\mathcal{O}_K$ is a Dedekind domain. □

Since $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ are the ring of integers of the algebraic number fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\omega)$ respectively, by Theorem 10.2, $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ are Dedekind domains.

Theorem 10.3. *[3] If $\mathcal{O}_K$ is the ring of integers in an algebraic number field K then every nonzero ideal I in $\mathcal{O}_K$ can be written uniquely as a product of powers of distinct prime ideals,*

$$I = P_1^{a_1} \cdot P_2^{a_2} \cdot ... \cdot P_n^{a_n}$$

where $P_1^{a_1}, P_2^{a_2}, ..., P_n^{a_n}$ are distinct prime ideals and $a_i \geqslant 1$ for $i = 1, 2, ..., n$.

Theorem 10.4. *(Chinese Remainder Theorem [3]) Suppose R is a Dedekind domain and $P_1, P_2, ..., P_n$ are distinct prime ideals in R and $a_i \geqslant 0$ are integers for $i = 1, 2, ..., n$. Let I be as in theorem 10.3. Then,*

$$R/I \cong R/P_1^{a_1} \times R/P_2^{a_2} \times .... \times R/P_n^{a_n}$$

Further for any elements $r_1, r_2, ...r_n \in R$ there exists an element $r \in R$ unique up to an element in $P_1^{a_1}, P_2^{a_2}, ..., P_n^{a_n}$ with,

$$\begin{aligned} r &\equiv r_1 (\mathrm{mod} P_1^{a_1}) \\ r &\equiv r_2 (\mathrm{mod} P_2^{a_2}) \\ &\dots \\ r &\equiv r_n (\mathrm{mod} P_n^{a_n}). \end{aligned}$$

This theorem will have an important application in the Moat problem.

11 The Moat Problem

Suppose someone wants to walk to infinity along the real line, taking steps only on the primes. Can this be done by taking steps of bounded length? The answer to this problem is no.

Theorem 11.1. *There are arbitrarily large gaps between consecutive primes.*

Proof. To find the gap of length n between two consecutive primes, consider the following consecutive integers.

$$(n+1)!+2, (n+1)!+3, (n+1)!+4, ..., (n+1)!+n, (n+1)!+(n+1)$$

It can be seen that the first number is divisible by 2, the second number is divisible by 3, the third number is divisible by 4 and so on. The last number is divisible by $n+1$. All consecutive numbers in the list are not primes. So the proof is complete. □

We are concerned with the analogy of the problem in the Gaussian integers. The Gaussian moat problem asks whether it is possible to walk to infinity on the Gaussian integers using the Gaussian primes as stepping stones and taking steps of bounded length.

As in the case for rational primes, if we can find moat of width k, for any k, then a walk to infinity on Gaussian primes would not exists. The problem was first posed in 1962 by Basil Gordon. Although it remains unsolved, first computational explorations of this problem were done by Jordan and Rabung in 1969, where they constructed moats of length $1, \sqrt{2}, 2, \sqrt{8}$ and $\sqrt{10}$, see [11].

In 1998, Ellen Gethner, Stan Wagon and Brian Wick constructed moats of width 4, $\sqrt{18}$, and showed the existence of a moat of width $\sqrt{26}$. Therefore they showed that the steps of length five are insufficient to reach infinity. Tschimura established the existence of moats of width $\sqrt{32}, \sqrt{34}$ and 6 in 2004 [7].

Since the Gaussian integers have the fourfold symmetry, the existence of a k-moat can be shown by considering the existence of such a path in the first octant of the plane. It has been conjectured that

$$\lim_{n\to\infty}(\sqrt{p_{n+1}} - \sqrt{p_n}) = 0$$

where p_n denotes the nth prime [7]. If this conjecture is true it support in proving existence of Gaussian moats. There would be not be an annular moat of composite Gaussian integers. Then circles, with Gaussian primes will be more crowded and one can travel far away from the origin in the complex plane.

In this thesis, we apply the moat problem to the Eisenstein integers. Eisenstein primes have sixfold symmetry in the complex plane. Hence it is sufficient to consider the first 30 degree angle in order to find the path to infinity on Eisenstein integers. The following theorem and proof is a restatement in terms of Eisenstein integers rather than the Gaussian integers [7].

Theorem 11.2. *Let L be a line that contains at least two distinct Eisenstein integers. There are Eisenstein integers $m \neq 0$ and b such that for $m = m_0 + m_1\omega$, m_0 and m_1 are relatively prime and the Eisenstein integer z is on this line if and only if there is an $x \in \mathbb{Z}$ such that $z = mx + b$.*

Proof. Let z_1 and z_2 be two Eisenstein integers on the line L. Let $b = z_1$ and $m' = z_2 - z_1 = a_1 + b_1\omega$. If $d = \gcd(a_1, b_1)$, let

$$\begin{aligned} m &= \frac{m'}{d} \\ &= \frac{a_1}{d} + \frac{b_1}{d}\omega \end{aligned}$$

where the coefficients are relatively prime. If follows that every point on this line is of the form $mx + b$.

If x is an integer, then $mx + b$ is an Eisenstein integer on the line. Suppose now z is an Eisenstein on the line. Then $z = mx + b$ and we will show that x is an integer. Recall $m = u + v\omega$ where u and v are relatively prime integers. Then $mx = ux + vx\omega = z - b$ is an Eisenstein integer. Thus, ux and uv are integers. Also, there exists integers r and s such that $ru + sv = 1$ and so $rux + svx = x$ is an integer. □

Theorem 11.3. *Let L be a line that contains at least two distinct Eisenstein integers and let k be a positive integer. There is an Eisenstein integer w on this line such that all Eisenstein integers within a distance k of w are composite.*

Proof. The proof is broken down into three cases. The first case, assume the line L is horizontal, so then we can set $m = 1$, see theorem 11.2. The second case, $m = \omega$, so this line L has slope $-\sqrt{3}/2$ in the complex plane. The third case, $m = m_0 + m_1\omega$ such that m_0 and m_1 are both nonzero.

Case I. Let $b = b_0 + b_1\,\omega$ and let $K = |b_1| + k$. Our goal will be to find an Eisenstein integer w_0 with the property that each Eisenstein integer z such that $|z - w_0| \leqslant K$ is composite. This follows that if $w = w_0 + b_1\omega$, then w is on L, and if z is any Eisenstein integer with the property that $|z - w| \leqslant k$, then z is composite.

The set of all Eisenstein integers z with the property that $|z| \leqslant K$ is a finite set, say with N elements, we may index its elements so that $z_j = u_j + v_j\,\omega$ with u_j and v_j being integers for $j = 1, ..., N$. Assume that $z_1 = 0$.

Inductively define a system of linear congruences $x \equiv a_j (\mathrm{mod}\, b_j)$, for $j = 1, ..., N$ so that;

- each a_j and b_j is an integer,
- each b_j is larger than 1,
- the b_js are pairwise relatively prime, and
- $z_j + a_j$ and b_j are not relatively prime.

Start with $a_1 = 0$ and $b_1 = 4$. The four conditions are satisfied. Now suppose that $a_1, ..., a_{j-1}, b_1, ..., b_{j-1}$ have been defined. Recall that $z_j = u_j + v_j\omega$. Next, we must find an integer s_j so that $s_j + v_j\omega$ has a Eisenstein prime factor p_j with the property that $p_j\overline{p_j}$ is larger than the product $b_1 \cdot b_2 \cdot .... \cdot b_{j-1}$. Let $s_j = v_j M$, where M is the product of all Eisenstein primes q such that $|q| < b_1 \cdot b_2 \cdot .... \cdot b_{j-1}$.

Then we have $s_j + v_j\,\omega = v_j(M + \omega)$, and the magnitude of any prime factor of $M + \omega$ is larger than $b_1 \cdot b_2 \cdot .... \cdot b_{j-1}$, as desired. Choose one such factor p_j. Now let $b_j = p_j\overline{p_j}$ and $a_j = s_j - u_j$. The four conditions stated above are trivially satisfied. The last condition follows from the identity $z_j + a_j = s_j + v_j\,\omega$. This concludes the induction.

Theorem 10.4 guarantees an infinite set of solutions to this system of linear congruences. Suppose w_0 is one of these solutions and let $P = \prod_{i=1}^{N} b_i$. We may assume that w_0 is larger than $P + K$. Let j be one of the integers $1, ..., N$. Since b_j and $z_j + a_j$ are not relatively prime, there is an Eisenstein prime q_j that divides them both. Since w_0 is a solution to the system of congruences, it follows that

$w_0 + z_j \equiv a_j + z_j (\mathrm{mod}\, b_j)$ and thus $w_0 + z_j \equiv 0 (\mathrm{mod}\, q_j)$. Since the magnitude of $w_0 + z_j$ is larger than $P(|w_0 + z_j| \geqslant ||w_0| - |z_j|| \geqslant |(P + K) - K| = P)$ and since the magnitude of q_j is less than P (q_j is a prime factor of the composite number P), the quotient $(\frac{w_0 + z_j}{q_j})$ has magnitude larger than 1. Hence, $w_0 + z_j$ is not an Eisenstein prime for $j = 1, ..., N$.

Case II. The proof is almost identical to the previous case, except instead of a horizontal line L, the line in the complex plane has slope $-\sqrt{3}/2$.

Case III. The proof is almost identical to case III in [7], and also easier to construct than case I. By applying theorem 10.4 and theorem 11.2, one will reach the appropriate conclusion.

□

Using Mathematica, Wagon plotted the graph of reachable Gaussian primes using steps of size at most two. The vertices of his graph are the Gaussian primes; the edges are those at distance two or less from one prime to the next. By slightly modifying his code, we plotted the graph of reachable Eisenstein primes also of steps of size at most two.

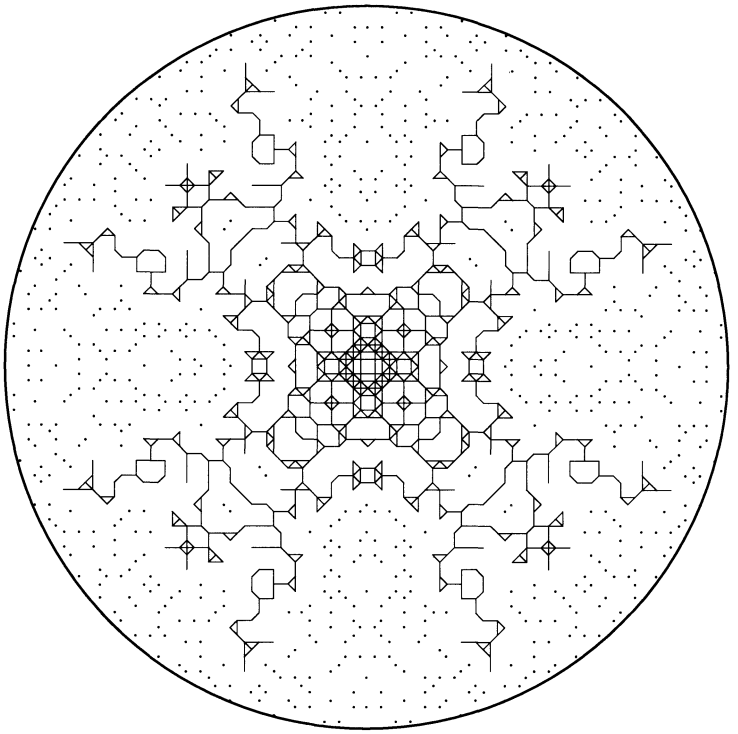


Figure 3: Gaussian Walk of steps of size at most two.

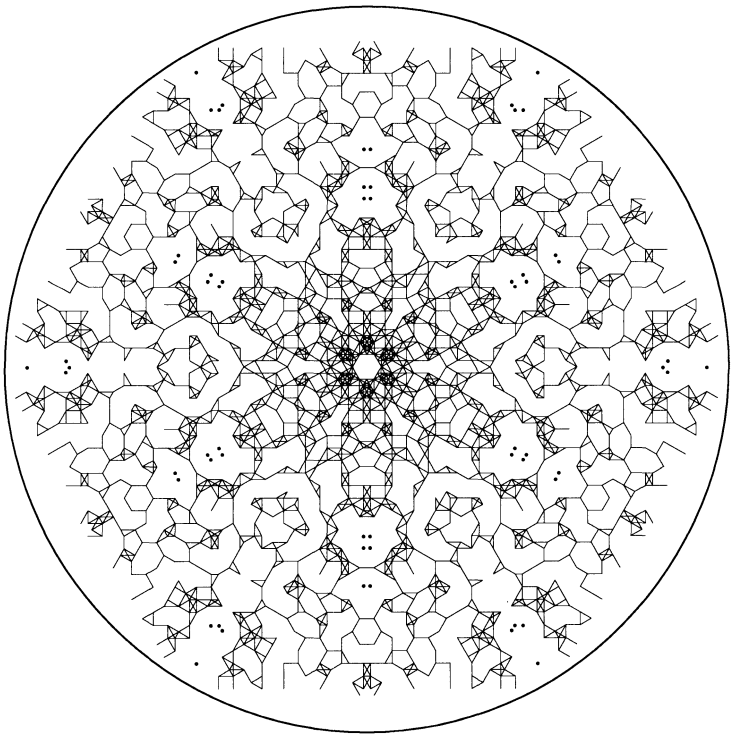


Figure 4: Eisenstein Walk of steps of size at most two.

12 Conclusion

In 1966 Stark showed that if $m = -1, -2, -3, -7, -11, -19, -43, -67, -163$, then the ring of imaginary integers $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{m})$ forms a principal ideal domain and these are the only imaginary quadratic ring of integers with unique factorization [8]. If $m = -1, -2, -3, -7, -11$, then $\mathcal{O}_K$ is a Euclidean domain. If $m = -19, -43, -67, -163$, then $\mathcal{O}_K$ is a unique factorization domain but not a Euclidean domain.

Pradad investigated the Moat problem for $m = -1, -2, -3, -7$ and steps of various sizes. He conjectured that moats of arbitrary large sizes exist, thus a walk to infinity impossible. He did find that among the four ring of integers, for a given step bound k, he was able to travel furthest away from the origin on the Eisenstein primes [11].

It would be interesting to also consider the case $m = -11$. Another comparison to make is whether m is, or is not, congruent to one modulo four. Will this make a difference in how far one can travel away from the origin, for a given step bound?

In this thesis, we used the software Mathematica to plot the prime walk for Eisenstein primes. It would be interesting to construct similar plots for other imaginary quadratic fields $\mathbb{Q}(\sqrt{m})$.

13 Appendix

The functions EisensteinIntegerQ, EisensteinUnits, EisensteinPrimeMod, EisensteinNorm, EisensteinPrimeQ, EisensteinToComplex, and EisensteinCoeffs are courtesy of Wagon via email communication.

Below is code for factoring an Eisenstein prime, as described in theorem 8.4.

```
Efactor[z_?EisensteinIntegerQ] :=
  Module[{Elist = {}, ei = Expand[z]},
  While[MemberQ[EisensteinUnits, ei] == False  && !SameQ[ei, 0],
    While[EisensteinPrimeMod[ei, 1 - ω] == 0,
      Elist = Append[Elist, 1 - ω];
```

```
      ei = Expand[ei*(1 - ω^2)/EisensteinNorm[1 - ω]]];
      For[a = 2-(EisensteinNorm[ei]-Mod[EisensteinNorm[ei], 3]),
        a <= EisensteinNorm[ei], a = a + 3,
        For[b = -(EisensteinNorm[ei]-Mod[EisensteinNorm[ei], 3]),
          b <= EisensteinNorm[ei], b = b + 3,
          If[EisensteinPrimeQ[a + b ω] == True,
            If[EisensteinPrimeMod[ei, a + b ω] == 0,
              Elist = Append[Elist, a + b ω];
              ei = Expand[ei*(a+bω^2)/EisensteinNorm[a+bω]]]]]]
  If[EisensteinPrimeQ[ei],
    For[i = 1, i <= 6, i++,
      If[Mod[EisensteinCoeffs[ei*EisensteinUnits][[i,1]],3]==2
      && Mod[EisensteinCoeffs[ei*EisensteinUnits][[i,2]],3]==0,
        Elist = Append[Elist, ei*EisensteinUnits[[i]]];
      ei = EisensteinUnits[[i]]]]];
      Elist = Append[Elist, ei]]
```

Below is code for finding the greatest common divisor g between two Eisenstein integers n_1 and n_2 as well as r_1 and r_2 such that $g = r_1 n + 1 + r_2 n_2$. This function is similar to ExtendedGCD in Mathematica.

```
EisensteinExtendedGCD[z_, u_] := Module[{erst = {{z, 1, 0},
  {u, 0, 1}}},
  While[EisensteinCoeffs[erst[[2, 1]]][[1]] != 0 ||
    EisensteinCoeffs[erst[[2, 1]]][[2]] != 0,
    uconjedit = EisensteinCoeffs[erst[[2, 1]]][[1]] +
      EisensteinCoeffs[erst[[2, 1]]][[2]]ω^2;
    qtedit =
      Floor[EisensteinCoeffs[Expand[erst[[1, 1]](uconjedit)]]/
        EisensteinNorm[erst[[2, 1]]]];
      (erst = {{0,1}, {1,-(qtedit[[1]] + qtedit[[2]]ω)}}.erst);];
  Expand[{erst[[1, 1]], erst[[1, {2, 3}]]}]]
```

Below is code for plotting the walk on the Eisenstein primes. This is a slightly

modified version of code found in [2].

```
Eplist60 = Select[Flatten[Table[{a - b/2, b*Sqrt[3]/2},
    {a, 0, 50}, {b, 0, a}], 1], EisensteinPrimeQ[#[[1]]
    + #[[2]]/Sqrt[3] + #[[2]]*2/Sqrt[3]* ω] &];
Steps = {}; For[i = 1, i <= 6, i++,
  Steps = Append[Steps,
    {Re[EisensteinToComplex[EisensteinUnits][[i]]],
    Im[EisensteinToComplex[EisensteinUnits][[i]]]}];
Steps = Append[Steps,
  {Re[EisensteinToComplex[2*EisensteinUnits][[i]]],
  Im[EisensteinToComplex[2*EisensteinUnits][[i]]]}];
Steps = Append[Steps,
  {Re[EisensteinToComplex[(2+ω)*EisensteinUnits][[i]]],
  Im[EisensteinToComplex[(2+ω)*EisensteinUnits][[i]]]}]];
Steps;
Neighbors[pt_, 2] := Select[Map[pt + # &, Steps],
  EisensteinPrimeQ[#[[1]]+#[[2]]/Sqrt[3]+#[[2]]*2/Sqrt[3]*ω] &]
Edges[p_, d_] := Map[Sort[{p, #}] &, Neighbors[p, d]];
Roads = Union[Flatten[Map[Edges[#, 2] &, Eplist60], 1]];
EFindComp[s_, {m_, n_}] :=
    Module[{New, Component, NewNeighbors, Compl},
    NewNeighbors[{3/2, Sqrt[3]/2}] :=
    Intersection[{{5/2, Sqrt[3]/2}, {7/2, Sqrt[3]/2},
    {1, Sqrt[3]}, {1/2, (3 Sqrt[3])/2}, {0, Sqrt[3]}, {2, 0},
    {5/2, -(Sqrt[3]/2)}, {3/2, -(Sqrt[3]/2)}, {2, Sqrt[3]},
    {5/2, (3 Sqrt[3])/2}}, Compl];
NewNeighbors[pt_] := Intersection[Map[pt+# &, Steps], Compl];
Component = New = {{m, n}};
  While[New != {}, Compl = Complement[s, Component];
    New = Union @@ (NewNeighbors /@ New);
    Component = Join[Component, New]]; Component]
Esymmetrize[{u_, v_}] := {{u, v}, {-u, -v}, {(u + v*Sqrt[3])/2,
```

```
  (v - u*Sqrt[3])/2}, {-(u + v*Sqrt[3])/2, -(v - u*Sqrt[3])/2},
  {(u - v*Sqrt[3])/2, (v + u*Sqrt[3])/2}, {-(u - v*Sqrt[3])/2,
  -(v + u*Sqrt[3])/2}};
Esymmetrize[{p_List, q_List}] :=
  Transpose[{Esymmetrize[p], Esymmetrize[q]}];
Esymmetrize[pts_List] :=
  Flatten[Esymmetrize /@ pts, 1] /; Depth[pts] == 5;
Efirst60 = Select[Roads, MemberQ[Component, #[[1]]] &];
RoadNetwork = Union[Flatten[Esymmetrize /@ Efirst60, 1]];
UnreachablePrimes = Union[Esymmetrize[Complement[Eplist60,
  Component]]];
Show[Graphics[{Circle[{0, 0}, 50], {AbsolutePointSize[2],
  Point /@ UnreachablePrimes}, {AbsoluteThickness[0.4],
  Line /@ RoadNetwork}}], AspectRatio -> Automatic]
```

References

[1] Alaca, Saban, and Williams, Kenneth S. (2004). *Introductory Algebraic Number Theory*, United Kingdom.: Cambridge University Press.

[2] Bressoud, David, and Wagon, Stan. (2000). *A Course in Computational Number Theory*, Emeryville, California, USA.: Key College Publishing.

[3] Dummit, David S., and Foote, Richard M. (2004). *Abstract Algebra*, River Street, Hoboken, NJ, USA.:John Wiley and Sons, Inc.111.

[4] Eisenstein prime. (2016, April 13). In *Wikipedia, The Free Encyclopedia.* Retrieved May 1, 2016 from https://en.wikipedia.org/wiki/Eisenstein_prime.

[5] Eisenstein prime image. (2016, April 13). In *Wikipedia, The Free Encyclopedia.* Retrieved May 1, 2016 https://commons.wikimedia.org/wiki/File:EisensteinPrimes-01.svg.

[6] Gaussian primes. (2010, August 8). In *Wikipedia, The Free Encyclopedia.* Retrieved May 1, 2016, from https://commons.wikimedia.org/wiki/File:Gaussian-primes.svg.

[7] Gethner, Ellen, Wagon, Stan, and Wick, Brian.(1998). *A stroll through the Gaussian primes*, The American Mathematical Monthly 105 (4) :pp 327–337, doi:10.2307/2589708, MR 1614871, Zbl 0946.11002.

[8] Ireland, Kenneth, and Rosen, Michael. (1972). *Elements of Number Theory-Including an Introduction to Equations Over Finite Fields*, Tarrytown on Hudson, New York/ Belmont, Calfornia, USA.: Bogden and Quigkey, Inc. Publishers.

[9] Ireland, Kenneth, and Rosen, Michael. (1990). *A Classical Introduction to Modern Number Theory*, New York, USA.: Springer-Verlag.

[10] Number theory. (2016, April 26). In *Wikipedia, The Free Encyclopedia.* Retrieved May 1, 2016, from https://en.wikipedia.org/wiki/Number_theory.

[11] Prasad, Siddharth. *Walks on primes in imaginary quadratic fields*, http://arxiv.org/pdf/1412.2310.pdf.

[12] Stillwell, John. (2003). *Elements of Number Theory*, New York, USA.: Springer-Verlag.