Prime-Generating Polynomials

Quadratics over norm-Euclidean Domains

by

Daniel Packer

A Thesis Submitted to the Faculty

in partial fulfillment of the requirements for the

Bachelor of Arts

Accepted

William Dunbar, Thesis Advisor

Timothy Susse, Second Reader

Ian Bickford, Provost and Vice President

ABSTRACT

This thesis examines the relationship between elements of integral domains and polynomials over those domains. Alternatively, we can view the same problem as examining the conditions necessary for a specific element to be representable as a sum of specific factors of powers of another element. The first chapter provides a summary of topics to be covered without proof or much examination of the precise structure. The second chapter describes the Algebraic and Number Theoretical bases that the remainder of the thesis is built around. Next, the third chapter introduces well-researched properties of prime-generating polynomials. The final chapter presents original research by the author that builds upon the findings presented in the second and third chapters.

ACKNOWLEDGEMENTS

While a thesis is theoretically a work produced by a singular individual, it would be unreasonable and dishonest to not recognize the people who have made it possible for me to write this thesis. Thank you to my thesis advisor, Bill Dunbar, whose adaptability to my own schedule and subject choice has made the process far less painful than it could have been and to Li-Mei Lim, who introduced me to the study of number theory. Thanks also to my parents, whose continued emotional (and financial) support has made pursuing a B.A. a possibility and to my sister, whose excitement over my work has probably exceeded my own. Finally, I would like to thank the Simon's Rock community, which has become my home over the past four years and remains the place where I feel most comfortable.

Contents

Chapter 1

For the Lay Reader

Number theory is frequently described as the study of the "natural numbers" (frequently denoted $\mathbb{N}$) [Apo13]:

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

The natural numbers are frequently called the "whole" or "counting" numbers. A *prime number* is a whole number that is not divisible by any other numbers (except for 1 and itself) and is not equal to one; non-prime whole numbers not equal to 1 are called composite. The first few prime numbers are

$$2, 3, 5, 7, 11, \ldots$$

While the smallest composite numbers are made of the remaining natural numbers (without 1):

$$4, 6, 8, 9, 10, 12, \ldots$$

Mathematicians have been studying prime numbers for millenia, and over the years our understanding of these numbers has developed and grown more subtle. The definition of a prime number can be restated in a variety of ways depending on what task we need them to solve. For instance, a number, p, is prime if and only if the only numbers that share a factor (not equal to one) with p are multiples of p. Another description is that if a prime

divides the product of two other numbers, then it also divides at least one of the two other numbers.

Initially, these numbers appear to be the more difficult sort to work with despite the variety of ways we can understand them. For instance, prime numbers lack divisibility, a property that frequently makes a number more simple to work with. It is for the sake of divisibility that eggs come in dozens and feet in twelve inches. Highly divisible numbers make the task of equal distribution significantly easier. If we want to share 12 slices of pie between 4 people, the task is simple: we give 3 slices to each person. However, if the total number of slices is prime, say 13, then there is no easy way to distribute the pie slices without either dividing a slice further, or getting 13 people to share the pie between. Thus, prime numbers often are an inconvenience in the real world because they are less manipulable than composite numbers.

However, these are practical applications that do not consider an understanding of the structure of numbers themselves. That is, the example described an everyday use of the numbers, where composite values appear to be more helpful. Within the field of number theory (the study of the structure of the integers—the positive and negative whole numbers), applying the properties of prime numbers often results in simplified proofs. The discovery of the Fundamental Theorem of Arithmetic provided a basis on which mathematicians built number theory by making a statement about the relationship between prime numbers and all natural numbers. The theorem states that every natural number is the product of a unique combination of prime numbers, called a "prime factorization". This tool allows us to entirely understand any natural number as the product of some (perhaps large) number of prime numbers without worrying about whether any properties we observe are a result of the specific factorization that we chose to represent the number. No matter how one goes about factoring a number, they will always arrive at the same prime factorization eventually. Frequently, this alternate understanding of a number eases our ability to prove properties of the natural numbers. Many properties of numbers are preserved under multiplication. An intuitive example is "square-ness;" the product of two square numbers is a square. We can

see this clearly through some simple algebra, $(a^2)(b^2) = abab = (ab)^2$. Many more subtle mathematical properties also follow this pattern, so if we can classify when a property is present in the set of primes, then we quickly discover how the property is realized in all numbers, since every number is uniquely a product of prime numbers.

For instance, we can consider the example from before with the tool of prime factorization. Suppose we want to check whether a number, n, is square. Then, we can express n as a product of primes in a unique way (up to reordering): $n = p_1 \cdot \ldots \cdot p_\ell$. Each prime alone is not a square, but the product of a prime with itself an even number of times is a square, so we can group each prime with each of its repetitions in the factorization, so we get $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, where $p_i \neq p_j$ if $i \neq j$. Furthermore, neither the product of a square with a non-square, nor the product of two non-squares that share no factors is a square. Thus, n is a square if each exponentiated prime, $p_i^{r_i}$, is square, which is only the case if r_i is even. By simply examining the prime factorization of a number, we were able to deduce properties of the number, such as whether it is a square. This convenient happenstance is ultimately because many of the properties of composite numbers are entirely determined by their prime factors, as the property of "square-ness" was.

Thus, most of the theory of the natural numbers (i.e., number theory), is based around understanding properties of the prime numbers, since the structure of all of the other numbers is heavily affected by the properties of these somewhat uncommon numbers. However, for all of the structure that the prime numbers provide, these numbers themselves have poorly understood structure themselves. Despite a simple definition, prime numbers occur almost randomly among the natural numbers. Only recently (in the timeline of number theory beginning at least as early as Euclid's time, 300 B.C.E.) have mathematicians developed a model for an approximate distribution of the prime numbers, and even then, there still is no proven estimate for how well the approximation holds. The specific result, known as the prime number theorem, states that as n gets very large, the number of prime numbers less than n will grow close to $\frac{n}{\ln(n)}$, where $\ln(n)$ is the natural logarithm of n. We have no (proven) bound on how quickly this approximation becomes accurate, but there are bounds

that appear to be true if we assume certain unproven conjectures [vK01]. Specifically, the needed assumption is that the Riemann hypothesis holds, which states that the function of complex numbers,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \tag{1.1}$$

known as the Riemann zeta function, is only equal to zero if the real part of the complex number s is $\frac{1}{2}$. Not only is this problem incredibly complicated and apparently far from being solved—there is a million dollar prize offered for its solution—but it also seems practically disconnected from the sorts of questions that we were considering when we asked about the distribution of primes. Before, we were considering the size of a subset of whole numbers, but somehow the question became about the nature of an infinite sum of complex numbers.

Number theory is rife with examples such as this, where questions about simple properties become unexpectedly complicated with little warning. Other classical questions of this sort include the Goldbach conjecture, which asks whether every even number greater than 2 is the sum of two prime numbers, and the twin prime conjecture, which asks if there are infinitely many primes with a difference of 2. Remarkably, there has been even less progress on these questions than there has been on the asymptotic[1] distribution of primes, which has at least been reduced to the Riemann hypothesis and received a vague approximation. A recent leap forward in the twin prime conjecture was the discovery that there are infinitely many primes within 600 of each other [May15]. However, the methods being applied in all of these approaches is vastly more complicated than the elementary phrasing needed to state the initial problems. This pattern is frequent within number theory and is particularly present when it comes to prime numbers, which maintain an incredible stubornness towards any sort of structured comprehension.

However, there does appear to be some inherent structure within the prime numbers, but quantifying this structure is not so easy. An illustration of this structure is a diagram known as the Ulam spiral seen in Figure 1.2. This image is generated by writing the natural

[1] Meaning the structure as numbers get arbitrarily large.

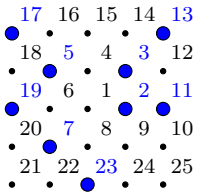

Figure 1.1: A demonstration of how the Ulam spiral is constructed.

numbers in an outward spiral, so that the numbers coil around themselves like a snake in the manner demonstrated in Figure 1.1 (where each point corresponds to the number to the upper right). Then, we mark out which of the written numbers is a prime. A cursory examination with even a relatively small spiral reveals an apparent but unclear pattern. In order to be convinced that the pattern is meaningful and distinguishable from white noise, compare Figures 1.3 and 1.2. While both figures appear to encode some amount of a pattern (the white noise is chosen to avoid marking numbers divisible by 2 or 3; we only marked numbers of the form $6n \pm 1$), the streaks are longer and more defined in the Ulam spiral than they were in the white noise.

The Ulam spiral demonstrates that though the prime numbers may appear to be distributed randomly, there is an underlying pattern in the numbers. In fact, the pattern we observe in the Ulam spiral is related to the properties of polynomials over the integers, which are functions of the form, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, where each a_i is an

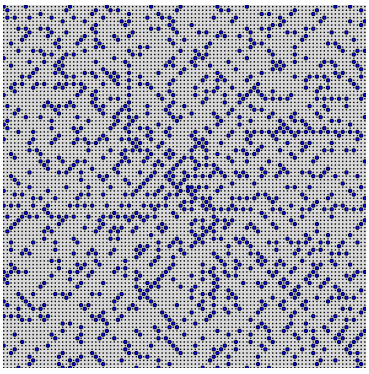

Figure 1.2: The Ulam spiral, where primes are marked, written out up to 11,000.

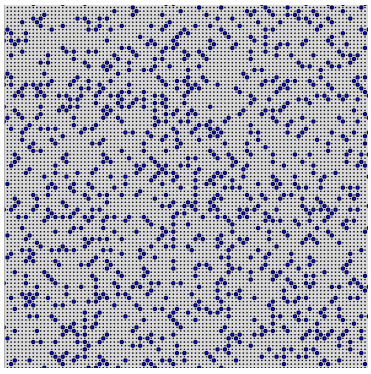

Figure 1.3: A "fake" Ulam spiral where random numbers of the form $6n \pm 1$ are selected instead of primes.

integer. The degree of a polynomial is the largest exponent on x, so for the polynomial f, the degree is n. Each diagonal of the Ulam spiral corresponds to a specific polynomial of the form $4x^2 + bx + c$, where both a and b are constant integers (positive or negative whole numbers), and x varies over the natural numbers. Thus, the pattern that the Ulam spiral appears to suggest is a tendency for certain quadratics (polynomials of degree 2) to generate prime numbers more frequently than others. This is a remarkable property. Prime numbers have a largely unpredictable distribution while quadratics and other polynomials are well structured. We can easily predict the nth output of a polynomial: we just plug n into the polynomial. Despite these qualitative differences, the correlation between these two mathematical objects is real and measurable.

While we are able to measure the correlations between prime numbers and polynomials, it is more difficult to actually prove that these correlations are real for arbitrary polynomials over large scales. For instance, we might notice that there are a large number of prime numbers corresponding to the polynomial $x^2 + x + 41$ (called Euler's polynomial, the properties of which we will explore in later chapters). In fact, this polynomial yields a prime number for the first 39 inputs. However, we can ask what properties of this polynomial led to such a high frequency of primes to be generated (in fact, this polynomial seems to generate primes more frequently than arbitrary polynomials even after its streak is broken at $x = 40$)[2]. There are a variety of conjectures that attempt to answer questions of this sort that estimate these properties based on the discriminant, roots, or coefficients.

In this thesis, we examine the relationship between polynomials and prime numbers. All three of the methods of quantifying the properties of a polynomial mentioned in the last paragraph will be used to predict the nature of the prime production of that polynomial. At times, we will examine the length of prime-production; i.e., how long a single streak in the Ulam spiral can continue for. We will ultimately place an upper bound on the length of a streak for a given polynomial, and demonstrate that given other conjectures from

[2]At this value, the polynomial achieves the value $40^2 + 40 + 41 = 41 \cdot 40$, which is composite. The asymptotic property follows from Conjecture F of Littlewood and Hardy [HL23].

mathematics, that these streaks can get arbitrarily large for specifically chosen polynomials. Further, we will also consider how frequently a polynomial will generate prime numbers, a sort of analog of the prime number theorem for quadratics. However, the conjectures associated with this path of study will prove impenentrable to rigorous progress.

The integers are not the only set that "prime elements" can be defined over. In fact, there are a large variety of sets for which we can define prime elements and polynomials. That being said, some of such sets are finite, so there are both a finite number of prime numbers and polynomials of a specific degree in these sets. As we put more requirements on these sets, they begin to more closely approximate the structure of the integers, so that prime elements become more familiar as well. We will explore the development of these sets toward those of a specific form that are similar enough to the integers that they allow similar proofs throughout the first two chapters. Then, we will explore the nature of these sets and develop proofs for these new sets to try to mirror findings for the integers, although we will lose some strength in our proofs along the way. We create these proofs by extending properties that are obvious to the integers to these other sets, so that we can create analogous theorems over new sets that mirror the proof structure followed over the integers.

1.1 The Norm of a Complex Number

The *norm* is a mapping from the complex numbers (numbers of the form $a + bi$, where $i = \sqrt{-1}$ and a, b are real numbers) to the nonnegative real numbers that measures the square of the number's distance from the origin. Specifically, the norm of a complex number (written $N(\alpha)$, where α is a complex number) is the sum of the squares of its two components. For instance, $N(1+2i) = 1^2+2^2 = 5$. Of course, using the norm to represent a complex number means that we lose a lot of information about the number along the way, but it also enables us to analyze the complex numbers as if they were all along one (the real number) line For instance, the norm of the product of two numbers is the same as the product of the

norms of two integers. That is, $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$. In this way, the norm preserves a structure of the complex numbers.

This connection allows us to extend concepts from the integers to more complicated sets. The norm becomes particularly potent when it comes to examining specifically structured subsets of the complex numbers that correspond to the integers in some manner. Then, the norm can become a tool for understanding the new set in terms of the integers.

Consider for instance, the Gaussian integers: any sum of an integer and another integer times i. If we embed this set in the complex plane, we see that these new numbers form a square lattice (see Figure 1.1). In this new set, the relationships between elements are

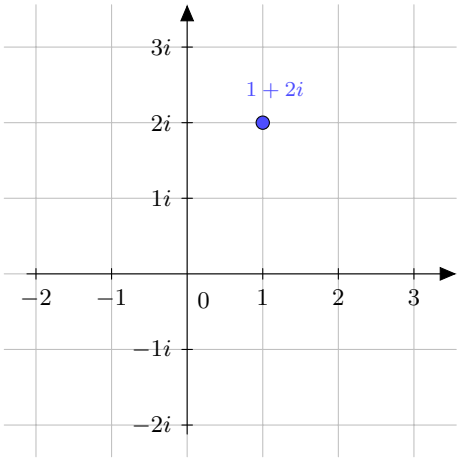

Figure 1.4: The Gaussian lattice, where Gaussian integers occur at the intersections of lines, with the point $1 + 2i$ noted as an example.

different from what we learned to expect from the integers. For instance, if two integers are not equal, then one is greater than the other. This fact is so obvious it hardly seems worth stating as an important property of the integers. But in the Gaussian integers, the concepts of "greater than" or "less than" are not well-defined. When we do not have a one-dimensional line to work with, it is harder to say what it means to compare the sizes of two elements. However, there are still some other rules that held over the integers that extend to the Gaussians.

For instance, prime numbers still exist, but we need to carefully generalize our defini-

tion, so that the concept is meaningful in the Gaussians. In fact, we can use the concept of the norm to define what a prime number is in the Gaussians. In the Gaussians, there are more pairs of numbers whose product is 1. These pairs are 1 and 1, -1 and -1, and i and $-i$. Each of these numbers individually has a norm of 1. Thus, we call a number in the Gaussians, p, prime if it is not divisible by any other numbers except for those of norm 1 or those who have the same norm as p. While this definition may seem more abstract than the definition that we had over the integers, the norm provides a helpful way to understand that these two descriptions are closely connected by the exclusion of divisors of other sizes. This new set of primes is different from the primes over the integers, even if we only consider the Gaussian primes that also have an imaginary part of 0. For example, 2 is not a prime in the Gaussian integers because it can be written as the product of two numbers of norm not equal to 1 or $N(2) = 2^2 = 4$. Specifically, $(1+i)(1-i) = 1-i+i+1 = 2$ and $N(1+i) = N(1-i) = 1+1 = 2$. That being said, some integers are prime numbers in both sets, such as 3. In fact, integers are also Gaussian primes if and only if their remainder under division by 4 is 3 [Ros93]. A Gaussian integer that is not an integer (i.e., has nonzero imaginary part) is prime if its norm is prime, as is the case for $(1+i)$ and $(1-i)$.

This correspondence of rules using the norm becomes useful when we want to prove theorems on the Gaussians that have corresponding forms in the real integers. One such theorem is unique factorization in the Gaussians. The proof (which is presented rigorously in Chapter 2) uses induction on the norm of the Gaussian integers and effectively treats the Gaussian integers as rational[3] integers to complete the proof.

1.2 Prime Generating Polynomials over the Integers

A polynomial is an expression of the form, $f(x) = a_n x^n + \ldots + a_1 x + a_0$. For our purposes, we will require that the coefficients (the a_i's) are integers and that x always has to be an integer. Thus, the output of a polynomial, $f(x)$ will necessarily also be an integer, since the

[3]Gaussian integers with zero imaginary part are called rational.

addition and multiplication of integers yields an integer. A question arising naturally from number theory is then whether there are certain polynomials that generate prime numbers more frequently than others.

Euler, a dominant Swiss mathematician of the eighteenth century, found that the polynomial x^2+x+41, which as mentioned before, generates prime numbers for the first 39 inputs. This raised a variety of questions as to how frequently polynomials that are so prime rich appear and how frequently a general quadratic will generate prime numbers. In 1837, Dirichlet, a German mathematician, showed that any linear function (i.e., a polynomial of degree one), $ax + b$, where a and b share no factors, will generate infinitely many primes [Dir37]. This answers the question for a small class of polynomials, but leaves is open even for quadratics. That question has largely remained unanswered even until the present time. Hardy and Littlewood, two[4] of the greatest mathematicians of the early twentieth century provided a conjecture that, if proven, would answer the question, but it has so far resisted progress despite its apparent veracity. Some smaller properties have been shown of quadratics, though. For instance, modern mathematicians have demonstrated that of polynomials of the form, $x^2 + x + A$ where A is an integer, Euler's polynomial is the one with the largest A value such that the polynomial is prime up until $x = A - 1$ [Mol97]. It has also been shown that if an extension of the twin prime conjecture holds, then for any number, N, there will be a polynomial of the form $x^2 + x + A$ that generates a streak of prime numbers at least N long (but it will still eventually halt at $N = A - 2$).

Moving beyond the theorem of Dirichlet has been rather difficult. The generalization of Dirichlet's theorem on arithmetical sequences is known as the Bunyakowsky Conjecture and states that a irreducible polynomial with relatively prime coefficients and a positive leading term coefficient will necessarily generate infinitely many prime numbers [Bun59]. However, in reality, while we have gotten better at making conjectures (Hardy and Littlewood presented a claim on the frequency of the appearance of primes for a given quadratic

[4]Because Hardy and Littlewood published so frequently together, a joke goes that the three greatest mathematicians of the early twentieth century are Hardy, Littlewood, and Hardy and Littlewood.

[HL23]) Bunyakowsky's Conjecture remains unanswered. Perhaps more remarkable, we are unable to even say whether a given polynomial generates any prime numbers at all. Other questions can be asked with more success, though. For example, we may wonder how many prime numbers in a row a given quadratic could possibly generate. We call this bound the "prime-generating radius," and there has been successful research in bounding this value strongly while also showing that it can grow large for specific polynomials [Mol97]. In fact, work on this matter has developed to the level of exactly classifying how well a polynomial generates primes if it has a small constant term.

These questions about the prime-generating radius are easily extended to the Gaussian integers, and a rather simple bound has been put on the length of such a radius for quadratics [FMT17]. The proof here relied on tactics developed in the integers and applied to the Gaussians through the use of the norm.

1.3 Using the Correspondence for Other Domains

So far, we have only discussed the connection that the norm provides between the Gaussians and the integers. However, there are other domains (this is actually a mathematically precise term that will be defined later) that also have a norm mapping (in general, we call it a Euclidean function), although it will be different on account of being a map from a different domain. The Eisenstein integers, which are generated by adjoining the cube roots (as opposed to fourth roots) of one to the integers, is another domain with a well-defined norm. Much of the original research in this thesis explores extensions of results on integers to the Eisensteins.

Even more helpfully, the correspondence between the Gaussians and the integers matches up well to the correspondence between the Eisensteins and the integers. Thus, by using an analogy of analogies (the relationship between the two norms), we can construct many of the proofs that are known over the Gaussians in the Eisensteins. Furthermore, as long as we are able to make this connection between a domain and the integers using a mapping

that preserves multiplication, we can stand a chance of proving rather powerful properties with relatively little work by relying on the analogy that the norm provides.

Chapter 2

An Introduction to Number Theory

2.1 A Little Bit of Algebra

Before we delve into the more specific framework of number theory, we will provide a more abstract understanding of the important structures that will be developed in the remainder of the thesis. Much of number theory is done within the specific algebraic structure of the integers, but important properties of the integers are proven by extending one's study outside of this domain. Thus, this thesis will look at various structural properties of the integers to enable the discussion to extend to other sets (e.g., the Gaussian and Eisenstein Integers).

The concepts in "algebra" introduced here were only brought formally into the study in the past two centuries. Much of the work done in number theory was performed without the help of algebra. Regardless, certain algebraic definitions and theorems have proven helpful both in developing new theorems in number theory and generalizing old ones. Thus, because some later work will require reference to certain algebraic structures, we will introduce some of the relevant terms here.

The relevant basis that we will construct use to construct our properties is very bare.

For a large part, we simply introduce the concepts of multiplication and addition whose structure will be refined in later definitions.

Definition 2.1 (Ring)**.** A *ring* is a set of elements, R, and two binary operations, called respectively addition and multiplication, $+, \cdot : R \times R \to R$ that satisfy the following conditions. Let a, b, c be any elements of R.

- There exist identity elements for both addition and multiplication, 0 and 1, such that, $a + 0 = a \cdot 1 = a$.
- Both operations are associative and addition is commutative: $(a+b)+c = a+(b+c)$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, and $a + b = b + a$.
- There are inverses for addition, there exists an element, z, such that $a + z = 0$. If we know that z is the additive inverse of a, we write $z = -a$.
- Multiplication distributes over addition (both on the left and right):

$$(a + b) \cdot c = a \cdot c + b \cdot c, \text{ and } c \cdot (a + b) = c \cdot a + c \cdot b.$$

It is worth noting that R considered with only the $+$ operation is a group, which is a weaker form of structure that is the basic object of algebra. The most classical example of a ring is the integers with addition being the $+$ operation and multiplication being the $\cdot$ operation. We will encounter other rings as we explore number theory such as the Gaussian integers.

In particular, a type of ring with added structure we are concerned with is an *Integral Domain*.

Definition 2.2 (Integral Domain)**.** A ring with the extra properties that:

1. $a \cdot b = 0$ implies either $a = 0$ or $b = 0$
2. for any $a, b \in G$, $a \cdot b = b \cdot a$

is an integral domain.

In an integral domain, the operation of division is not allowed, so we can not ask what an element a divided by an element b is. Rather, the closest question we can ask is whether a divides b, written $a|b$, which is equivalent to asking if there exists a c such that $ac = b$. If the answer to this question is yes, then the c that we found to confirm $a|b$ could be considered the answer to our former question. However, the answer to the latter question always exists while the answer to the former question often does not exist, so we prefer to ask questions of the second kind. We can partition the elements of an integral domain into two parts: those that have a multiplicative inverse and those that do not.

Definition 2.3 (Unit)**.** Let R be a ring, $a \in R$. If there exists $b \in R$ s.t. $ab = 1$, then a (as well as b) is a *unit*. Note that we did not need to require that $ba = 1$, since we are in an integral domain where multiplication is commutative.

In contrast to units, we also introduce another type of element that will correspond to "primality."

Definition 2.4 (Irreducible)**.** A nonzero element of a domain that cannot be written as the product of two other non-unit domain elements is called *irreducible*.

This definition is actually rather close to that we used for a prime number, although the formal definition for a prime is different and in general defines a different set of numbers.

Definition 2.5 (Prime)**.** A nonzero element, p, of an integral domain such that for every a, b elements of the domain, $p|ab$ implies $p|a$ or $p|b$ is called *prime*.

This definition for prime is less intuitive than the definition for prime introduced at the beginning of Chapter 1, which is closer to the definition of irreducible, which is a different quality in general. However, there are sets for which these two properties are interchangable. These domains bring us closer to the integers by bringing the concepts of primality and irreducibility together.

Definition 2.6 (Unique Factorization Domain)**.** An integral domain where every element is expressible uniquely (up to multiplication by unit elements) as the product of irreducible elements is called a unique factorization domain (abbreviated UFD).

Irreducible and prime elements in a UFD are the same, and the two terms are used interchangeably whenever they belong to a UFD [Ros93].

2.2 The Natural Numbers and the Integers

We have already been introduced to the natural numbers, $\mathbb{N}$, in Chapter 1. Note that these numbers are not a ring because they lack an additive identity and inverses for any of the elements. However, if we consider $\mathbb{N}$, $\{0\}$, $-\mathbb{N}$ (i.e., the natural numbers, the set containing zero, and the additive inverses of the natural numbers) we do have a ring. This new set is called the integers and denoted $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}$.

The first mathematical proofs attempting for rigor in the modern sense, provided by Euclid c. 300 B.C.E., included (among various geometric proofs from which we derive Euclidean Geometry) proofs on elements of $\mathbb{N}$. Already at this point, mathematicians had found that the natural numbers larger than 1 could be partitioned into *prime* and *composite* numbers:

Definition 2.7 (Prime and Composite Numbers)**.** A number, $p \in \mathbb{N}$, is prime if p is greater than 1 and divisible only by itself and 1. A number, $n \in \mathbb{N}$, is composite if p is greater than 1 and not prime.

Note that we have defined the number 1 as neither prime nor composite. Instead, we call 1 a *unit*. Again, our terminology from integral domains holds over. Defining 1 as a unit is more than a formality, and suggests a partitioning of any UFD into its zero element, units, prime elements, and composite elements. With this definition of a prime number, we can prove that there are infinitely many prime natural numbers.

Theorem 2.8 (Euclid)**.** *There are infinitely many prime numbers.*

Proof. Proceed by contrapositive: Consider a set $P = \{p_1, p_2, \ldots, p_k\}$, a finite set of prime numbers. Let π be the product of all the elements of P, plus 1:

$$\pi = 1 + \prod_{p \in P} p. \tag{2.1}$$

Next, if $\hat{p} \in P$ divides π, then $\hat{p} | \pi - \prod_{p \in P} p$, so $\hat{p}|1$, which is only true for units (not primes). No $p \in P$ divides π, so π must also be a prime or divisible by a prime not in P. Thus, no finite set can contain all prime numbers, so there are infinitely many. □

The infinitude of primes is tangential to our current discussion, but as we progress to considerations of prime-generating polynomials, we will develop more powerful proofs of the distribution of these infinite primes.

Recalling our discussion from the previous section, we can prove that the integers have unique factorization (they are a UFD).

Theorem 2.9 (Fundamental Theorem of Arithmetic)**.** *Every integer can be represented as a product of prime elements uniquely up to reordering and multiplication by 1 and -1 (the only units).*
That is, for any $n \in \mathbb{Z}$,

$$n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}, \tag{2.2}$$

where each p_i is a (positive) prime and r_i is a natural number, $p_{i+1} > p_i$, and any other such factorization of n,

$$n = {p'_1}^{r'_1} {p'_2}^{r'_2} \ldots {p'_k}^{r'_{k'}} \tag{2.3}$$

has $k = k'$, $p'_i = p_i$, and $r'_i = r_i$.

Proof. First, we will show that there exists a set of primes that multiply to n. We proceed by strong induction: assume that the claim holds for all $m < n$. If n is prime, then the set of primes that multiply to n is just $p_1 = n$. If n is composite, then $n = ab$ for some $a, b \in \mathbb{N}$. Then both $a, b < n$, so by our inductive hypothesis, the claim holds for both a

and b. Thus, there exist $q_1, \ldots, q_\ell, r_1, \ldots, r_m$ such that

$$a = q_1 \cdot \ldots \cdot q_\ell \tag{2.4}$$

$$b = r_1 \cdot \ldots \cdot r_m \tag{2.5}$$

Thus $n = q_1 \cdot \ldots \cdot q_\ell \cdot r_1 \cdot \ldots \cdot r_m$ where all the terms are prime numbers, so existence is proven.

To show uniqueness, we proceed by contradiction: Assume that the set of numbers with non-unique prime factorizations is non-empty. Consider the smallest element of this set (the set must have a smallest element by the well-ordering principle[1]), call this element n (we will reuse variable names used in the first half of the proof, but the reader should not assume any connections between the two sections of the proof). We write the two expressions for n as

$$\begin{aligned} n &= p_1 \cdot \ldots \cdot p_k \\ &= q_1 \cdot \ldots \cdot q_\ell \end{aligned}$$

Since multiplication is commutative, we can assume that both expressions are written in non decreasing order. If $p_1 = q_1$, then $\frac{n}{p_1} = p_2 \cdot \ldots \cdot p_k = q_2 \cdot \ldots \cdot q_\ell$. Thus, there are two different ways to represent $\frac{n}{p_1}$, but $\frac{n}{p_1} < n$, and n was the smallest natural number with the two representations. So $p_1 \neq q_1$. Without loss of generality, we can assume that $p_1 < q_1$.[2] Note that $p_1 \neq q_1, q_2, \ldots, q_\ell$, since p_1 is less than q_1, which is less than or equal to all the q_i. So $p_1 | n = q_1 \cdot \ldots \cdot q_\ell$. But since p is prime, p must divide one of the q_i, which is a contradiction, since $p \neq q_i$, and each q_i is prime. Thus, our assumption that there are multiple representations must be false. $\square$

Thus, the integers, $\mathbb{Z}$ are a unique factorization domain (-1 is a unit since -1 has a multiplicative inverse: itself).

[1] Every subset of the natural numbers has a smallest element. This is generally taken as an axiom.
[2] If not, renotate q's as p's and vice-versa.

2.3 The Euclidean Algorithm

We will begin this section with a definition central to performing number theory on the integers:

Definition 2.10 (Greatest Common Divisor)**.** For integers, a, b, the greatest common divisor (GCD) of a and b, written (a, b), is the largest positive integer that divides both a and b.

For example, the greatest common divisor of 10 and 15 is $(10, 15) = 5$. As these numbers get larger, calculating their greatest common divisor will become more difficult than it was in this simple case. Luckily, there is a specific algorithm for finding the GCD of two numbers. We will present the algorithm first, then show that it works.

Definition 2.11 (The Euclidean Algorithm)**.** To find the GCD of two (positive) integers, a, b, we perform the Euclidean Algorithm:

1. Let r_{-1} be the maximum of a and b, and let r_0 be the minimum of a and b.
2. Write $r_{-1} = r_0 k_0 + r_1$, where $k_0, r_1 \in \mathbb{N} \cup \{0\}$ and $r_1 < r_0$.
3. Then write $r_0 = k_1 r_1 + r_2$, where $k_1, r_2 \in \mathbb{N} \cup \{0\}$ and $r_2 < r_1$.
4. Continue writing $r_i = k_{i+1} r_{i+1} + r_{i+2}$, where $k_{i+1}, r_{i+2} \in \mathbb{N} \cup \{0\}$ and $r_{i+2} < r_{i+1}$.
5. If r_{i+2} is zero, the algorithm terminates, and $r_{i+1} = (a, b)$.

We will now show that this algorithm is always successful:

Theorem 2.12. *The Euclidean Algorithm always terminates and yields the GCD of the inputted integers, a, b.*

Proof. To find the values of k_i and r_{i+2} that satisfy the conditions of step 2, we subtract r_{i+1} from r_i as many times as possible before the result becomes negative. We can do this at least once, since $r_i > r_{i+1}$, the condition required by the previous step (this is also initially

true from how we label a and b). Call the maximal number of subtractions before the value becomes negative, k_i, which is positive, since we could perform the subtraction at least once. Then assign r_{i+2} the value $r_i - k_i r_{i+1}$. Because k_i was maximal, $0 > r_i - k_i r_{i+1} - r_{i+1} = r_{i+2} - r_{i+1}$, so $r_{i+1} > r_{i+2}$, which is the other condition. Thus, we can perform step 4 arbitrarily many times.

Note that $r_{i+1} < r_i$, so each time the algorithm repeats step 4, r_i will get smaller by at least 1, but we require that $r_i \geq 0$, so the algorithm must terminate after a finite number of iterations. When the algorithm terminates, we will be left with an expression of the form: $r_j = k_{j+1} r_{j+1}$ (since $r_{j+2} = 0$). Then, proceeding backwards, we have $r_{j-1} = k_j r_j + r_{j+1} = k_j k_{j+1} r_{j+1} + r_{j+1}$, so $r_{j+1} | r_{j-1}$. In general, if $r_{j+1} | r_i, r_{i+1}$, then $r_i = d_{i,j+1} r_{j+1}$ and $r_{i+1} = d_{i+1,j+1}$, so $r_{i-1} = k_i r_i + r_{i+1} = k_i d_{i,j+1} r_{j+1} + d_{i+1,j+1} r_{j+1}$, so $r_{j+1} | r_{i-1}$. Thus, r_{j+1} divides all r_i, and, in particular, a and b.

Next, $(a, b) | r_{-1}, r_0$ by definition, and if $(a, b) | r_i, r_{i+1}$, then we can write

$$(a, b) d_i = (a, b) d_{i+1} + r_{i+2}, \tag{2.6}$$

where $(a, b) d_i = r_i$ and $(a, b) d_{i+1} = r_{i+1}$, so

$$(a, b)(d_i - d_{i+1}) = r_{i+2}. \tag{2.7}$$

Therefore, $(a, b) | r_{i+2}$ Thus, by induction, $(a, b) | r_i$ for any i. Namely, $(a, b) | r_{j+1}$, but r_{j+1} was a common divisor of a and b, so it must be no greater than (a, b). Thus, $r_j = (a, b)$. □

We can use this algorithm to extend properties of the integers to other domains:

Definition 2.13 (Euclidean Domain)**.** A UFD, D, where there exists a "Euclidean function", $f : D \to \mathbb{N} \cup \{0\}$ such that if $r_i, r_{i+1} \in D$ and $r_{i+1} \neq 0$, then we can write, $r_i = r_{i+1} k_{i+1} + r_{i+2}$, where $f(r_{i+1}) > f(r_{i+2})$, and $f(ab) \geq f(b)$ for nonzero $a, b \in D$ is called a *Euclidean Domain*.

Clearly, the integers are a Euclidean domain using as our Euclidean function a function that maps every (non-zero) number to its absolute value. This observation leads us to our final refinement of properties.

Definition 2.14 (Norm-Euclidean Domain)**.** If D is a Euclidean domain, where its Euclidean function is also a norm on D, then D is a *norm-Euclidean domain.*

Furthermore, if the Euclidean function is also a norm on the domain, then we call the domain, norm-Euclidean. Most of the domains that we are going to be considering are norm-Euclidean domains.

2.4 The Gaussian Integers

A natural extension of the integers yields a different Euclidean domain (that is not well-ordered, but rather partially-ordered). Let i be the square root of -1, that is, $i^2 = -1$. We can then consider the integers "extended" by i (since $i \notin \mathbb{Z}$), denoted as $\mathbb{Z}[i]$. This means that, in addition to the integers, we consider the integers multiplied by i, and the sums of the two "types" of integers.

So, $1, 1+i, i, -1+i, -1, -1-i, -1, -1+i \in \mathbb{Z}[i]$. In this new set, we have more units: instead of just 1 and -1, we also have i and $-i$, since $i \cdot (-i) = 1$. Note that some numbers that were prime in $\mathbb{N}$ are no longer prime in the Gaussian integers. As seen in Section 1.1, $2 = (1+i)(1-i)$ is not a prime number ($(1+i)$ and $(1-i)$ are non-unit factors). Furthermore, there are other new prime numbers, such as $1+i$ and $1-i$. Of course, some numbers, such as 3, are prime in both domains. We tend to denote Gaussian integers with Greek letters $(\alpha, \beta, \ldots)$ and integers with Latin letters $(a, b, \ldots)$.

The Gaussian integers are an integral domain, since multiplication is commutative and no two nonzero elements multiply to zero. To show that $\mathbb{Z}[i]$ has unique factorization, we will introduce an ordering on $\mathbb{Z}[i]$.

Definition 2.15 (Norm)**.** Let $\alpha \in \mathbb{Z}[i]$. Write $\alpha = a + bi$. Then, the *norm* is a map $N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ defined below:

$$N(\alpha) = a^2 + b^2.$$

We will also use $|\alpha|$ to refer to the square root of $N(\alpha)$, representing the distance of α from the origin. The standard ordering that we have for the natural numbers can then be applied to the norms of Gaussian integers in order to create a partial ordering on the Gaussian integers themselves. There are multiple Gaussian integers that map to the same norm (e.g., $N(1+i) = N(1-i) = 2$), so the well-ordering on the norm only offers a partial ordering of the Gaussian integers. Despite the disadvantage of this new environment, the norm will still prove useful in understanding the structure of the Gaussian integers.

Lemma 2.16. *If $\alpha, \beta \in \mathbb{Z}[i]$, then $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Proof. We can write out $\alpha = a_r + a_i i,\ \beta = b_r + b_i i$. Taking the norm of product, we get:

$$\begin{aligned} N\left((a_r + a_i i)(b_r + b_i i)\right) &= N\left((a_r b_r - a_i b_i) + (a_r b_i + a_i b_r)i\right) \\ &= (a_r b_r - a_i b_i)^2 + (a_r b_i + a_i b_r)^2 \\ &= a_r^2 b_r^2 + a_i^2 b_i^2 + a_r^2 b_i^2 + a_i^2 b_r^2 - 2a_r b_r a_i b_i + 2a_r b_r a_i b_i \\ &= a_r^2 b_r^2 + a_i^2 b_i^2 + a_r^2 b_i^2 + a_i^2 b_r^2. \end{aligned}$$

On the other hand, the product of the norms is:

$$\begin{aligned} N(a_r + a_i i)N(b_r + b_i i) &= (a_r^2 + a_i^2)(b_r^2 + b_i^2) \\ &= a_r^2 b_r^2 + a_i^2 b_r^2 + a_r^2 b_i^2 + a_i^2 b_i^2. \end{aligned}$$

Thus, the norm respects multiplication. □

We can use the norm to visualize $\mathbb{Z}[i]$ as a 2-d square lattice. The x-coordinate of a point corresponds to the real part of the number, and the y-coordinate corresponds to the imaginary part. Thus, the norm of a Gaussian integer measures the number's distance (squared) from the origin. When we take the product of two Gaussian integers, we can use some arithmetic tricks from complex analysis. Let $\alpha, \beta \in \mathbb{Z}[i]$. Call their angles from the (positive) x-axis $\theta_\alpha, \theta_\beta$ respectively. Then the product $\alpha\beta$ has an angle $\theta_\alpha + \theta_\beta$ and (from lemma 2.16) a norm of $N(\alpha)N(\beta)$, which yields a new point in the lattice, see figure 2.1.

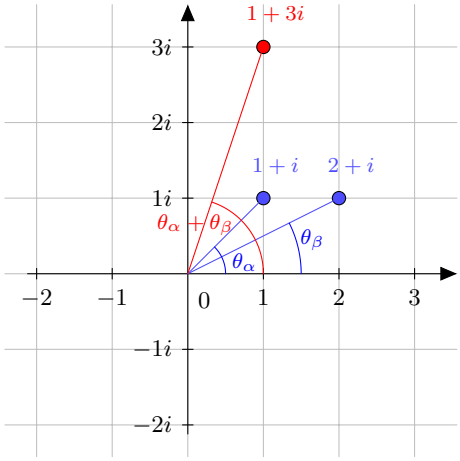

Figure 2.1: An illustration of the product $(2+i)(1+i) = 1+3i$ in the square lattice.

The norm also acts as a way to study the Gaussian integers as if they were solely integers. Instead of having concern for how two complex numbers multiply together, we are enabled to convert them into whole numbers and apply the ordering of the integers to perform a proof by induction. Before we continue, we will mention a short lemma on the relationship between units and the norm that will come in helpful later.

Lemma 2.17. *Suppose ν is an element of $\mathbb{Z}[i]$, then $N(\nu) = 1$ if and only if ν is a unit.*

Proof. Note that there are no norms of Gaussian integers between 0 and 1, since the square of an integer is an integer. From the definition of a unit, we require that if ν is a unit, then there exists ν^{-1} such that

$$\nu\nu^{-1} = 1. \tag{2.8}$$

Taking the norm of both sides and applying Lemma 2.16, we have

$$N(\nu\nu^{-1}) = N(1) \tag{2.9}$$

$$N(\nu) = \frac{1}{\nu^{-1}}. \tag{2.10}$$

However, the norm of a Gaussian integer must be a non-negative integer, so $N(\nu) = 1$.

To show the other implication, not that any Gaussian number can be written in the form $\alpha = a + bi$. Thus its conjugate, $\bar{\alpha} = a - bi$ is also a Gaussian integer of the same

norm. Furthermore, $\alpha\bar{\alpha} = a^2 + b^2 = N(\alpha)$. Thus, if a Gaussian integer α has norm 1, then $\alpha\bar{\alpha} = N(\alpha) = 1$, so α is a unit. $\square$

The next lemma provides another structure that we can use:

Lemma 2.18. *Let $\alpha, \beta \in \mathbb{Z}[i]$. Then if $\alpha|\beta$ then $N(\alpha)|N(\beta)$.*

Proof. If $\alpha|\beta$, there exists γ such that $\alpha \cdot \gamma = \beta$. Taking the norm of both sides and using Lemma 2.16, we get:

$$N(\alpha \cdot \gamma) = N(\beta) \tag{2.11}$$

$$N(\alpha)N(\gamma) = N(\beta) \tag{2.12}$$

Thus, $N(\alpha)|N(\beta)$. $\square$

The preservation of divisibility when we transform from $\mathbb{Z}[i]$ to $\mathbb{Z}$ enables us to bring many of the properties that we are familiar with in the integers to the Gaussian integers:

Theorem 2.19. *The Gaussian Integers are a unique factorization domain, namely $\alpha \in \mathbb{Z}[i]$ is factorable into prime elements uniquely up to multiplication by units.*

Proof. Existence of a factorization into primes:

Proceed by strong induction on values of the norm, n. In the base case, $n = 1$. The only Gaussian integers with norm 1 are the units by Lemma 2.17, which all have unique factorization into primes up to multiplication by a unit. If there are no Gaussian integers of norm n, then the statement holds vacuously. Suppose now that there is a Gaussian integer α of norm n. If α is a prime, then it has a factorization into primes and the statement holds. If α is not prime, then it has a factorization into two non-units, $\alpha = \beta\gamma$. However, both β and γ have factorization into primes, since they both have norm less than n (both their norms are greater than 1 and multiply to n).

Uniqueness:

Proceed again by strong induction on the norm, n. If there are no Gaussian integers with norm n, the statement holds vacuously. Assuming that there are Gaussian integers of

norm n, let α be one such element. Suppose that $\alpha \in \mathbb{Z}[i]$ has two prime factorizations. Write this as

$$\alpha = \pi_1 \cdot \ldots \cdot \pi_k = \rho_1 \cdot \ldots \cdot \rho_\ell. \tag{2.13}$$

Then, $\pi_1 | \alpha = \rho_1 \cdot \ldots \cdot \rho_\ell$. By the definition of a prime element of a domain, $\pi_1 | \rho_i$. However, ρ_i is irreducible, so it must be at most a unit multiple off from π_1. That is,

$$\pi_1 = \nu \rho_i, \tag{2.14}$$

where ν is a unit. Then, factoring out π_1 from Equation 2.13 with $\alpha = \pi_1 \alpha_1$, we get

$$\pi_1 \alpha_1 = \pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_k = \nu \pi_1 \cdot \rho_2 \cdot \ldots \cdot \rho_\ell. \tag{2.15}$$

Dividing by π_1 on both sides, we get

$$\pi_2 \cdot \ldots \cdot \pi_k = \nu \rho_2 \cdot \ldots \cdot \rho_\ell. \tag{2.16}$$

However, both sides of Equation 2.16 have norm less than n, since π_1 had norm greater than 1, so by the inductive hypothesis, they must have the same prime factorization up to multiplication by a unit. Thus, the two original factorizations were also the same, and α has a unique factorization. Again, we can use $n = 1$ as our base case, since multiplication by any prime forces a norm greater than 1, so the factorization into no primes is unique. □

Finally, we can show that the Gaussian integers are Euclidean domain:

Theorem 2.20. *The Gaussian integers are a Euclidean domain.*

Proof. We take as our Euclidean function, the norm on $\mathbb{Z}[i]$. Consider two Gaussian integers, $\alpha, \beta \in \mathbb{Z}[i]$. We need that there exists κ, ρ such that $\alpha = \beta\kappa + \rho$ and $N(\beta) > N(\rho)$.

If $N(\beta) > N(\alpha)$, we can set $\kappa = 0$ and $\rho = \alpha$. Then the equality is satisfied:

$$\alpha = \beta \cdot 0 + \alpha \tag{2.17}$$

and so is the inequality: $N(\alpha) = N(\rho) < N(\beta)$.

If $N(\alpha) \geq N(\beta)$, then our proof is more involved and geometric. Create an orthogonal coordinate system on $\mathbb{Z}[i]$ where the elements of $\mathbb{Z}[i]$ are vectors, and:

$$\vec{\beta} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ \vec{\beta i} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \ \vec{\alpha} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \tag{2.18}$$

Note that a_1 and a_2 are not necessarily whole numbers, and likely are not. Then the norm of a number is its dot product with itself times $|\beta|^2$, since we have rescaled distances so that $\vec{\beta} \cdot \vec{\beta} = 1$.

Suppose that $|a_1| \geq |a_2|$, and $a_1 > 0$ (the proof proceeds similarly for all other cases). Since $N(\alpha) \geq N(\beta) = 1$, $a_1 \geq \frac{1}{\sqrt{2}}$. Then,

$$\left| \begin{pmatrix} a_1 - 1 \\ a_2 \end{pmatrix} \right|^2 = a_1^2 - 2a_1 + 1 + a_2^2 \leq a_1^2 + a_2^2 + 1 - \sqrt{2} \leq a_1^2 + a_2^2 \leq \left| \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \right|^2. \tag{2.19}$$

If $a_1 < 0$, then we add $\vec{\beta}$ instead of subtracting it, and the underlying math remains the same. If $|a_2| > |a_1|$, then we perform the same math, except with $\vec{\beta i}$ instead of $\vec{\beta}$.

Thus, we can continue subtracting factors of β from α until the total value subtracted from α, $\kappa\beta$ has $|\alpha - \kappa\beta| < 1$. Then we can write, $\alpha = \beta\kappa + \rho$ where $\rho = \alpha - \beta\kappa$, and we know that $N(\rho) < |\beta|^2 = N(\beta)$. So the norm satisfies the conditions of a Euclidean function on $\mathbb{Z}[i]$ and $\mathbb{Z}[i]$ is a Euclidean domain. $\square$

We now can see that $\mathbb{Z}[i]$ has many of the same properties of the integers, so many of the claims we will make about the integers will be extendable to the Gaussians. In the next section we will introduce a third set that is very similar to the Gaussians called the Eisenstein integers, written $\mathbb{Z}[\omega]$, which forms a hexagonal lattice instead of the square lattice of $\mathbb{Z}[i]$. In this context, we will also have unique factorization and a (different) norm, and yet many of the same properties will still hold.

2.5 The Eisenstein Integers

In order to construct the Gaussian integers, we adjoined the square root of -1 to the integers. However, we can adjoin a variety of other complex numbers and still have a Euclidean domain. One of the most well-structured of these is the Eisenstein integers, denoted $\mathbb{Z}[\omega]$, where $\omega^3 = 1$. In the Gaussian integers, there were four values that satisfied $x^4 = 1$, $i, -i, 1$, and -1. However, as long as we adjoined a number with nonzero imaginary part, we developed the same structure. For the Eisenstein integers, there are actually three different values of ω that satisfy this equation, 1, $\frac{-1}{2} + \frac{\sqrt{3}}{2}i$, $\frac{-1}{2} - \frac{\sqrt{3}}{2}i$, and to avoid ambiguity, we will set $\omega = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$ (if we set $\omega = 1$, we would have been left with the integers).

To be able to talk about Eisenstein integers in terms of the sum of a real part and a complex part, we need to show that the product and sum of two Eisenstein integers is representable as $a+b\omega$. For addition, this is a simple task: $a+b\omega+c+d\omega = a+c+(b+d)\omega$. For multiplication, it takes slightly more effort: $(a+b\omega)(c+d\omega) = ac+(ad+bc)\omega+bd\omega^2 = ac - bd + (ad + bc + bd)\omega$, using: $\omega^2 = -\omega - 1$ (this can be quickly seen from considering the exact locations of the two roots in the complex plane).

Since the product and sum of any Eisenstein integers (with integer coefficients) also has integer coefficients, we can describe the Eisenstein integers as a lattice on the complex plane. However, in contrast to the Gaussian integers, the Eisenstein integers form a hexagonal lattice with its six unit elements.

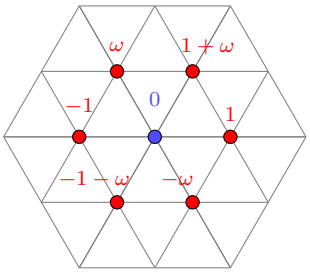

Figure 2.2: The units in $\mathbb{Z}[\omega]$ labeled in red, with the origin blue. The reader can observe that any combination of the units will line up along the surrounding triangular lattice.

Most of the claims we make about the Gaussian integers can be safely extended to the

Eisensteins. However, proofs of these concepts will not prove particularly more helpful in an understanding of the structure, since they will all align closely with the Gaussians. They are stated below here for reference. Proofs can be found in [Ros93]. Furthermore, we have a norm on $\mathbb{Z}[\omega]$, which is "different" from that on the Gaussians[3]:

Theorem 2.21 (Norm)**.** *The map $N : \mathbb{Z}[\omega] \to \mathbb{Z}$ with $a + b\omega \mapsto a^2 + b^2 - ab$ is a norm on $\mathbb{Z}[\omega]$.*

Using this norm, we get a strong piece of structure on $\mathbb{Z}[\omega]$:

Theorem 2.22. *$\mathbb{Z}[\omega]$ is a norm-Euclidean domain.*

2.6 Modular Arithmetic

A central tool for doing work in any UFD, D, is the concept of modular arithmetic (alternatively called clock arithmetic). For $a, b, m \in D$ we write

$$a \equiv b \mod (m)$$

if there exists $k \in D$ such that

$$a = b + km.$$

If $a \equiv b \mod (m)$, we say that a is equivalent to b modulo m. In order to justify the wording, we offer the following proposition:

Proposition 2.23. Equivalence modulo $m \in D$ where D is a UFD is an equivalence relation (it is symmetric, reflexive, and transitive).

Proof. For symmetry: if $a \equiv b \mod (m)$, then $a = b + km$ for some $k \in D$. Thus $b = a + (-k)m$, so $b \equiv a \mod (m)$. For reflexivity, start with $a = a$, we can write $a = a + 0 \cdot m$,

[3] In its formulation here, it appears different, but if we convert the notation of the Eisensteins into the standard $a + bi$ of the complex numbers, they will turn out to be the same norm.

so $a \equiv a \mod (m)$. To show transitivity, suppose $a \equiv b \mod (m)$ and $b \equiv c \mod (m)$. Rewriting the statements, we have

$$a = b + k_1 m$$

$$b = c + k_2 m$$

for $k_1, k_2 \in D$. Substituting b into the first from the second, we get

$$a = c + k_2 m + k_1 m$$

$$a = c + (k_2 + k_1) m$$

$$a \equiv c \mod (m)$$

□

Since this is an equivalence relation, modular equivalency partitions the UFD into disjoint equivalence classes. Addition and multiplication are also preserved modulo m:

$$(a + km) + (b + \ell m) = a + b + (k + \ell) m$$

$$(a + km)(b + \ell m) = ab + (bk + a\ell + k\ell m) m$$

To emphasize the importance of these equivalences, we introduce the concept of an ideal of a ring.

Definition 2.24 (Ideal)**.** A *two-sided ideal* of R is a subset, $I \subset R$, under the same operations $(+, \cdot)$ such that

1. I under $+$ is a subgroup of R under $+$,

2. $a \in I$, $r \in R$ implies $ar, ra \in I$.

Proposition 2.25. Let R be a ring where the multiplication operation is commutative, $m \in R$. Then $mR = (m) = \{md \mid d \in R\}$ is an ideal of R.

Proof. For property 1, we find the identity element, $0 = m \cdot 0$, additive inverses, $md + m(-d) = 0$, and closure, $md_1 + md_2 = m(d_1 + d_2)$, so mR is a group under addition.

For property 2, let $d_1 \in R$, $a \in mR$. By the definition of mR, there exists d_a such that $a = md_a$. Then $ad_1 = md_ad_1 \in mR$, since $d_ad_1 \in R$. □

Note that the equivalence class of 0 modulo m is exactly (m).

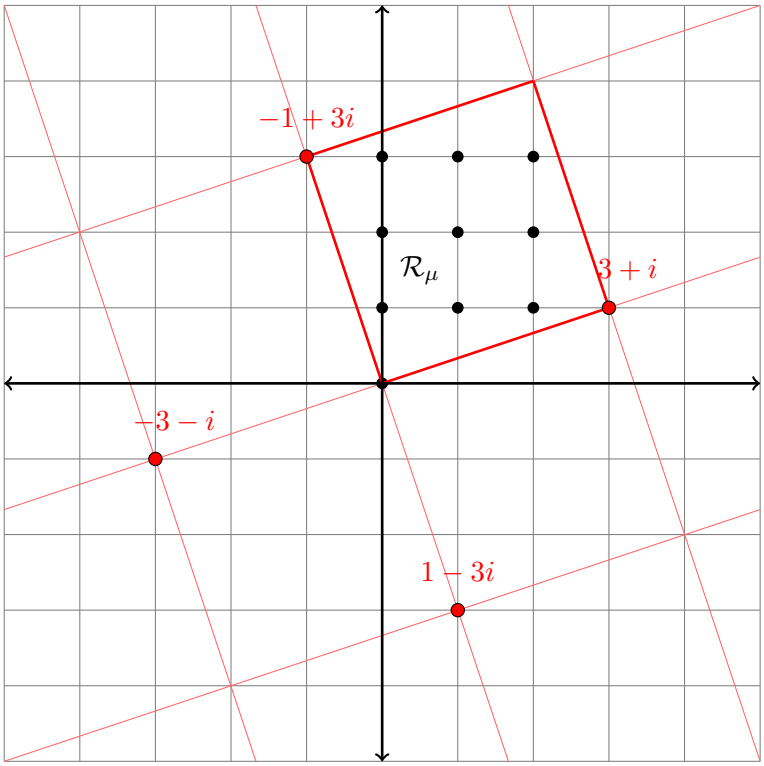

Figure 2.3: An illustration of a possible $\mathcal{R}_\mu$ (in black) in $\mathbb{Z}[i]$ for $\mu = 3 + i$.

We can also build up a finite set of elements, $\mathcal{R}$, where each element belongs to a different equivalence class, and every element of D is equivalent to exactly one element of $\mathcal{R}$ in D. These sets will become useful in proofs later on, so we formally define them:

Definition 2.26 (Representative Set)**.** Let S be an arbitrary set and $\sim$ an equivalence relation on that set. Then a set $\mathcal{R}_\sim \subset S$ that contains exactly one representative of each element of $S/\sim$ is a *representative set* of $S/\sim$.

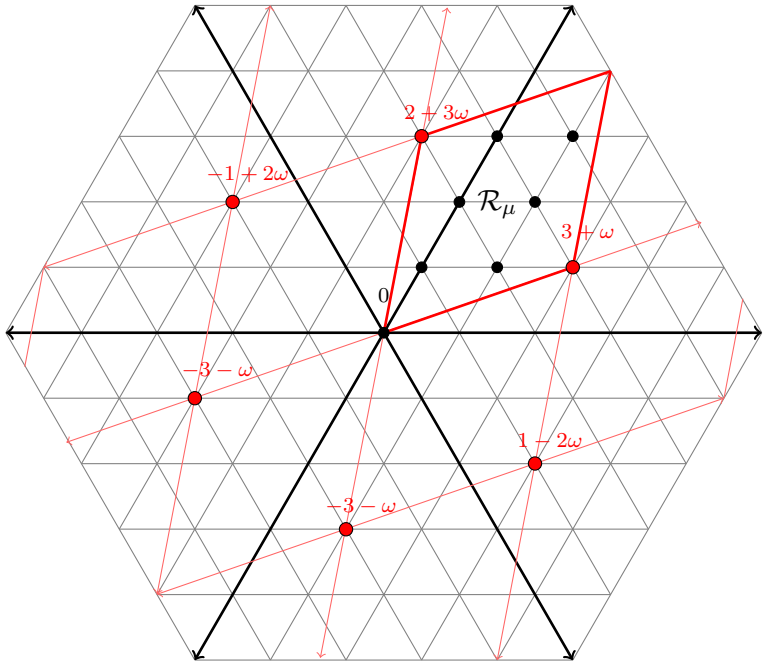

Figure 2.4: An illustration of a possible $\mathcal{R}_\mu$ (in black) in $\mathbb{Z}[\omega]$ for $\mu = 3 + \omega$.

In the integers, one valid representative set of $\mathbb{Z}_m$ is $\mathcal{R}_m = \{0, 1, \ldots, m-1\}$. In the Gaussian integers, by adding or subtracting unit multiples of μ from any element we can translate any point into or along the edges of a square with side lengths $|\mu|$. Furthermore, opposite sides of such a square are exactly an addition of unit multiple of μ apart from each other. Thus, a representative set, $\mathcal{R}_\mu$ in the Gaussians is made of the Gaussian integers covered by a square with side length $|\mu|$ including points on two adjacent edges, and excluding points on the other two. By a similar argument, a representative set in the Eisensteins is the set of Eisenstein integers included in a rhombus (with acute interior angle $\frac{\pi}{6}$) and side length $|\mu|$ with those along an adjacent pair of the edges included, and those along the other two edges excluded.

2.7 The Law of Quadratic Reciprocity

However, before we proceed further into more unusual domains, we will first introduce a remarkable property of the integers that is both beautiful for its own sake and a helpful

tool for applying theorems that we will prove later. In order to introduce the theorem, we first need a new operation on two prime numbers.

Definition 2.27. (Legendre Symbol) We define the Legendre symbol of two numbers, $a, p \in \mathbb{Z}$, where p is prime, written $\left(\frac{p}{q}\right)$ as

$$\left(\frac{1}{p}\right) = \begin{cases} 1 & \text{if there exists a nonzero } x \text{ such that } a \equiv x^2 \mod q \\ 1 & \text{if there is no nonzero } x \text{ such that } a \equiv x^2 \mod q \\ 0 & \text{if } a \equiv 0 \mod q \end{cases} . \tag{2.20}$$

An immediate consquence of the definition is that the Legendre symbol is multiplicative in a. That is,

Lemma 2.28. *If $a, b, p \in \mathbb{Z}$, and p is prime, then*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right). \tag{2.21}$$

.

Proof. If both a, b are quadratic residues (that is, there exists $x_a, x_b \in \mathbb{Z}$ such that $a \equiv x_a^2, b \equiv x_b^2 \mod p$), then

$$ab \equiv x_a^2 x_b^2 \equiv (x_a x_b)^2 \mod p \tag{2.22}$$

So ab is also a quadratic residue, which confirms

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1 \cdot 1 = \left(\frac{ab}{p}\right). \tag{2.23}$$

If a is a quadratic residue and b is not, then if ab were a square, we would get

$$ab \equiv x_a^2 b \equiv x_{ab}^2. \tag{2.24}$$

Dividing both sides by x_a^2, we get $b = \left(\frac{x_{ab}}{x_a}\right)^2$, which is a contradiction, since b was not a square.

Finally, if neither a nor b are quadratic residues, then pick n such that $a \equiv n x_a^2$, $b \equiv n x_b^2$ for some numbers x_a, x_b, which must exist since neither a nor b is square. Thus $ab \equiv n^2 x_a^2 x_b^2$ is a quadratic residue.

The following theorem, originally proven by Gauss, has a variety of different proofs.[4]

Theorem 2.29 (Quadratic Reciprocity [HW79])**.** *If p and q are odd primes, then*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right), \tag{2.25}$$

unless both p and q are of the form $4k+3$, in which case

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right). \tag{2.26}$$

We will soon apply an extension of this powerful property beyond the integers in order to examine features of proofs in the following chapters.

[4]Gauss is known for personally having proven it over ten different ways order to build up intuition for why the statement was true.

Chapter 3

Prime Generating Polynomials

We define a polynomial as a function of the form

$$f(x) = a_n x^n + \ldots + a_1 x + a_0. \tag{3.1}$$

If each $a_i \in R$, a ring, then f defines a map, $R \to R$. So far, we will avoid defining the ring, R, which is both the domain and range of these functions, since they can be realized as functions over any ring that their coefficients belong to. In order for the map to be well defined, we simply need to have addition and multiplication to both be well-defined concepts. That being said, we hope to relate polynomials to the appearance of prime numbers, so there we would prefer to examine the behavior of polynomials over rings where the primes have properties that we can recognize familiarly. Specifically, we would like to examine polynomials over norm-Euclidean domains.

We are most familiar with polynomials defined over the integers, $f : \mathbb{Z} \to \mathbb{Z}$. However, this is not the only setting for such a map to be realized. Natural extensions of the integers, such as the Gaussian or Eisenstein integers are also reasonable places to define these functions, since they are both rings. We will examine the Gaussian case briefly towards the end of this chapter and more throughly in the next one, where it will naturally lead us into a discussion of the Eisensteins and other Euclidean domains.

3.1 Polynomials and Prime Numbers

We call a polynomial with $a_i = 0$ for every $i > 1$ and $a_1 \neq 0$ a linear function, and for $i > 2$ with $a_2 \neq 0$, a quadratic function. From here on out, we will focus on the relationship between polynomials and prime elements of the domains to which they belong. With linear functions, we stand much more of a chance of proving connections with prime numbers. We derive this ability from the equivalence between arithmetic progressions (linear functions), $xa_1 + a_0$ and the equivalence class of a_0 modulo a_1, which number theorists have already derived a great deal of structure from.

Theorem 3.1 (Dirichlet)**.** *Let $f(x) = ax + b$ be a linear polynomial on the integers with a relatively prime to b. Let the set, $\mathcal{P}_{a,b}$ be the set of prime numbers in the range of f. Then $|\mathcal{P}_{a,b}| = \infty$.*

The proof of this theorem [Apo13] involves algebraic and analytic methods that are tangential to the subject matter of this thesis and otherwise overwhelmingly complicated. To justify ignoring the proof while we are interested in the properties of other polynomials, we will show that the same method that Dirichlet used would not be effective for polynomials of greater degree. The meat of Dirichlet's proof is the demonstration that the sum,

$$\sum_{p \in \mathcal{P}_{a,b}} \left(\frac{1}{p}\right) \tag{3.2}$$

diverges. However, for any quadratic this can not be the case:

Suppose that $f(x) = ax^2 + bx + c$ is a quadratic over the integers with $a > 0$. Let $\mathcal{P}_{a,b,c}$ be the set of prime numbers in the set of all numbers generated by f, R_f. Then, $\mathcal{P}_{a,b,c} \subseteq R_f$, so $|\mathcal{P}_{a,b,c}| \leq |R_f|$. Thus,

$$\sum_{x=0}^{\infty} \left(\frac{1}{f(x)}\right) \geq \sum_{p \in \mathcal{P}_{a,b,c}} \left(\frac{1}{p}\right). \tag{3.3}$$

However, the left hand side is bounded as well by the comparison test from calculus:

$$\sum_{x=0}^{\infty} \left(\frac{1}{f(x)}\right) = \sum_{x=0}^{\infty} \left(\frac{1}{ax^2 + bx + c}\right) \leq \sum_{x=0}^{\infty} \left(\frac{C}{x^2}\right) < \infty, \tag{3.4}$$

for some constant C. Thus the sum,

$$\sum_{p \in \mathcal{P}_{a,b,c}} \left(\frac{1}{p}\right) \tag{3.5}$$

converges.

Thus, while a quadratic may generate prime numbers more frequently than a linear function, the rate at which the prime numbers generated by the quadratic grows is qualitatively greater. For this reason, we cannot attempt a proof in the same style as Dirichlet, since that proof relied entirely on the divergence of a sum that for quadratics always converges.

Nevertheless, the statement that we would be aiming for was formalized by Littlewood and Hardy in their Conjecture F, which does provide some insight into the structure that modern mathematics believes is the case [HL23]:

Conjecture 3.2 (F)**.** *Let $a, b, c \in \mathbb{Z}$ with $a > 0$, $(a, b, c) = 1$, $a + b$ or c (or both) be odd, and $D = b^2 - 4ac$ is not a square*[1]*. Then, there are infinitely many primes of the form $am^2 + bm + c$, with the number $P(n)$ of such primes less than n is asymptotically given by*

$$P(n) \sim \frac{\varepsilon C}{\sqrt{a}} \frac{\sqrt{n}}{\log n} \prod \frac{\mathfrak{p}}{\mathfrak{p} - 1} \tag{3.6}$$

where $\mathfrak{p}$ is an odd prime divisor of both a and b, ε is 1 if $a + b$ is odd and 2 if it is even, and

$$C = \prod_{\varpi \geq 3, \varpi \nmid a} \left(1 - \frac{1}{\varpi - 1} \frac{D}{\varpi}\right).^2 \tag{3.7}$$

Note that within the conjecture, the only terms with an n-dependence were $\frac{\sqrt{n}}{\log(n)}$, which is what we would expect from a quadratic. The number of primes less than n that are values of the polynomial ought to have frequency of approximately a square root, since the quadratic will skip over terms at a square rate.

Despite its difficulty, Conjecture F is only helpful for the analysis of quadratics. For the purpose of any general polynomial, there is the Bunyakovsky Conjecture:

[1] This condition is equivalent to requiring that the quadratic factors over $\mathbb{Z}$.

[2] ϖ is a cursive π and the notation used within the original work.

Conjecture 3.3. *If $f(x)$ is an irreducible polynomial with positive leading coefficient and its coefficients are relatively prime, then $f(n)$ is prime for infinitely many n.*

However, this statement is not only unproven (of course), but there is not even a proof that such a polynomial as f generates a prime number at least once. Furthermore, this conjecture lacks any statement of the asymptotic nature of the prime generation—largely because the conjecture was formulated before many of the analytic findings were made in number theory. Both these conjectures alone are difficult tasks, but even if we attempt to make our lives easier and ask the Bunyakovsky conjecture solely about quadratics, at the intersection between the two conjectures, there is still no proof.

There is a generalization of these conjectures [BH62], but it is significantly more difficult to state and largely unrelated to the matter that this thesis is concerned with. However, there are other prime related properties of quadratics that are simpler to analyze.

3.2 Prime-Production Length

A simpler property of polynomials to study is how long of a streak of prime-generation they go on. This property was heavily examined by Mollin [Mol97], so we will use his definition here:

Definition 3.4 (Prime-production Length)**.** Consider $f(x) = ax^2 + bx + c$ $(a, b, c \in \mathbb{Z})$, $a \neq 0$. Suppose that $|f(x)|$ is prime for all integers, $x = 0, 1, \ldots, \ell_f - 1$ for some ℓ_f. If ℓ_f is the value such that $|f(\ell_f)|$ is composite, equal to 1 or equal to $|f(x)|$ for $x = 0, 1, \ldots, \ell_f - 1$, then $f(x)$ has prime-producing length ℓ_f.

In order to make a few quick assertions about the prime production length of polynomials over the integers, we will assume that prime k-tuple conjecture, which will require the following definition

Definition 3.5. A set, S, is admissible if for all primes p, there exists an $a_p \in \mathbb{Z}_p$ such

that,

$$\prod_{s \in S}(s + a_p) \neq 0. \tag{3.8}$$

In other words, for each prime p, there is a residue modulo p that no element of S is equivalent to. That is, there is no prime p such that S contains a member of each residue class modulo p.

Now we can state the conjecture.

Conjecture 3.6. *If S is an admissible set, then there are infinitely many $n \in \mathbb{Z}$ such that for every $s \in S$, $n + s$ is prime.*

Thus, the admissibility condition of the prime k-tuple conjecture states that as long as there is no obvious reason why a set of differences between numbers should not have infinitely many prime representations, then it will have infinitely realizations as the differences between primes.

A simple application of the conjecture is examined by Louboutin, Mollin, and Williams [LMW92]:

Theorem 3.7. *If the prime k-tuple conjecture holds, then for any integer $M > 0$, there exists a quadratic polynomial of the form $f(x) = x^2 + x + n$ such that $f(x)$ is prime for all integers x such that $1 \leq x \leq M$.*

We will skip the proof here. A sketch of the proof is to prove that the set $R = \{x^2 + x | x = 1, 2, \ldots, M\}$ is admissible. Later, we will attempt to generalize this to more polynomials by classifying when sets of the form, $R_{a,b} = \{ax^2 + bx | x = 1, 2, \ldots, M\}$ are admissible.

Looking more closely at the polynomials of the form described in Theorem 3.7, we can examine how "efficient" a polynomial is at generating its prime-producing radius. Specifically, we can ask about polynomials of the form $f(x) = x^2 + x + A$ that generate prime numbers until it is specifically denied at the x value, $A - 1$:

$$f(A-1) = A^2 - 2A + 1 + A - 1 + A = A^2.$$

We use Rabinowitsch's Criterion to make this task significantly easier.

Theorem 3.8 (Rabinowitsch's Criterion [Rab13])**.** *Let $f(x) = x^2 + x + A$ be a polynomial with discriminant $D = 1 - 4A \equiv 1 \mod 4$. Then $f(x)$ is prime for $x = 0, 1, \ldots, A-2$ if and only if the class number of the field $\mathbb{Q}(\sqrt{D})$ is 1.*

Combining this with the result of Gauss' class number one problem (for $D < 0$), that a field of the form $Q(\sqrt{D})$ has class number one if and only if $-D \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$ [Cox89], we find that the largest quadratic that produces only prime numbers up to the absolute bound of $A-1$ has discriminant 163. Of polynomials of the form x^2+x+A, whose discriminants are of the form, $D = 1 - 4A$, the value 163 corresponds to $A = 41$. This corresponds to the polynomial, $f(x) = x^2 + x + 41$, known as Euler's polynomial, which does indeed generate prime numbers for $x = 1, \ldots, 39$. Furthermore, there is no quadratic of the same form that has a prime-production radius of $A-2$ for a constant term, A which is larger than 41. Any polynomial of prime-production length $A-2$ must fit Rabinowitsch's Criterion, but if $A > 41$, then $D < -163$, so $h_D \neq 1$. Thus, the criterion is not satisfied for larger A.

3.3 The Prime-Production Radius

However, we would like to be able to extend our discussion to Euclidean domains other than the integers. The Gaussian integers are closely linked with the integers, and with the addition of the norm, form a Euclidean domain. In order to generalize our discussion of the prime-production length of a function, we need to alter our definition, since the norm only offers a partial ordering on $\mathbb{Z}[i]$.

Definition 3.9 (Prime-Production Radius)**.** Let $f(z) = az^2 + bz + c$ be a polynomial over some Euclidean domain, D, equipped with a Euclidean function, $N : D \to \mathbb{Z}$. Suppose that for every $z \in D$ such that $N(z) \leq \ell$, $f(z)$ is prime. If ℓ is the largest natural number such

that this holds (there exists $z' \in D$ such that $N(z') = \ell + 1$ and $f(z')$ is not prime), then $\ell = \ell_f$ is the prime-production radius of the polynomial, f.

In fact, this definition is more general than immediately necessary and describes a condition on any domain that we can define a Euclidean function on. For the Gaussian integers, the Euclidean function is the norm, and the definition mirrors that given in [FMT17]. Using this definition on the Gaussian integers, a proof by Fuentes, Meirose, and Tou [FMT17] allows us to bound the prime-production radius of a polynomial of the form in Theorem 3.7. There appears to be a minor counting error in the original paper, which has been corrected here. This correction leads to a weaker bound on the prime-production radius.

Theorem 3.10. *Let $f(\eta) = \eta^2 + \eta + \pi$ be a polynomial, $\mathbb{Z}[i] \to \mathbb{Z}[i]$ with π prime in $\mathbb{Z}[i]$. Let μ be a prime of minimal norm such that $D_f = 1 - 4\pi$ is a square modulo μ. Then, the prime-production radius, ℓ_f, is bounded above by $\frac{10}{4}N(\mu)$.*

Proof. Since D_f is a square modulo μ, the roots of f modulo μ are rational complex numbers modulo μ. By Gauss' Lemma, a special case of the rational root theorem, if the roots of a polynomial with integer coefficients are rational, then the roots are integers. Thus, the roots of f are integer residues modulo μ. That is, there are two solutions to the equation in $\mathbb{Z}[\omega]_\mu$,

$$f(\eta) \equiv 0 \mod \mu. \tag{3.9}$$

Recall that a residue square with corners at $0, \mu, \mu + i\mu, i\mu$ is a representative set for $\mathbb{Z}[i]_\mu$. By the fundamental theorem of algebra, f can achieve any value exactly twice. Note that there are exactly 4 primes that are multiples of μ: $\mu, i\mu, -\mu, -i\mu$. Thus, there are at most eight η values such that $f(\eta)$ is a prime multiple of μ. Since each residue square contains 2 multiples of μ (at the solutions to Equation 3.9), if we include 5 residue squares in a disk centered at the origin, the disk will necessarily contain at least one multiple of μ that is not a prime.

Thus, we are left with the question of how large a disk is needed to cover 5 residue squares. We claim that we need a disk of radius $\frac{\sqrt{10}}{2}|\mu|$, as sketched out in Figure 3.1.

The disk already contains four residue classes each with one corner on the origin, since the furthest corners of representative set are unit multiples of $\mu + i\mu$, which have a distance to the origin of $\sqrt{2}|\mu| < \frac{\sqrt{10}}{2}|\mu|$. Then the fifth representative set will be made up of the half square bounded by the points, $\frac{3}{2}\mu + \frac{1}{2}\mu i$, $\mu + \frac{1}{2}\mu i$, $\mu - \frac{1}{2}\mu i$, and $\frac{3}{2}\mu - \frac{1}{2}\mu i$.

Finally, to make sure that we are not double counting any edges, we will take those edges of each representative set that are facing upward to be the included adjacent edges of the representative set. If the orientation is such that only one edge is facing upward, we take the upward facing edge and the rightward facing edge.

Together, these sections cover five residue squares.

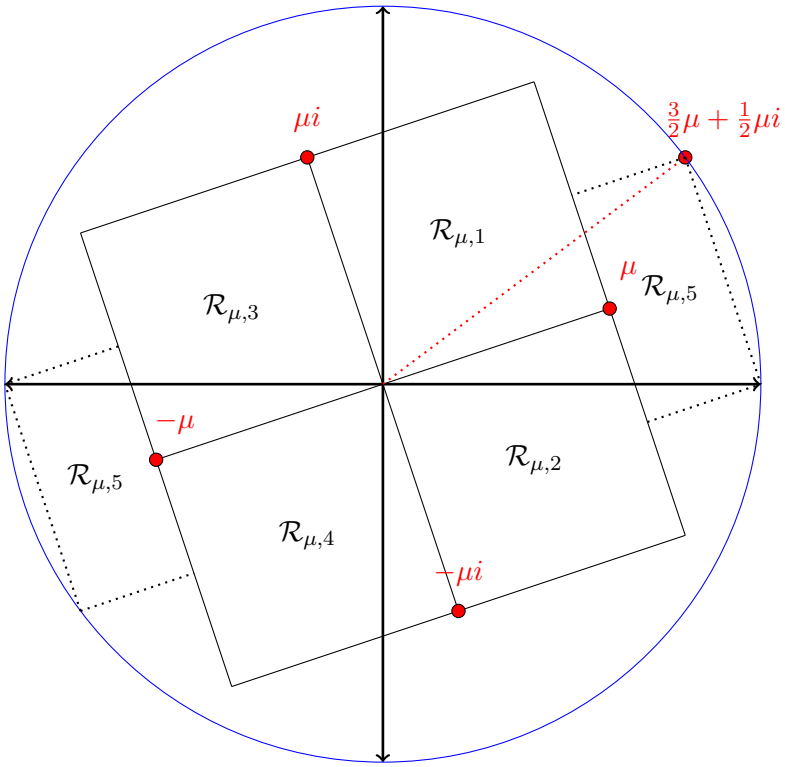

Figure 3.1: Five representative sets fitted within a circle of radius $\frac{\sqrt{10}}{2}|\mu|$.

Thus, a disk of radius $\frac{\sqrt{10}}{2}|\mu|$ will include at least two η-values such that $f(\eta)$ is not prime. Thus $N(\frac{\sqrt{10}}{2}\mu)$ is an upper bound on the prime-producing radius of the polynomial. That is, $\ell_f \leq \frac{10}{4}N(\mu)$. $\square$

In the next chapter, we will generalize this fact in a variety of ways. First, there is no reason why the same proof would not also work for an arbitrary quadratic, not just one of the restricted form of Theorem 3.10. Furthermore, we can generalize to any Euclidean domain as long as we are careful about what a "disk" is in the new space. Finally, by avoiding a discussion of the discriminant, a similar concept can be extended to polynomials of any degree.

Chapter 4

New Results on Prime Generating Polynomials

4.1 Bounds on the Prime Production Radius

As promised, this chapter begins with extensions of Theorem 3.10. The first extension does not require much effort. We state it formally, though, since it makes the same claim as the last theorem on a wider set of polynomials. Furthermore, we will not bother proving the theorem, since it follows the same proof as the one presented in [FMT17].

Theorem 4.1. *Let $f(\eta) = \eta^2 + \alpha z + \pi$ be an irreducible quadratic, $\mathbb{Z}[i] \to \mathbb{Z}[i]$ with π a prime element of $\mathbb{Z}[i]$. Let μ be a prime of minimal norm such that $D_f = \alpha^2 - 4\pi$ is a nonzero square modulo μ. Then the prime-production radius, ℓ_f, is bounded above by $\frac{10}{4}N(\mu)$.* $\square$

The same method of the proof for Theorem 3.10 can be extended to other norm-Euclidean domains, where the proof is altered but the crux of the proof is still the same. As a first step, we extend the theorem to the Eisenstein integers.

Theorem 4.2. *Let $f(\eta) = \eta^2 + \beta\eta + \pi$ be a monic quadratic with coefficients in $\mathbb{Z}[\omega]$. Furthermore, let μ be a prime of minimal norm such that $\Delta = \beta^2 - 4\pi$ is a nonzero square*

modulo μ. Then the prime production radius, ℓ_f, is bounded above by $3N(\mu)$.

Proof. Since D_f is a square modulo μ, the roots of the polynomial are of the form $\frac{-\beta \pm \sqrt{\Delta}}{2}$. Using a the contrapositive of [Her75, Lemma 3.11.4], we know that if f factors at all into rational parts, it must factor into linear polynomials with integer coefficeints, that is, the roots, ρ_1, ρ_2, are in $\mathbb{Z}[\omega]$. Thus, we can write

$$f(\eta) = \eta^2 + \alpha\eta + \pi \equiv (\eta - \rho_1)(\eta - \rho_2) \mod \mu. \tag{4.1}$$

Thus, over a given representative set for $\mathbb{Z}[\omega]_\mu$ written $\mathcal{R}_\mu$, $f(\eta) \equiv 0 \mod \mu$ for two values of η.

There are six units in $\mathbb{Z}[\omega]$, so there are six prime multiples of μ. Each of these values can be attained exactly a maximum of twice because f is a quadratic. Thus, the function can attain a prime multiple of μ 12 times before it must generate a composite multiple. This means that we need to include 7 representative sets for $\mathbb{Z}[\omega]_\mu$ (which will necessarily have 14 multiples of μ, since each representative set has two solutions to Equation 4.1) to be certain that we get at least one non-prime multiple.

Recall that we can take as a representative set all lattice points covered by a rhombus with with an acute angle of $\frac{\pi}{6}$ and side length of $|\mu| = \sqrt{N(\mu)}$. Furthermore, we can tile these efficiently across the Eisensteins in the manner suggested by Figure 4.1. The lattice suggested by the figure will not line up with the Eisenstein integers themselves. While they are both centered at the origin, the figure will be off by the angle between μ and 1. Examining Figure 4.1, within a circle of Eisenstein integers of norm $3N(\mu)$, we can encircle slightly more than 9 representative sets for $\mathbb{Z}[\omega]_\mu$ though we only need 7.

Sets 1, 2, and 3 are clearly representative sets from our discussion in Chapter 2. Adding μ to all elements of the upper triangle marked "4," we get a new set that is representative if and only if the earlier set was also representative. This set, though, is clearly representative, though, for the same reason that 1,2, and 3 were. For 5, we can subtract μ from the elements of the upper triangle, and for 6, we can subtract $\omega\mu$ from the lower upper triangle. Finally, we can add 3μ to the left seven set to see that 7 is also a representative set.

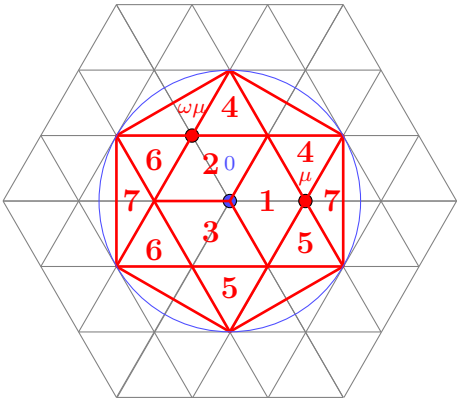

Figure 4.1: The circle on $\mathbb{Z}[\omega]$ that encircles all elements of a norm of $3\mu^2$. Note that it includes at least seven representative sets for $\mathbb{Z}[\omega]_\mu$.

Finally, this means that inside the circle of radius $\sqrt{3N(\mu)}$, there must be at least one η value such that $f(\eta)$ is not prime. Thus, the prime-production radius of f, $\ell_f \leq 3N(\mu)$. □

Note that there were two entirely unused representative sets (similar to the representative set 7) as well as a variety of Eisenstein integers that were left unused by the proof. Hypothetically, we could more precisely calculate a slightly lower bound that uses these other representative sets.

The significant difference between this proof and the same proof over the Gaussian integers is the larger number of units in $\mathbb{Z}[\omega]$, so there are more prime multiples of μ. On the other hand, representative sets in the two domains contain the same number of lattice points for μ's of the same norm. Thus, we needed an extra set of representative sets, which translated to needing to consider an increased radius to fit the extra representative sets. In general, the hexagonal structure of the Eisensteins is more conducive to fitting into circles. However, in our specific case, the number of representative sets that we needed to fit was not convenient and led to a lot of wasted space.

Furthermore, the Eisensteins have other structural features that weaken the strength of the proof. Namely, more lattice points fit within a certain radius in the Eisensteins than in the Gaussians. Gauss himself actually explored the issue for his eponymous set [Har59]:

Theorem 4.3 (Gauss' Circle Problem)**.** *The number of Gaussian integers with norm less than R^2, written $\mathcal{N}(R)$ is:*

$$\mathcal{N}(R) = \pi R^2 + E(R), \tag{4.2}$$

where $|E(R)| \leq 2\sqrt{2}\pi R$. □

The first part of the result is actually quite natural, since each square should correspond to a single lattice point. So, for every square of unit area of the circle, we should expect approximately a lattice point. However, in the case of the Eisensteins, we do not have so simple a problem. In order to be able to compare the structure of these lattices, we need a way of measuring the space taken up by various lattice types.

Without pursuing a tangent to too great an extreme, we claim without proof that the number of Gaussians with norm less than R^2, $\mathcal{N}(R)$ is [LP82]

$$\mathcal{N}(R) = \pi R^2 + O(R^{2/3}(\ln(R))^{1/2}), \tag{4.3}$$

which gives a slightly stronger error on the bound than the earlier solution to the problem. The value of the same counting function for the Eisensteins is [LP82]

$$\mathcal{N}(R) = \frac{2\pi R^2}{\sqrt{3}} + O(R^{2/3}(\ln(R))^{1/2}). \tag{4.4}$$

Now, we can finally more honestly compare the strength of the two proofs. The Gaussian proof yielded a bound of $10N(\mu)/4$, while the Eisenstein proof gave a bound of $3N(\mu)$. Thus the former bounded approximately $\frac{10\pi N(\mu)}{4}$ lattice points, and the latter $\frac{6\pi N(\mu)}{\sqrt{3}}$. The ratio of the two bounds is $8\sqrt{3} : 10$ or almost 1.4, so within the two bounds of the proofs, the Eisenstein proof contains nearly 40% more lattice points, making it that much less "efficient."

4.2 Finding μ

Of course, this proof is only really helpful if we are able to find a value of μ that satisfies the conditions of the theorem. Using the law of quadratic reciprocity (Theorem 2.29) we

can break down the question about squares modulo a large prime into questions about progressively smaller numbers until the answer becomes obvious.

Furthermore, it turns out that this theorem holds even more elegantly if we consider the same structure in Gaussians [Buc10]. We just need to consider the natural extension of the Legendre symbol to the Gaussians, where it has the same basic meaning.

Theorem 4.4. *If α, β are Gaussian primes, then*

$$\left(\frac{\alpha}{\beta}\right) = \left(\frac{\beta}{\alpha}\right). \tag{4.5}$$

This tool will prove helpful in telling whether a discriminant is a square modulo μ.

So, to check if D_f is a square mod μ, we can express the question as whether the equation $x^2 \equiv D_f \mod \mu$ has any solutions. If we factor D_f into its prime factorization, this becomes:

$$x^2 \equiv p_1^{r_1} \cdots p_n^{r_n} \mod \mu. \tag{4.6}$$

We are interested in telling whether this expression is a square. The expression is still a square under multiplication or division by other squares, so equation 4.6 is equivalent to

$$x^2 \equiv p_1' \cdots p_m' \mod \mu, \tag{4.7}$$

Where the p_i''s are the primes from equation 4.6 that had odd exponents. Furthermore, the multiplicativity of the Legendre symbol (Lemma 2.28) implies that the product of two quadraitic residues or two quadratic non-residues is a quadratic residue, while the product of one quadratic residue and one quadratic non-residue is not a quadratic reside. Thus, by checking whether each p_i' is a quadratic residue, we can evaluate whether D_f is a quadratic residue. Namely, we are left with expressions of the form

$$x^2 \equiv p_i' \mod \mu. \tag{4.8}$$

If an even number of them do not have a solution, then D_f is a square modulo μ, if an odd number do, then D_f is not a square modulo μ.

Example 4.5. In this example, we will examine the classic polynomial, $x^2 + x + 41$, but now as a polynomial over the Gaussian integers, where, in sticking with the complex number/Greek alphabet notation, we write $f(\eta) = \eta^2 + \eta + 41$. This polynomial still has the same discriminant as it did over the integers, -163. Selecting $\mu = 3 + 0i$, we see that:

$$-163 \equiv -1 \equiv i \cdot i \mod 3. \tag{4.9}$$

Thus, this value of μ has the necessary property for Theorem 3.10 to hold. Then, we can calculate the bound on the prime-production radius of f:

$$\ell_f \leq \frac{10}{4} N(\mu) = \frac{10 \cdot 9}{4} = 22.5. \tag{4.10}$$

That is, there must be some value of η with $N(\eta) < 22.5$ such that $f(\eta)$ is composite. This bound corresponds to a containing circle of radius $\sqrt{22.5} = 4.75$, which is much smaller compared to the prime generating length of f considered as a polynomial over the integers. Thus, we were able to make a claim about the polynomial f without ever having to plug a number in but simply by analyzing the structure of the discriminant. In fact, $f(1+i) = (1+i)^2 + 1 + i + 41 = 1 + 2i - 1 + 1 + i + 41 = 42 + 3i = 3(14 + i)$, so $f(1+i)$ is composite. So f actually has a prime-generating radius less than 2, so the bound that we developed is not as strong as it could be. That being said, the theorem did still prove enlightening in showing that f is not nearly as efficient over the Gaussians as it was over the integers.

4.3 Extensions to More Polynomials

So far, we have only addressed the problem for quadratics and linear polynomials. It turns out that a similar proof works for polynomials of any (finite) degree, but we have to be more careful about describing what μ is. For quadratics, we have the idea of a discriminant, which, if square, implies the existence of (Gaussian or Eisenstein) integral solutions to the quadratic by Gauss' Lemma [Ros93].

For a general polynomial the discriminant does not provide as much insight into the structure of the polynomial. We derive the discriminant from the quadratic formula. For, if the discriminant is a square, then every part of the expression is a whole (maybe imaginary) number. Thus, the discriminant encodes the factorability of polynomials in the Gaussians and Eisensteins. For the zeroes of a cubic polynomial, there does exist a formula corresponding to the same formula for the quadratic, but it is much larger and uses both square-roots and cube-roots. Thus, checking for a similar condition on the cubics would be a more difficult task.

Values that we could use like the quadratic discriminant do exist, but they two quantities, one of which lives under a square root and the other a cube root. For a cubic of the form $f(z) = az^3 + bz^2 + cz + d$, with $a, b, c, d \in \mathbb{Z}[\omega]$ or $\in \mathbb{Z}[i]$ to have integer solutions, we need $\Delta_1 = (2b^3 - 9abc + 27a^2d)^2 - 4(b^2 - 3ac)^3$ to be a square, and $\Delta_2 = \frac{1}{2}\left(2b^3 - 9abc + 27a^2d \pm \sqrt{\Delta_1}\right)$ needs to be a cube for both the plus and minus options. Furthermore, Eisenstein proved a corresponding principle to Gauss's called the law of cubic reciprocity that can be used in a similar manner to determine whether a number is a cube in a certain modulus [Ros93].

Extending this approach beyond the cubics is not impossible but quickly gets more difficult. Quartic polynomials also have a corresponding and even more complicated formula with more conditions to be satisfied, which we will not bother stating here. Beyond that, the quintic does not have a closed form solution in the same manner as lower order polynomials, so the same method no longer works [Ste15]. Furthermore, no polynomials of order 5 or greater have a general closed form solutions at all. This means that calculating the smallest possible value of μ for such polynomials would mostly be guesswork. However, on the chance that someone else finds an effective way to do this, we can extend our proof generally to polynomials of any order. We can do this over both the Eisensteins and the Gaussians, but the proof will be essentially the same in both cases, so we will perform it over the Gaussians and then make a similar statement over the Eisensteins without proof.

Theorem 4.6. *Let f be an irreducible polynomial with coefficients in $\mathbb{Z}[i]$ of degree n.*

Then, let μ be a prime of minimal norm such that f has n distinct roots in $\mathbb{Z}[i]_\mu$. That is,

$$f(z) \equiv \prod_{i=1}^{n}(z - r_i) \mod \mu, \tag{4.11}$$

where $r_i \neq r_j$ if $i \neq j$. Then the prime-production radius of f is bounded by $\frac{10}{4}N(\mu)$.

Proof. From the condition on μ, we know that for any representative set $\mathcal{R}_{1\mu}$ for $\mathbb{Z}[i]_\mu$, there will be n elements of $\mathcal{R}_{1\mu}$, $z_{11}, z_{12}, \ldots, z_{1n}$ such that $f(z_{1i}) \equiv 0 \mod \mu$. There are four units in $\mathbb{Z}[i]$, so there are four prime multiples of μ, each of which can be achieved by f n times. Thus, f can achieve a prime multiple of μ no more than $4n$ times.

Each representative set will include n multiples of μ, so if we include five representative sets, we have $5n$ multiples of μ, which exceeds the number of times that a prime multiple may be achieved. Thus a non-prime value will be achieved within the five representative sets. So, if we pick a radius that includes five representative sets, the prime-production radius will be less than that value. As seen in chapter 3, a norm-radius of $\frac{10}{4}N(\mu)$ satisfies the condition. □

We will state without proof the corresponding theorem for the Eisenstein integers.

Theorem 4.7. *Let f be an irreducible polynomial of order n with coefficients in $\mathbb{Z}[\omega]$. Then, let μ be a prime of minimal norm such that f has n distinct roots in $\mathbb{Z}[\omega]_\mu$, i.e.,*

$$f(z) \equiv \prod_{i=1}^{n}(z - r_i) \mod \mu \tag{4.12}$$

Where each r_i is unique. Then the prime-production radius of the polynomial is $3N(\mu)$. □

The bounds introduced by the two theorems are the same as for the quadratic case for a given μ value. However, we would expect that the value of μ that we can find to satisfy the condition to increase as n increases. As our discussion of the conditions on the cubic and quartic illustrated, μ needs to satisfy more conditions, so finding a value that satisfies all of them is going to simply be harder than it was in the quadratic case. Thus, while the bounds might look similar, their effective result would actually be rather different, and the

value of μ, not its coefficient would increase as the degree of the polynomial increases (in general).

4.4 Making Use of the Prime k-Tuple Conjecture

In chapter 3, we also asked how long the prime-production length of a polynomial could get over the integers, and Mollin showed that for quadratics of the form $z^2 + z + A$, we could expect A values such that the prime-production length gets arbitrarily long. He does note that none of these values past a streak of length 39 are known, though, and the A value for 39 is 41. Furthermore, Mollin's proof relies on acceptance of the Prime k-Tuple Conjecture, which is, unproven [Mol97].

This will not stop us from extending his results, though! In his proof, Mollin shows that $\{j^2 + j\}_{j=1}^{B}$ is admissible for any positive value of B. This corresponds directly to the fact that $z^2 + z + A$ has an arbitrarily long prime-production length. If we want to extend the proof to a larger set of quadratics, we want to explore what kind of sets of the form $\{r_j\} = \{aj^2 + bj\}_{j=1}^{B}$ are admissible sets.

There are some clear cases where $\{r_j\}$ is inadmissible. If $a + b$ is odd, then for $B \geq 2$ the set is clearly inadmissible, since it fails the definition of admissibility for $p = 2$. The set covers all residue classes of $\mathbb{Z}_2$, so it will necessarily always contain an element divisible by 2. Similarly, for sets of the form $\{3j^2 + j\}_{j=1}^{B}$, we quickly lose admissibility for $B \geq 3$. The set fails the admissibility test for $q = 3$, since the quadratic term will always be equivalent to 0 modulo 3 and the linear term will go through all possible residue classes, presenting the set from being admissible.

However, not all hope is lost. In fact, it appears that these are the only two conditions for a quadratic set not being admissible. These conditions, stated as requirements for admissibility are:

1. $a + b \equiv 0 \mod 2$, and
2. If $p|a$ then $p|b$.

Now, we will show that most other conditions do not seem to matter.

Theorem 4.8. *Sets of the form* $\{\ell(j^2+j(2k+1))\}_{j=1}^{B}$ *are admissible for any* $k \in \mathbb{N}$, $\ell \in \mathbb{Z}$.

Proof. Start with the fact that $\{j^2+j\}_{j=1}^{B}$ is admissible. Any subset of an admissible set is also admissible, since the same a_q's will still work in the definition of admissibility. We pick the subset, $\{j^2+j\}_{j=k+1}^{B}$. Reindexing, this set becomes $\{(j+k)^2+(j+k)\}_{j=1}^{B-k}$, which is equivalent to the set $\{j^2+(2k+1)j+k+k^2\}_{j=1}^{B-k}$. Since a constant shift does not alter whether a set is admissible (we just subtract that shift to each a_p), this means that the set $\{j^2+(2k+1)j\}_{j=1}^{B'}$ is also admissible (with $B'=B-k$).

Then, suppose that $\{r_j\}$ is an admissible set. For each q, there exists an a_q such that

$$\prod_{j=1}^{B}(r_j+a_q) \equiv r \mod q, \tag{4.13}$$

where $r \not\equiv 0 \mod q$. If we then consider the set $\{pr_j\}$, where p is prime, then, if $p \neq q$, we can consider the product,

$$\prod_{j=1}^{B}(pr_j+pa_q) \equiv pr \mod q. \tag{4.14}$$

(Since $p \neq q$, pr is still not equivalent to 0 modulo q). Thus, for all $q \neq p$, we can take a new $a'_q = pa_q$. Using this value, we can ascertain that $\{pr_j\}$ is admissible for all $q \neq p$.

If $p=q$, then the product becomes:

$$\prod_{j=1}^{B}(pr_j+a_p) \equiv \prod_{j=1}^{B} a_p \mod p. \tag{4.15}$$

Then, setting $a_p = 1$, the condition that the product is nonzero is satisfied. Thus, if a set is admissible, then any multiple of that set is also admissible. Using this principle in conjuction with the claim in the first half of the proof, the hypothesis is confirmed. □

This theorem almost provides all of the conditions that we need, but we are still missing the ability to multiply the quadratic term alone by a prime number that the linear term has already been multiplied by. What we do know is the admissibility of sets of the form $\{\ell(j^2+(2k+1)j)\}$. Thus, we can make the following statement about the corresponding quadratics.

Theorem 4.9. *If the prime k-tuple conjecture holds, then for any quadratic of the form* $f_A(z) = \ell z^2 + \ell(2k+1)z + A$*, where* $\ell, k \in \mathbb{Z}$*,* $A \in \mathbb{N}$ *and any value of* $N \in \mathbb{N}$*, there exists a value of* A *such that* f_A *has prime production length of at least* N*.* □

4.5 Areas of Further Research

In this thesis, we examined the prime-production properties of quadratics over two norm-Euclidean domains and the integers themselves. The similarity of the properties of these three algebraic structures allowed us to extend many of the concepts from the integers to the other two. However, there are a significant number of other norm-Euclidean domains. These domains, though, have different structures making generalization a difficult task. However, enough of the same structure remains, so we should expect the proof to proceed largely in the same manner only with a more difficult time spent bounding the size of the representative sets.

Beyond the norm-Euclidean domains, we begin to lose some of the structure that makes the question of prime-production well-defined. For instance, we need some amount of ordering in order to define the prime-production radius. Over norm-Euclidean domains, we defined the radius using the norm, but losing that structure, our ability to answer any such questions are weaker. Thus, we can ultimately only make claims about the total of 21 norm-Euclidean domains that exist [Slo13]. That being said, the proofs for higher order polynomials provided here do not make good use of the different structure of higher order polynomials, since the proof used was developed particularly for quadratic functions. However, as Galois Theory tells us, the structure of polynomials gets quantifiably more complicated as they increase in degree. Thus, it is not entirely unreasonable to expect no such effective proof as we were able to construct for quadratics.

With regards to the proofs on the length of prime number generation, there is room for improvement. Of course, none of the claims made are validated unless the Prime k-Tuple conjecture is proven, but even just a proof of the twin prime conjecture, a special case of the

prime k-tuple conjecture, is a long ways away from being proven [May15]. More reasonably, there is a gap in the statement of what we know excludes a sequence from being admissible and what we know forces a sequence to be admissible. It would not be entirely unreasonable to attempt to connect these two and develop a statement of the necessary and sufficient conditions for a quadratic set to be admissible.

Further research into the sets could examine polynomials sets of other degrees. While Mollin's proof of the admissibility of $\{j^2 + j\}$ relied on the quadratic nature of the set, it is not unreasonable to expect that a similar proof could show the admissibility of a set such as $\{j^3 + j^2\}$. Thus, with enough work, we could classify all the "types" of polynomials that can generate polynomials of any length.

Other topics for examination are the sizes of "prime-dense patches." These are regions (intervals in the integers, and circles of elements less than a certain norm in arbitrary norm-Euclidean domains) where the total ratio of prime numbers to total numbers generated is above some arbitrarily chosen ratio, r. These regions could yield to analyses such as those we applied to the Gaussians and Eisensteins in this thesis. Furthermore, by examining the sizes of these prime-dense patches as r gets smaller, we might be able to develop an approach to Littlewood and Hardy's unanswered Conjecture F.

Appendix A

An Introduction to Math-Speak

Below we explain a variety of formalisms used to make mathematical statements precisely. The reader is encouraged to read through the thesis as best as they can without looking here. If one finds themselves puzzled by a strange symbol, they can come here for to find its meaning.

A.1 Set Theory

A frequently used approach to expressing mathematical objects is through set theory. Sets are collections of objects that do not keep track of repetition, so the set $\{a, b, c, a\}$ is the same as the set $\{a, b, c\}$. Frequently, we need to build the sets that we will be working with. For this, we use set-builder notation:

$$A = \{\text{expression} \mid \text{condition on the expression}\}$$

This notation creates the set A of expressions that satisfy the conditions after the $|$. For instance, we can express the rational numbers in terms of the integers this way:

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z} \right\}.$$

In this expression, we used the element inclusion symbol, '$\in$.' The set symbols used in thiis thesis are all listed below.

$\in$: Inclusion of an element in a set. For instance, $1 \in \mathbb{Z}$.

$\subset$: Set inclusion: all the elements of one set are in another set too, $\mathbb{N} \subset \mathbb{Z}$.

A^c : The complement of A. That is, all the elements of the containing set that are not in A.

$\cup$: The union of two sets: $\{a, b\} \cup \{b, c\} = \{a, b, c\}$

$\cap$: The intersection of two sets: $\{a, b\} \cap \{b, c\} = \{b\}$.

$\setminus$: Set subtraction; can also be written $A \setminus B = B^c \cap A$.

$\bigcup, \bigcap$: The indexed intersections of sets: $\bigcup_{i=1}^{\infty} \{i\} = \mathbb{N}$.

A.2 List of Important Sets

$\varnothing$: The empty set, the set containing no elements.

$\mathbb{N}$: The natural numbers.

$\mathbb{Z}$: The integers.

$\mathbb{Z}[i]$: The Gaussian integers, $\{a + bi \mid a, b \in \mathbb{Z}\}$.

$\mathbb{Z}[\omega]$: The Eisenstein integers, $\{a + b\omega \mid a, b \in \mathbb{Z}\}$.

$\mathbb{Q}$: The rational numbers.

$\mathbb{R}$: The real numbers.

$\mathbb{C}$: The complex numbers, $\{a + bi \mid a, b \in \mathbb{R}\}$.

A.3 Logical Statements

s.t. : "Such that:" exactly what it means.

$\exists$: "There exists:" there is an element (frequently with a specific property). For instance, $\exists \alpha \in \mathbb{R}$ s.t. $\alpha^2 = 2$ (that is, $\sqrt{2}$ exists and is in $\mathbb{R}$).

$\forall$: "For all:" some statement holds for all elements of a set: $\forall x \in \mathbb{Z}, x + 0 = x$.

$\neg$: "Not:" the logical negation.

$\Rightarrow$: "Implies" or "only if".

$\Leftarrow$ "Is implied by" or "if".

$\Leftrightarrow$ "Is equivalent to" or "if and only if".

Appendix B

Tangential Number Thoery

Because number theory is such a large and diverse field of study, there are a variety of tools and theorems that are helpful for understanding the context of this work. Since describing many of these ideas in-line would be distracting and ultimately unhelpful, this appendix provides clarification as to the nature of many of these concepts.

B.1 The Prime Number Theorem

The prime number theorem gives an asymptotic limit of the frequency of primme numbers in the integers as their size increases. The original proof uses many concepts from analytic number theory that are truly entirely tangential to the purposes of this thesis. However, the statement of the theorem is very important for understanding the structure of the prime numbers, so we will produce it here.

Theorem B.1 (Prime Number Theorem)**.** *Let $\pi(n)$ be the number of prime numbers less than n. Then,*

$$\frac{\pi(n)}{n} \sim \frac{1}{\ln(n)}. \tag{B.1}$$

Or alternatively without the $\sim$ notation,

$$\lim_{n\to\infty} \frac{\pi(n)\ln(n)}{n} = 1. \tag{B.2}$$

Thus, the nth prime number will be approximately $n\ln(n)$.

Bibliography

[Apo13] Tom M Apostol. *Introduction to Analytic Number Theory*. Springer Science & Business Media, 2013.

[BH62] Paul T. Bateman and Roger A. Horn. A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, 16:363–367, 1962.

[Buc10] Nancy Buck. *Quadratic reciprocity for the rational integers and the Gaussian integers*. The University of North Carolina at Greensboro, 2010.

[Bun59] Viktor Bunjakovskii. *Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs*. Number v. 7. Academie impériale des sciences, 1859.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.

[Dir37] Peter Gustav Lejeune Dirichlet. Beweis des satzes, dass jede unbegrenzte arithmetische progression, deren erstes glied und differenz ganze zahlen ohne gemeinschaftlichen factor sind, unendlich viele primzahlen enthält. *Mathematische Werke*, pages 313–342, 1837.

[Euc08] Euclid. *Euclid's Elements of Geometry*. 2008.

[FMT17] Frank Fuentes, Monta Meirose, and Erik R. Tou. Quadratic prime-generating polynomials over the Gaussian integers. *Pi Mu Epsilon J.*, 14(6):365–372, 2017.

[GS00] Robert Gross and John H. Smith. A generalization of a conjecture of Hardy and Littlewood to algebraic number fields. *Rocky Mountain J. Math.*, 30(1):195–215, 2000.

[Har59] G. H. Hardy. *Ramanujan: twelve lectures on subjects suggested by his life and work*. Chelsea Publishing Company, New York, 1959.

[Hen76] Douglas Hensley. An asymptotic inequality concerning primes in contours for the case of quadratic number fields. *Acta Arith.*, 28(1):69–79, 1975/76.

[Her75] I. N. Herstein. *Topics in algebra.* Xerox College Publishing, Lexington, Mass.-Toronto, Ont., second edition, 1975.

[HL23] G. H. Hardy and J. E. Littlewood. Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes. *Acta Math.*, 44(1):1–70, 1923.

[HPS14] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An introduction to mathematical cryptography.* Undergraduate Texts in Mathematics. Springer, New York, second edition, 2014.

[HW79] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers.* The Clarendon Press, Oxford University Press, New York, fifth edition, 1979.

[JW03] Michael J. Jacobson, Jr. and Hugh C. Williams. New quadratic polynomials with high densities of prime values. *Math. Comp.*, 72(241):499–519, 2003.

[LMW92] Stéphane Louboutin, Richard A Mollin, and HC Williams. Class numbers of real quadratic fields, continued fractions, reduced ideals, prime-producing quadratic polynomials and quadratic residue covers. *Canad. J. Math*, 44:824–842, 1992.

[LP82] Peter D. Lax and Ralph S. Phillips. The asymptotic distribution of lattice points in Euclidean and non-Euclidean spaces. In *Toeplitz centennial (Tel Aviv, 1981)*, volume 4 of *Operator Theory: Adv. Appl.*, pages 365–375. Birkhäuser, Basel-Boston, Mass., 1982.

[May15] James Maynard. Small gaps between primes. *Ann. of Math. (2)*, 181(1):383–413, 2015.

[Mol97] R. A. Mollin. Prime-producing quadratics. *Amer. Math. Monthly*, 104(6):529–544, 1997.

[Rab13] Georg Rabinowitsch. Eindeutigkeit der zerlegung in primzahlfaktoren in quadratischen zahlkörpern. *Journal für die reine und angewandte Mathematik*, 142:153–164, 1913.

[Ros93] Kenneth H Rosen. *Elementary Number Theory and its Applications*. Addison-Wesley, 1993.

[RR07] Beata Randrianantoanina and Narcisse Randrianantoanina, editors. *Banach spaces and their applications in analysis*. Walter de Gruyter GmbH & Co. KG, Berlin, 2007.

[Sha59] Daniel Shanks. A sieve method for factoring numbers of the form $n^2 + 1$. *Math. Tables Aids Comput.*, 13:78–86, 1959.

[Sha60] Daniel Shanks. On the conjecture of Hardy & Littlewood concerning the number of primes of the form $n^2 + a$. *Math. Comp.*, 14:320–332, 1960.

[Slo13] N. J. A. Sloane. The on-line encyclopedia of integer sequences. *Ann. Math. Inform.*, 41, 2013.

[Ste15] Ian Stewart. *Galois theory*. CRC Press, Boca Raton, FL, fourth edition, 2015.

[TZ14] Mu-Tsun Tsai and Alexandru Zaharescu. On the distribution of algebraic primes in small regions. *Manuscripta Math.*, 145(1-2):111–123, 2014.

[vK01] Helge von Koch. Sur la distribution des nombres premiers. *Acta Math.*, 24(1):159–182, 1901.

[Yam17] Shuntaro Yamagishi. Prime solutions to polynomial equations in many variables and differing degrees. *arXiv preprint arXiv:1703.03332*, 2017. preprint.