Spring 5-16-2020

The Distribution of the Greatest Common Divisor of Elements in Quadratic Integer Rings

Asimina S. Hamakiotes
CUNY Bernard M Baruch College

The Distribution of the Greatest Common Divisor of Elements in Quadratic Integer Rings

Asimina S. Hamakiotes

Submitted to the committee of Undergraduate Honors at Baruch College of the City University of New York on April 27, 2020 in partial fulfillment of the requirements for the degree of Bachelor of Arts in Mathematics with Honors.

X 

Andrew Obus
Thesis Advisor

X Miriam Hausman

Miriam Hausman
Faculty Reader 1

Carlos Julio Moreno

X

Carlos Moreno
Faculty Reader 2

The Distribution of the Greatest Common Divisor of Elements in Quadratic Integer Rings

Asimina S. Hamakiotes

Abstract

For a pair of quadratic integers $\mathfrak{n}$ and $\mathfrak{m}$ chosen randomly, uniformly, and independently from the set of quadratic integers of norm x or less, we calculate the probability that the greatest common divisor of $(\mathfrak{n},\mathfrak{m})$ is $\mathfrak{K}$. We also calculate the expected norm of the greatest common divisor $(\mathfrak{n},\mathfrak{m})$ as x tends to infinity, with explicit error terms. We determine the probability and expected norm of the greatest common divisor for quadratic integer rings that are unique factorization domains. We also outline a method to determine the probability and expected norm of the greatest common divisor of elements in quadratic integer rings that are not unique factorization domains.

1 Introduction

In this paper, we study the distribution of the greatest common divisor of two elements in quadratic integer rings. We are specifically interested in the probability that two elements a,b chosen randomly, uniformly, and independently from a set will have greatest common divisor c. After calculating the probability, it is then natural to also want to calculate the expected norm of the greatest common divisor between a pair of elements in the same set. A more basic, motivating question is: what is the probability that two random positive integers are relatively prime?

To solve such a problem, first we have to define the probability. In order to define the probability, we have to restrict ourselves to the positive integers less than or equal to $n \in \mathbb{Z}^+$. We are interested in how likely it is that two positive integers x,y chosen randomly, uniformly, and independently from $0 \leq x,y \leq n$, will have greatest common divisor 1. In other words, for $x,y \in \mathbb{N}$, we want to count the ordered pairs (x,y) such that $x,y \leq n$ and x,y are relatively prime. We want to find:

$$\lim_{n\to\infty} \frac{\#\{x,y \leq n; x,y \in \mathbb{N}; (x,y) = 1\}}{n^2}.$$

What follows is a heuristic argument for how to calculate the probability that two integers are relatively prime, not a rigorous argument. In order to evaluate the limit above, we need to find the probability that x and y are divisible by the primes less than or equal to n. The probability that x is divisible by 2 is $\frac{1}{2}$ and the probability that y is divisible by 2 is $\frac{1}{2}$. The probability that both x and y are divisible by 2 is $\frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}$. We can repeat this for every prime less than or equal to n and express this limit in the following way:

$$\left(1-\frac{1}{2^2}\right)\cdot\left(1-\frac{1}{3^2}\right)\cdot\left(1-\frac{1}{5^2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p^2}\right) = \prod_p \left(1-\frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2},$$

where p is prime. Thus, the probability that two positive integers have greatest common divisor 1 (i.e. are relatively prime) is $\frac{1}{\zeta(2)}$, which equals $\frac{6}{\pi^2}$.

Bradley, Cheng, and Luo [1] change the integers to the Gaussian integers and calculate the probability, in a similar sense to that above, that two Gaussian integers $\mathfrak{n}$ and $\mathfrak{m}$ (chosen randomly, uniformly, and independently from the set of Gaussian integers) have greatest common denominator $\pm\kappa$ or $\pm i\kappa$, for a fixed Gaussian integer κ. Since this is a non-standard definition of probability, we will define what probability means for quadratic integer rings in Section

3.1. In addition, Bradley, Cheng, and Luo derive the expected norm of the greatest common divisor between a pair of Gaussian integers with norm x or less.

The goal of this paper is to extend the results of Bradley, Cheng, and Luo to principal ideal domains. Specifically, we present results for quadratic integer rings with unique factorization. We present results for $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, where $d = -3, -7, -11, -19, -43, -67,$ and -163. These are precisely the values of d such that the corresponding quadratic field has class number 1. We begin by calculating the probability that two nonzero ideals $\mathfrak{n}$ and $\mathfrak{m}$ in $\mathbb{Z}[\omega_d]$ have greatest common divisor $\mathfrak{K}$, where $\omega_d = \sqrt{d}$ if $d \equiv 2,3 \pmod 4$ and $\omega_d = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$. We then use the probability to determine the expected norm of the greatest common divisor of $\mathfrak{n}$ and $\mathfrak{m}$.

In Section 3.2 we present and prove our results for $\mathbb{Z}[\sqrt{-2}]$. First we establish and prove the probability that two nonzero ideals will have greatest common divisor $\mathfrak{K}$:

Theorem (3.2.5)**.** *Let $\mathfrak{n}$ and $\mathfrak{m}$ be nonzero ideals chosen independently and uniformly at random from the set of ideals in $\mathbb{Z}[\sqrt{-2}]$ with norm x or less. Let $\mathfrak{K}$ be a nonzero ideal of $\mathbb{Z}[\sqrt{-2}]$. The probability that $(\mathfrak{n},\mathfrak{m}) = \mathfrak{K}$ is*

$$\frac{1}{\zeta_{\mathbb{Q}(\sqrt{-2})}(2)N(\mathfrak{K})^2} + O\left(\frac{1}{x^{2/3}N(\mathfrak{K})^{4/3}}\right),$$

where $\zeta_{\mathbb{Q}(\sqrt{-2})}$ is the Dedekind zeta function for $\mathbb{Q}(\sqrt{-2})$.

We then use this probability to compute the expected norm of $\mathfrak{n}$ and $\mathfrak{m}$:

Theorem (3.2.6)**.** *Let $\mathfrak{n}$ and $\mathfrak{m}$ be nonzero ideals chosen independently and uniformly at random from the set of ideals in $\mathbb{Z}[\sqrt{-2}]$ with norm x or less. The expected norm of the greatest common divisor of $\mathfrak{n}$ and $\mathfrak{m}$ is*

$$\frac{\pi \log x}{2\sqrt{2}\zeta_{\mathbb{Q}(\sqrt{-2})}(2)} + O(1),$$

where $\zeta_{\mathbb{Q}(\sqrt{-2})}$ is the Dedekind zeta function for $\mathbb{Q}(\sqrt{-2})$.

In Section 3.3 we present and prove our results for $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, where $d = -3, -7, -11, -19, -43, -67,$ and -163. First we establish and prove the probability that two nonzero ideals will have greatest common divisor $\mathfrak{K}$:

Theorem (3.3.5)**.** *Let $\omega_d = \frac{1+\sqrt{d}}{2}$. For $d \leq -3$, let $\mathfrak{n}$ and $\mathfrak{m}$ be nonzero ideals chosen independently and uniformly at random from the set of ideals in $\mathbb{Z}[\omega_d]$ with norm x or less. The probability that $(\mathfrak{n},\mathfrak{m}) = \mathfrak{K}$ is*

$$\frac{1}{\zeta_{\mathbb{Q}(\omega_d)}(2)N(\mathfrak{K})^2} + O\left(\frac{1}{x^{2/3}N(\mathfrak{K})^{4/3}}\right),$$

where $\zeta_{\mathbb{Q}(\omega_d)}$ is the Dedekind zeta function for $\mathbb{Q}(\omega_d)$.

The following corollary is a direct consequence of Theorem 3.2.5 for the case when $\mathfrak{K} = (1)$:

Corollary (3.3.6)**.** *For $\mathbb{Q}(\omega_d)$ with class number 1, the probability that a pair of two ideals in $\mathbb{Z}[\omega_d]$ with norm x or less are relatively prime as $x \to \infty$ is:*

$$\frac{1}{\zeta_{\mathbb{Q}(\omega_d)}(2)}.$$

We then use the probability from Theorem 3.2.5 to compute the expected norm of $\mathfrak{n}$ and $\mathfrak{m}$:

Theorem (3.3.7)**.** *Let* $\omega_d = \frac{1+\sqrt{d}}{2}$*. For* $d \leq -3$*, let* $\mathfrak{n}$ *and* $\mathfrak{m}$ *be nonzero ideals chosen independently and uniformly at random from the set of ideals in* $\mathbb{Z}[\omega_d]$ *with norm x or less. The expected norm of the greatest common divisor of* $\mathfrak{n}$ *and* $\mathfrak{m}$ *is*

$$\frac{2\pi \log x}{|\mathbb{Z}[\omega_d]^\times| \cdot \sqrt{|d|} \cdot \zeta_{\mathbb{Q}(\omega_d)}(2)} + O(1),$$

where $\zeta_{\mathbb{Q}(\omega_d)}$ *is the Dedekind zeta function for* $\mathbb{Q}(\omega_d)$*.*

In addition to these results, we outline a method to compute the probability and expected norm for quadratic integer rings that are not unique factorization in Section 3.4. We provide an example of how to do so with $\mathbb{Z}[\sqrt{-5}]$.

2 Background

In order to understand how to calculate the distribution of the greatest common divisor of elements in quadratic integer rings, we need to first understand what quadratic integer rings are and how they behave. It is important that we define the algebraic and analytic number theoretic tools used in the proofs of this paper. We will also explain the number theoretic terms and concepts mentioned throughout the proofs that are neither algebraic nor analytic.

2.1 Algebraic Number Theory

In this section we will define the algebraic number theory concepts that we are studying in this paper. The following definitions will be used throughout the whole paper. We will begin by defining a quadratic integer ring.

A *quadratic integer* is an algebraic integer that solves an equation of the form $x^2 + Bx + C = 0$, where B and C are integers. For a squarefree integer d s.t. $d \neq 0, 1$, we define ω_d as follows:

$$\omega_d = \begin{cases} \sqrt{d} & \text{if } d \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Every quadratic integer can be written as $a + b\omega_d$. We define a *quadratic field*

$$K = \mathbb{Q}(\omega_d) = \{x + y\omega_d : x, y \in \mathbb{Q}\},$$

and say that K is a quadratic field with degree 2 over $\mathbb{Q}$. From K, we get O_K the ring of all algebraic integers of K. We define a *quadratic integer ring* as follows:

$$\mathbb{Z}[\omega_d] = \{a + b\omega_d : a, b \in \mathbb{Z}\}.$$

The ring $\mathbb{Z}[\omega_d]$ is the ring of all algebraic integers of $\mathbb{Q}(\omega_d)$. When $d > 0$, we say that $\mathbb{Z}[\omega_d]$ is a *real* quadratic integer ring. When $d < 0$, we say that $\mathbb{Z}[\omega_d]$ is an *imaginary* quadratic integer ring. Let D_K denote the *discriminant* of the quadratic field $K = \mathbb{Q}(\omega_d)$:

Definition 2.1.1. The *discriminant* of a quadratic field $K = \mathbb{Q}(\omega_d)$ is:

$$D_K = \begin{cases} 4d & \text{if } d \equiv 2,3 \pmod 4 \\ d & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Note that the minimal polynomial for ω_d when $d \equiv 2,3 \pmod 4$ is $x^2 - d$, and the minimal polynomial for ω_d when $d \equiv 1 \pmod 4$ is $x^2 - x - \frac{d-1}{4}$.

In order to understand how to work with quadratic integer rings, we will need to review some commutative ring theory. Let R be a ring (commutative, with identity). We say that $I \subseteq R$ is an *ideal* if

1. $a, b \in I$ implies $a+b \in I$, and
2. if $a \in I, r \in R$, then $ra \in I$.

Let $I \subseteq R$ be the ideal defined as follows:

$$I := \{r_1a_1 + r_2a_2 + ... + r_na_n : r_i \in R\}.$$

We say that I is the smallest ideal containing $a_1, a_2, ..., a_n$. This is equivalent to saying that I is the ideal *generated* by $a_1, a_2, ..., a_n$. A *principal ideal* I is an ideal that can be generated by one element. We say that a ring R is *noetherian* if every ideal of R is finitely generated. We define the product of two nonzero ideals $\mathfrak{a} = (\alpha_1, ..., \alpha_n)$ and $\mathfrak{b} = (\beta_1, ..., \beta_m)$ as simply $\mathfrak{ab} = (\alpha_1\beta_1, ..., \alpha_i\beta_j, ..., \alpha_n\beta_m)$.

For an element $\alpha = x + y\omega_d \in \mathbb{Z}[\omega_d]$, we define the *norm* of α as follows: $N(\alpha) = x^2 - y^2\omega_d^2$ when $d \equiv 2, 3 \pmod 4$ and $N(\alpha) = x^2 + xy + \left(\frac{1-d}{4}\right)y^2$ when $d \equiv 1 \pmod 4$. Similarly, we define the norm of an ideal $\mathfrak{a}$ to be the positive integer generating the ideal $\mathfrak{a}\overline{\mathfrak{a}}$. Note that the norm is multiplicative for both elements and ideals (i.e. $N(xy) = N(x)N(y)$ when x, y are elements of R and when x, y are ideals of R) and that the norm of a quadratic integer is always an integer.

Let $\mathbb{Z}[\omega_d]^\times$ denote the unit group of the quadratic integer ring $\mathbb{Z}[\omega_d]$. An element $x \in \mathbb{Z}[\omega_d]$ is a *unit* if and only if $N(x) = \pm 1$. If an ideal $I \subseteq R$ contains an invertible element a, then it also contains 1, because $a^{-1}a = 1$. Thus, I contains every element in R, so we write $I = R = (1)$ and call I the *unit ideal*, because it is the only ideal containing units. For most imaginary quadratic rings $\mathbb{Z}[\omega_d]$ there are two units ± 1. The exceptions are as follows: when $d = -1$ there are 4 units and when $d = -3$ there are 6 units. For real quadratic rings, it is not as easy to count units and we will soon see this.

We say that an element p of a ring R is *prime* if $p|ab$ implies either $p|a$ or $p|b$. We say that an element p of a ring R is *irreducible* if p is a prime such that $p = ab$ implies that either a or b must be a unit. A *maximal ideal* $I \subseteq R$ is an ideal $I \neq (1)$ such that if $J \supseteq I$ is an ideal, then $J = (1)$ or $J = I$. If R is a ring and M is a maximal ideal, then R/M is a field. Conversely, if M is an ideal and R/M is a field, then M is maximal. A *prime ideal* $I \subseteq R$ is an ideal $I \neq (1)$ such that if $a, b \in R$ with $ab \in I$, then $a \in I$ or $b \in I$. Every maximal ideal is a prime ideal. We say that R is an *integral domain* if it is commutative, nonzero, and has no divisors of 0 (i.e. $\forall a, b \in R$ such that $a, b \neq 0$, $ab \neq 0$). In an integral domain, every prime element is irreducible. If R is a ring and I is a prime ideal, then R/I is an integral domain. Conversely, if R/I is an integral domain, then I is a prime ideal.

Given a ring R and a subring K, an element $x \in K$ is said to be *integral over* R if x is a root of the monic polynomial with coefficients in R. We say that a ring R is *integrally closed* if when we let K be the fraction field of R, then the set $\{x \in K : x \text{ is integral over } R\} = R$. A ring R is called a *Dedekind domain* if:

1. R is an integral domain,
2. R is noetherian,
3. R is integrally closed,
4. and every nonzero prime ideal in R is maximal in R.

A Dedekind domain is an integral domain in which every nonzero, nonunit ideal factors into a product of prime ideals, unique up to the order of the factors. The ring of algebraic integers of any number field is a Dedekind domain.

An integral domain with a division algorithm is called a *Euclidean domain*. If a ring R is a Euclidean domain, then it is a *unique factorization domain* (UFD). In other words, if R is a Euclidean domain, then every nonzero element of R that is also not a unit can be written as a product of prime elements, uniquely up to order and units. If R is an integral domain in which every ideal is principal, then it is a *principal ideal domain* (PID). If R is a Euclidean domain, then it is also a PID. In other words, if R is a Euclidean domain, then every ideal of R it can be generated by one element.

Theorem 2.1.2. *If R is a principal ideal domain, then R is a unique factorization domain.*

Although it is true that every PID is a UFD, the converse is not true: it is not true that every UFD is a PID. Every polynomial ring $F[x_1, x_2, ..., x_n]$ is a UFD, but not a PID if $n > 1$, because $F[x_1, x_2, ..., x_n]$ cannot be generated by one element. If we look at the Gaussian integers $\mathbb{Z}[i]$, we see that $\mathbb{Z}[i]$ is a PID and a UFD. The ring $\mathbb{Z}[i]$ can be generated by a single element, and we can write every element in $\mathbb{Z}[i]$ as a unique product of primes, up to order and units. If we

look at the ring $\mathbb{Z}[\sqrt{-5}]$, we see that this is not the case: $\mathbb{Z}[\sqrt{-5}]$ is neither a UFD nor a PID. If we take an element $\alpha \in \mathbb{Z}[\sqrt{-5}]$ s.t. $N(\alpha) = 6$, we can see that $N(\alpha) = 6 = (2)(3) = (1+\sqrt{-5})(1-\sqrt{-5})$, where $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. The two factorizations are composed of irreducilbles and result with the same integer 6, so the factorizations of the integer 6 are not unique. Thus, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, and therefore, it is not a PID.

One way to keep track of the extent to which unique factorization fails in a ring $R = O_K$ is to use the *class number* of the field K, denoted h_K which we now define. A *fractional ideal* J_K is contained in K, but has the property that there exists an element $r \in R$ such that $rJ_K = \{rx : x \in J_K\}$ is an ideal in R. The *ideal class group* of a quadratic field K is the quotient group J_K/P_K, where J_K is the group of fractional ideals of O_K and P_K is the subgroup of principal ideals of O_K. The ideal class group measures the extent to which unique factorization fails in O_K. The order of the ideal class group is the class number of K.

In order to determine how many ideal classes there are in the ideal class group, we can use the *Minkowski bound* to give us an upper bound for the norm of the ideals we need to check. Minkowski's theorem says that every ideal class contains an ideal I with $N(I) \leq M_K$, where there is an explicit formula for M_K:

Proposition 2.1.3. *Let D_K be the discriminant of the field K and n be the degree of K over $\mathbb{Q}$ s.t. $n = 2r_2 + r_1$, where r_1 is the number of real embeddings and r_2 is the number of complex embeddings. Then every class in the ideal class group of K contains an integral ideal of norm not exceeding Minkowski's bound:*

$$M_K = \sqrt{|D_K|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}.$$

The ideal class group is generated by the prime ideals with norm not exceeding M_K. When looking at the Minkowski bound for real quadratic fields, we see that $n = 2, r_2 = 0$, so $M_K = \sqrt{|d|}\left(\frac{1}{2}\right)$. When looking at the Minkowski bound for imaginary quadratic fields, we see that $n = 2, r_2 = 1$, so $M_K = \sqrt{|d|}\left(\frac{2}{\pi}\right)$. The Minkowski bound is used to prove that every ideal class $[I]$ in the ideal class group of O_K can be represented by an ideal $I \subseteq O_K$ of small norm. It follows that the ideal class group is finite.

We have seen that a Dedekind domain need not be a PID with the example of the ring $\mathbb{Z}[\sqrt{-5}]$. Although the unique factorization of elements in such a ring does not hold, unique factorization of ideals does. We will review some properties of ideals and then state the fundamental theorem of arithmetic for ideals in Dedekind domains and define the greatest common divisor of ideals.

Let $\mathfrak{a}$ be a nonzero ideal in a ring R. For nonzero ideals $\mathfrak{b}, \mathfrak{c} \in R$, we have that $\mathfrak{ab} = \mathfrak{ac}$ if and only if $\mathfrak{b} = \mathfrak{c}$. For each nonzero ideal $\mathfrak{b} \in R$, we have that $\mathfrak{b} \subset \mathfrak{a}$ if and only if $\mathfrak{a}|\mathfrak{b}$. If $\mathfrak{a} \neq (1)$, then for each nonzero ideal $\mathfrak{b} \in R$, we have that $\mathfrak{ab} \subset \mathfrak{b}$ with strict inclusion. For two nonzero ideals $\mathfrak{a}, \mathfrak{b} \in R$, the two ideals are equivalent $\mathfrak{a} = \mathfrak{b}$ if and only if $\mathfrak{a}$ and $\mathfrak{b}$ are equal up to multiplication by a unit in R.

Theorem 2.1.4 (Fundamental theorem of arithmetic [2], Theorem 1.12)**.** *If R is a Dedekind domain, then every nonzero, nonunit ideal I of R can be represented uniquely in the form:*

$$I = \mathfrak{p}_1\mathfrak{p}_2...\mathfrak{p}_n,$$

where the $\mathfrak{p}_i$ are prime ideals, unique up to order of factors and units.

We can also express the ideal I as $\prod_i \mathfrak{p}_i^{\alpha_i}$, where the $\mathfrak{p}_i$ are distinct prime ideals and there are finitely many nonzero α_i's such that the α_i are positive integers.

Consider the imaginary quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$. We saw that the unique factorization of elements in $\mathbb{Z}[\sqrt{-5}]$ does not hold because we can express 6 as $(2)(3)$ and as $(1+\sqrt{-5})(1-\sqrt{-5})$. However, since $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain, the unique factorization of ideals does hold because we can express the ideal (2) as $(2, 1+\sqrt{-5})^2$, the ideal (3) as $(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$, the ideal $(1+\sqrt{-5})$ as $(2, 1+\sqrt{-5})(3, 1+\sqrt{-5})$, and the ideal $(1-\sqrt{-5})$

as $(2,1+\sqrt{-5})(2,1-\sqrt{-5})$. This is an example of a ring that has unique factorization of ideals, but not unique factorization of elements.

We now know about the unique factorization of ideals in quadratic integer rings $\mathbb{Z}[\omega_d]$, which are Dedekind domains. We also know how to compare and multiply two ideals $\mathfrak{a}$ and $\mathfrak{b}$. Now we will see what happens when we add two ideals $\mathfrak{a}$ and $\mathfrak{b}$. For nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathbb{Z}[\omega_d]$, let $\mathfrak{a}=\prod_i \mathfrak{p}_i^{\alpha_i}$ and $\mathfrak{b}=\prod_i \mathfrak{p}_i^{\beta_i}$, where the $\mathfrak{p}_i$'s are distinct nonzero prime ideals. We define the sum of two ideals $\mathfrak{a}+\mathfrak{b}$ as follows:

$$\mathfrak{a}+\mathfrak{b}=\prod_i \mathfrak{p}_i^{\min(\alpha_i,\beta_i)}.$$

We call the sum of two ideals $\mathfrak{a}$ and $\mathfrak{b}$ the *greatest common divisor* of the two ideals $\mathfrak{a}$ and $\mathfrak{b}$. Since divisibility among integral ideals is the same as containment, the greatest common divisor of two integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ is the same as the smallest ideal containing both of them, which is their sum $\mathfrak{a}+\mathfrak{b}$. We can also see this in a definition in terms of containment. The greatest common divisor $(\mathfrak{a},\mathfrak{b})$ is defined to be the ideal $\mathfrak{K}\subset\mathbb{Z}[\omega_d]$ which satisfies the following:

1. $\mathfrak{a}\subset\mathfrak{K}$ and $\mathfrak{b}\subset\mathfrak{K}$, and
2. if there exists some ideal $\mathfrak{c}\subset\mathbb{Z}[\omega_d]$ s.t. $\mathfrak{a}\subset\mathfrak{c}$ and $\mathfrak{b}\subset\mathfrak{c}$, then $\mathfrak{K}\subset\mathfrak{c}$.

The ideal $(\mathfrak{a},\mathfrak{b})$ is the smallest ideal that contains all the elements of both $\mathfrak{a}$ and $\mathfrak{b}$. Since $\mathbb{Z}[\omega_d]$ is a Dedekind domain, it is clear that the greatest common divisor of two ideals is unique.

Here we will briefly describe the behavior of primes in quadratic integer rings of quadratic fields. Let p be a prime such that $p\in\mathbb{Z}[\omega_d]$. We say that p behaves in the following way if it falls under the following conditions:

$$p=\begin{cases} split & \text{if there exist distinct primes } \mathfrak{p}_1,\mathfrak{p}_2\in\mathbb{Z}[\omega_d] \text{ s.t. } (p)=\mathfrak{p}_1\mathfrak{p}_2,\\ ramified & \text{if there exists a prime } \mathfrak{p}\in\mathbb{Z}[\omega_d] \text{ s.t. } (p)=\mathfrak{p}^2, \text{ and}\\ inert & \text{if there exists a prime } \mathfrak{p}\in\mathbb{Z}[\omega_d] \text{ s.t. } (p)=\mathfrak{p}. \end{cases}$$

For example, in $\mathbb{Z}[i]$ we can see that (2) is ramified since $(2)=(1+i)^2$. Here we see that $(2)=(2i)$, where i is a unit in $\mathbb{Z}[i]$, so (2) is ramified in $\mathbb{Z}[i]$. In general, a prime p is ramified if and only if p divides the discriminant D_K. If p is an odd prime that does not divide the discriminant D_K, then p splits if and only if d is a quadratic residue modulo p. If p is an odd prime that does not divide the discriminant D_K, then p is inert if and only if d is not a quadratic residue modulo p.

2.2 Analytic Number Theory

In this section we will define the analytic number theoretic concepts that appear in the proofs of the main theorems of this paper. The following definitions are applicable and important to several other areas of mathematics as well. We will begin by defining the ζ-function.

The *Riemann zeta function* ζ is the complex function defined on the half-plane for $s\in\mathbb{C}$ as the series:

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\ldots \text{ for } Re(s)>1.$$

The function $\zeta(s)$ does not apply to numbers that have $Re(s)<1$, because the sum does not converge for an infinite sum. If $Re(s)<1$, then $\zeta(s)$ will diverge, which means that instead of approaching a value, $\zeta(s)$ will get infinitely large. Thus, $\zeta(s)$ is only defined for $Re(s)>1$, where it converges. Riemann used analytic continuation (a method to extend the domain of a given analytic function) in order to give a value to every number except 1. When $s=1$, the series is a harmonic series which diverges to $+\infty$.

The zeta function is especially interesting because it can also be expressed as an infinite product of primes:

$$\zeta(s) = \prod_{p \text{ prime}}^{\infty} \frac{1}{1-p^{-s}} = \frac{1}{1-2^{-s}} \cdot \frac{1}{1-3^{-s}} \cdot \frac{1}{1-5^{-s}} \cdots \text{ for } s > 1.$$

This representation is also known as the Euler product representation of the zeta function. One of the many reasons that the Euler product is so significant is that it was the first connection between zeta functions and prime numbers.

It is particularly interesting to study the zeros of the Riemann zeta function. For $s \in \mathbb{C}$, the region $0 < Re(s) < 1$ is defined as the *critical strip*. The critical strip is where all of the nontrivial zeros (the zeros that are not at negative even integers) of the Riemann zeta function lie. The line defined by $Re(s) = \frac{1}{2}$ is called the *critical line*. The famous Riemann hypothesis states that all the nontrivial zeros of the Riemann zeta function lie on the critical line. Although the hypthesis has yet to be proved, Hardy proved that there are infinitely many zeros of the Riemann zeta function on the critical line. Since then, there have also been several other theorems proved that describe the density of the zeros on the critical line.

In this paper, we are interested in the similarly defined *Dedekind zeta function* of a number field. The Dedekind zeta function is a generalization of the Riemann zeta function.

Definition 2.2.1. For the number field K and the ring of integers O_K, the complex-valued *Dedekind zeta function* is defined for $Re(s) > 1$ by:

$$\zeta_K(s) = \sum_{\mathfrak{a} \subset O_K} \frac{1}{N(\mathfrak{a})^s},$$

where the summation is over the nonzero ideals $\mathfrak{a}$ of the ring O_K.

Let's observe the definition of the Dedekind zeta function for the Gaussian integers $\mathbb{Z}[i]$:

$$\zeta_{\mathbb{Q}(i)}(s) = \sum_{\mathfrak{a} \subset \mathbb{Z}[i]} \frac{1}{N(\mathfrak{a})^s} = \frac{1}{4} \sum_{\substack{(a,b) \in \mathbb{Z} \\ (a,b) \neq (0,0)}} \frac{1}{(a^2+b^2)^s},$$

where the first summation is over the nonzero ideals $\mathfrak{a}$ of the ring of Gaussian integers $\mathbb{Z}[i]$. The $\frac{1}{4}$ that appears is $\frac{1}{|O^{\times}_{\mathbb{Z}[i]}|}$, where $|O^{\times}_{\mathbb{Z}[i]}|$ is the number of units in $\mathbb{Z}[i]$. Dividing the summation by the number of units in the ring eliminates any over counting of pairs corresponding to the same ideal. For example, for $\alpha = a + bi \in \mathbb{Z}[i]$, the ideal $\mathfrak{a} = (\alpha)$ can be equivalently expressed as $(a+bi), (-a-bi), (a-bi)$, and $(-a+bi)$, so it is necessary to divide by 4, the number of units in $\mathbb{Z}[i]$, in order to not over count the ideals. This allows us to only count the distinct ideals in $\mathbb{Z}[i]$. The Dedekind zeta function appears in many parts of the paper, so it is important to understand the definition of it.

In order to relate the important invariants of a number field K to a special value of its Dedekind zeta function $\zeta_K(s)$ we will need to use the *class number formula*. The class number formula was first proved by Dirichlet only for quadratic fields. The formula for the limit in the theorem was proved by Dedekind and analytic continuation was proved by Hecke. We will first begin by explaining the components involved in the class number formula.

We are interested in the quadratic fields $K = \mathbb{Q}(\omega_d)$ s.t. d is square free and $d \neq 0, 1$. When $d > 0$, K is a real quadratic field, and when $d < 0$, K is an imaginary quadratic field. For a quadratic field K, r_1 is the number of real embeddings of K and r_2 is the number of complex embeddings of K. The degree of K is $n = r_1 + 2r_2$ and the rank of the unit group of O_K is $r = r_1 + r_2 - 1$. The rank of the unit group of a real quadratic field K is 1 ($r_1 = 2, r_2 = 0$), and the rank of an imaginary quadratic field K is 0 ($r_1 = 0, r_2 = 1$). The *regulator* of a quadratic field is defined as follows. For an imaginary quadratic field, it is 1, and for a real quadratic field it is the logarithm of its fundamental unit (a generator, modulo the roots of unity, for the unit group of $O_K = \mathbb{Z}[\omega_d]$ of K). The fundamental unit of O_K is $\frac{a+b\sqrt{D_K}}{2}$, where (a,b) is the smallest solution to $x^2 - D_K y^2 = \pm 4$ in $\mathbb{Z}^+$. We can see the definition of the discriminant

of K in Definition 2.1.1. The class number h_K of K is the order of the ideal class group of K, as seen in the previous section.

Now that we have defined everything we will need, we can state the class number formula:

Theorem 2.2.2 (Class number formula [3], Corollary 5.11)**.** *Let K be a number field of degree $n = r_1 + 2r_2$, where r_1 is the number of real embeddings of K and r_2 is the number of complex embeddings of K. The Dedekind zeta function $\zeta_K(s)$ converges absolutely for $Re(s) > 1$ and extends to a meromorphic function defined for all complex numbers $s \in \mathbb{C}$ with only one simple pole at $s = 1$, with residue*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}\cdot(2\pi)^{r_2}\cdot Reg_K \cdot h_K}{\omega_K \cdot \sqrt{|D_K|}},$$

where Reg_K is the regulator of K, h_K is the class number, ω_K is the number of roots of unity contained in K, and D_K is the discriminant of $K/\mathbb{Q}$.

Knowing the embeddings and regulator for quadratic integer fields, we can slightly simplify the class number formula. For real quadratic integer fields, we can simplify the right hand side of the class number formula to $\frac{4\cdot Reg_K\cdot h_K}{\omega_K\cdot\sqrt{D_K}}$, since $r_1 = 2, r_2 = 0$. For imaginary quadratic fields, we can simplify the right hand side of the class number formula to $\frac{2\pi\cdot h_K}{\omega_K\cdot\sqrt{D_K}}$, since $r_1 = 0, r_2 = 1, Reg_K = 1$. Now that we have the statement of the class number formula and understand what the embeddings of K, the regulator of K, the class number of K, the roots of unity of K, and the discriminant of K are, where K is either a real or imaginary quadratic field, we can use the class number formula in our calculations.

2.3 Extra Number Theory

In this section we will define a few concepts that appear in the proofs of the main theorems of this paper. The following definitions play a crucial role in understanding the roots of the theorems in this paper. We will begin by defining the function $r_d(n,2)$.

For an integer n and a quadratic integer ring $\mathbb{Z}[\omega_d]$, we define the function $r_d(n,2)$ to represent the distinct number of ways that n can be expressed as the norm of an element in $\mathbb{Z}[\omega_d]$, where d is a squarefree integer such that $d \neq 0, 1$. The function $r_d(n,2)$ is defined uniquely for every ring as follows:

Definition 2.3.1. Let n be an integer, d be a squarefree integer $(d \neq 0, 1)$, and $\mathbb{Z}[\omega_d]^\times$ denote the units of $\mathbb{Z}[\omega_d]$. Then

$$r_d(n,2) = \frac{1}{|\mathbb{Z}[\omega_d]^\times|}\#\{\alpha \in \mathbb{Z}[\omega_d] : N(\alpha) = n\}.$$

Let's observe the definition of $r_d(n,2)$ for the Gaussian integers $\mathbb{Z}[i]$:

$$r_{-1}(n,2) = \frac{1}{4}\#\{\alpha \in \mathbb{Z}[i] : N(\alpha) = n\}.$$

For the Gaussian integers, we know that there are 4 units $(\pm 1, \pm i)$, hence the $\frac{1}{4}$ in the definition. For $\alpha = a + bi \in \mathbb{Z}[i]$, we have that $N(\alpha) = a^2 + b^2$. For $r_{-1}(n,2)$ we are specifically looking for all of the $\alpha \in \mathbb{Z}[i]$ such that $N(\alpha) = a^2 + b^2 = n$. In particular, the function $r_{-1}(n,2)$ defined for $\mathbb{Z}[i]$ is the *sum of two squares function*. Carlos Moreno pointed out that $r_{-1}(n,2)$ is a special case of a theorem of Dirichlet giving a representation of $r_d(n,2)$ as a sum of Kronecker symbols taken over the divisors of n.

The definition of $r_d(n,2)$ as counting elements with norm n is analogous to counting integer lattice points in ellipses. Going back to the example of $r_{-1}(n,2)$ for $\mathbb{Z}[i]$, we can think of $r_{-1}(n,2)$ as counting all of the distinct integral points (a,b) in the circle $x^2 + y^2 = n$, centered at the origin with radius $\sqrt{n}$ and then dividing by 4. *Gauss'*

circle problem asks how many integral points of the form (a,b) lie in the circle $x^2+y^2=r^2$, centered at the origin with radius r. In other words, Gauss' circle problem asks how many pairs of integers (a,b) there are such that:

$$a^2+b^2 \leq r^2.$$

When we start to look at other rings, we realize that we are no longer dealing with norms that give us the equation of a circle, but rather norms that give us the equation of an ellipse. For example, let's observe what happens when we look at $r_d(n,2)$ for the imaginary quadratic ring $\mathbb{Z}[\sqrt{-2}]$:

$$r_{-2}(n,2) = \frac{1}{2}\#\{\alpha \in \mathbb{Z}[\sqrt{-2}] : N(\alpha) = n\}. \tag{1}$$

Here, the norm of an element $\alpha = a+\sqrt{-2}b \in \mathbb{Z}[\sqrt{-2}]$ is defined as $N(\alpha) = a^2+2b^2$, which is the equation of an ellipse. Analogous to Gauss' circle problem, we want to find how many integral points (a,b) lie in the ellipse $a^2+2b^2 = n = r^2$, centered at the origin. In other words, we want to know how many pairs of integers (a,b) there are such that:

$$a^2+2b^2 \leq r^2.$$

Thinking of $r_d(n,2)$ in terms of integral lattice points in a closed curve allows us to express $r_d(n,2)$ in different ways. The Polish mathematician Wacław Sierpiński used $r_{-1}(n,2)$ in the following result [4]:

$$\sum_{n=1}^{x} r_{-1}(n,2) = \pi x + O(x^{\frac{1}{3}}). \tag{2}$$

If we think of $r_{-1}(x,2)$ as the number of integral points that lie in the circle $a^2+b^2=x$, then we can see how the summation of all the integral points in the circle $a^2+b^2=x$ with all possible integral norms 1 through x is simply equal to the area of the circle plus an error term. The error term $O(x^{1/3})$ is the same for all continuous closed curves and has been improved upon by Huxley [5] to $O(x^{\frac{131}{416}+\varepsilon})$.

In addition to equation (2), Sierpiński also formed the following result using $r_{-1}(n,2)$ [6]:

$$\sum_{n=1}^{x} \frac{r_{-1}(n,2)}{n} = \pi(S+\log x) + O\left(x^{\frac{-1}{2}}\right), \tag{3}$$

where S denotes the *Sierpiński constant* $S \approx 2.58/\pi$. Sierpiński's constant is more concretely defined as follows:

$$S = \frac{1}{\pi}\lim_{z\to\infty}\left(4\zeta(z)\beta(z) - \frac{\pi}{z-1}\right) = \gamma + \frac{\beta'(1)}{\beta(1)},$$

where $\beta(z)$ is the Dirichlet beta function (defined in Section 1.7 of [7]) and γ is the Euler-Mascheroni constant (defined in Section 1.5 of [7]). In this paper, we will not use Sierpiński's constant, but it is important to know that for equation (3) there is some constant $C+\log x$.

Here we will state and prove a result using $r_d(n,2)$ and $\sigma_0(n)$, where $\sigma_0(n)$ represents the number of divisors of n.

Proposition 2.3.2. *For a unique factorization domain $\mathbb{Z}[\omega_d]$ and a positive integer n,*

$$r_d(n,2) \leq \sigma_0(n).$$

Proof. An element n has norm n^2 and every element with norm n divides n, so we want to count the factors of n in $\mathbb{Z}[\omega_d]$ whose norm is n. When we factor n over $\mathbb{Z}$ into prime factors, we express the prime factorization of n as:

$$n = \prod_{p \text{ prime}} p_i^{a_i},$$

where the a_i's are positive integers. The prime factorization of n over $\mathbb{Z}[\omega_d]$ is the same except that some factors may split or ramify, so we express the prime factorization of n as:

$$n = \prod_{p_i \text{ ramified}} \mathfrak{r}_i^{2a_i} \cdot \prod_{p_i \text{ inert}} (p_i)^{a_i} \cdot \prod_{p_i \text{ split}} (\mathfrak{q}_i\overline{\mathfrak{q}_i})^{a_i},$$

where $\mathfrak{r}_i^2 = (p_i)$, $\mathfrak{q}_i\overline{\mathfrak{q}_i} = (p_i)$, the p_i's are distinct primes, and b, a_i's are positive integers. The question is, how many ways are there to choose a factor with norm n from the product above? Note that we are only concerned with finding an upper bound.

For the primes that ramify (ω_d^b), there is one way to choose a factor. For the primes that are inert $\left(\prod_{\mathfrak{p}_i \text{ inert}} \mathfrak{p}_i^{a_i}\right)$, there is also only one way to choose a factor. For the primes that split $\left(\prod_{\mathfrak{p}_i \text{ split}} (\mathfrak{q}_i\overline{\mathfrak{q}_i})^{a_i}\right)$, we have a choice of how many of each of the two prime factors we use. For $\mathfrak{q}_i\overline{\mathfrak{q}_i} = \mathfrak{p}_i$, we have that $N(\mathfrak{q}_i) = N(\overline{\mathfrak{q}_i}) = \mathfrak{p}_i$. The norm of the $\mathfrak{p}_i$-part, $(\mathfrak{q}_i\overline{\mathfrak{q}_i})$, of this product is $\mathfrak{p}_i^{a_i}$, where a_i is a positive integer. So the number of ways we can choose primes $\mathfrak{q}_i, \overline{\mathfrak{q}_i}$ is $a_i + 1$. We can express the overall upper bound for the number of ideals of $\mathbb{Z}[\omega_d]$ with norm n as:

$$r_d(n,2) \leq \prod_{\mathfrak{p}_i \text{ split}} (a_i + 1) \leq \sigma_0(n),$$

where $\sigma_0(n)$, the number of prime factors of n, is equal to $\prod_{p_i \text{ prime}}(a_i + 1)$. □

We will use this statement to find bounds for terms in our future calculations.

In order to equip ourselves with the tools we need to complete certain steps of the proofs in this paper, we must familiarize ourselves with *Stieltjes integration by parts*. Stieltjes integration allows you to integrate a continuous real-valued function $f(x)$ with respect to a discontinuous real-valued function $g(x)$. The integral $\int_a^b f(x)dg(x)$ is defined to be the limit of the sum

$$\sum_{i=1}^{n} f(t_i)(g(x_i) - g(x_{i-1})) \text{ as } n \to \infty,$$

where $t_i \in [x_{i-1}, x_i]$ and the norm of the partition (the length of the longest subinterval) $\{a = x_0 < x_1 < \ldots < x_n = b\}$ of the interval $[a,b]$ approaches 0. We can use any continuous function for $f(x)$ and any continuous or discontinuous function for $g(x)$, such as $\lfloor x \rfloor$ or in our case $r(n,2)$. When both $f(x)$ and $g(x)$ are continuous and g is differentiable, the integral $\int_a^b f(x)dg(x)$ equals $\int_a^b f(x)g'(x)dx$.

Theorem 2.3.3. *Let f, g be two real-valued functions such that f is continuous. Then*

$$\int_a^b f(x)dg(x) = f(b)g(b) - f(a)g(a) - \int_a^b g(x)df(x).$$

In order to express Sierpiński's results for other quadratic integer rings, we will use Stieltjes integration by parts to evaluate $\sum_{n=1}^{x} \frac{r_d(n,2)}{n}$. To do this, we think of the sum as $\sum_{n=1}^{x} \frac{1}{n} \cdot r_d(n,2)$ and let $f(n) = \frac{1}{n}$ and $g(n) = \sum_{n=1}^{x} r_d(n,2)$. We can then express equation (3) as follows:

$$\sum_{n=1}^{x} \frac{r_d(n,2)}{n} = \int_1^x \frac{1}{n} d\left(\sum_{i=1}^{n} r_d(i,2)\right) = \frac{1}{x}\sum_{n=1}^{x} r_d(n,2) - 1 - \int_1^x \left[\sum_{i=1}^{n} r_d(i,2)\right] \frac{-1}{n^2} dn. \tag{4}$$

We will later evaluate this equation for $r_d(n,2)$ of other quadratic integer rings in order to calculate necessary results for the proofs of the main theorems of this paper.

In addition to this background, we will need to introduce the *Möbius function*. The Möbius function has an identity, inversion formula, and generating function.

Definition 2.3.4. For an ideal $\mathfrak{n}$, the *Möbius function* $\mu(\mathfrak{n})$ is defined by:

$$\mu(\mathfrak{n}) = \begin{cases} 1 & \text{if } \mathfrak{n} = (1); \\ (-1)^t & \text{if } \mathfrak{n} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_t \text{ for distinct prime ideals } \mathfrak{p}_i; \\ 0 & \text{if } \mathfrak{p}^2|\mathfrak{n} \text{ for some prime } \mathfrak{p}. \end{cases}$$

We can see that when $\mu(\mathfrak{n}) \neq 0$, n is squarefree. The following identity holds as a consequence:

Proposition 2.3.5 (Möbius identity function)**.** *For an ideal* $\mathfrak{n}$ *in a quadratic ring (or Dedekind domain), we have that the sum of the Möbius function over the divisors* $\mathfrak{d}$ *of* $\mathfrak{n}$*, is*

$$\sum_{\mathfrak{d}|\mathfrak{n}} \mu(\mathfrak{d}) = \begin{cases} 1 & \text{if } \mathfrak{n} = (1); \\ 0 & \text{if } \mathfrak{n} \neq (1). \end{cases}$$

A proof of this can be seen in Theorem 2.1 of [8]. It is important to note that the division of ideals makes sense because of unique factorization of ideals, as seen in Section 2.1. This identity is useful in the proof of the Möbius inversion formula, which states that:

Theorem 2.3.6 (Möbius inversion formula)**.** *Any arithmetic function* $f(\mathfrak{n})$ *can be expressed in terms of its sum function* $g(\mathfrak{n}) = \sum_{\mathfrak{d}|\mathfrak{n}} f(\mathfrak{d})$ *as*

$$f(\mathfrak{n}) = \sum_{\mathfrak{d}|\mathfrak{n}} \mu(\mathfrak{d}) g\left(\frac{\mathfrak{n}}{\mathfrak{d}}\right).$$

The functions $f(\mathfrak{n})$ *and* $g(\mathfrak{n})$ *are said to be Möbius transformations of each other.*

The Möbius function also has the following generating function:

$$\sum_{\mathfrak{n}\subset\mathbb{Z}[i]} \frac{\mu(\mathfrak{n})}{N(\mathfrak{n})^s} = \frac{1}{\zeta_{\mathbb{Q}(i)}(s)}, \text{ for } \mathrm{Re}(s) > 1. \tag{5}$$

We will need to use this generating function in parts of the proofs for the main theorems of this paper.

3 Results

We provide a method to find distribution of the greatest common divisor of elements in quadratic integer rings. Specifically, we describe how to find the probability that the greatest common divisor of two elements in a quadratic integer ring (chosen uniformly and independent from the set of all quadratic integers in the ring with norm x or less) is $\mathfrak{K}$ and how to find the expected norm of the greatest common divisor of two elements in a quadratic integer ring.

3.1 Summary of Results for $\mathbb{Z}[i]$

Bradley, Cheng, and Luo [1] calculate the probability that a pair of random Gaussian integers (chosen uniformly and independent from the set of all Gaussian integers with norm x or less) has greatest common divisor (κ) for a fixed Gaussian integer κ, with explicit error terms. They then derive the expected norm of the greatest common divisor between a pair of Gaussian integers with norm x or less, with explicit error terms. Here we will state Bradley, Cheng, and Luo's main results.

The probability that two nonzero ideals $\mathfrak{n}$ and $\mathfrak{m}$, having norm at most x, will have greatest common divisor $\mathfrak{K}$ is defined to be the number of pairs of ideals of norm x or less which have greatest common divisor $\mathfrak{K}$ divided by the total number of pairs of ideals of norm x or less. The first theorem calculates the probability that two nonzero ideals $\mathfrak{n}$ and $\mathfrak{m}$ in $\mathbb{Z}[i]$ have greatest common divisor $\mathfrak{K}$ in $\mathbb{Z}[i]$.

Theorem 3.1.1 ([1], Theorem 1)**.** *Let* $\mathfrak{n}$ *and* $\mathfrak{m}$ *be nonzero ideals chosen independently and uniformly at random from the set of ideals in* $\mathbb{Z}[i]$ *with norm x or less. Let* $\mathfrak{K}$ *be an ideal of* $\mathbb{Z}[i]$*. The probability that* $(\mathfrak{n},\mathfrak{m}) = \mathfrak{K}$ *is*

$$\frac{1}{\zeta_{\mathbb{Q}(i)}(2)N(\mathfrak{K})^2} + O\left(\frac{1}{x^{2/3}N(\mathfrak{K})^{4/3}}\right).$$

This theorem allows us to calculate the expected norm of the greatest common divisor between a pair of ideals:

Theorem 3.1.2 ([1], Theorem 2)**.** *Let* $\mathfrak{n}$ *and* $\mathfrak{m}$ *be nonzero ideals chosen independently and uniformly at random from the set of ideals in* $\mathbb{Z}[i]$ *with norm x or less. The expected norm of the gcd of* $\mathfrak{n}$ *and* $\mathfrak{m}$ *is*

$$\frac{\pi}{4\zeta_{\mathbb{Q}(i)}(2)}\log x + O(1).$$

3.2 Results for $\mathbb{Z}[\sqrt{-2}]$

We present similar results for the imaginary quadratic integer ring $\mathbb{Z}[\sqrt{-2}]$. We calculate the probability that a pair of nonzero ideals $\mathfrak{n}$ and $\mathfrak{m}$ in $\mathbb{Z}[\sqrt{-2}]$ (chosen uniformly and independently at random from the set of ideals in $\mathbb{Z}[\sqrt{-2}]$ with norm x or less) has greatest common divisor $(\mathfrak{n},\mathfrak{m}) = \mathfrak{K}$, with an explicit error term. We then calculate the expected norm of the greatest common divisor $(\mathfrak{n},\mathfrak{m})$, with an explicit error term. We will begin by defining the important functions that we will use.

We can recall the definition of $r_{-2}(n,2)$ from equation (1), where an element $\alpha = a + \sqrt{-2}b \in \mathbb{Z}[\sqrt{-2}]$ has norm $N(\alpha) = a^2 + 2b^2$. As mentioned earlier, we think of $r_{-2}(n,2)$ as the number of integral points (a,b) in the ellipse $a^2 + 2b^2 = n$. In terms of Gauss' circle problem, we want to know how many pairs of integers (a,b) there are such that $a^2 + 2b^2 \leq n$.

Using this definition or $r_d(n,2)$ for $\mathbb{Z}[\sqrt{-2}]$, we are able to write a similar result to Sierpiński's equation (2):

Lemma 3.2.1. *The following counts the sum of the function* $r_{-2}(n,2)$ *for* $1 \leq n \leq x$*:*

$$\sum_{n=1}^{x} r_{-2}(n,2) = \frac{\pi x}{\sqrt{2}} + O\left(x^{1/3}\right).$$

Proof. Sierpiński [4] shows that $\sum_{n=1}^{x} r_{-1}(n,2)$ equals $A + O(x^{1/3})$, where A is the area of the circle $a^2 + b^2 = x$. Calculating this for $d = -2$, we find that $\sum_{n=1}^{x} r_{-2}(n,2)$ equals $A + O(x^{1/3})$, where A equals $\frac{\pi x}{\sqrt{2}}$, which is the area of the ellipse $a^2 + 2b^2 = x$. As a result, we get that the summation equals $\frac{\pi x}{\sqrt{2}} + O\left(x^{1/3}\right)$, where the error term $O(x^{1/3})$ appears as a result from summing $r_{-2}(n,2)$ for $1 \leq n \leq x$. □

The error term $O(x^{1/3})$ is the same for every continuous, closed curve and has been improved upon by Huxley [5]. In addition, we are also able to produce a similar result to Sierpiński's equation (3):

Lemma 3.2.2. *Then,*

$$\sum_{n=1}^{x} \frac{r_{-2}(n,2)}{n} = \frac{\pi}{\sqrt{2}}\left(1 - \frac{\sqrt{2}}{\pi} + \log x\right) + O\left(x^{-2/3}\right).$$

Proof. We begin by viewing the left-hand side as the product of two functions $f(n) = \frac{1}{n}$ and $g(n) = \sum_{i=1}^{n} r_{-2}(i,2)$. We then use Stieltjes integration by parts from Theorem 2.3.3 to evaluate the left-hand side, as in equation (4):

$$\sum_{n=1}^{x} \frac{r_{-2}(n,2)}{n} = \int_1^x \frac{1}{n} d\left(\sum_{i=1}^{n} r_{-2}(i,2)\right) = \frac{1}{x}\sum_{n=1}^{x} r_{-2}(n,2) - 1 - \int_1^x \left[\sum_{i=1}^{n} r_{-2}(i,2)\right] \frac{-1}{n^2} dn.$$

We can replace $\sum_{n=1}^{x} r_{-2}(n,2)$ with $\frac{\pi x}{\sqrt{2}} + O(x^{1/3})$, as in Lemma 3.2.1, and reduce the equation to:

$$\begin{aligned}
&= \frac{1}{x}\left(\frac{\pi x}{\sqrt{2}} + O\left(x^{1/3}\right)\right) - 1 + \int_1^x \left[\frac{\pi n}{\sqrt{2}} + O\left(n^{1/3}\right)\right]\frac{1}{n^2}dn \\
&= \frac{\pi}{\sqrt{2}} + \frac{O\left(x^{1/3}\right)}{x} - 1 + \int_1^x \left[\frac{\pi}{\sqrt{2}n} + \frac{O\left(n^{1/3}\right)}{n^2}\right]dn \\
&= \frac{\pi}{\sqrt{2}} + O(x^{-2/3}) - 1 + \frac{\pi}{\sqrt{2}}\left(\log n + O(n^{-2/3})\Big|_1^x\right) \\
&= \frac{\pi}{\sqrt{2}} - 1 + \frac{\pi}{\sqrt{2}}\log x + O\left(x^{-2/3}\right) \\
&= \frac{\pi}{\sqrt{2}}\left(1 - \frac{\sqrt{2}}{\pi} + \log x\right) + O\left(x^{-2/3}\right),
\end{aligned}$$

where $\left(1 - \frac{\sqrt{2}}{\pi}\right)$ is our version of Sierpiński's constant for $\mathbb{Z}[\sqrt{-2}]$. □

Since $\left(1 - \frac{\sqrt{2}}{\pi}\right)$ is a small constant, in future calculations we may approximate this result as $\frac{\pi}{\sqrt{2}}\log x + O\left(x^{-2/3}\right)$. Lemma 3.2.1 and Lemma 3.2.2 are used to perform calculations throughout the rest of this section.

Proposition 3.2.3. *The total number of pairs of nonzero ideals* $\mathfrak{n}$ *and* $\mathfrak{m}$ *in* $\mathbb{Z}[\sqrt{-2}]$ *with norm x or less is:*

$$\frac{\pi^2 x^2}{8} + O(x^{4/3}).$$

Proof. In the proof below, $\mathfrak{n}$ and $\mathfrak{m}$ always range through nonzero ideals of $\mathbb{Z}[\sqrt{-2}]$. Then

$$\#\{\mathfrak{n},\mathfrak{m} \subset \mathbb{Z}[\sqrt{-2}]^2 : N(\mathfrak{n}), N(\mathfrak{m}) \le x\} \quad = \quad \sum_{\substack{\mathfrak{n}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{n})\le x}} \sum_{\substack{\mathfrak{m}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{m})\le x}} 1.$$

We can rewrite this as follows and use Lemma 3.2.1 to simplify:

$$\begin{aligned}
= \quad \left[\frac{1}{2}\sum_{N(\mathfrak{n})=1}^{\lfloor x\rfloor} r_{-2}(N(\mathfrak{n}),2)\right]\left[\frac{1}{2}\sum_{N(\mathfrak{m})=1}^{\lfloor x\rfloor} r_{-2}(N(\mathfrak{m}),2)\right] \quad &= \quad \frac{1}{4}\sum_{N(\mathfrak{n})=1}^{\lfloor x\rfloor} r_{-2}(N(\mathfrak{n}),2)\sum_{N(\mathfrak{m})=1}^{\lfloor x\rfloor} r_{-2}(N(\mathfrak{m}),2) \\
= \quad \frac{1}{4}\left[\frac{\pi x}{\sqrt{2}} + O(x^{1/3})\right]^2 \quad = \quad \frac{1}{4}\left[\frac{\pi^2 x^2}{2} + \frac{2\pi x}{\sqrt{2}}O(x^{1/3}) + O(x^{2/3})\right] \quad &= \quad \frac{\pi^2 x^2}{8} + O(x^{4/3}).
\end{aligned}$$

□

In order to be able to calculate the probability that $\mathfrak{n}$ and $\mathfrak{m}$, having norm less than or equal to x, will have the greatest common divisor $\mathfrak{K}$, we will also need to calculate the total number of pairs of nonzero ideals $\mathfrak{n}$ and $\mathfrak{m}$ in $\mathbb{Z}[\sqrt{-2}]$ with norm x or less having greatest common divisor $\mathfrak{K}$.

Proposition 3.2.4. *Let* $\mathfrak{K}$ *be a nonzero ideal in* $\mathbb{Z}[\sqrt{-2}]$. *The total number of pairs of nonzero ideals* $\mathfrak{n}$ *and* $\mathfrak{m}$ *in* $\mathbb{Z}[\sqrt{-2}]$ *with norm x or less having greatest common divisor* $(\mathfrak{n},\mathfrak{m}) = \mathfrak{K}$ *is:*

$$\frac{\pi^2 x^2}{8\zeta_{\mathbb{Q}(\sqrt{-2})}(2)N(\mathfrak{K})^2} + O\left(\frac{x^{4/3}}{N(\mathfrak{K})^{4/3}}\right).$$

Proof. In the proof below, $\mathfrak{n}$ and $\mathfrak{m}$ always range through nonzero ideals of $\mathbb{Z}[\sqrt{-2}]$. We will first prove the proposition for $\mathfrak{n}$ and $\mathfrak{m}$ relatively prime (i.e. for $(\mathfrak{n},\mathfrak{m}) = \mathfrak{K} = 1$). Then

$$\#\{\mathfrak{n},\mathfrak{m} \subset \mathbb{Z}[\sqrt{-2}]^2 : N(\mathfrak{n}), N(\mathfrak{m}) \leq x \text{ and } (\mathfrak{n},\mathfrak{m}) = 1\} = \sum_{\substack{\mathfrak{n}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{n})\leq x}} \sum_{\substack{\mathfrak{m}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{m})\leq x \\ (\mathfrak{n},\mathfrak{m})=(1)}} 1$$

$$= \sum_{\substack{\mathfrak{n}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{n})\leq x}} \sum_{\substack{\mathfrak{m}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{m})\leq x}} \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\sqrt{-2}] \\ \mathfrak{d}|(\mathfrak{n},\mathfrak{m})}} \mu(\mathfrak{d}),$$

where in the last line we use the Möbius function identity from Proposition 2.3.5. Reindexing with $\mathfrak{n} = \mathfrak{d}\mathfrak{n}'$ and $\mathfrak{m} = \mathfrak{d}\mathfrak{m}'$ where the norms of $\mathfrak{n}'$ and $\mathfrak{m}'$ range from 1 to $x/N(\mathfrak{d})$, we may rewrite this as:

$$\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{d})\leq x}} \mu(\mathfrak{d}) \sum_{\substack{\mathfrak{n}'\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{n}')\leq \frac{x}{N(\mathfrak{d})}}} \sum_{\substack{\mathfrak{m}'\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{m}')\leq \frac{x}{N(\mathfrak{d})}}} 1$$

Using equation (1), we can write:

$$= \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{d})\leq x}} \mu(\mathfrak{d}) \left[\frac{1}{2} \sum_{N(\mathfrak{n}')=1}^{\lfloor \frac{x}{N(\mathfrak{d})} \rfloor} r_{-2}(N(\mathfrak{n}'),2)\right] \left[\frac{1}{2} \sum_{N(\mathfrak{m}')=1}^{\lfloor \frac{x}{N(\mathfrak{d})} \rfloor} r_{-2}(N(\mathfrak{m}'),2)\right].$$

As in Proposition 3.2.3, this reduces to:

$$= \frac{1}{4} \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{d})\leq x}} \mu(\mathfrak{d}) \left[\frac{\pi^2 x^2}{2N(\mathfrak{d})^2} + O\left(\frac{x}{N(\mathfrak{d})}\right)^{4/3}\right].$$

We then distribute the summation to obtain the following:

$$= \frac{\pi^2 x^2}{8} \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{d})\leq x}} \frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2} + O\left(\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{d})\leq x}} \left(\frac{x}{N(\mathfrak{d})}\right)^{4/3}\right). \tag{6}$$

To evaluate the main term, we need to use the Möbius generating function from equation (5) to see that:

$$\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{d})\leq x}} \frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2} = \frac{1}{\zeta_{\mathbb{Q}(\sqrt{-2})}(2)} - \sum_{n=x+1}^{\infty} \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{d})=n}} \frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2},$$

which implies

$$\left|\frac{1}{\zeta_{\mathbb{Q}(\sqrt{-2})}(2)} - \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{d})\leq x}} \frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2}\right| \quad \leq \quad \sum_{n=x+1}^{\infty} \frac{1}{n^2} \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\sqrt{-2}] \\ N(\mathfrak{d})=n}} 1 \quad = \quad \frac{1}{2} \sum_{n=x+1}^{\infty} \frac{r_{-2}(n,2)}{n^2}.$$

Let $\sigma_0(n)$ represent the number of divisors of n. Using Proposition 2.3.2, we get that $r_{-2}(n,2) \leq \sigma_0(n) = o(n^{\varepsilon})$ for all $\varepsilon > 0$, where the divisor bound $o(n^{\varepsilon})$ comes from [9]. Thus, $\frac{1}{2}\sum_{n=x+1}^{\infty} \frac{r_{-2}(n,2)}{n^2}$ is less than or equal to $\sum_{n=x+1}^{\infty} \frac{o(n^{\varepsilon})}{n^2}$

which is equal to $o(x^{\varepsilon-1})$, and so

$$\Big|\frac{1}{\zeta_{\mathbb{Q}(\sqrt{-2})}(2)} - \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\sqrt{-2}]\\ N(\mathfrak{d})\leq x}} \frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2}\Big| \leq o(x^{\varepsilon-1}) \quad \text{or} \quad \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\sqrt{-2}]\\ N(\mathfrak{d})\leq x}} \frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2} = \frac{1}{\zeta_{\mathbb{Q}(\sqrt{-2})}(2)} + o(x^{\varepsilon-1}).$$

For the error term of equation (6), we have that:

$$\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\sqrt{-2}]\\ N(\mathfrak{d})\leq x}} \left(\frac{x}{N(\mathfrak{d})}\right)^{4/3} = \sum_{n=1}^{x} \frac{1}{n^{4/3}} \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\sqrt{-2}]\\ N(\mathfrak{d})=n}} 1 = \frac{1}{2}\sum_{n=1}^{x} \frac{r_{-2}(n,2)}{n^{4/3}}.$$

We can use the bound $r_{-2}(n,2) \leq o(n^{\varepsilon})$ to see that $\frac{1}{2}\sum_{n=1}^{x} \frac{r_{-2}(n,2)}{n^{4/3}}$ is less than or equal to $\sum_{n=1}^{x} o(n^{\varepsilon-4/3})$ which is equal to $o(x^{\varepsilon-1/3}) + o(1)$. From this we can see that $O\left(x^{4/3}\sum_{n=1}^{x} \frac{r_{-2}(n,2)}{n^{4/3}}\right)$ equals $O(o(x^{4/3}))$, which is equal to $O(x^{4/3})$ and thus, also equal to $o(x^{4/3})$. We can now rewrite (6) as follows:

$$\frac{\pi^2 x^2}{8\zeta_{\mathbb{Q}(\sqrt{-2})}(2)} + o(x^{\varepsilon-1}) + O(x^{4/3}).$$

This allows us to conclude:

$$\#\{\mathfrak{n},\mathfrak{m}\subset\mathbb{Z}[\sqrt{-2}]^2 : N(\mathfrak{n}),N(\mathfrak{m})\leq x \text{ and } (\mathfrak{n},\mathfrak{m})=(1)\} = \frac{\pi^2 x^2}{8\zeta_{\mathbb{Q}(\sqrt{-2})}(2)} + O(x^{4/3}).$$

We have calculated the number of $\mathfrak{n}$ and $\mathfrak{m}$ such that $(\mathfrak{n},\mathfrak{m}) = 1$ (i.e. $\mathfrak{n}$ and $\mathfrak{m}$ are relatively prime), and now we want to reindex to count the number of $\mathfrak{n}$ and $\mathfrak{m}$ such that $(\mathfrak{n},\mathfrak{m}) = \mathfrak{K}$. Let $\mathfrak{n} = \mathfrak{n}'\mathfrak{K}$ and $\mathfrak{m} = \mathfrak{m}'\mathfrak{K}$. Note that $\mathfrak{n}'$ and $\mathfrak{m}'$ are relatively prime if and only if $\mathfrak{n}$ and $\mathfrak{m}$ have $\mathfrak{K}$ as their greatest common divisor. Therefore, the number of relatively prime pairs $\mathfrak{n}'$ and $\mathfrak{m}'$ with norm y or less must be equal to the number of pairs $\mathfrak{n}$ and $\mathfrak{m}$, with norm $y\cdot N(\mathfrak{K})$ or less, having greatest common divisor $\mathfrak{K}$:

$$\begin{aligned}
&\#\{\mathfrak{n},\mathfrak{m}\subset\mathbb{Z}[\sqrt{-2}]^2 : N(\mathfrak{n}),N(\mathfrak{m})\leq x \text{ and } (\mathfrak{n},\mathfrak{m})=(\mathfrak{K})\} \\
&\qquad = \#\{\mathfrak{n}',\mathfrak{m}'\subset\mathbb{Z}[\sqrt{-2}]^2 : N(\mathfrak{n}'),N(\mathfrak{m}')\leq \frac{x}{N(\mathfrak{K})} \text{ and } (\mathfrak{n}',\mathfrak{m}')=(1)\} \\
&\qquad = \frac{\pi^2 x^2}{8\zeta_{\mathbb{Q}(\sqrt{-2})}(2)N(\mathfrak{K})^2} + O\left(\frac{x^{4/3}}{N(\mathfrak{K})^{4/3}}\right).
\end{aligned}$$

□

Now that we have Proposition 3.2.3 and Proposition 3.2.4, we can calculate the probability that the greatest common divisor of two nonzero ideals $\mathfrak{n}$ and $\mathfrak{m}$ is $\mathfrak{K}$:

Theorem 3.2.5. *Let $\mathfrak{n}$ and $\mathfrak{m}$ be nonzero ideals chosen independently and uniformly at random from the set of ideals in $\mathbb{Z}[\sqrt{-2}]$ with norm x or less. Let $\mathfrak{K}$ be a nonzero ideal of $\mathbb{Z}[\sqrt{-2}]$. The probability that $(\mathfrak{n},\mathfrak{m}) = \mathfrak{K}$ is:*

$$\frac{1}{\zeta_{\mathbb{Q}(\sqrt{-2})}(2)N(\mathfrak{K})^2} + O\left(\frac{1}{x^{2/3}N(\mathfrak{K})^{4/3}}\right).$$

Proof. The probability that $\mathfrak{n}$ and $\mathfrak{m}$, having norm less than or equal to x, will have greatest common divisor $\mathfrak{K}$ is defined to be the number of pairs of ideals of norm x or less which have greatest common divisor $\mathfrak{K}$ (Proposition 3.2.4) divided by the total number of pairs of ideals of norm x or less (Proposition 3.2.3). Therefore,

$$P_x\{\mathfrak{n},\mathfrak{m} \subset \mathbb{Z}[\sqrt{-2}]^2 : N(\mathfrak{n}),N(\mathfrak{m}) \leq x \text{ and } (\mathfrak{n},\mathfrak{m}) = \mathfrak{K}\}$$
$$= \left[\frac{\pi^2 x^2}{8\zeta_{\mathbb{Q}(\sqrt{-2})}(2)N(\mathfrak{K})^2} + O\left(\frac{x^{4/3}}{N(\mathfrak{K})^{4/3}}\right)\right] \cdot \left[\frac{\pi^2 x^2}{8} + O(x^{4/3})\right]^{-1}$$

We can rewrite $[\frac{\pi^2 x^2}{8} + O(x^{4/3})]^{-1}$ as $8\pi^{-2}x^{-2}[1+O(x^{-2/3})]^{-1}$ which is equal to $8\pi^{-2}x^{-2}[1+O(x^{-2/3})]$ since $[1+f(x)]^{-1}$ equals $1+O(f(x))$ for $f(x)$ tending towards 0 as $x \to \infty$. We can simplify the probability as:

$$= \left[\frac{\pi^2 x^2}{8\zeta_{\mathbb{Q}(\sqrt{-2})}(2)N(\mathfrak{K})^2} + O\left(\frac{x^{4/3}}{N(\mathfrak{K})^{4/3}}\right)\right] \cdot \left[8\pi^{-2}x^{-2}\left[1+O(x^{-2/3})\right]\right]$$
$$= \left[\frac{1}{\zeta_{\mathbb{Q}(\sqrt{-2})}(2)N(\mathfrak{K})^2} + O\left(\frac{1}{x^{2/3}N(\mathfrak{K})^{4/3}}\right)\right] \cdot \left[1+O(x^{-2/3})\right]$$
$$= \frac{1}{\zeta_{\mathbb{Q}(\sqrt{-2})}(2)N(\mathfrak{K})^2} + O\left(\frac{1}{x^{2/3}N(\mathfrak{K})^{4/3}}\right) + O\left(\frac{1}{x^{2/3}N(\mathfrak{K})^2}\right) + O\left(\frac{1}{x^{4/3}N(\mathfrak{K})^{4/3}}\right)$$
$$= \frac{1}{\zeta_{\mathbb{Q}(\sqrt{-2})}(2)N(\mathfrak{K})^2} + O\left(\frac{1}{x^{2/3}N(\mathfrak{K})^{4/3}}\right).$$

□

This probability will allow us to calculate the expected norm of the greatest common divisor between a pair of ideals $\mathfrak{n}$ and $\mathfrak{m}$.

Theorem 3.2.6. *Let* $\mathfrak{n}$ *and* $\mathfrak{m}$ *be nonzero ideals chosen independently and uniformly at random from the set of ideals in* $\mathbb{Z}[\sqrt{-2}]$ *with norm x or less. The expected norm of the greatest common divisor of* $\mathfrak{n}$ *and* $\mathfrak{m}$ *is:*

$$\frac{\pi \log x}{2\sqrt{2}\zeta_{\mathbb{Q}(\sqrt{-2})}(2)} + O(1).$$

Proof. We want to find the expected value of $N(\mathfrak{n},\mathfrak{m}) =: k$, where the norm of $\mathfrak{n}$ and $\mathfrak{m}$ ranges from 1 to x. In order to do this, we have to express the probability that for a nonzero ideal $\mathfrak{K} \in \mathbb{Z}[\sqrt{-2}]$, $\mathfrak{n}$ and $\mathfrak{m}$ have greatest common divisor $k = N(\mathfrak{K})$ in terms of k as well. The number of ideals with norm k in $\mathbb{Z}[\sqrt{-2}]$ is equal to $r_{-2}(k,2)/2$, where we divide $r_{-2}(k,2)$ by the number of units in $\mathbb{Z}[\sqrt{-2}]$. We can use Theorem 3.2.5 to express the probability that the greatest common divisor of $\mathfrak{n}$ and $\mathfrak{m}$ has norm k in terms of k as:

$$P_x\{N(\mathfrak{n},\mathfrak{m}) = k\} = \frac{r_{-2}(k,2)}{2\zeta_{\mathbb{Q}(\sqrt{-2})}(2)k^2} + O\left(\frac{r_{-2}(k,2)}{x^{2/3}k^{4/3}}\right).$$

By defintion, the expected value is:

$$E_x\{N(\mathfrak{n},\mathfrak{m})\} = \sum_{k=1}^{x} k \cdot P_x\{N(\mathfrak{n},\mathfrak{m}) = k\}$$
$$= \sum_{k=1}^{x} k \cdot \left[\frac{r_{-2}(k,2)}{2\zeta_{\mathbb{Q}(\sqrt{-2})}(2)k^2} + O\left(\frac{r_{-2}(k,2)}{x^{2/3}k^{4/3}}\right)\right]$$
$$= \frac{1}{2\zeta_{\mathbb{Q}(\sqrt{-2})}(2)} \sum_{k=1}^{x} \frac{r_{-2}(k,2)}{k} + O\left(\frac{1}{x^{2/3}} \sum_{k=1}^{x} \frac{r_{-2}(k,2)}{k^{1/3}}\right). \quad (7)$$

First, we want to simplify the error term in equation (7). We begin by using Stieltjes integration by parts from Theorem 2.3.3 to evaluate the summation:

$$\sum_{k=1}^{x} \frac{r_{-2}(k,2)}{k^{1/3}} = x^{-1/3} \sum_{k=1}^{x} r_{-2}(k,2) - 1 - \int_1^x \left(\frac{\pi k}{\sqrt{2}} + O\left(k^{1/3}\right) \right) \left(-\frac{1}{3} k^{-4/3} dk \right).$$

We then use Lemma 3.2.1 to simplify:

$$\begin{aligned} &= \frac{1}{x^{1/3}} \left(\frac{\pi x}{\sqrt{2}} + O\left(x^{1/3}\right) \right) - 1 + \frac{1}{3} \int_1^x \left[\frac{\pi}{\sqrt{2} k^{1/3}} + \frac{O(k^{1/3})}{k^{4/3}} \right] dk \\ &= \frac{\pi x^{2/3}}{\sqrt{2}} + O(1) - 1 + \frac{\pi}{3\sqrt{2}} \left(\frac{3k^{2/3}}{2} + O(\log k) \Big|_1^x \right) \\ &= \frac{3\pi x^{2/3}}{2\sqrt{2}} + O(\log x). \end{aligned}$$

This implies that the error term is:

$$\begin{aligned} O\left(\frac{1}{x^{2/3}} \sum_{k=1}^{x} \frac{r_{-2}(k,2)}{k^{1/3}} \right) &= O\left(\frac{1}{x^{2/3}} \cdot \left(\frac{3\pi x^{2/3}}{2\sqrt{2}} + O(\log x) \right) \right) \\ &= O\left(\frac{3\pi}{2\sqrt{2}} + x^{-2/3} O(\log x) \right) \\ &= O(1 + x^{-2/3} O(\log x)) \\ &= O(1). \end{aligned}$$

Now we want to rewrite the main term of equation (7) using our result from Lemma 3.2.2:

$$\begin{aligned} \frac{1}{2\zeta_{\mathbb{Q}(\sqrt{-2})}(2)} \sum_{k=1}^{x} \frac{r_{-2}(k,2)}{k} &= \frac{1}{2\zeta_{\mathbb{Q}(\sqrt{-2})}(2)} \left[\frac{\pi}{\sqrt{2}} \left(1 - \frac{\sqrt{2}}{\pi} + \log x \right) + O\left(x^{-2/3}\right) \right] \\ &= \frac{\pi \log x}{2\sqrt{2}\zeta_{\mathbb{Q}(\sqrt{-2})}(2)}. \end{aligned}$$

Combining the evaluated main term and error term from equation (7), we get that:

$$E_x\{N(\mathfrak{n},\mathfrak{m})\} = \frac{\pi \log x}{2\sqrt{2}\zeta_{\mathbb{Q}(\sqrt{-2})}(2)} + O(1).$$

□

3.3 Results for $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

In this section, we will present similar results for the imaginary quadratic rings of algebraic integers of $\mathbb{Q}(\omega_d)$ with class number 1. The class number is 1 for precisely the values $d = -3, -7, -11, -19, -43, -67,$ and -163, in addition to the values $d = -1$ and -2 that we have already seen. Except for -1 and -2, these are all values such that $d \equiv 1 (\text{mod } 4)$, so the quadratic ring will be of the form $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, where $d < 0$. The results in this section are strictly for $d \leq -3$ such that this refers to the values $d = -3, -7, -11, -19, -43, -67,$ and -163, unless stated otherwise.

Let $\omega_d = \frac{1+\sqrt{d}}{2}$. We can use Definition 2.3.1 to define $r_d(n,2)$ for $\mathbb{Z}[\omega_d]$. For $d < -3$, the quadratic integer ring $\mathbb{Z}[\omega_d]$ has 2 units (± 1) and an element $\alpha = a + \omega_d b \in \mathbb{Z}[\omega_d]$ has norm $N(\alpha) = a^2 + ab + \left(\frac{1-d}{4}\right) b^2$. For $d = -3$, the quadratic integer ring $\mathbb{Z}[\omega_{-3}]$ has 6 units $\left(\pm 1, \pm\frac{1\pm\sqrt{-3}}{2}\right)$ and an element $\alpha = a + \omega_{-3} b \in \mathbb{Z}[\omega_{-3}]$ has norm $N(\alpha) = a^2 + ab + b^2$. As mentioned earlier, we think of $r_d(n,2)$ as the number of integral points (a,b) in the ellipse $a^2 + ab + \left(\frac{1-d}{4}\right) b^2 = x$. In terms of Gauss' circle problem, we want to know how many pairs of integers (a,b) there are such that $a^2 + ab + \left(\frac{1-d}{4}\right) b^2 \leq n$.

Using this definition of $r_d(n,2)$ for $\mathbb{Z}[\omega_d]$, we are able to write a similar result to Lemma 3.2.1 from the previous section:

Lemma 3.3.1. *For $d \leq -3$, the following counts the sum of the function $r_d(n,2)$ for $1 \leq n \leq x$:*

$$\sum_{n=1}^{x} r_d(n,2) = \frac{2\pi x}{\sqrt{|d|}} + O(x^{1/3}),$$

where $|d|$ is the absolute value of d.

Proof. Sierpiński [4] shows that $\sum_{n=1}^{x} r_{-1}(n,2)$ equals $A + O(x^{1/3})$, where A is the area of the circle $a^2 + b^2 = x$. Calculating this for $d \leq -3$, we find that $\sum_{n=1}^{x} r_d(n,2)$ equals $A + O(x^{1/3})$, where A equals $\frac{2\pi x}{\sqrt{|d|}}$, which is the area of the ellipse $a^2 + ab + \left(\frac{1-d}{4}\right) b^2 = x$. As a result, we get that the summation equals $\frac{2\pi x}{\sqrt{|d|}} + O\left(x^{1/3}\right)$, where the error term $O(x^{1/3})$ appears as a result from summing $r_d(n,2)$ for $1 \leq n \leq x$. □

In addition, we are also able to produce a similar result to Lemma 3.2.2 from the previous section:

Lemma 3.3.2. *Then, for $d \leq -3$,*

$$\sum_{n=1}^{x} \frac{r_d(n,2)}{n} = \frac{2\pi}{\sqrt{|d|}} \left(1 - \frac{\sqrt{|d|}}{2\pi} + \log x\right) + O(x^{-2/3}),$$

where $|d|$ is the absolute value of d.

Proof. We begin by viewing the left-hand side as the product of two functions $f(n) = \frac{1}{n}$ and $g(n) = \sum_{i=1}^{n} r_d(i,2)$. We then use Stieltjes integration by parts from Theorem 2.3.3 to evaluate the left-hand side, as in equation (4):

$$\sum_{n=1}^{x} \frac{r_d(n,2)}{n} = \int_1^x \frac{1}{n} d\left(\sum_{i=1}^{n} r_d(i,2)\right) = \frac{1}{x}\sum_{n=1}^{x} r_d(n,2) - 1 - \int_1^x \left[\sum_{i=1}^{n} r_d(i,2)\right] \frac{-1}{n^2} dn.$$

We can replace $\sum_{n=1}^{x} r_d(n,2)$ with Lemma 3.3.1 and reduce the equation to:

$$\begin{aligned}
&= \frac{1}{x}\left(\frac{2\pi x}{\sqrt{|d|}} + O\left(x^{1/3}\right)\right) - 1 + \int_1^x \left[\frac{2\pi n}{\sqrt{|d|}} + O\left(n^{1/3}\right)\right] \frac{1}{n^2} dn \\
&= \frac{2\pi}{\sqrt{|d|}} + \frac{O\left(x^{1/3}\right)}{x} - 1 + \int_1^x \left[\frac{2\pi}{\sqrt{|d|} n} + \frac{O\left(n^{1/3}\right)}{n^2}\right] dn \\
&= \frac{2\pi}{\sqrt{|d|}} + O(x^{-2/3}) - 1 + \frac{2\pi}{\sqrt{|d|}} \left(\log n + O(n^{-2/3})\Big|_1^x\right) \\
&= \frac{2\pi}{\sqrt{|d|}} - 1 + \frac{2\pi}{\sqrt{|d|}} \log x + O\left(x^{-2/3}\right) \\
&= \frac{2\pi}{\sqrt{|d|}} \left(1 - \frac{\sqrt{|d|}}{2\pi} + \log x\right) + O\left(x^{-2/3}\right),
\end{aligned}$$

where $\left(1-\frac{\sqrt{|d|}}{2\pi}\right)$ is our version of Sierpiński's constant for $\mathbb{Z}[\omega_d]$. □

Since $\left(1-\frac{\sqrt{|d|}}{2\pi}\right)$ is a small constant, in future calculations we may approximate this result as $\frac{2\pi}{\sqrt{|d|}}\log x + O\left(x^{-2/3}\right)$. Lemma 3.3.1 and Lemma 3.3.2 are used to perform calculations throughout the rest of this section.

Proposition 3.3.3. *For $d \leq -3$, the total number of pairs of nonzero ideals $\mathfrak{n}$ and $\mathfrak{m}$ in $\mathbb{Z}[\omega_d]$ with norm x or less is:*

$$\frac{4\pi^2 x^2}{|\mathbb{Z}[\omega_d]^\times|^2 \cdot |d|} + O(x^{4/3}).$$

Proof. In the proof below, $\mathfrak{n}$ and $\mathfrak{m}$ always range through nonzero ideals of $\mathbb{Z}[\omega_d]$. Then

$$\#\{\mathfrak{n},\mathfrak{m} \subset \mathbb{Z}[\omega_d]^2 : N(\mathfrak{n}), N(\mathfrak{m}) \leq x\} \quad = \quad \sum_{\substack{\mathfrak{n}\subset\mathbb{Z}[\omega_d] \\ N(\mathfrak{n})\leq x}} \sum_{\substack{\mathfrak{m}\subset\mathbb{Z}[\omega_d] \\ N(\mathfrak{m})\leq x}} 1.$$

We can rewrite this as follows and use Lemma 3.3.1 to simplify:

$$= \left[\frac{1}{|\mathbb{Z}[\omega_d]^\times|}\sum_{N(\mathfrak{n})=1}^{\lfloor x\rfloor} r_d(N(\mathfrak{n}),2)\right]\left[\frac{1}{|\mathbb{Z}[\omega_d]^\times|}\sum_{N(\mathfrak{m})=1}^{\lfloor x\rfloor} r_d(N(\mathfrak{m}),2)\right] = \frac{1}{|\mathbb{Z}[\omega_d]^\times|^2}\sum_{N(\mathfrak{n})=1}^{\lfloor x\rfloor} r_d(N(\mathfrak{n}),2)\sum_{N(\mathfrak{m})=1}^{\lfloor x\rfloor} r_d(N(\mathfrak{m}),2)$$

$$= \frac{1}{|\mathbb{Z}[\omega_d]^\times|^2}\left[\frac{2\pi x}{\sqrt{|d|}} + O(x^{1/3})\right]^2 = \frac{1}{|\mathbb{Z}[\omega_d]^\times|^2}\left[\frac{4\pi^2x^2}{|d|} + \frac{4\pi x}{\sqrt{|d|}}O(x^{1/3}) + O(x^{2/3})\right] = \frac{4\pi^2x^2}{|\mathbb{Z}[\omega_d]^\times|^2\cdot|d|} + O(x^{4/3}).$$

□

In order to be able to calculate the probability that $\mathfrak{n}$ and $\mathfrak{m}$, having norm less than or equal to x, will have the greatest common divisor $\mathfrak{K}$, we will also need to calculate the total number of pairs of nonzero ideals $\mathfrak{n}$ and $\mathfrak{m}$ in $\mathbb{Z}[\omega_d]$ with norm x or less having greatest common divisor $\mathfrak{K}$.

Proposition 3.3.4. *Let $\mathfrak{K}$ be a nonzero ideal in $\mathbb{Z}[\omega_d]$. For $d \leq -3$, the total number of pairs of nonzero ideals $\mathfrak{n}$ and $\mathfrak{m}$ in $\mathbb{Z}[\omega_d]$ with norm x or less having greatest common divisor $(\mathfrak{n},\mathfrak{m}) = \mathfrak{K}$ is:*

$$\frac{4\pi^2x^2}{|\mathbb{Z}[\omega_d]^\times|^2\cdot|d|\cdot\zeta_{\mathbb{Q}(\omega_d)}(2)N(\mathfrak{K})^2} + O\left(\frac{x^{4/3}}{N(\mathfrak{K})^{4/3}}\right).$$

Proof. In the proof below, $\mathfrak{n}$ and $\mathfrak{m}$ always range through the nonzero ideals of $\mathbb{Z}[\omega_d]$. We will first prove the proposition for $\mathfrak{n}$ and $\mathfrak{m}$ relatively prime (i.e. for $(\mathfrak{n},\mathfrak{m}) = \mathfrak{K} = 1$). Then,

$$\#\{\mathfrak{n},\mathfrak{m} \subset \mathbb{Z}[\omega_d]^2 : N(\mathfrak{n}), N(\mathfrak{m}) \leq x \text{ and } (\mathfrak{n},\mathfrak{m}) = 1\} = \sum_{\substack{\mathfrak{n}\subset\mathbb{Z}[\omega_d] \\ N(\mathfrak{n})\leq x}} \sum_{\substack{\mathfrak{m}\subset\mathbb{Z}[\omega_d] \\ N(\mathfrak{m})\leq x \\ (\mathfrak{n},\mathfrak{m})=(1)}} 1$$

$$= \sum_{\substack{\mathfrak{n}\subset\mathbb{Z}[\omega_d] \\ N(\mathfrak{n})\leq x}} \sum_{\substack{\mathfrak{m}\subset\mathbb{Z}[\omega_d] \\ N(\mathfrak{m})\leq x}} \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\omega_d] \\ \mathfrak{d}\mid(\mathfrak{n},\mathfrak{m})}} \mu(\mathfrak{d}),$$

where in the last line we use the Möbius function identity from Proposition 2.3.5. Reindexing with $\mathfrak{n} = \mathfrak{d}\mathfrak{n}'$ and $\mathfrak{m} = \mathfrak{d}\mathfrak{m}'$ where the norms of $\mathfrak{n}'$ and $\mathfrak{m}'$ range from 1 to $x/N(\mathfrak{d})$, we may rewrite this as:

$$\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\omega_d] \\ N(\mathfrak{d})\leq x}} \mu(\mathfrak{d}) \sum_{\substack{\mathfrak{n}'\subset\mathbb{Z}[\omega_d] \\ N(\mathfrak{n}')\leq \frac{x}{N(\mathfrak{d})}}} \sum_{\substack{\mathfrak{m}'\subset\mathbb{Z}[\omega_d] \\ N(\mathfrak{m}')\leq \frac{x}{N(\mathfrak{d})}}} 1$$

Using the definition of $r_d(n,2)$, we can write:

$$= \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\omega_d]\\ N(\mathfrak{d})\leq x}} \mu(\mathfrak{d}) \left[\frac{1}{|\mathbb{Z}[\omega_d]^\times|}\sum_{N(\mathfrak{n}')=1}^{\lfloor\frac{x}{N(\mathfrak{d})}\rfloor} r_d(N(\mathfrak{n}'),2)\right]\left[\frac{1}{|\mathbb{Z}[\omega_d]^\times|}\sum_{N(\mathfrak{m}')=1}^{\lfloor\frac{x}{N(\mathfrak{d})}\rfloor} r_d(N(\mathfrak{m}'),2)\right].$$

As in Proposition 3.3.3, this reduces to:

$$= \frac{1}{|\mathbb{Z}[\omega_d]^\times|^2}\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\omega_d]\\ N(\mathfrak{d})\leq x}} \mu(\mathfrak{d})\left[\frac{4\pi^2x^2}{|d|N(\mathfrak{d})^2}+O\left(\frac{x}{N(\mathfrak{d})}\right)^{4/3}\right].$$

We then distribute the summation to obtain the following:

$$= \frac{4\pi^2x^2}{|\mathbb{Z}[\omega_d]^\times|^2\cdot|d|}\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\omega_d]\\ N(\mathfrak{d})\leq x}}\frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2}+O\left(\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\omega_d]\\ N(\mathfrak{d})\leq x}}\left(\frac{x}{N(\mathfrak{d})}\right)^{4/3}\right). \tag{8}$$

To evaluate the main term, we need to use the Möbius generating function from equation (5) to see that:

$$\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\omega_d]\\ N(\mathfrak{d})\leq x}}\frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2} = \frac{1}{\zeta_{\mathbb{Q}(\omega_d)}(2)} - \sum_{n=x+1}^{\infty}\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\omega_d]\\ N(\mathfrak{d})=n}}\frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2},$$

which implies

$$\left|\frac{1}{\zeta_{\mathbb{Q}(\omega_d)}(2)} - \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\omega_d]\\ N(\mathfrak{d})\leq x}}\frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2}\right| \qu\leq\quad \sum_{n=x+1}^{\infty}\frac{1}{n^2}\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\omega_d]\\ N(\mathfrak{d})=n}}1 \quad=\quad \frac{1}{|\mathbb{Z}[\omega_d]^\times|}\sum_{n=x+1}^{\infty}\frac{r_d(n,2)}{n^2}.$$

Let $\sigma_0(n)$ represent the number of divisors of n. Using Proposition 2.3.2, we get that $r_d(n,2)\leq\sigma_0(n)=o(n^\varepsilon)$ for all $\varepsilon>0$, where the divisor bound $o(n^\varepsilon)$ comes from [9]. Thus, $\frac{1}{|\mathbb{Z}[\omega_d]^\times|}\sum_{n=x+1}^{\infty}\frac{r_d(n,2)}{n^2}$ is less than or equal to $\sum_{n=x+1}^{\infty}\frac{o(n^\varepsilon)}{n^2}$ which is equal to $o(x^{\varepsilon-1})$, and so

$$\left|\frac{1}{\zeta_{\mathbb{Q}(\omega_d)}(2)} - \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\omega_d]\\ N(\mathfrak{d})\leq x}}\frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2}\right|\leq o(x^{\varepsilon-1}) \quad\text{or}\quad \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\omega_d]\\ N(\mathfrak{d})\leq x}}\frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2} = \frac{1}{\zeta_{\mathbb{Q}(\omega_d)}(2)}+o(x^{\varepsilon-1}).$$

For the error term of equation (8), we have that:

$$\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\omega_d]\\ N(\mathfrak{d})\leq x}}\left(\frac{x}{N(\mathfrak{d})}\right)^{4/3} \quad=\quad \sum_{n=1}^{x}\frac{1}{n^{4/3}}\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[\omega_d]\\ N(\mathfrak{d})=n}}1 \quad=\quad \frac{1}{|\mathbb{Z}[\omega_d]^\times|}\sum_{n=1}^{x}\frac{r_d(n,2)}{n^{4/3}}.$$

We can use the bound $r_d(n,2)\leq o(n^\varepsilon)$ to see that $\frac{1}{|\mathbb{Z}[\omega_d]^\times|}\sum_{n=1}^{x}\frac{r_d(n,2)}{n^{4/3}}$ is less than or equal to $\sum_{n=1}^{x}o(n^{\varepsilon-4/3})$ which is equal to $o(x^{\varepsilon-1/3})+o(1)$. From this we can see that $O\left(x^{4/3}\sum_{n=1}^{x}\frac{r_d(n,2)}{n^{4/3}}\right)$ equals $O(o(x^{4/3}))$, which is equal to $O(x^{4/3})$. We can now rewrite equation (8) as follows:

$$\frac{4\pi^2x^2}{|\mathbb{Z}[\omega_d]^\times|^2\cdot|d|\cdot\zeta_{\mathbb{Q}(\omega_d)}(2)}+o(x^{\varepsilon-1})+O(x^{4/3}).$$

This allows us to conclude:

$$\#\{\mathfrak{n},\mathfrak{m}\subset\mathbb{Z}[\omega_d]^2 : N(\mathfrak{n}),N(\mathfrak{m})\leq x \text{ and } (\mathfrak{n},\mathfrak{m})=(1)\} = \frac{4\pi^2x^2}{|\mathbb{Z}[\omega_d]^\times|^2\cdot|d|\cdot\zeta_{\mathbb{Q}(\omega_d)}(2)}+O(x^{4/3}).$$

We have calculated the number of $\mathfrak{n}$ and $\mathfrak{m}$ such that $(\mathfrak{n},\mathfrak{m})=1$ (i.e. $\mathfrak{n}$ and $\mathfrak{m}$ are relatively prime), and now we want to reindex to count the number of $\mathfrak{n}$ and $\mathfrak{m}$ such that $(\mathfrak{n},\mathfrak{m})=\mathfrak{K}$. Let $\mathfrak{n}=\mathfrak{n}'\mathfrak{K}$ and $\mathfrak{m}=\mathfrak{m}'\mathfrak{K}$. Note that $\mathfrak{n}'$ and $\mathfrak{m}'$ are relatively prime if and only if $\mathfrak{n}$ and $\mathfrak{m}$ have $\mathfrak{K}$ as their greatest common divisor. Therefore, the number of relatively prime pairs $\mathfrak{n}'$ and $\mathfrak{m}'$ with norm y or less must be equivalent to the number of pairs $\mathfrak{n}$ and $\mathfrak{m}$, with norm $y\cdot N(\mathfrak{K})$ or less, having greatest common divisor $\mathfrak{K}$:

$$\begin{aligned}
&\#\{\mathfrak{n},\mathfrak{m}\subset\mathbb{Z}[\omega_d]^2 : N(\mathfrak{n}),N(\mathfrak{m})\leq x \text{ and } (\mathfrak{n},\mathfrak{m})=(\mathfrak{K})\}\\
&\qquad = \#\{\mathfrak{n}',\mathfrak{m}'\subset\mathbb{Z}[\omega_d]^2 : N(\mathfrak{n}'),N(\mathfrak{m}')\leq \frac{x}{N(\mathfrak{K})} \text{ and } (\mathfrak{n}',\mathfrak{m}')=(1)\}\\
&\qquad = \frac{4\pi^2x^2}{|\mathbb{Z}[\omega_d]^\times|^2\cdot|d|\cdot\zeta_{\mathbb{Q}(\omega_d)}(2)N(\mathfrak{K})^2}+O\left(\frac{x^{4/3}}{N(\mathfrak{K})^{4/3}}\right).
\end{aligned}$$

□

Now that we have Proposition 3.3.3 and Proposition 3.3.4, we can calculate the probability that the greatest common divisor of two nonzero ideals $\mathfrak{n}$ and $\mathfrak{m}$ is $\mathfrak{K}$:

Theorem 3.3.5. *For $d\leq -3$, let $\mathfrak{n}$ and $\mathfrak{m}$ be nonzero ideals chosen independently and uniformly at random from the set of ideals in $\mathbb{Z}[\omega_d]$ with norm x or less. The probability that $(\mathfrak{n},\mathfrak{m})=\mathfrak{K}$ is:*

$$\frac{1}{\zeta_{\mathbb{Q}(\omega_d)}(2)N(\mathfrak{K})^2}+O\left(\frac{1}{x^{2/3}N(\mathfrak{K})^{4/3}}\right).$$

Proof. The probability that $\mathfrak{n}$ and $\mathfrak{m}$, having norm less than or equal to x, will have greatest common divisor $\mathfrak{K}$ is defined to be the number of pairs of ideals of norm x or less which have greatest common divisor $\mathfrak{K}$ (Proposition 3.3.4) divided by the total number of pairs of ideals of norm x or less (Proposition 3.3.3). Therefore,

$$\begin{aligned}
&P_x\{\mathfrak{n},\mathfrak{m}\subset\mathbb{Z}[\omega_d]^2 : N(\mathfrak{n}),N(\mathfrak{m})\leq x \text{ and } (\mathfrak{n},\mathfrak{m})=\mathfrak{K}\}\\
&= \left[\frac{4\pi^2x^2}{|\mathbb{Z}[\omega_d]^\times|^2\cdot|d|\cdot\zeta_{\mathbb{Q}(\omega_d)}(2)N(\mathfrak{K})^2}+O\left(\frac{x^{4/3}}{N(\mathfrak{K})^{4/3}}\right)\right]\cdot\left[\frac{4\pi^2x^2}{|\mathbb{Z}[\omega_d]^\times|^2\cdot|d|}+O(x^{4/3})\right]^{-1}
\end{aligned}$$

We can rewrite $[\frac{4\pi^2x^2}{|\mathbb{Z}[\omega_d]^\times|^2\cdot|d|}+O(x^{4/3})]^{-1}$ as $\frac{1}{4}\cdot|\mathbb{Z}[\omega_d]^\times|^2\cdot|d|\cdot\pi^{-2}x^{-2}[1+O(x^{-2/3})]^{-1}$ which is equal to $\frac{1}{4}\cdot|\mathbb{Z}[\omega_d]^\times|^2\cdot|d|\cdot\pi^{-2}x^{-2}[1+O(x^{-2/3})]$ since $[1+f(x)]^{-1}$ equals $1+O(f(x))$ for $f(x)$ tending towards 0 as $x\to\infty$. We can simplify the probability as:

$$\begin{aligned}
&= \left[\frac{4\pi^2x^2}{|\mathbb{Z}[\omega_d]^\times|^2\cdot|d|\cdot\zeta_{\mathbb{Q}(\omega_d)}(2)N(\mathfrak{K})^2}+O\left(\frac{x^{4/3}}{N(\mathfrak{K})^{4/3}}\right)\right]\cdot\left[\frac{1}{4}\cdot|\mathbb{Z}[\omega_d]^\times|^2\cdot|d|\cdot\pi^{-2}x^{-2}\left[1+O(x^{-2/3})\right]\right]\\
&= \left[\frac{1}{\zeta_{\mathbb{Q}(\omega_d)}(2)N(\mathfrak{K})^2}+O\left(\frac{1}{x^{2/3}N(\mathfrak{K})^{4/3}}\right)\right]\cdot\left[1+O(x^{-2/3})\right]\\
&= \frac{1}{\zeta_{\mathbb{Q}(\omega_d)}(2)N(\mathfrak{K})^2}+O\left(\frac{1}{x^{2/3}N(\mathfrak{K})^{4/3}}\right)+O\left(\frac{1}{x^{2/3}N(\mathfrak{K})^2}\right)+O\left(\frac{1}{x^{4/3}N(\mathfrak{K})^{4/3}}\right)\\
&= \frac{1}{\zeta_{\mathbb{Q}(\omega_d)}(2)N(\mathfrak{K})^2}+O\left(\frac{1}{x^{2/3}N(\mathfrak{K})^{4/3}}\right).
\end{aligned}$$

□

The following corollary is a direct consequence of Theorem 3.2.5 for the case when $\mathfrak{K} = (1)$:

Corollary 3.3.6. *For $\mathbb{Q}(\omega_d)$ with class number 1, the probability that a pair of two ideals in $\mathbb{Z}[\omega_d]$ with norm x or less are relatively prime as $x \to \infty$ is:*

$$\frac{1}{\zeta_{\mathbb{Q}(\omega_d)}(2)}.$$

Proof. Let $\mathfrak{K} = (1)$. We want to take the limit as $x \to \infty$ of the expression in Theorem 3.2.5:

$$\lim_{x\to\infty} \frac{1}{\zeta_{\mathbb{Q}(\omega_d)}(2)} + O\left(\frac{1}{x^{2/3}}\right).$$

As x gets large, we see that the error term $O\left(\frac{1}{x^{2/3}}\right)$ approaches 0, and we are left with the statement in the corollary. □

The probability from Theorem 3.2.5 will allow us to calculate the expected norm of the greatest common divisor between a pair of ideals $\mathfrak{n}$ and $\mathfrak{m}$.

Theorem 3.3.7. *For $d \leq -3$, let $\mathfrak{n}$ and $\mathfrak{m}$ be nonzero ideals chosen independently and uniformly at random from the set of ideals in $\mathbb{Z}[\omega_d]$ with norm x or less. The expected norm of the greatest common divisor of $\mathfrak{n}$ and $\mathfrak{m}$ is:*

$$\frac{2\pi \log x}{|\mathbb{Z}[\omega_d]^\times| \cdot \sqrt{|d|} \cdot \zeta_{\mathbb{Q}(\omega_d)}(2)} + O(1).$$

Proof. We want to find the expected value of $N(\mathfrak{n},\mathfrak{m}) =: k$, where the norm of $\mathfrak{n}$ and $\mathfrak{m}$ ranges from 1 to x. In order to do this, we have to express the probability that for a nonzero ideal $\mathfrak{K} \in \mathbb{Z}[\omega_d]$, $\mathfrak{n}$ and $\mathfrak{m}$ have greatest common divisor $k = N(\mathfrak{K})$ in terms of k as well. The number of ideals with norm k in $\mathbb{Z}[\omega_d]$ is equal to $r_d(k,2)/|\mathbb{Z}[\omega_d]^\times|$, where we divide $r_d(k,2)$ by the number of units in $\mathbb{Z}[\omega_d]$. We can use Theorem 3.3.5 to express the probability that the greatest common divisor of $\mathfrak{n}$ and $\mathfrak{m}$ has norm k in terms of k as:

$$P_x\{N(\mathfrak{n},\mathfrak{m}) = k\} = \frac{r_d(k,2)}{|\mathbb{Z}[\omega_d]^\times| \cdot \zeta_{\mathbb{Q}(\omega_d)}(2) k^2} + O\left(\frac{r_d(k,2)}{x^{2/3}k^{4/3}}\right).$$

By defintion, the expected value is:

$$\begin{aligned} E_x\{N(\mathfrak{n},\mathfrak{m})\} &= \sum_{k=1}^{x} k \cdot P_x\{N(\mathfrak{n},\mathfrak{m}) = k\} \\ &= \sum_{k=1}^{x} k \cdot \left[\frac{r_d(k,2)}{|\mathbb{Z}[\omega_d]^\times| \cdot \zeta_{\mathbb{Q}(\omega_d)}(2) k^2} + O\left(\frac{r_d(k,2)}{x^{2/3}k^{4/3}}\right)\right] \\ &= \frac{1}{|\mathbb{Z}[\omega_d]^\times| \cdot \zeta_{\mathbb{Q}(\omega_d)}(2)} \sum_{k=1}^{x} \frac{r_d(k,2)}{k} + O\left(\frac{1}{x^{2/3}} \sum_{k=1}^{x} \frac{r_d(k,2)}{k^{1/3}}\right). \end{aligned} \tag{9}$$

First, we want to simplify the error term in equation (9). We begin by using Stieltjes integration by parts from Theorem 2.3.3 to evaluate the summation:

$$\sum_{k=1}^{x} \frac{r_d(k,2)}{k^{1/3}} = x^{-1/3} \sum_{k=1}^{x} r_d(k,2) - 1 - \int_1^x \left(\frac{2\pi k}{\sqrt{|d|}} + O\left(k^{1/3}\right)\right)\left(-\frac{1}{3}k^{-4/3}dk\right).$$

We then use Lemma 3.3.1 to simplify:

$$\begin{aligned} &= \frac{1}{x^{1/3}}\left(\frac{2\pi x}{\sqrt{|d|}}+O\left(x^{1/3}\right)\right)-1+\frac{1}{3}\int_1^x\left[\frac{2\pi}{\sqrt{|d|}k^{1/3}}+\frac{O(k^{1/3})}{k^{4/3}}\right]dk \\ &= \frac{2\pi x^{2/3}}{\sqrt{|d|}}+O(1)-1+\frac{2\pi}{3\sqrt{|d|}}\left(\frac{3k^{2/3}}{2}+O(\log k)\Big|_1^x\right) \\ &= \frac{3\pi x^{2/3}}{\sqrt{|d|}}+O(\log x). \end{aligned}$$

This implies that the error term is:

$$\begin{aligned} O\left(\frac{1}{x^{2/3}}\sum_{k=1}^{x}\frac{r_d(k,2)}{k^{1/3}}\right) &= O\left(\frac{1}{x^{2/3}}\cdot\left(\frac{3\pi x^{2/3}}{\sqrt{|d|}}+O(\log x)\right)\right) \\ &= O\left(\frac{3\pi}{\sqrt{|d|}}+x^{-2/3}O(\log x)\right) \\ &= O(1+x^{-2/3}O(\log x)) \\ &= O(1). \end{aligned}$$

Now we want to rewrite the main term of equation (9) using our result from Lemma 3.3.2:

$$\begin{aligned} \frac{1}{|\mathbb{Z}[\omega_d]^\times|\cdot\zeta_{\mathbb{Q}(\omega_d)}(2)}\sum_{k=1}^{x}\frac{r_d(k,2)}{k} &= \frac{1}{|\mathbb{Z}[\omega_d]^\times|\cdot\zeta_{\mathbb{Q}(\omega_d)}(2)}\left[\frac{2\pi}{\sqrt{|d|}}\left(1-\frac{\sqrt{|d|}}{2\pi}+\log x\right)+O\left(x^{-2/3}\right)\right] \\ &= \frac{2\pi\log x}{|\mathbb{Z}[\omega_d]^\times|\cdot\sqrt{|d|}\cdot\zeta_{\mathbb{Q}(\omega_d)}(2)}. \end{aligned}$$

Combining the evaluated main term and error term from equation (9), we get that:

$$E_x\{N(\mathfrak{n},\mathfrak{m})\} = \frac{2\pi\log x}{|\mathbb{Z}[\omega_d]^\times|\cdot\sqrt{|d|}\cdot\zeta_{\mathbb{Q}(\omega_d)}(2)}+O(1).$$

□

3.4 Results for $\mathbb{Z}[\sqrt{-5}]$

In this section, we will outline a method for counting $\sum_{n=1}^{x} r_d(n,2)$ for non-UFDs. Specifically, we will look at the ring $\mathbb{Z}[\sqrt{-5}]$. Once we are equipped with $\sum_{n=1}^{x} r_d(n,2)$, calculating the probability that a pair of nonzero ideals $\mathfrak{n}$ and $\mathfrak{m}$ in $\mathbb{Z}[\omega_d]$ (chosen uniformly and independently at random from the set of ideals in $\mathbb{Z}[\omega_d]$ with norm x or less) has greatest common divisor $\mathfrak{K}$ will follow similarly to the proofs in Sections 3.2 and 3.3. Likewise, once we have calculated the probability that two nonzero ideals $\mathfrak{n}$ and $\mathfrak{m}$ have greatest common divisor $\mathfrak{K}$, we can easily calculate the expected norm of $\mathfrak{n}$ and $\mathfrak{m}$, with an explicit error term. We will begin by defining the important functions that we will use and highlighting differences in the definitions for a non-UFD.

In Definition 2.3.1, we define $r_d(n,2)$ in terms of elements that have norm n. In UFDs this is simple because we know that every factorization of an element is unique. As we have seen, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, which means that unique factorization does not hold for elements in the ring. We can see this if we take an element $\alpha\in\mathbb{Z}[\sqrt{-5}]$ such that $N(\alpha)=6$, because in $\mathbb{Z}[\sqrt{-5}]$ we can express $N(\alpha)=6$ as $(2)(3)$ and as $(1+\sqrt{-5})(1-\sqrt{-5})$. We need to find

a way to properly count the number of distinct elements with norm n for non-UFDs. In order to do this, we will need to use the ideal class group of $\mathbb{Q}(\omega_d)$ and thus, define $r_d(n,2)$ in terms of ideals in $\mathbb{Z}[\omega_d]$ with norm n. We will show how to do so for $\mathbb{Z}[\sqrt{-5}]$.

We can use Minkowski's bound from Proposition 2.1.3 to find the upper bound of the minimal norm of an ideal in any given ideal class of $\mathbb{Q}(\sqrt{-5})$. This will tell us that we only need to check for ideals with norm not exceeding Minkowski's bound. Once we find these ideals, we will then have the ideals in the ideal class group of $\mathbb{Q}(\sqrt{-5})$, which is finite. The order of the ideal class group then gives us the class number of $\mathbb{Q}(\sqrt{-5})$.

The Minkowski bound $M_{\mathbb{Q}(\omega_d)}$ for imaginary quadratic fields has $n = 2, r_2 = 0$ and can be expressed as:

$$M_{\mathbb{Q}(\omega_d)} = \sqrt{|D_{\mathbb{Q}(\omega_d)}|}\left(\frac{2}{\pi}\right),$$

where $D_{\mathbb{Q}(\omega_d)}$ is the discriminant of $\mathbb{Q}(\omega_d)$. For $\mathbb{Q}(\sqrt{-5})$, the discriminant is equal to -20, so we can calculate Minkowski's bound to be $\frac{4\sqrt{5}}{\pi}$, which is approximately 2.85. Now we know that we have to check for ideals with norm less than 2.8. Since we are dealing with integral values, we only need to check for ideals with norm less than or equal to 2. As a result, we get that the ideal class group has two elements: the classes $[(1)]$ and $[(2,1+\sqrt{-5})]$. The only ideal of norm 1 is the trivial ideal (1). We want to find the ideals of norm 2. The ideal $(2,1+\sqrt{-5})$ has norm $(2,1+\sqrt{-5})(2,1-\sqrt{-5}) = (4,6,2+2\sqrt{-5},2-2\sqrt{-5})$ which equals the ideal (2). It is important to note that $(2,1+\sqrt{-5})$ is the same ideal class as $(2,1-\sqrt{-5})$, because $1+\sqrt{-5} = 2-(1-\sqrt{-5})$ is contained in the ideal $(2,1-\sqrt{-5})$ and $1-\sqrt{-5} = 2-(1+\sqrt{-5})$ is contained in the ideal $(2,1+\sqrt{2})$. Since 2 ramifies in $\mathbb{Z}[\sqrt{-5}]$, there is only one ideal of norm 2 in $\mathbb{Z}[\sqrt{-5}]$, so there is nothing else to consider. Thus, the class number of $\mathbb{Q}(\sqrt{-5})$ is 2.

The main difficulty is being able to count $\sum_{n=1}^{x} r_{-5}(n,2)$. We will define $r_d(n,2)$ in terms of ideals as follows:

$$r_d^{'}(n,2) = \#\{\mathfrak{a} \subset \mathbb{Z}[\omega_d] : N(\mathfrak{a}) = n\}.$$

Now that we know the two different ideal class groups of $\mathbb{Q}(\sqrt{-5})$, we know that for an element $\alpha \in \mathbb{Z}[\sqrt{-5}]$ the norm can take one of the following two forms:

$$N(\alpha(1)) = N(\alpha) = n, \text{ and}$$
$$N(\alpha(2,1+\sqrt{-5})) = 2N(\alpha) = n \Rightarrow N(\alpha) = \frac{n}{2}.$$

Thus, when taking into account the number of ideals with norm n in $\mathbb{Z}[\sqrt{-5}]$, we want to consider the number of elements $\alpha \in \mathbb{Z}[\sqrt{-5}]$ with norm n and the number of elements $\beta \in \mathbb{Z}[\sqrt{-5}]$ with norm $\frac{n}{2}$. In other words, we want to express $r_{-5}^{'}(n,2)$ in terms of $r_{-5}(n,2) + r_{-5}(\frac{n}{2},2)$.

Using the definition of $r_d(n,2)$ for elements, we can express $r_{-5}^{'}(n,2)$ for ideals as follows:

$$\begin{aligned} r_{-5}^{'}(n,2) &= r_{-5}(n,2) + r_{-5}\left(\frac{n}{2},2\right) \\ &= \frac{1}{2}\#\{\alpha = a+\sqrt{-5}b \in \mathbb{Z}[\sqrt{-5}] : N(\alpha) = a^2+5b^2 = n\} \\ &+ \frac{1}{2}\#\left\{\beta = 2a+(1+\sqrt{-5})b \in \mathbb{Z}[\sqrt{-5}] : N(\beta) = 2a^2+2ab+3b^2 = \frac{n}{2}\right\}. \end{aligned}$$

In order to calculate $\sum_{n=1}^{x} r_{-5}^{'}(n,2)$, we need to calculate $\sum_{n=1}^{x} r_{-5}(n,2)$ and $\sum_{n=1}^{x} r_{-5}(\frac{n}{2},2)$. For $\sum_{n=1}^{x} r_{-5}(n,2)$, we want to count the integral points (a,b) in the ellipse $a^2+5b^2 = n$. For $\sum_{n=1}^{x} r_{-5}(\frac{n}{2},2)$, we want to count the integral points (a,b) in the ellipse $2a^2+2ab+3b^2 = \frac{n}{2}$. Similar to Sierpiński's result from equation (2), we are able to write:

$$\begin{aligned} \sum_{n=1}^{x} r_{-5}^{'}(n,2) &= \sum_{n=1}^{x} r_{-5}(n,2) + \sum_{n=1}^{x} r_{-5}(\frac{n}{2},2) \\ &= \frac{\pi x}{\sqrt{5}} + \frac{\pi x}{2\sqrt{5}} + O(x^{1/3}). \end{aligned}$$

Now that we have done the difficult part of counting $\sum_{n=1}^{x} r'_{-5}(n,2)$, the rest of the results follow similarly to the other proofs in this paper. In order to produce a result similar to Sierpiński's result from equation (3), we need to use Stieltjes integration by parts as used in the proofs of Lemmas 3.2.2 and 3.3.2. We can then use these two lemmas to get similar results to Propositions 3.2.3, 3.2.4, 3.3.3, and 3.3.4. We can then use these two propositions to calculate the probability that two nonzero ideals $\mathfrak{n}$ and $\mathfrak{m}$ have greatest common divisor $\mathfrak{K}$ as in Theorem 3.2.5 and Theorem 3.3.5. Lastly, we can use this theorem to calculate the expected norm of $\mathfrak{n}$ and $\mathfrak{m}$ as in Theorem 3.2.6 and Theorem 3.3.7.

Acknowledgements

I would like to thank my thesis advisor Andrew Obus for all of his help and guidance. I would also like to thank Miriam Hausman and Carlos Moreno for serving as faculty readers for my thesis.

References

[1] Tai-Danae Bradley, Yin Choi Cheng, and Yan Fei Luo. On the Distribution of the Greatest Common Divisor of Gaussian Integers. *Involve, a Journal of Mathematics*, 9(1):27–40, 2015.

[2] Władysław Narkiewicz. Elementary and Analytic Theory of Algebraic Numbers. *Springer Science & Business Media*, 2013.

[3] Jürgen Neukirch. Algebraic Number Theory. *Springer Science & Business Media*, 322, 2013.

[4] Wacław Sierpiński. O Pewnym Zagadnieniu z Rachunku Funkcyj Asymptotycznych (On a Problem in the Theory of Asymptotic Functions). *Prace Matematyczno-Fizyczne*, 17:77–118, 1906.

[5] Martin N. Huxley. Exponential Sums and Lattice Points III. *Proc. London Math. Soc.*, 87(3):591–609, 2003.

[6] Wacław Sierpiński. O Sumowanic Szeregu $\sum_{n>a}^{n\leq b} \tau(n) f(n)$, Gdzie $\tau(n)$ Oznacza Liczbrę Rozkładów Liczby n na Sumę Kwadratów Dwóch Liczb Całkowitych (On the Summation of the Series $\sum_{n>a}^{n\leq b} \tau(n) f(n)$, where $\tau(n)$ denotes the number of decompositions of n into a sum of two squares of integers). *Prace Matematyczno-Fizyczne*, 18:1–59, 1908.

[7] Steven R. Finch. Mathematical Constants. *Cambridge University Press*, 2003.

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

[9] Terence Tao. The Divisor Bound. *terrytao.wordpress.com/2008/09/23/the-divisor-bound/*, 2008.