Some Consequences of Unique Factorization in
Imaginary Quadratic Number Fields of Class Number 1

by

Mark William Bannar-Martin
B Sc , University of Auckland, 1974
B A , University of Auckland, 1976

A Thesis Submitted in Partial Fulfilment of the
Requirements for the Degree of

MASTER OF SCIENCE

in the Department of Mathematics & Statistics

We accept this thesis as conforming
to the required standard

[redacted]

Dr. Gary MacGillivray, Co-Supervisor (Department of Mathematics & Statistics)

[redacted]

Dr. Ernest Cockayne, Co-Supervisor (Department of Mathematics & Statistics)

[redacted]

Dr. Frank Ruskey, Outside Member (Department of Computer Science)

[redacted]

Dr. Allen Herman, External Examiner (Department of Mathematics & Statistics, University of Regina, Regina, Saskatchewan)

Co-Supervisors: Dr. Gary MacGillivray and Dr. Ernest Cockayne

Abstract

For square-free m, the imaginary quadratic number fields $\mathbb{Q}(\sqrt{m})$ of class number 1 occur when $m = -1, -2, -3, -7, -11, -19, -43, -67, -163$. The unique factorization of algebraic integers in these number fields allows an elementary derivation of nine series involving π and of nine algebraic identities. Full details of the calculation of these series and identities are given.

Examiners:

[redacted]

Dr. Gary MacGillivray, Co-Supervisor (Department of Mathematics & Statistics)

[redacted]

Dr. Ernest Cockayne, Co-Supervisor (Department of Mathematics & Statistics)

[redacted]

Dr. Frank Ruskey, Outside Member (Department of Computer Science)

[redacted]

Dr. Allen Herman, External Examiner (Department of Mathematics & Statistics, University of Regina, Regina, Saskatchewan)

Table of Contents

List of Figures

Chapter 1

Introduction

A highlight of a first course in number theory is the assertion first made by Girard[8], detailing the integers that can be expressed as the sum of two squares.

> *Determinaison d'un nombre qui se peut diviser en deux quarrez entiers*
>
> i. *Tout nombre quarré*
>
> ii. *Tout nombre premier qui excede in nombre quaternaire de l'unité*
>
> iii. *Le produict de ceux qui sont tels*
>
> iv. *Et le double d'un chacun d'iceux*

Perhaps, the most natural setting for a proof of this assertion lies in the ring of Gaussian integers. Dedekind[2][3] certainly thought so, giving two separate proofs of this assertion based on the unique factorization of the ring of Gaussian integers.

The broader question of the number of representations of a positive integer as the sum of two squares was completely answered by Jacobi[10] using the theory of elliptic functions but an elementary proof using the Gaussian integers is to be found in Hardy and Wright[7]. It is while reading this proof that it occurred to me that this same elementary approach could be applied to other rings of algebraic integers. In fact, I had also been reading Stewart and Tall[14] and I

knew the ideal setting for this work lay in the imaginary quadratic number fields of class number 1. Curiosity then led me to Dirichlet's famous paper[4] where he thought it noteworthy to mention

$$1 = \frac{4}{\pi}\left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + - \quad\right) \tag{1.1}$$

and

$$\begin{aligned} &2(q^{1^2} + q^{3^2} + q^{5^2} + \quad)(1 + 2q^{2\,1^2} + 2q^{2\,2^2} + 2q^{2\,3^2} + \quad) \\ &= \frac{q}{1-q^2} + \frac{q^3}{1-q^6} - \frac{q^5}{1-q^{10}} - \frac{q^7}{1-q^{14}} + + - - \quad , \end{aligned} \tag{1.2}$$

as consequences of his work. The purpose of Dirichlet's paper was to prove that any arithmetic progression in which the first term and the common difference are relatively prime contains infinitely many primes, while the purpose of this thesis is to calculate nine series including (1.1) and nine identities such as (1.2). These eighteen calculations come as consequences of the unique factorization of the rings of integers in imaginary quadratic number fields of class number 1.

The ideas in this thesis are hardly original but the development is motivated and at a more elementary level than is usual for this material. For example, the defining properties of the real Dirichlet character emerge as requirements of our chosen line of argument and are not imposed. Overall, the emphasis is not analytical but rather combinatorial, therefore, bringing out the essentially numerical nature of these nine series and nine identities.

Chapter 2

Preliminaries

The purpose of this chapter is to provide an overview of the background necessary to read this thesis

2.1 Algebra

Let G and G' be groups. A *homomorphism* ϕ from G to G' is a function from G into G' that satisfies $\phi(ab) = \phi(a)\phi(b)$ for all a, b in G.

Let R be a commutative ring with unity. An element u in R is called a *unit* if u has a multiplicative inverse in R. Two elements a and b are said to be *associates,* if $b = ua$ for some unit u in R. If R has no zero-divisors then R is called an *integral domain*.

The next theorem follows easily.

Theorem 2.1.1 *The units $U(R)$ of the ring R form a group under multiplication. In particular, the units of the ring of integers modulo n is a group under multiplication, that is, $(U(\mathbb{Z}_n), \times_n)$ is a group.*

A non-zero element a of an integral domain D is called *irreducible* if, whenever $a = bc$ with b, c both in D, then one of b or c is a unit in D. A non-zero element

of an integral domain D is called a *prime* if a is not a unit and $a \mid bc$ implies $a \mid b$ or $a \mid c$.

An integral domain D is called a *Euclidean domain* if there is a function f from D^* to $\mathbb{N}$ such that

(a) $f(a) \leq f(ab)$ for all a and b in D^*, and

(b) if a and b are in D with b non-zero, then there exist elements q and r in D such that $a = bq + r$ where $r = 0$ or $f(r) < f(b)$.

A subring S of a commutative ring R is called an *ideal,* if for every r in R and a in S we have ra in S. For any a in R, the set of all multiples ra of a is an ideal. Such an ideal is known as a *principal ideal*. An integral domain in which every ideal is principal is called a *principal ideal domain*.

An integral domain D is called a *unique factorization domain* if every non-unit a in D^* can be written as a product of irreducibles of D and this factorization into irreducibles is unique up to associates and the order in which the factors appear.

Suppose $\{e_1, e_2, \ldots e_m\}$ is a linear independent subset of vectors in $\mathbb{R}^n$. Then the additive subgroup of $(\mathbb{R}^n, +)$ generated by $\{e_1, e_2, \ldots e_m\}$ is called a *lattice* of *dimension* m and the generating set $\{e_1, e_2, \ldots e_m\}$ is called a *lattice basis*. We will only concern ourselves with *plane lattices,* that is lattices of dimension 2 in $\mathbb{R}^2$, or what amounts to the same, lattices of dimension 2 in $\mathbb{C}$.

The lattice in $\mathbb{R}^2$ generated by $\{(1,0),(0,1)\}$ is $\mathbb{Z}^2$, the standard rectangular lattice. We will need a well-known result due to Gauss on the number of lattice points of $\mathbb{Z}^2$ that lie within an ellipse.

Theorem 2.1.2 *The number of lattice points N of the lattice $\mathbb{Z}^2$ that lie within the ellipse $Ax^2 + Bxy + Cy^2 = n$ is*

$$N = \frac{2\pi n}{\sqrt{4AC - B^2}} + O(\sqrt{n})$$

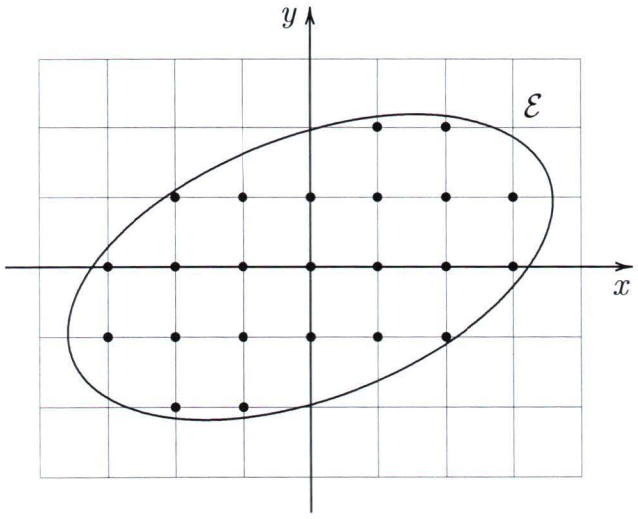

Figure 1: The lattice points of $\mathbb{Z}^2$ lying within the ellipse $\mathcal{E}$

If further background on algebra is required the reader is referred to Herstein[9].

2.2 Elementary number theory

If an integer m, different from zero, divides the difference $a - b$, then we say that a is *congruent* to b modulo m and write $a \equiv b \pmod{m}$ or $a \equiv b\ (m)$.

If the integers a and m are relatively prime, and the equation $x^2 \equiv a\ (m)$ has a solution then a is called a *quadratic residue* modulo m.

If p is an odd prime and a is an integer relatively prime to p, the *Legendre symbol,* denoted (a/p), is defined by

$$(a/p) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1, & \text{if } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

From the definition of the Legendre symbol follow two well known theorems, the latter first proved and highly regarded by Gauss

Theorem 2.2.1 *If p is an odd prime and a and b are both relatively prime to p, then*

(a) $(ab/p) = (a/p)(b/p)$,

(b) $(a/p) \equiv a^{(p-1)/2}\ (p)$, *in particular* $(-1/p) = (-1)^{(p-1)/2}$,

(c) $(2/p) = (-1)^{(p^2-1)/8}$

Theorem 2.2.2(Quadratic reciprocity) *If p and q are distinct odd primes, then*

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

It is convenient to extend the domain of the Legendre symbol (a/p) to allow p to be any odd number P.

Suppose the odd integer $P = \pm p_1 p_2 \cdots p_n$ where the primes $p_1, p_2, \ldots, p_n$ are not necessarily distinct and that a is an integer relatively prime to P. Then the *Jacobi symbol,* denoted (a/P), is defined by

$$(a/\pm 1) = 1 \quad \text{and} \quad (a/P) = (a/p_1)(a/p_2)\cdots(a/p_n)$$

Notice that when the odd integer P is prime the Jacobi symbol agrees with the Legendre symbol, justifying the use of the same notation.

As with the Legendre symbol, we have two important but less well-known theorems which follow from the definition of the Jacobi symbol.

Theorem 2.2.3 *If P and Q are odd integers, and a and b are integers both relatively prime to P and Q, then*

(a) $(a/P)(a/Q) = (a/PQ)$,

(b) $(a/P)(b/P) = (ab/P)$,

(c) $(a/P) = (b/P)$, whenever $a \equiv b\ (P)$.

Theorem 2.2.4 *If P and Q are odd relatively prime integers, then*

(a) $(-1/P) = (-1)^{(P-1)/2}$, whenever $P > 0$,

(b) $(2/P) = (-1)^{(P^2-1)/8}$,

(c) $(P/Q)(Q/P) = (-1)^{\frac{(P-1)}{2}\frac{(Q-1)}{2}}$.

It is important to note that if a is a quadratic residue modulo the odd positive integer P then the Jacobi symbol $(a/P) = 1$ but the converse is false, unlike the equivalence that occurs with the more restrictive Legendre symbol

A *numerical function* or *arithmetic function* is a function whose domain is the set of positive integers A numerical function f is *multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all pairs of relatively prime positive integers m and n A numerical function f is *completely multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all pairs of positive integers m and n

The *Mobius function* μ is the the multiplicative numerical function whose values on prime powers are

$$\mu(p^a) = \begin{cases} 1, & \text{if } a = 0, \\ -1, & \text{if } a = 1, \\ 0, & \text{if } a \geq 2 \end{cases}$$

The completely multiplicative numerical function J_k is defined by $J_k(n) = n^k$

A *Dirichlet character modulo* $\mathfrak{m}$ is a completely multiplicative numerical function with period $\mathfrak{m}$ such that

$$\chi(n) = \begin{cases} \text{root of unity}, & \text{if } \gcd(n, \mathfrak{m}) = 1, \\ 0, & \text{otherwise} \end{cases}$$

If the roots of unity are real then χ is called a *real Dirichlet character* The real Dirichlet character modulo $\mathfrak{m}$ such that

$$\chi(n) = \begin{cases} 1, & \text{if } \gcd(n, \mathfrak{m}) = 1, \\ 0, & \text{otherwise,} \end{cases}$$

is called the *principal Dirichlet character modulo* $\mathfrak{m}$

If f and g are numerical functions we define a sum and a product by

$$(f+g)(n) = f(n) + g(n) \quad \text{and} \quad (f*g)(n) = \sum_{d|n} f(d)g(n/d)$$

This product is known as the *Dirichlet product* or the *Dirichlet convolution* of f and g.

It easily follows that the set $\mathcal{A}$ of all numerical functions equipped with the above sum and product is a commutative ring with unity. For our purposes, we will need a well-known theorem concerning the algebraic structure of the multiplicative functions.

Theorem 2.2.5. *The multiplicative functions form a subgroup of the group of units of $\mathcal{A}$.*

An important consequence of this theorem is that the constant multiplicative function J_0 has the Mobius function μ as its inverse.

Another approach to Dirichlet convolution rests on the introduction of a generating function for the sequence defined by a numerical function. This approach, first introduced by Dirichlet, leads to the use of the Euler product, which in turn leads to a fruitful application of analysis in number theory. We however, will principally concern ourselves with the formal theory of these generating functions and pay scant regard to questions of convergence. To begin then, if f is a numerical function, the formal series

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s},$$

is called the *Dirichlet series generating function* for the numerical function f or equivalently the sequence $\{f(n)\}_1^\infty$. This is also written

$$F(s) \overset{ds}{\longleftrightarrow} f$$

It then follows that if f and g are numerical functions with Dirichlet series generating functions $F(s)$ and $G(s)$ respectively, that

$$F(s)\ G(s) \overset{ds}{\longleftrightarrow} f * g$$

A theorem which connects the Dirichlet series generating function to a product over primes is crucial to the work of this thesis. Its earliest form is due to Euler but the theorem was much generalised and used to great effect by both Dedekind and Dirichlet. We state a form which is sufficient to our present purposes.

Theorem 2.2.6(Euler product) *If f is a multiplicative numerical function then we have the formal identity*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p (1 + f(p)p^{-s} + f(p^2)p^{-2s} + \quad),$$

in which the product is over all prime numbers p.

Corollary 2.2.7 *If f is a completely multiplicative numerical function then we have the formal identity*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \frac{1}{(1 - f(p)p^{-s})},$$

in which the product is over all prime numbers p

Of particular interest is the *Riemann zeta function* $\zeta(s)$, which is the Dirichlet series generating function for the sequence $\{1\}_1^\infty$. In other words

$$\zeta(s) \overset{ds}{\longleftrightarrow} J_0$$

The Euler product takes its simplest and eponymous form in the case of the Riemann zeta function, as

$$\zeta(s) = \prod_p \frac{1}{(1 - p^{-s})}$$

We shall also make use of two other generating functions, namely the power series generating function and the Lambert series generating function.

If f is a numerical function then the formal power series

$$\sum_{n=1}^{\infty} f(n) x^n$$

is called the *power series generating function* for the numerical function f.

If f is a numerical function then the formal Lambert series

$$\sum_{n=1}^{\infty} f(n) \frac{x^n}{1 - x^n}$$

is called the *Lambert series generating function* for the numerical function f.

Next, we have a rather pretty theorem connecting Dirichlet convolution, power series generating functions and Lambert series generating functions.

Theorem 2.2.8. *Suppose f and g are numerical functions. Then the Lambert series generating function for f is the power series generating function for g if and only if $g = f * J_0$.*

If further background on number theory is required the reader is referred to Hardy and Wright[7] or Niven and Zuckerman[11]. For background on Dirichlet generating functions the reader is referred to Wilf[16].

2.3 Imaginary quadratic number fields

A complex number α is called an *algebraic number* if it satisfies a polynomial with rational coefficients. If the leading coefficient of a polynomial is 1, the polynomial is called *monic*. The monic polynomial of least degree with rational coefficients, which α satisfies is called the *minimal* polynomial for α over $\mathbb{Q}$.

An *algebraic number field* is a subfield of the complex numbers that is a finite dimensional vector space over the rational numbers. A *quadratic number field* is an algebraic number field of dimension 2 over the rational numbers.

An *extension field* K of a field F is a field which contains F as a subfield. The extension field of F which is generated by adjoining a single element α in K to F, denoted $F(\alpha)$, is known as a *simple extension* of F. The ring generated by adjoining α in K to F is denoted $F[\alpha]$ and consists of all elements in K which can be written as polynomials in α with coefficients in F. The following well known theorem guarantees that any algebraic number field is a simple extension

of the field of rational numbers and that the elements of this field extension can be written as polynomials over $\mathbb{Q}$

Theorem 2.3.1 *If K is an algebraic number field, then $K = \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$ for some algebraic number α*

For a quadratic number field $\mathbb{Q}[\alpha]$, it is always possible to choose a most convenient α

Theorem 2.3.2 *If K is a quadratic number field, then $K = \mathbb{Q}[\sqrt{m}]$ for some unique square-free integer m*

When $m > 0$, $K = \mathbb{Q}[\sqrt{m}]$ is called a *real* quadratic number field and when $m < 0$, $K = \mathbb{Q}[\sqrt{m}]$ is called an *imaginary* quadratic number field

A complex number is called an *algebraic integer* if it satisfies a monic polynomial with integer coefficients

It follows that the algebraic integers in the field of rational numbers alone are just the integers $\mathbb{Z}$ For this reason we will henceforth refer to the integers $\mathbb{Z}$ as *rational integers* and the superset of algebraic integers, simply as integers This terminology is standard and reflects our broader perspective To determine the algebraic integers within an algebraic number field, we have the following useful criterion

Theorem 2.3.3 *An algebraic number is an algebraic integer if and only if its minimum polynomial over $\mathbb{Q}$ has integer coefficients.*

This means that the integers of a quadratic number field satisfy monic quadratic polynomials with integer coefficients. Of course, the rational integers are integers in any quadratic number field, which happen to also satisfy monic linear polynomials with integer coefficients. A well known theorem characterizes the integers of quadratic number fields.

Theorem 2.3.4 *Let m be a square-free integer. The algebraic integers of the quadratic number field $K = \mathbb{Q}[\sqrt{m}]$ are $\mathbb{Z}[\xi]$ where $\xi = \sqrt{m}$, if $m \not\equiv 1\ (4)$ or $\xi = (1 + \sqrt{m})/2$, if $m \equiv 1\ (4)$.*

As a consequence, the integers of a quadratic number field form either a rectangular lattice as in Figure 2, or an isosceles triangular lattice as in Figure 3. The rectangular lattice occurs whenever $m \not\equiv 1\ (4)$ and the isosceles triangular lattice occurs whenever $m \equiv 1\ (4)$. This geometric interpretation will be of some importance in Chapter 3. It is also easy to check that the integers of a quadratic number field form a ring.

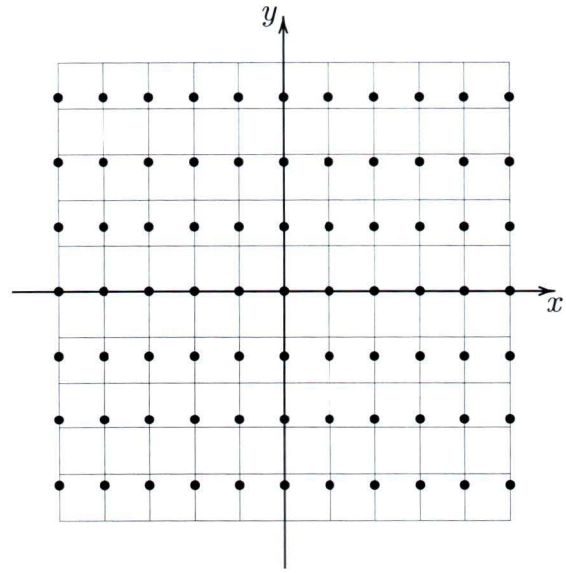

Figure 2 The rectangular lattice $\mathbb{Z}[\xi]$ where $\xi = \sqrt{-2}$

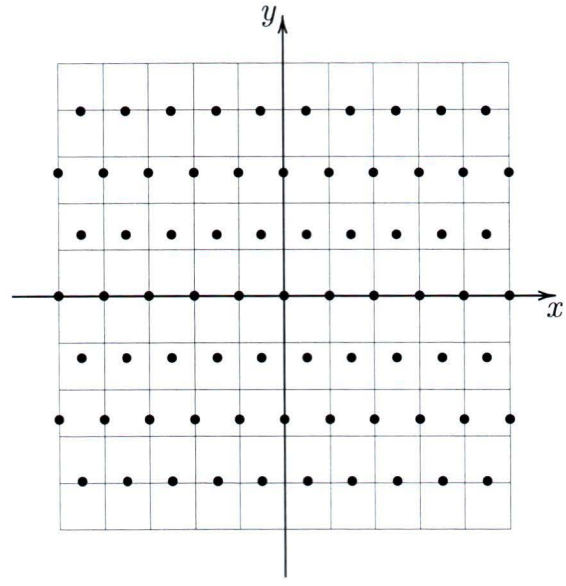

Figure 3 The isosceles triangular lattice $\mathbb{Z}[\xi]$ where $\xi = \dfrac{1+\sqrt{-7}}{2}$

To make progress in algebraic number theory and specifically in the theory of quadratic number fields, it is necessary to relate the algebraic numbers to the rational numbers. The norm provides the standard homomorphism on the multiplicative structures. Any number α in the quadratic number field $K = \mathbb{Q}[\sqrt{m}]$ has the form $a + b\sqrt{m}$, where $a, b, \in \mathbb{Q}$. We define the *conjugate* $\overline{\alpha}$ and the *norm* $\|\alpha\|$ by

$$\overline{\alpha} = a - b\sqrt{m} \quad \text{and} \quad \|\alpha\| = \alpha\overline{\alpha}.$$

The ring of integers $\mathbb{Z}[\xi]$ in the quadratic number field $\mathbb{Q}[\sqrt{m}]$ is often denoted $A(m)$. Since our focus is on certain rings in imaginary quadratic number fields, it will better serve our purpose to write our number fields as $\mathbb{Q}[\sqrt{-m}]$ and their respective rings of integers as $A(-m)$, where it is understood that $m > 0$.

We have two useful theorems that follow fairly readily from the introduction of the norm.

Theorem 2.3.5. *Suppose α and β lie in $A(-m)$. Then*

(a) α is a unit if and only if $\|\alpha\| = 1$,

(b) if α and β are associates then $\|\alpha\| = \|\beta\|$,

(c) $\|\alpha\|$ is a rational integer,

(d) if $\|\alpha\|$ is a rational prime then α is irreducible in $A(-m)$.

Theorem 2.3.6. *The group of units in $A(-m)$ is*

(a) $\{\pm 1, \pm\imath\}$ when $m = 1$,

(b) $\{\pm 1, \pm e^{\pi\imath/3}, \pm e^{2\pi\imath/3}\}$ when $m = 3$,

(c) $\{\pm 1\}$ when $m \neq 1, 3$.

We now turn to some important results on factorization in the rings $A(-m)$, which will play a central role in this thesis.

Birkhoff[1] was the first to show that the ring $A(-m)$ is norm-Euclidean for $m = 1, 2, 3, 7, 11$, thus establishing these rings as unique factorization domains. That these rings were the only Euclidean domains amongst the imaginary quadratic number fields, irrespective of the Euclidean function used, was first established by Dubois and Steger[6]. Interestingly, this provides the first confirmed example of a principal ideal domain that is not Euclidean, since the ring $A(-19)$ was known by Dedekind[3] to be a principal ideal domain.

That there are unique factorization domains that are not principal ideal domains is well-known, the polynomials with integer coefficients providing the classic counterexample. However, for the rings $A(-m)$, the two concepts coincide.

Theorem 2.3.7. *The ring of integers $A(-m)$ is a unique factorization domain if and only if it is a principal ideal domain.*

Gauss was the first to state the values of m for which the ring $A(-m)$ is a unique factorization domain, namely the nine values

$$m = 1, 2, 3, 7, 11, 19, 43, 67, 163.$$

However, it was over one hundred and fifty years before Stark[13] was able to prove that this list was indeed complete.

A measure of the extent to which a number field departs from unique factorization is its *class number*. Of course, it is the ring of integers within the number field that enjoys unique factorization, but this abuse of language is standard. Although, we will not pursue the idea of class number in this thesis, we will use the phrases, as is the common practice, 'a number field of class number 1' and 'a number field enjoying unique factorization' synonymously. In the remainder of this section we will only concern ourselves with imaginary quadratic number fields of class number 1.

The factorization of the rational prime p in the unique factorization domain $A(-m)$ is a key idea in this thesis. There are essentially two ways in which this can occur. Firstly, p may still be prime in $A(-m)$, in which case p is said to be *inert*. Secondly, p may factor in a non-trivial way in $A(-m)$. We wish to distinguish between two ways in which such a non-trivial factorization may occur. To appreciate the manner in which this distinction is made, suppose that $p = \alpha\beta$, where neither α nor β is a unit in $A(-m)$. Then, since $\|\alpha\|$ is a rational integer, we have $\|\alpha\| = p$. So $\alpha\overline{\alpha} = p$ and we conclude $\beta = \overline{\alpha}$. More importantly, by Theorem 2.3.5, α and $\overline{\alpha}$ must both be prime in $A(-m)$. Now, if α and $\overline{\alpha}$ are associates, we say p *ramifies* otherwise we say p *splits*. The following two theorems are well-known and determine precisely when the rational prime p ramifies, splits or is inert.

Theorem 2.3.8. *Suppose p is an odd rational prime in the unique factorization domain $A(-m)$. Then*

(a) if $(-m/p) = 1$ then p splits,

(b) if $(-m/p) = -1$ then p is inert,

(c) if $p \mid -m$ then p ramifies.

Theorem 2.3.9. *In the unique factorization domain $A(-m)$, the prime number 2 splits if $-m \equiv 1\ (8)$, is inert if $-m \equiv 5\ (8)$ and ramifies if $-m = -1$ or $-m = -2$.*

From Theorem 2.3.5, we know that if the norm of an integer is a rational prime then the integer is prime. As we have just seen this does not categorize all primes in terms of their norms since an inert prime has a norm which is the square of a rational prime. However, we have another well-known theorem which is almost a converse.

Theorem 2.3.10. *The norm of a prime in the unique factorization domain $A(-m)$ is either a rational prime or the square of a rational prime.*

It follows readily from Theorem 2.3.10, that the primes of $A(-m)$ are the inertial rational primes and the prime factors of the rational primes which ramify or split. This means we only need examine the rational primes to discover all primes in $A(-m)$. This is a very happy state of affairs.

If further background is required in algebraic number theory or in imaginary quadratic number fields in particular, the reader is referred to Stewart and Tall[14] or Pollard[12].

Chapter 3

Development

3.1 Lattice points

By Theorem 2.3.4, the ring of integers $A(-m)$ in the imaginary quadratic number field $\mathbb{Q}(\sqrt{-m})$ is $\mathbb{Z}[\xi]$. Recall that ξ depends on the value of m modulo 4, in fact $\xi = \sqrt{-m}$ when $-m \not\equiv 1\ (4)$ and $\xi = (1+\sqrt{-m})/2$ when $-m \equiv 1\ (4)$. Viewed geometrically, the ring of integers $A(-m)$ is a plane lattice in which the integers with norm n are lattice points lying on the circle of radius $\sqrt{n}$ with centre the origin. For example, in the lattice of Figure 3, there are six lattice points lying on the circle of radius 2 with centre the origin. This, of course, corresponds to the six integers of $\mathbb{Z}[(1+\sqrt{-7})/2]$ with norm 4. For our present purposes however, we prefer an alternative view. We subject the complex plane containing our plane lattice to either the linear transformation

$$\begin{pmatrix} 1 & 0 \\ 0 & 1/\sqrt{m} \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} 1 & -1/\sqrt{m} \\ 0 & 2/\sqrt{m} \end{pmatrix},$$

according to whether $-m \not\equiv 1\ (4)$ or $-m \equiv 1\ (4)$ respectively. Then the lattice $\mathbb{Z}[\xi]$ is mapped onto the standard rectangular lattice $\mathbb{Z}^2$. Moreover the circles of constant norm are mapped onto ellipses of constant norm.

Put more algebraically, any integer α in $A(-m)$ can be written as $\alpha = a+b\imath$ and the norm of α is $\|\alpha\| = a^2+b^2$. However the numbers a and b are in general not

integers nor even rational numbers But Theorem 2 3 4 guarantees that $\{1, \xi\}$ is an integral basis for the ring of integers $A(-m)$ That is, there always exist rational integers x and y so that $\alpha = x + y\xi$ The norm however, loses its circular form in favour of two possible elliptic forms Specifically, an easy calculation gives the the norm of the integer $x + y\xi$ as either

$$x^2 + my^2, \ -m \not\equiv 1 \ (4) \quad \text{or} \quad x^2 + xy + y^2\frac{(1+m)}{4}, \ -m \equiv 1 \ (4)$$

Now, let $\mathcal{E}_n(-m)$ denote the ellipse $x^2 + my^2 = n$ whenever $-m \not\equiv 1$ (4) and the ellipse $x^2 + xy + y^2(1+m)/4 = n$ whenever $-m \equiv 1$ (4) Hence we have

Theorem 3 1 1. *There is a one-to-one correspondence between the integers of $A(-m)$ whose norms are at most n and the lattice points of $\mathbb{Z}^2$ within the ellipse $\mathcal{E}_n(-m)$*

Theorem 3 1 1 is the source of much of what is to follow For we will count the lattice points within the ellipse $\mathcal{E}_n(-m)$ using the Theorem 2 1 2 and count the integers of $A(-m)$ whose norms are at most n with the help of a zeta function for $A(-m)$ These rather different approaches to counting together with the bijection of Theorem 3 1 1 lead to the main results of the chapter

By Theorem 2 1 2, the number of lattice points N within the ellipse $Ax^2 + Bxy + Cy^2 = n$ is

$$N = \frac{2\pi n}{\sqrt{-\Delta}} + O(\sqrt{n})$$

where Δ is the discriminant for the ellipse. Since $\Delta = B^2 - 4AC$, the ellipse $x^2 + my^2 = n$ has discriminant $-4m$ and the ellipse $x^2 + xy + y^2(1+m)/4 = n$ has discriminant $-m$. Hence we have

Theorem 3.1.2. *The number of lattice points N within the ellipse $\mathcal{E}_n(-m)$ is either*

$$N = \frac{\pi n}{\sqrt{m}} + O(\sqrt{n}),\ -m \not\equiv 1\ (4) \quad \text{or} \quad N = \frac{2\pi n}{\sqrt{m}} + O(\sqrt{n}),\ -m \equiv 1\ (4)$$

Theorem 3.1.2 completes one half of the count implied in the statement of Theorem 3.1.1. To complete the other and significantly more difficult half of the count we begin by introducing the concept of a zeta function for $A(-m)$.

3.2 A zeta function for $A(-m)$

Where no confusion can arise we will denote the ring of integers $A(-m)$ by A in order to simplify notation. The use of the zeta function ζ_A and its subsequent expansion as an Euler product follows a standard line of argument.

Definition 3.2.1. *In the ring of integers A we define a zeta function ζ_A by*

$$\zeta_A(s) = \sum_{a \in A^*} \frac{1}{\|a\|^s} \quad \text{where } A^* = A - \{0\}$$

By Theorem 2.3.5, the norm of an integer $a \in A^*$ is a positive rational integer and letting $r(n)$ denote the number of integers in A whose norm is exactly n, we

see the motivation for definition 3 2 1, since

$$\zeta_A(s) = \sum_{n=1}^{\infty} \frac{r(n)}{n^s}$$

That is, ζ_A is a Dirichlet series generating function for the sequence $\{r(n)\}_1^\infty$

In this thesis, we are only interested in the imaginary quadratic number fields with class number one Consequently the ring A is a unique factorization domain and every $a \in A^*$ can be written uniquely, up to units, as a product of prime elements Let $\{q_i\}$ be a system of representatives for the prime elements of A and denote the number of units in A by λ Then we can expand ζ_A as the Euler product

$$\zeta_A(s) = \lambda \prod_q \left(1 + \frac{1}{\|q\|^s} + \frac{1}{\|q\|^{2s}} + \quad \right) = \lambda \prod_q \left(\frac{1}{1 - \|q\|^{-s}}\right) \qquad (3\ 2\ 2)$$

Theorem 2 3 5 and Theorem 2 3 10 ensure the norms of integers in A^* are positive rational integers, moreover the norm of a prime in A is a rational prime or the square of a rational prime Whereas, Theorem 2 3 8 and Theorem 2 3 9 ensure that a rational prime must ramify, split or be inertial in A — there are no other possibilities These observations motivate the definition

Definition 3 2 3 *The function χ is defined on the domain of rational primes by*

$$\chi(p) = \begin{cases} 0, & \text{if } p \text{ ramifies in } A, \\ -1, & \text{if } p \text{ is inertial in } A, \\ 1, & \text{if } p \text{ splits in } A \end{cases}$$

The function χ allows us to index the product of equation 3 2 2 over the rational primes p rather than the integral primes q We can now rewrite equation 3 2 2 as

$$\zeta_A(s) = \lambda \prod_{\chi=0} \left(\frac{1}{1-p^{-s}}\right) \prod_{\chi=1} \left(\frac{1}{1-p^{-s}}\right)^2 \prod_{\chi=-1} \left(\frac{1}{1-p^{-2s}}\right) \tag{3 2 4}$$

To see that equation 3 2 4 does indeed follow from equation 3 2 2, note that a rational prime which ramifies is the norm of exactly one prime in A, a rational prime which splits is the norm of exactly two primes in A and finally a rational prime that is inertial has only its square as the norm of a prime in A Again these remarks must be considered up to units and this is of course the reason for the factor λ

Rearranging the factors of equation 3 2 4 gives

$$\zeta_A(s) = \lambda \prod_{p} \left(\frac{1}{1-p^{-s}}\right) \prod_{\chi=1} \left(\frac{1}{1-p^{-s}}\right) \prod_{\chi=-1} \left(\frac{1}{1+p^{-s}}\right) \tag{3 2 5}$$

Now $\prod_p (1-p^{-s})^{-1}$ is the Euler product for the rational integer zeta function $\zeta(s)$ Hence equation 3 2 5 can be written more simply as

$$\begin{aligned} \zeta_A(s) &= \lambda \ \zeta(s) \prod_{\chi=1} \left(\frac{1}{1-p^{-s}}\right) \prod_{\chi=-1} \left(\frac{1}{1+p^{-s}}\right) \\ &= \lambda \ \zeta(s) \prod_{p} \left(\frac{1}{1-\chi(p)p^{-s}}\right) \end{aligned} \tag{3 2 6}$$

By Corollary 2 2 7, the product in the result 3 2 6 could be written as a sum if the function χ were completely multiplicative This motivates the extension of

the domain of χ to all positive rational integers by defining χ to be completely multiplicative. We can now write

$$\zeta_A(s) = \lambda \zeta(s) \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \tag{3 2 7}$$

This last result gives ζ_A as the product of two Dirichlet series but we know from Section 3 1 that ζ_A is the Dirichlet generating function for the number $r(n)$ of integers in A whose norm is n. As a consequence, we have

Theorem 3 2 8. *The function r/λ is a Dirichlet convolution of the functions χ and J_0. That is, $r/\lambda = \chi * J_0$ or equivalently $r(n) = \lambda \sum_{d|n} \chi(d)$.*

Corollary 3 2 9. *The numerical function r/λ is multiplicative and the numerical function χ satisfies $\chi = r/\lambda * \mu$ where μ is the Mobius function.*

Proof. Since r/λ is the Dirichlet convolution of two multiplicative functions, it in turn must be multiplicative. This proves the first part of the corollary. Secondly, the inverse under convolution of the numerical function J_0 is the Mobius function μ and this combined with Theorem 3 2 8 proves the second part.

Corollary 3 2 10.

$$\sum_{n=1}^{\infty} r(n)x^n = \lambda \sum_{n=1}^{\infty} \chi(n) \frac{x^n}{1 - x^n}$$

Proof. Since $r/\lambda = \chi * J_0$, we may invoke Theorem 2 2 8 and the result is immediate.

Corollary 3.3.3 *With respect to the integers $A(-m)$ we have*

$$\frac{\pi}{\lambda\sqrt{m}} = \frac{1}{n}\sum_{k=1}^{\infty}\chi(k)\left\lfloor\frac{n}{k}\right\rfloor + O(1/\sqrt{n}),\ -m \not\equiv 1\ (4)$$

and

$$\frac{2\pi}{\lambda\sqrt{m}} = \frac{1}{n}\sum_{k=1}^{\infty}\chi(k)\left\lfloor\frac{n}{k}\right\rfloor + O(1/\sqrt{n}),\ -m \equiv 1\ (4)$$

Proof For $-m \not\equiv 1\ (4)$, we combine Theorem 3.1.1, Theorem 3.1.2 and the above theorem to give

$$1 + \lambda\sum_{k=1}^{\infty}\chi(k)\left\lfloor\frac{n}{k}\right\rfloor = \frac{\pi n}{\sqrt{m}} + O(\sqrt{n})$$

Rearrangement of factors and the absorbtion of the number 1 by $O(\sqrt{n})$ complete the proof in the case of $-m \not\equiv 1\ (4)$. The proof of the case when $-m \equiv 1\ (4)$ is all but identical.

Our next goal is to remove the floor symbol in the formulas of Corollary 3.3.3. We could make some progress in that direction now but it is better to first discover more about the numerical function χ. To do this we will consider the cases $-m \equiv 1\ (4)$ and $-m \not\equiv 1\ (4)$ separately. This leads us to the next chapter.

Chapter 4

$A(-m)$ where $-m \not\equiv 1\ (4)$

The only imaginary quadratic number fields $A(-m)$ of class number one with $-m \not\equiv 1\ (4)$ occur when $-m = -1$ or $-m = -2$. In this chapter, we will focus on these two cases. However, we will prove two more general results, namely Theorems 4.2.2 and 4.2.3, which will be used both in this Chapter and in Chapter 5.

4.1 The function χ is a real non-principal Dirichlet character for $A(-1)$ and $A(-2)$

From Corollary 3.3.3 we have

$$\frac{\pi}{\lambda\sqrt{m}} = \frac{1}{n}\sum_{k=1}^{\infty}\chi(k)\left\lfloor\frac{n}{k}\right\rfloor + O(1/\sqrt{n}),\ -m \not\equiv 1\ (4) \qquad (4.1.1)$$

We would like to simplify equation 4.1.1 and we begin by taking a closer look at the arithmetic function χ. Although we know about the multiplicative behaviour of χ, we know nothing of its sequential behaviour. To this end we note by Theorem 2.3.8 that in a unique factorization domain $A(-m)$ an odd rational prime splits if and only if $-m$ is a quadratic residue modulo p and is inertial if and only if $-m$ is a quadratic non-residue modulo p. Recalling that 2 is the only

rational prime that ramifies when $-m = -1, -2$ and using the Legendre symbol we may now write

$$\chi(p) = \begin{cases} (-m/p), & \text{if } p \text{ is an odd prime,} \\ 0, & \text{if } p = 2 \end{cases} \tag{4 1 2}$$

Furthermore, since χ is completely multiplicative, we conclude $\chi(n) = 0$ for all even rational integers n Taking advantage of the Jacobi symbol of Section 2 2, we now have for any positive rational integer n

$$\chi(n) = \begin{cases} (-m/n) & \text{if } n \text{ is odd,} \\ 0, & \text{if } n \text{ is even} \end{cases} \tag{4 1 3}$$

Theorem 4 1 4 *The numerical function χ is a real non-principal Dirichlet character modulo 4 with respect to $A(-1)$ and modulo 8 with respect to $A(-2)$*

Proof By definition, χ is completely multiplicative and by equation 4 1 3, χ takes its values from the set $\{0, \pm 1\}$ We are left to show that χ is periodic in order to establish that χ is a real Dirichlet character We break the proof into two cases

Case 1 With respect to $A(-1)$

By Theorem 2 2 4, the Jacobi symbol $(-1/n) = (-1)^{(n-1)/2}$ when n is an odd rational integer So it follows that

$$\chi(n) = \begin{cases} 0, & \text{if } n \text{ is even,} \\ 1, & \text{if } n \equiv 1 \ (4), \\ -1, & \text{if } n \equiv 3 \ (4) \end{cases}$$

We conclude that χ is a real Dirichlet character modulo 4 working with respect to $A(-1)$ and is obviously non-principal

Case 2 With respect to $A(-2)$

By Theorem 2 2 3 and Theorem 2 2 4, we have for an odd rational integer n that

$$\begin{aligned}(-2/n) &= (-1/n)(2/n) \\ &= (-1)^{(n-1)/2} \quad (-1)^{(n^2-1)/8} \\ &= (-1)^{(n^2+4n-5)/8} \\ &= (-1)^{(n-1)(n+5)/8}\end{aligned}$$

Of course, it is not necessary to check that $(n-1)(n+5)$ is divisible by 8 as this follows from the multiplicative property of the Jacobi symbol It is the quotient when $(n-1)(n+5)$ is divided by 8 that we are really interested in and we have

$$(n_1-1)(n_1+5)/8 \equiv (n_2-1)(n_2+5)/8 \pmod 2 \quad \text{whenever} \quad n_1 \equiv n_2 \pmod 8$$

Straight calculation then gives

$$\chi(n) = \begin{cases} 0, & \text{if } n \text{ is even,} \\ 1, & \text{if } n \equiv 1,3 \ (8), \\ -1, & \text{if } n \equiv 5,7 \ (8) \end{cases}$$

We conclude that χ is a real Dirichlet character modulo 8 working with respect to $A(-2)$ and again χ is obviously non-principal

Theorem 4 1 4 provides justification for the choice of the symbol χ, this being the traditional symbol for the Dirichlet character

4.2 Dirichlet character series

The series found in 4.1.1, namely

$$\frac{1}{n}\sum_{k=1}^{\infty}\chi(k)\left\lfloor\frac{n}{k}\right\rfloor=\sum_{k=1}^{\infty}\chi(k)\frac{\lfloor n/k\rfloor}{n},$$

has the form

$$\sum_{k=1}^{\infty}\chi(k)a_k$$

Definition 4.2.1 *If χ is a Dirichlet character modulo $\mathfrak{m}$ then we will call the series*

$$\sum_{k=1}^{\infty}\chi(k)a_k$$

a Dirichlet character series modulo $\mathfrak{m}$

We now present a general theorem not restricted to any particular character modulus $\mathfrak{m}$.

Theorem 4.2.2 *Suppose χ is a real non-principal Dirichlet character modulo $\mathfrak{m}$ and suppose $\{a_k\}_1^{\infty}$ is a non-negative decreasing sequence of real numbers with $a_k \to 0$ as $k \to \infty$. Then the Dirichlet character series*

$$\sum_{k=1}^{\infty}\chi(k)a_k$$

converges. Moreover the absolute value of its sum does not exceed $a_1\mathfrak{m}/2$.

Proof A real non-principal Dirichlet character χ maps the group of units of the ring of rational integers modulo $\mathfrak{m}$ onto the real roots of unity homomorphically. That is,

$$\chi : U(\mathbb{Z}_{\mathfrak{m}}) \to \{\pm 1\}$$

is a surjective group homomorphism. So χ takes on an equal number of positive and negative values amongst the terms of the sequence $\{\chi(k)a_k\}_1^{\mathfrak{m}}$. Denote the sum of the positive elements of this sequence by P_1 and the sum of the absolute values of the negative elements by N_1. Since χ has period $\mathfrak{m}$, we continue the notation by labelling the sum of the positive elements in the sequence $\{\chi(k)a_k\}_{(r-1)\mathfrak{m}+1}^{r\mathfrak{m}}$ by P_r and the corresponding sum of the absolute values of the negative elements by N_r. Since the sequence $\{a_k\}$ is decreasing we have

$$\frac{a_1\mathfrak{m}}{2} \geq P_1 \geq P_2 \geq P_3 \geq \ldots$$

and

$$\frac{a_1\mathfrak{m}}{2} \geq N_1 \geq N_2 \geq N_3 \geq \ldots$$

Without loss of generality suppose that $P_1 \geq N_1$, then by the periodic nature of χ we have $P_r \geq N_r$ for all $r \in \mathbb{N}$. So the series

$$P_1 - N_1 + P_2 - N_2 + \ldots$$

is an alternating series satisfying the conditions of the Alternating Series theorem[15] and therefore converges to a limit L whose absolute value does not exceed $a_1\mathfrak{m}/2$. Now denote the nth partial sum of the series $\sum \chi(k)a_k$ by S_n. Using the notation of partial sums we may write our result as

$$\lim_{n\to\infty} S_{\mathfrak{m}n} = L$$

Next, we have $S_{\mathfrak{m}n+t} = S_{\mathfrak{m}n} + a_{\mathfrak{m}n+t}$, whenever $1 \leq t \leq \mathfrak{m}-1$. So the sequence $\{S_{\mathfrak{m}n+t}\}_1^{\infty}$ converges to L since we know $a_{\mathfrak{m}n+t} \to 0$ as $n \to \infty$. So we conclude that S_n converges to L and the theorem is proved.

Corollary 4.2.3. *The real non-principal Dirichlet character series modulo* $\mathfrak{m}$

$$\frac{1}{n}\sum_{k=1}^{\infty}\chi(k)\frac{n}{k}=\sum_{k=1}^{\infty}\frac{\chi(k)}{k}$$

converges. Moreover its sum is bounded by $\mathfrak{m}/2$, *which we note is independent of* n.

Proof. This is immediate since $\{1/k\}_1^{\infty}$ is a non-negative decreasing sequence with $1/k \to 0$ as $k \to \infty$ and $a_1 = 1$.

That the Dirichlet character series of Corollary 4.2.3 converges is useful but we need more information than this corollary provides. The following theorem addresses this need.

Theorem 4.2.4. *Suppose* χ *is a real non-principal Dirichlet character modulo* $\mathfrak{m}$, *then*

$$\frac{1}{n}\sum_{k=1}^{\infty}\chi(k)\left\lfloor\frac{n}{k}\right\rfloor=\sum_{k=1}^{\lfloor\sqrt{n}\rfloor}\frac{\chi(k)}{k}+O(1/\sqrt{n})$$

Proof. Firstly,

$$\frac{1}{n}\sum_{k=1}^{\infty}\chi(k)\left\lfloor\frac{n}{k}\right\rfloor=\frac{1}{n}\sum_{k=1}^{\lfloor\sqrt{n}\rfloor}\chi(k)\left\lfloor\frac{n}{k}\right\rfloor+\frac{1}{n}\sum_{k=\lfloor\sqrt{n}\rfloor+1}^{\infty}\chi(k)\left\lfloor\frac{n}{k}\right\rfloor$$

Secondly,

$$\left|\sum_{k=1}^{\lfloor\sqrt{n}\rfloor}\chi(k)\frac{n}{k}-\sum_{k=1}^{\lfloor\sqrt{n}\rfloor}\chi(k)\left\lfloor\frac{n}{k}\right\rfloor\right|\leq\sqrt{n}$$

since there are at most $\sqrt{n}$ differences and each difference is non-negative and less than one. So

$$\sum_{k=1}^{\lfloor\sqrt{n}\rfloor} \chi(k)\left\lfloor\frac{n}{k}\right\rfloor = \sum_{k=1}^{\lfloor\sqrt{n}\rfloor} \chi(k)\frac{n}{k} + O(\sqrt{n}),$$

and hence that

$$\frac{1}{n}\sum_{k=1}^{\infty} \chi(k)\left\lfloor\frac{n}{k}\right\rfloor = \sum_{k=1}^{\lfloor\sqrt{n}\rfloor} \frac{\chi(k)}{k} + \frac{1}{n}\sum_{k=\lfloor\sqrt{n}\rfloor+1}^{\infty} \chi(k)\left\lfloor\frac{n}{k}\right\rfloor + O(1/\sqrt{n}) \qquad (4\ 2\ 5)$$

Now the series

$$\frac{1}{\sqrt{n}}\sum_{k=\lfloor\sqrt{n}\rfloor+1}^{\infty} \chi(k)\left\lfloor\frac{n}{k}\right\rfloor = \sum_{k=\lfloor\sqrt{n}\rfloor+1}^{\infty} \chi(k)\frac{\lfloor n/k\rfloor}{\sqrt{n}}$$

is a Dirichlet character series satisfying the requirements of Theorem 4 2 2. So it converges and is bounded by the number $\mathfrak{m}/2$ since

$$\frac{\lfloor n/k\rfloor}{\sqrt{n}} < 1 \text{ when } k = \lfloor\sqrt{n}\rfloor + 1$$

So

$$\frac{1}{\sqrt{n}}\sum_{k=\lfloor\sqrt{n}\rfloor+1}^{\infty} \chi(k)\left\lfloor\frac{n}{k}\right\rfloor \text{ is } O(1)$$

Returning to equation 4 2 5, we now have

$$\begin{aligned}\frac{1}{n}\sum_{k=1}^{\infty} \chi(k)\left\lfloor\frac{n}{k}\right\rfloor &= \sum_{k=1}^{\lfloor\sqrt{n}\rfloor} \frac{\chi(k)}{k} + \frac{1}{\sqrt{n}}O(1) + O(1/\sqrt{n}) \\ &= \sum_{k=1}^{\lfloor\sqrt{n}\rfloor} \frac{\chi(k)}{k} + O(1/\sqrt{n})\end{aligned}$$

This completes the proof.

Corollary 4.2.6. *With respect to $A(-m)$ with $-m \not\equiv 1\ (4)$ we have*

$$\frac{\pi}{\lambda\sqrt{m}} = \sum_{k=1}^{\lfloor\sqrt{n}\rfloor} \frac{\chi(k)}{k} + O(1/\sqrt{n})$$

and

$$\frac{\pi}{\lambda\sqrt{m}} = \sum_{k=1}^{\infty} \frac{\chi(k)}{k}$$

Proof. The first equality follows immediately from Corollary 3.3.3 and Theorem 4.2.4. Letting n approach infinity, gives the second equality.

4.3 Calculations

By Theorem 2.3.6, the number of units λ in $A(-1)$ and $A(-2)$ equals 4 and 2 respectively. So by Theorem 4.1.4 and Corollary 4.2.6 we calculate to obtain

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + - \ldots$$

and

$$\frac{\pi}{2\sqrt{2}} = 1 + \frac{1}{3} - \frac{1}{5} - \frac{1}{7} + + - - \ldots$$

The first series is due to Leibniz and the second to Newton.

When working with respect to $A(-1)$, the numerical function $r(n)$ counts the elements of the set $\{(x, y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n\}$. The power series generating function for $r(n)$ in this case, is therefore $(1+2x+2x^4+2x^9+\ldots)^2$. By Corollary 3.2.10, we conclude

$$(1+2x+2x^4+2x^9+\ldots)^2 = 1+4\left(\frac{x}{1-x} - \frac{x^3}{1-x^3} + \frac{x^5}{1-x^5} - + \ldots\right) \quad (4.3.1)$$

The argument for Identity 4.3.1 follows that found in Hardy and Wright[7]. The identity was first discovered by Jacobi[10] using the theory of elliptic functions. Interestingly, Jacobi applied this identity to subsequently determine $r(n)$ in the case of the sum of two squares, a complete reversal of the present method.

We now wish to extend the method to determine a similar identity for $r(n)$ when working with respect to $A(-2)$. Here, the function $r(n)$ counts the elements of the set $\{(x, y) \in \mathbb{Z}^2 \mid x^2 + 2y^2 = n\}$. The power series generating function for $r(n)$ is therefore

$$(1 + 2x + 2x^4 + 2x^9 + \ldots)(1 + 2x^2 + 2x^8 + 2x^{18} + \ldots)$$

By Corollary 3.2.10, we conclude

$$(1 + 2x + 2x^4 + 2x^9 + \ldots)(1 + 2x^2 + 2x^8 + 2x^{18} + \ldots)$$

$$= 1 + 2\left(\frac{x}{1-x} + \frac{x^3}{1-x^3} - \frac{x^5}{1-x^5} - \frac{x^7}{1-x^7} + + - - \ldots\right) \qquad (4.3.2)$$

Identity 4.3.2, extends a result found in Dirichlet[4].

Chapter 5

$A(-m)$ where $-m \equiv 1\ (4)$

The imaginary quadratic number fields $\mathbb{Q}(\sqrt{-m})$ of class number one with $-m \equiv 1\ (4)$ occur when $-m \in \{-3, -7, -11, -19, -43, -67, -163\}$. In this chapter we are only concerned with these values of $-m$ and we will denote this set of numbers by $\mathbb{M}$.

5.1 The function χ is a real non-principal Dirichlet character for $A(-m)$ where $-m$ is in $\mathbb{M}$

From Theorem 4.2.4 we have established that if χ is a real non-principal Dirichlet character modulo $\mathfrak{m}$ then

$$\frac{1}{n}\sum_{k=1}^{\infty}\chi(k)\left\lfloor\frac{n}{k}\right\rfloor = \sum_{k=1}^{\lfloor\sqrt{n}\rfloor}\frac{\chi(k)}{k} + O(1/\sqrt{n})$$

So if we can show that χ is a real non-principal Dirichlet character for $A(-m)$ where $-m \in \mathbb{M}$, we can apply this result with Corollary 3.3.3 to establish series like those of Section 4.3. As in the proof of Theorem 4.1.4, the major task is to show that χ is periodic. Using Theorem 2.3.8 and Theorem 2.3.9 with $-m \equiv 1\ (4)$, we have a result similar to equation 4.1.2, namely

$$\chi(p) = \begin{cases} (-m/p), & \text{if } p \neq m \text{ is an odd prime,} \\ 0, & \text{if } p = m, \\ (-1)^{(m^2-1)/8}, & \text{if } p = 2 \end{cases} \qquad (5.1.1)$$

Theorem 5.1.2 *The numerical function χ for the ring of integers $A(-m)$ where $-m \in \mathbb{M}$ is periodic. Moreover the period is m.*

Proof. We must show that for any two rational integers a and b that $\chi(a) = \chi(b)$ whenever $a \equiv b\ (m)$.

First, if $a \equiv b \equiv 0\ (m)$ then $\chi(a) = \chi(b) = 0$ because m divides both a and b. So in what follows we may suppose that neither a nor b is congruent to 0 modulo m.

We claim that it suffices to consider either a or b to be odd. To see this, suppose $a = 2^r\alpha$ and $b = 2^s\beta$ with $\gcd(2, \alpha) = \gcd(2, \beta) = 1$ and without loss of generality take $r \geq s$. Then $a \equiv b\ (m)$ or equivalently $2^r\alpha \equiv b = 2^s\beta\ (m)$, which in turn is equivalent to $2^{r-s}\alpha \equiv \beta\ (m)$ as m is odd. Since β is odd, the initial claim is established.

Next, without loss of generality suppose that $a = p_1p_2 \cdots p_r$ is odd with the primes $p_i (1 \geq i \geq r)$ not necessarily distinct. Further suppose that $b = 2^s\beta$ with $\gcd(2, \beta) = 1$ and $s \geq 0$. Then

$$\begin{aligned}
\chi(a) &= \chi(p_1p_2 \cdots p_r) \\
&= \chi(p_1)\chi(p_2) \cdots \chi(p_r) \\
&= (-m/p_1)(-m/p_2) \cdots (-m/p_r) \\
&= (-m/a), \quad \text{the Jacobi symbol.}
\end{aligned}$$

Now since a and m are both odd and $-m \equiv 1\ (4)$ we can use Theorem 2 2 3 and Theorem 2 2 4 concerning the Jacobi symbol, to give

$$\begin{aligned}
\chi(a) &= (a/-m) \\
&= (b/-m) \\
&= (2^s\beta/-m) \\
&= (2/-m)^s(\beta/-m) \\
&= \left[(-1)^{(m^2-1)/8}\right]^s(-m/\beta) \\
&= [\chi(2)]^s\chi(\beta) \\
&= \chi(b)
\end{aligned}$$

This completes the proof

Corollary 5 1 3 *The numerical function χ with respect to the ring of integers $A(-m)$ is a real non-principal Dirichlet character modulo m*

Proof By definition, χ is completely multiplicative, by equation 5 1 1, χ takes its values from the set $\{0, \pm 1\}$ and we have just seen that χ has period m What remains to be shown is that χ is non-principal To do this it suffices to exhibit an inertial prime in $A(-m)$ Now, the non-rational integer of least norm is ξ and $\|\xi\| = (1+m)/4$ for $-m \equiv 1\ (4)$ So $\|\xi\| > 2$ whenever $m > 7$, and therefore 2 is certainly inertial for $-m < -7$ For $A(-3)$ and $A(-7)$, it is easy to check that 2 and 3 respectively are inertial We could also have made use of Theorem 2 3 9 to show that 2 is inertial for all our $A(-m)$ except $A(-7)$ However, this argument would require checking the residue classes modulo 8 and consequently is a less appealing argument

The following corollary mirrors Corollary 4 2 6 and its proof is all but identical

Corollary 5.1 4 *Working with respect to the ring of integers $A(-m)$ with m in $\mathbb{M}$, we have*

$$\frac{2\pi}{\lambda\sqrt{m}} = \sum_{k=1}^{\infty} \frac{\chi(k)}{k}$$

5 2 Calculations

Corollary 5 1 4 gives us a formula relating an expression in π to a Dirichlet character series However, it would be satisfying to see the numerical values By Theorem 2 3 6, $\lambda = 6$ when $-m = -3$ and the period of χ in this case is 3 A simple calculation gives the series

$$\frac{\pi}{3\sqrt{3}} = 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + - \quad ,$$

which was first discovered by Euler

For the remaining values of m for which $A(-m)$ is a unique factorization domain, we have $\lambda = 2$ on appealing to Theorem 2 3 6 once again The calculation of χ for these remaining values of m is tedious but at least its periodicity means it suffices to calculate the values of χ from 1 to m, and of course $\chi(m) = 0$ To ease the burden of hand calculation we use Waterloo Maple V4 in conjunction with the multiplicative nature of χ and the result 5 1 1 to calculate the values of χ The required calculations result in the series

$$\frac{\pi}{\sqrt{7}} = 1 + 1/2 - 1/3 + 1/4 - 1/5 - 1/6 + \ldots$$

$$\frac{\pi}{\sqrt{11}} =$$

$$1 - 1/2 + 1/3 + 1/4 + 1/5 - 1/6 - 1/7 - 1/8 + 1/9 - 1/10 + \ldots$$

$$\frac{\pi}{\sqrt{19}} =$$

$$1 - 1/2 - 1/3 + 1/4 + 1/5 + 1/6 + 1/7 - 1/8 + 1/9 - 1/10 + 1/11 - 1/12 - 1/13 -$$
$$1/14 - 1/15 + 1/16 + 1/17 - 1/18 + \ldots$$

$$\frac{\pi}{\sqrt{43}} =$$

$$1 - 1/2 - 1/3 + 1/4 - 1/5 + 1/6 - 1/7 - 1/8 + 1/9 + 1/10 + 1/11 - 1/12 + 1/13 +$$
$$1/14 + 1/15 + 1/16 + 1/17 - 1/18 - 1/19 - 1/20 + 1/21 - 1/22 + 1/23 + 1/24 +$$
$$1/25 - 1/26 - 1/27 - 1/28 - 1/29 - 1/30 + 1/31 - 1/32 - 1/33 - 1/34 + 1/35 +$$
$$1/36 - 1/37 + 1/38 - 1/39 + 1/40 + 1/41 - 1/42 + \ldots$$

$$\frac{\pi}{\sqrt{67}} =$$

$$1 - 1/2 - 1/3 + 1/4 - 1/5 + 1/6 - 1/7 - 1/8 + 1/9 + 1/10 - 1/11 - 1/12 - 1/13 +$$
$$1/14 + 1/15 + 1/16 + 1/17 - 1/18 + 1/19 - 1/20 + 1/21 + 1/22 + 1/23 + 1/24 +$$
$$1/25 + 1/26 - 1/27 - 1/28 + 1/29 - 1/30 - 1/31 - 1/32 + 1/33 - 1/34 + 1/35 +$$
$$1/36 + 1/37 - 1/38 + 1/39 + 1/40 - 1/41 - 1/42 - 1/43 - 1/44 - 1/45 - 1/46 +$$
$$1/47 - 1/48 + 1/49 - 1/50 - 1/51 - 1/52 - 1/53 + 1/54 + 1/55 + 1/56 - 1/57 -$$
$$1/58 + 1/59 + 1/60 - 1/61 + 1/62 - 1/63 + 1/64 + 1/65 - 1/66 + \ldots$$

$$\frac{\pi}{\sqrt{163}} =$$

$$1-1/2-1/3+1/4-1/5+1/6-1/7-1/8+1/9+1/10-1/11-1/12-1/13+$$
$$1/14+1/15+1/16-1/17-1/18-1/19-1/20+1/21+1/22-1/23+1/24+$$
$$1/25+1/26-1/27-1/28-1/29-1/30-1/31-1/32+1/33+1/34+1/35+$$
$$1/36-1/37+1/38+1/39+1/40+1/41-1/42+1/43-1/44-1/45+1/46+$$
$$1/47-1/48+1/49-1/50+1/51-1/52+1/53+1/54+1/55+1/56+1/57+$$
$$1/58-1/59+1/60+1/61+1/62-1/63+1/64+1/65-1/66-1/67-1/68+$$
$$1/69-1/70+1/71-1/72-1/73+1/74-1/75-1/76+1/77-1/78-1/79-1/80+$$
$$1/81-1/82+1/83+1/84+1/85-1/86+1/87+1/88-1/89+1/90+1/91-1/92+$$
$$1/93-1/94+1/95+1/96+1/97-1/98-1/99+1/100-1/101-1/102-1/103+$$
$$1/104-1/105-1/106-1/107-1/108-1/109-1/110+1/111-1/112+1/113-$$
$$1/114+1/115-1/116-1/117+1/118+1/119-1/120+1/121-1/122-1/123-$$
$$1/124-1/125+1/126-1/127-1/128-1/129-1/130+1/131+1/132+1/133+$$
$$1/134+1/135+1/136-1/137-1/138-1/139+1/140-1/141-1/142+1/143+$$
$$1/144+1/145+1/146-1/147-1/148-1/149+1/150+1/151+1/152-1/153-$$
$$1/154+1/155+1/156-1/157+1/158-1/159+1/160+1/161-1/162+\ldots$$

We would also like to calculate identities such as 4 3 1 and 4 3 2 when working with respect to $A(-m)$ for $-m$ in $\mathbb{M}$. Unfortunately, here $r(n)$ counts the elements of the set $\{(x,y) \in \mathbb{Z}^2 \mid x^2+xy+(1+m)/4y^2 = n\}$, and it is not easy to see how to obtain a power series generating function for the numerical function r in this case. However, on substituting $(2x+y, y)$ for (x, y), it follows that $x^2+my^2 = 4n$

has a solution if and only if $x^2 + xy + y^2(1+m)/4 = n$ has a solution. So $r(n)$ counts the elements in the set

$$\{(x,y) \in \mathbb{Z}^2 \mid x^2 + my^2 = 4n\} = \{(x,y) \in \mathbb{Z}^2 \mid (x/2)^2 + m(y/2)^2 = n\}$$

Now, the coefficients of the terms with integral powers in the expansion of

$$(1 + 2x^{1/4} + 2x^{4/4} + 2x^{9/4} + \ldots)(1 + 2x^{m/4} + 2x^{4m/4} + 2x^{9m/4} + \ldots)$$

correspond to our required values of r. That is, the power series within this expansion is the power series generating function for r. Let us denote the power series within a series by POW(*series*). So in the case of $-m = -3$, we have by Corollary 3.2.10 that

$$\text{POW}\left\{(1 + 2x^{1/4} + 2x^{4/4} + 2x^{9/4} + \ldots)(1 + 2x^{3/4} + 2x^{12/4} + 2x^{27/4} + \ldots)\right\}$$

$$= 1 + 6\left(\frac{x}{1-x} - \frac{x^2}{1-x^2} + \frac{x^4}{1-x^4} - \frac{x^5}{1-x^5} + - \ldots\right)$$

For any other value of $-m$ in $\mathbb{M}$, we have

$$\text{POW}\left\{(1 + 2x^{1/4} + 2x^{4/4} + 2x^{9/4} + \ldots)(1 + 2x^{m/4} + 2x^{4m/4} + 2x^{9m/4} + \ldots)\right\}$$

$$= 1 + 2\sum_{n=1}^{\infty} \chi(n)\frac{x^n}{1-x^n},$$

where the values of χ have already been determined and may be ascertained from the previously calculated series involving π.

References

[1] G. B. Birkhoff, *Note on certain quadratic number systems for which factorization is unique*, American Mathematical Monthly **13** (1906), 156–159.

[2] R. Dedekind, *Sur la Théorie des Nombres Entiers Algébriques*, Gauthiers-Villars (1877).

[3] R. Dedekind, *Supplement XI to P. G. L. Dirichlet, "Vorlesungen uber Zahlentheorie"*.

[4] P. G. L. Dirichlet, *Recherches sur diverse applications de l'analyse infinitésimale a la théorie des nombres*, Journal fúr die reine und angewandte Mathematik **19** (1839), 324–369.

[5] P. G. L. Dirichlet, *Vorlesungen uber Zahlentheorie*, fourth edition, reprinted by Chelsea, 1968.

[6] D. Dubois and A. Steger, *A note on division algorithms in imaginary quadratic number fields*, Canadian Journal of Mathematics **19** (1958), 285–286.

[7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fourth edition, Oxford, 1960.

[8] T. L. Heath, *Diophantus of Alexandria*, second edition, reprinted by Dover, 1964, p. 106.

[9] I. N. Herstein, *Topics in Algebra*, second edition, John Wiley and Sons, 1975.

[10] C G Jacobi, *Fundamenta Nova Theoriae Functionum Ellipticarum*, 1829

[11] I Niven and H S Zuckerman, *An Introduction to the Theory of Numbers*, second edition, John Wiley and Sons, 1966

[12] H Pollard, *The Theory of Algebraic Numbers*, Mathematical Association of America, 1950

[13] H M Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Mathematical Journal **14** (1967), 1–27

[14] I N Stewart and D O Tall, *Algebraic Number Theory*, second edition, Chapman and Hall, 1987

[15] D V Widder, *Advanced Calculus*, second edition, Prentice-Hall, 1961, p 293

[16] H S Wilf, *Generatingfuctionology*, second edition, Academic Press, 1994

Vita

Surname: Bannar-Martin Given Names: Mark William

Place of Birth: Port Elizabeth, South Africa

Educational Institutions Attended:

University of Auckland	1971–1975
University of Victoria	1992–1998

Degrees Awarded:

B Sc.	University of Auckland	1974
B A.	University of Auckland	1976

Honours and Awards:

The Senior Chemistry Prize	University of Auckland	1974

Partial Copyright License

I hereby grant the right to lend my thesis to users of the University of Victoria Library, and to make single copies only for such users, or in response to a request from the Library of any other university or similar institution, on its behalf or for one of its users. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by me or a member of the university designated by me. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Title of Thesis:

Some Consequences of Unique Factorization in Imaginary Quadratic Number Fields of Class Number 1

Author: [redacted]

Mark William Bannar-Martin

December 6, 1998