AN EXAMINATION OF CLASS NUMBER FOR $\mathbb{Q}(\sqrt{d})$ WHERE $\sqrt{d}$ HAS CONTINUED FRACTION EXPANSION OF PERIOD THREE

Brent O. J. Young

A Thesis Submitted to
University North Carolina Wilmington in Partial Fulfillment
Of the Requirements for the Degree of
Master of Science

Department of Mathematics and Statistics

University North Carolina Wilmington

2005

Approved by

Advisory Committee

Chair

Accepted by

Dean, Graduate School

This thesis has been prepared in the style and format

consistent with the journal

American Mathematical Monthly.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

We begin by finding an appropriate parametrization for d that will ensure $\sqrt{d}$ has continued fraction expansion of period three. After finding this parametrization, we use elementary arguments to limit the possible values of d leading to real quadratic number fields $\mathbb{Q}(\sqrt{d})$ of class number one to a set of 30 congruence classes modulo 9240. We then examine the class number formula, and using an analytic result we are able to place an upper bound on d beyond which the class number must exceed one (with at most one exception).

We conclude by examining algorithms that enable us to compute the class number more efficiently. Using such algorithms (as programmed in PARI) we give an enumeration of all such fields with class number one.

ACKNOWLEDGMENTS

There are many people who have made this thesis possible. I would first like to thank Dr. Michael Freeze for his invaluable help and considerable patience while working with me on this project. I would also like to thank Dr. John Karlof and Dr. Kenneth Spackman for serving on my committee.

I would like to thank all the UNCW Mathematics and Statistics faculty with whom I have had the pleasure to work and from whom I have learned a great deal. I would especially like to thank Dr. Yaw Chang and Dr. Mark Lammers for taking time to pursue independent study courses with me.

Finally, and certainly not least, I would like to thank my parents Ricky and Betty Jo Young and my younger brother Brett Young. Without their support, none of this would have been possible.

1 INTRODUCTION

In 1966, H. M. Stark published a paper proving that the number of complex quadratic number fields with class number one is finite. This paper was an extension of ideas originally published by Heegner. The related question of the number of real quadratic number fields with class number one is still unsolved. Gauss himself conjectured that the number of such fields is infinite.

Short of proving the conjecture for all real quadratic number fields, many papers have been published looking at the number of such fields where the discriminant takes on special forms. In two papers published in Acta Arithmetica in 2003, Biro considered real quadratic number fields of the form $\mathbb{Q}(\sqrt{d})$ where $d = p^2 + 4$ (p an odd positive integer) [7] and where $d = 4p^2 + 1$ (p a positive integer) [8]. In both cases, the natural assumption that d be squarefree was in force.

We consider real quadratic number fields $\mathbb{Q}(\sqrt{d})$ where d is a squarefree positive integer with a continued fraction expansion of period three. The continued fraction assumption will lead to a parametrization for these numbers and provide nice limits on possible norms for elements in the associated number rings.

We first give some background on continued fraction expansions of quadratic surds and then develop the parametrization of our class of numbers. Finally, we tackle the question of class number.

2 CONTINUED FRACTIONS

A continued fraction is any expression of the form

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\cdots + \frac{1}{a_n}}}}$$

where n can be arbitrarily large or infinite. The quantities $a_0, a_1, \ldots, a_n$ are called *partial quotients* and can be integers, real numbers, or even complex. For our purposes, we limit ourselves to *regular continued fractions* - ones that have positive integers as partial quotients (except a_0 which can be any integer). We typically write continued fractions in the form $[a_0; a_1, a_2, \ldots, a_n]$ to save space.

If a continued fraction has only a finite number of partial quotients, then it represents a rational number. We will be dealing with an infinite sequence of partial quotients - $[a_0; a_1, a_2, \ldots]$. An infinite continued fraction is necessarily irrational [6][p.4]. In what follows, it is critical that we be able to find the *convergents* of the continued fraction. These are the rational numbers we obtain by truncating our continued fraction expansion after a finite number of partial quotients. We label these convergents $C_n = [a_0; a_1, a_2, \ldots, a_n]$. Thus,

$$\begin{aligned} C_0 &= a_0 \\ C_1 = a_0 + \frac{1}{a_1} &= \frac{a_0 a_1 + 1}{a_1} \\ C_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} &= \frac{a_0(a_1 a_2 + 1) + a_2}{a_1 a_2 + 1} \end{aligned}$$

This suggests we develop a recursive formula for the convergents. This can be done, and the results are two recursively defined sequences A_k and B_k such that $C_k = \frac{A_k}{B_k}$. The number A_k is called the numerator of the convergent while B_k is called the denominator of the convergent. They are given by

$$A_{-1} = 1 \qquad B_{-1} = 0$$

$$A_0 = a_o \qquad B_0 = 1$$

and for $k \geq 0$

$$A_{k+1} = a_{k+1}A_k + A_{k-1} \qquad B_{k+1} = a_{k+1}B_k + B_{k-1} \tag{1}$$

and satisfy the linear diophantine equation $A_kB_{k-1} - A_{k-1}B_k = (-1)^{k-1}$ (c.f. [6][pp. 1-2]).

If $t = [a_0; a_1, a_2, \ldots]$, then we wish to determine the relationship between t and its convergents. We first define the *k-th complete quotient* ζ_k of t:

$$\zeta_k = [a_k; a_{k+1}, a_{k+2}, \ldots].$$

It turns out that t satisfies the following relationship for all $k \geq 0$ [6][pp.4-5]:

$$t = \tfrac{A_k\zeta_{k+1} + A_{k-1}}{B_k\zeta_{k+1} + B_{k-1}}. \tag{2}$$

This result is crucial for what follows on periodic continued fractions.

The convergents of a continued fraction are a sequence of rational numbers whose limit is the irrational number t represented by the continued fraction. These convergents are not just random rational numbers, but turn out to be the *best rational approximations* to t in the sense that a convergent $\frac{a}{b}$ of t is the closest rational number to t with denominator less than or equal to b [6][pp.19-37]. This is a powerful result and drives many of the applications of continued fractions - including the result on norms we eventually wish to use.

Now that we have made basic definitions and motivated the use of continued fractions, we need a means of calculating the continued fraction expansion of a given irrational number. In what follows, we use $\lfloor x \rfloor$ to indicate the greatest integer less than x (or the floor function of x) and T to represent the transformation $T(x) = \frac{1}{x}$. We can see that $a_0 = \lfloor t \rfloor$ and that $t - a_0 = [0; \zeta_1]$ is an irrational number in the interval $(0, 1)$. Using the transformation T on $t - a_0$ gives $T(t - a_0) = \zeta_1 = [a_1; a_2, a_3, \ldots]$. Thus, $a_1 = \lfloor T(t - a_0) \rfloor$. Repeating this process with $\zeta_1 - a_1$ will give us a_2 and so forth. Thus, we obtain the continued fraction expansion of any irrational number by a sequence of integer approximations and inversions [6][pp.8-9]. We note that with the exception of a_0, none of the partial quotients $a_1, a_2, \ldots$ can ever be zero. We see this since each such quotient is found by finding the greatest integer less than a quantity which is the multiplicative inverse of an irrational number between zero and one. Hence, each quotient is at least one.

We now wish to consider continued fraction expansions where the partial quotients repeat in some block. To that end, we write

$$t = [a_0; a_1, \ldots, a_{n-1}, \overline{a_n, \ldots, a_{n+m-1}}]$$

to represent a continued fraction expansion with *initial block of length* n (of non-repeating partial quotients $a_0, a_1, \ldots, a_{n-1}$) and *repeating block of length* m $(a_n, \ldots, a_{n+m-1})$. We are supposing that there is no shorter possible repeating block and that the initial block does not contain a copy of the repeating block.

Lagrange was the first to prove that t has a periodic continued fraction expansion if and only if t is a quadratic surd. The fact that a periodic continued fraction represents a quadratic surd is a consequence of the fact that the complete quotients are themselves periodic (namely, $\zeta_n = \zeta_{n+m} = \zeta_{n+2m} = \cdots$) combined with equation (2) above.

For our purposes, we wish to consider expansions of $\sqrt{d}$ where d is a non-square positive integer. It turns out that for numbers of this form, the continued fraction expansion has a nice symmetry property [6][p.47]:

$$\sqrt{d} \quad = \quad [a_0; \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}]. \tag{3}$$

This result along with the periodicity of the complete quotients will give us a means of determining which of these numbers have period three.

3 A PARAMETRIZATION FOR $\sqrt{d}$ WITH CONTINUED FRACTION EXPANSION OF PERIOD LENGTH THREE

Now that we have given some background on continued fractions, we wish to utilize these results to determine a parametrization for numbers of the form $\sqrt{d}$ with d a non-square positive integer having a continued fraction expansion of period length three.

Theorem 3.1 *Let d be a positive integer that is not a perfect square, and let ℓ and n be strictly positive integers. Then $\sqrt{d}$ has a continued fraction expansion of period length three if and only if d is of the form*

$$d = [\ell(4n^2+1)+n]^2 + 4\ell n + 1. \tag{4}$$

In this case, the continued fraction expansion of $\sqrt{d}$ is given by

$$\sqrt{d} = [\ell(4n^2+1)+n;\ \overline{2n,\ 2n,\ 2(\ell(4n^2+1)+n)}].$$

We note that though the parametrization is slightly unwieldy, the two parameters ℓ and n are completely free with the exception that they be positive integers. This gives as an immediate consequence that there are an infinite number of integers d giving rise to continued fractions of period length three (a result which actually holds for every period length). In addition, this form will lead to certain divisibility properties that will be crucial in later discussions.

Proof of Theorem 3.1:

We begin with the sufficiency of the parametrization. To that end, we assume that d is of the form given in (4) for some choice of parameters ℓ and n (which are assumed to be positive integers). We put to use the method for finding the continued fraction expansion briefly outlined above. First, we need to find a_0.

$$\begin{aligned} a_0 &= \lfloor\sqrt{d}\rfloor \\ &= \lfloor\sqrt{[\ell(4n^2+1)+n]^2+4\ell n+1}\rfloor \end{aligned}$$

We note that

$$[\ell(4n^2+1)+n]^2 \quad < [\ell(4n^2+1)+n]^2+4\ell n+1 < \quad [\ell(4n^2+1)+n+1]^2$$

or

$$\ell(4n^2+1)+n \quad < \sqrt{[\ell(4n^2+1)+n]^2+4\ell n+1} < \quad \ell(4n^2+1)+n+1$$

which gives us that $a_0 = \ell(4n^2+1)+n$.

To find a_1, we need to determine $\left\lfloor\frac{1}{\sqrt{d}-a_0}\right\rfloor$.

$$\begin{aligned} a_1 &= \left\lfloor\frac{1}{\sqrt{d}-a_0}\right\rfloor \\ &= \left\lfloor\frac{\sqrt{d}+a_0}{d-a_0^2}\right\rfloor \\ &= \left\lfloor\frac{\sqrt{d}+a_0}{4\ell n+1}\right\rfloor \end{aligned}$$

Since

$$2a_0 \quad < \quad \sqrt{d}+a_0 \quad < \quad 2a_0+1$$

we have

$$\tfrac{8\ell n^2+2\ell+2n}{4\ell n+1} \quad < \quad \tfrac{\sqrt{d}+a_0}{4\ell n+1} \quad < \quad \tfrac{8\ell n^2+2\ell+2n+1}{4\ell n+1}$$

The left most term gives a lower bound of

$$2n \quad < \quad 2n+\tfrac{2\ell}{4\ell n+1} \quad = \quad \tfrac{8\ell n^2+2\ell+2n}{4\ell n+1}$$

while the right most term gives an upper bound of

$$\tfrac{8\ell n^2+2\ell+2n+1}{4\ell n+1} \quad = \quad 2n + \tfrac{2\ell+1}{4\ell n+1} \quad < \quad 2n+1 \ \cdot$$

Thus, we must have $a_1 = 2n$.

To find a_2, we must determine

$$\begin{aligned} a_2 &= \left\lfloor \frac{1}{\frac{\sqrt{d}+a_0}{4\ell n+1} - a_1} \right\rfloor \\ &= \left\lfloor \frac{4\ell n+1}{\sqrt{d}+a_0-8\ell n^2-2n} \right\rfloor \end{aligned}$$

Since $\sqrt{d}+a_0 > 2a_0$ we have that

$$\begin{aligned} \frac{4\ell n+1}{\sqrt{d}+a_0-8\ell n^2-2n} &< \frac{4\ell n+1}{2a_0-8\ell n^2-2n} \\ &= \frac{4\ell n+1}{2\ell} \\ &< 2n+1. \end{aligned}$$

To give an effective lower bound on this quantity, we must tighten our upper bound on $\sqrt{d}+a_0$. To that end we show $\sqrt{d} < a_0 + \frac{1}{2n}$.

$$\begin{aligned} \sqrt{d} &= \sqrt{a_0^2+4\ell n+1} \\ &< \sqrt{a_0^2+4\ell n+\frac{\ell}{n}+\frac{1}{4n^2}+1} \\ &= \sqrt{a_0^2+\frac{a_0}{n}+\frac{1}{4n^2}} \\ &= \sqrt{(a_0+\frac{1}{2n})^2} \\ &= a_0+\frac{1}{2n}. \end{aligned}$$

Using this result, we see that

$$\begin{aligned}\frac{4\ell n+1}{\sqrt{d}+a_0-8\ell n^2-2n} &> \frac{4\ell n+1}{2a_0+\frac{1}{2n}-8\ell n^2-2n}\\ &= \frac{4\ell n+1}{2\ell+\frac{1}{2n}}\\ &= 2n\end{aligned}$$

which when combined with the upper bound given above shows that $a_2 = 2n$.

For a_3 we must determine $\left\lfloor \frac{1}{\frac{4\ell n+1}{\sqrt{d}+a_0-8\ell n^2-2n}-2n} \right\rfloor$:

$$\begin{aligned}a_3 &= \left\lfloor \frac{1}{\frac{4\ell n+1}{\sqrt{d}+a_0-8\ell n^2-2n}-2n} \right\rfloor\\ &= \left\lfloor \frac{\sqrt{d}+a_0-8\ell n^2-2n}{2na_0+1-2n\sqrt{d}} \right\rfloor\\ &= \left\lfloor \frac{(\sqrt{d}+a_0-8\ell n^2-2n)(2na_0+1+2n\sqrt{d})}{4\ell n+1} \right\rfloor\\ &= \left\lfloor \sqrt{d}+a_0 \right\rfloor\\ &= 2a_0.\end{aligned}$$

When we compute a_4 we find that

$$\begin{aligned}a_4 &= \left\lfloor \frac{1}{\sqrt{d}+a_0-2a_0} \right\rfloor\\ &= \left\lfloor \frac{1}{\sqrt{d}-a_0} \right\rfloor\\ &= a_1.\end{aligned}$$

At this point, we can see that the quotients repeat. Thus, we have shown that if d has the form given by (4), then $\sqrt{d} = [\ell(4n^2+1)+n;\ \overline{2n,\ 2n,\ 2(\ell(4n^2+1)+n)}]$.

We now show the necessity of the parametrization. We assume that d is a positive integer (not a perfect square) such that $\sqrt{d}$ has a continued fraction expansion of period three:

$$\sqrt{d} \;=\; [a_0; \overline{a_1, a_1, 2a_0}].$$

We have used the result in (3) above to restrict the number of parameters appropriately. It appears that there should be two parameters. We note that a_0 is not zero (as $\sqrt{d} > 1$) and that a_1 cannot be zero. In addition, we cannot have $a_1 = 2a_0$ as then we would have period length one - which are known to be of the form $m^2 + 1$ for any strictly positive integer m.

Aside from the restrictions above, it is far from clear how a_0 and a_1 are related. The requirement that d be an integer is fairly restrictive. It can be shown for example that the continued fraction expression $[1; \overline{1, 1, 2}]$ is the expansion of $\sqrt{\frac{10}{4}}$. So, the parameters a_0 and a_1 are not the ones we seek.

Letting $\zeta_1 = [\overline{a_1; a_1, 2a_0}]$, we have that

$$[a_0; \zeta_1] \;=\; [a_0; a_1, a_1, 2a_0, \zeta_1].$$

Solving this equation for ζ_1 we find that

$$\frac{A_0\zeta_1 + A_{-1}}{B_0\zeta_1 + B_{-1}} \;=\; \frac{A_3\zeta_1 + A_2}{B_3\zeta_1 + B_2}$$

where the A_k and B_k are the numerator and denominator of the k-th convergent as determined in (1).

After some laborious algebra, we find that ζ_1 satisfies the quadratic expression

$$(2a_0a_1 + 1)\zeta_1^2 - (2a_0a_1^2 + 2a_0)\zeta_1 - (a_1^2 + 1) \;=\; 0.$$

Since ζ_1 is positive, we can use the quadratic formula to find its exact value in terms of a_0 and a_1. In fact, we find that

$$\zeta_1 \;=\; \frac{2a_0a_1^2+2a_0+\sqrt{(2a_0a_1^2+2a_0)^2+4(2a_0a_1+1)(a_1^2+1)}}{2(2a_0a_1+1)}.$$

From our definition of ζ_1 we have $\sqrt{d} = a_0 + \frac{1}{\zeta_1}$ so that

$$\sqrt{d} \;=\; a_0 + \frac{2(2a_0a_1+1)}{2a_0a_1^2+2a_0+\sqrt{(2a_0a_1^2+2a_0)^2+4(2a_0a_1+1)(a_1^2+1)}}$$

which reduces to

$$\sqrt{d} \;=\; \sqrt{a_0^2+\frac{2a_0a_1+1}{a_1^2+1}}.$$

If d is to be an integer then we will need conditions on a_0 and a_1 that will ensure

$$\frac{2a_0a_1+1}{a_1^2+1} \tag{5}$$

is an integer. We first observe that if a_1 is odd, the denominator of (5) will be even. But then (5) cannot be an integer as the numerator is obviously an odd integer. Hence a_1 must be even. Parameterize a_1 by setting $a_1 = 2n$ where n is any positive integer.

Using n in favor of a_1 we find that (5) becomes

$$\frac{4a_0n+1}{4n^2+1}. \tag{6}$$

For (6) to be an integer, we must have

$$4a_0n+1 \;\equiv\; 0(\text{mod } 4n^2+1)$$

or what is equivalent

$$4a_0n \equiv 4n^2 (\text{mod } 4n^2+1).$$

Since both 4 and n are relatively prime to $4n^2+1$ we must have

$$a_0 \equiv n (\text{mod } 4n^2+1).$$

Let ℓ be an integer. Then

$$a_0 = \ell(4n^2+1)+n.$$

Thus, we have shown that for a square free positive integer d if $\sqrt{d} = [a_0; \overline{a_1, a_1, 2a_0}]$ then we must have

$$\begin{aligned} a_0 &= \ell(4n^2+1)+n \\ &\text{and} \\ a_1 &= 2n \end{aligned}$$

where ℓ and n are a pair of non-negative integers.

We note that $n \neq 0$ as then $a_1 = 0$. Also, $\ell \neq 0$ since then $a_0 = n$ and our continued fraction would have period one. Hence, we must restrict ℓ and n to the positive integers. We then have for our integer d

$$d = (\ell(4n^2+1)+n)^2 + 4\ell n + 1. \textbf{ QED}$$

We note that characterizations of $\sqrt{d}$ with period one and two are well known. We mentioned the parametrization for period one above. For period two, we must have $d = a^2 + b$ where b divides $2a$. The parametrization for period three is a little complicated, but still tractable. For longer period lengths, it seems that finding reasonably nice parametrizations is difficult at best.

For example, if $\sqrt{d} = [a_0; \overline{a_1, a_2, a_1, 2a_0}]$ (period four), then we eventually find that the quantity

$$\tfrac{2a_0a_1a_2+2a_0+a_2}{a_1(a_2a_1+2)}$$

is required to be integral. We can certainly find conditions on the parameters, but they do not seem to lead to a definite parametrization. We see, for example, that a_0 can be any positive integer greater than 1. This is true since the continued fraction $[n; \overline{1, n-1, 1, 2n}]$ satisfies the above condition and has period four if $n \neq 1$. It seems that one of the other parameters can be chosen freely, but the conditions on the third parameter are complicated.

For the remainder of the paper, we focus on the case of period three since these numbers admit a reasonable parametrization. For definiteness, we give a table of the first few of these numbers with their continued fraction expansion (see Appendix A).

4 DIVISIBILITY PROPERTIES OF d

We have determined a parametrization of numbers d such that $\sqrt{d}$ has a continued fraction expansion of period three. Specifically $\sqrt{d}$ has period three if and only if

$$d(\ell, n) \;=\; [\ell(4n^2+1)+n]^2 + 4\ell n + 1.$$

We now seek to determine certain divisibility properties of these numbers. We first note that

$$d(\ell, n) \;\equiv\; (\ell+n)^2 + 1 \pmod 4.$$

Since any square modulo 4 is either 0 or 1, we must have $d \equiv 1, 2 \pmod 4$. In particular, if ℓ and n have the same parity, then $(\ell+n)^2 \equiv 0 \pmod 4$ so that $d \equiv 1 \pmod 4$. If ℓ and n have opposite parity, then $(\ell+n)^2 \equiv 1 \pmod 4$ so that $d \equiv 2 \pmod 4$.

We further classify the numbers $d \equiv 1 \pmod 4$. We know that in this case ℓ and n are congruent modulo 2. Expanding the representation of d and reducing modulo 8 we find that

$$d \;\equiv\; \ell^2 + n^2 + 6\ell n + 1 \pmod 8.$$

Suppose further that ℓ and n are congruent modulo 4. Then $\ell = 4r+s$, $n = 4t+s$, and

$$\begin{aligned} d &\equiv (4r+s)^2 + (4t+s)^2 + 6(4r+s)(4t+s) + 1 \pmod 8 \\ &\equiv 1 (\mathrm{mod}\ 8). \end{aligned}$$

Now suppose ℓ and n are not congruent modulo 4. Then $\ell = 4r + s$, $n = 4t + u$ where $s \equiv u \pmod 2$ but s and u are not congruent modulo 4. Then

$$\begin{aligned} d &\equiv (4r+s)^2 + (4t+u)^2 + 6(4r+s)(4t+u) + 1 \pmod 8 \\ &\equiv s^2 + u^2 + 6su + 1 \pmod 8 \end{aligned}$$

Since this last congruence is symmetric with respect to s and u we need only consider two cases : 1) $s = 0$ and $u = 2$, and 2) $s = 1$ and $u = 3$. In both cases $d \equiv 5 \pmod 8$.

So, we have shown the following:

Theorem 4.1 *If $d(\ell, n)$ has the form indicated in Theorem 3.1 then*

$$\begin{array}{rll} \textit{if } \ \ell \equiv n \pmod 4 & \textit{then} & d \equiv 1 \pmod 8 \\ \textit{if } \ \ell \equiv n+2 \pmod 4 & \textit{then} & d \equiv 5 \pmod 8 \\ \textit{if } \ \ell \equiv n+1 \pmod 2 & \textit{then} & d \equiv 2 \pmod 4\ . \end{array}$$

Now we consider d modulo 3. Expanding our representation of d and reducing coefficients modulo 3 we find that

$$d \ \equiv \ \ell^2 n^4 + 2\ell^2 n^2 + 2\ell n^3 + \ell^2 + n^2 + 1 \pmod 3.$$

Examining all possible values of ℓ and n modulo 3 we find the results in the following table.

Table 1: d modulo 3

$\ell \pmod 3$	$n \pmod 3$	$d(\ell, n) \pmod 3$
0	0	1
1	0	2
2	0	2
0	1	2
1	1	2
2	1	1
0	2	2
1	2	1
2	2	2

Thus, for no pair ℓ and n is d divisible by 3. Similar arguments show that no d is divisible by 7,11, or 23.

It is natural to ask whether d is divisible by any prime congruent to 3 (mod 4). Searching the first 100,000 values of d show that none are divisible by such primes.

We can readily find a sufficient condition that will guarantee that a prime congruent to 3 modulo 4 cannot divide d. To that end, we begin by supposing that the Jacobi symbol $(\frac{4\ell n+1}{p}) = 1$ (or that $4\ell n + 1$ is a square modulo p).

If $d \equiv 0$ (mod p), then we must have

$$[\ell(4n^2 + 1) + n]^2 \equiv (-1)(4\ell n + 1) \text{ (mod p)}$$

which implies that $(\frac{(-1)(4\ell n+1)}{p}) = 1$. Since $(\frac{(-1)(4\ell n+1)}{p}) = (\frac{-1}{p})(\frac{4\ell n+1}{p})$ and $p \equiv 3$ (mod 4) gives $(\frac{-1}{p}) = -1$, we must have $1 = -1(\frac{4\ell n+1}{p})$. By assumption, $(\frac{4\ell n+1}{p}) = 1$, and we have a contradiction.

Thus, if $4\ell n+1$ is a square modulo p, then p cannot divide d. While this condition is sufficient, it is clearly not necessary. For example, when $\ell = n = 1$ then $d = 41$ which is prime itself. In particular, 7 does not divide 41. But $(\frac{7}{41}) = (\frac{41}{7}) = (\frac{6}{7}) = -1$.

While the question of whether certain categories of primes can never divide d for any pair of ℓ and n is an interesting one, it will not be crucial in what follows. Hence, we do not pursue it further.

5 ON SOLUTIONS TO PELL'S EQUATION

We have spent considerable time developing a parametrization for numbers $\sqrt{d}$ having continued fractions expansions with period three. Why would such information be of value in trying to determine properties of the associated number field $\mathbb{Q}(\sqrt{d})$? The answer lies in the field norm associated with $\mathbb{Q}(\sqrt{d})$.

In what follows, we will define the field norm for an element α in a number field to be the product of its algebraic conjugates raised to an appropriate power. Since $\mathbb{Q}(\sqrt{d}) = \{a+b\sqrt{d} \mid a, b \in \mathbb{Q}\}$and the algebraic conjugate of an element $q = a+b\sqrt{d}$ is $a - b\sqrt{d}$, we have that $N(q) = a^2 - db^2$ (the appropriate power for our numbers is one). If we restrict a and b to the integers, we see that we have a variant of Pell's Equation. This gives the connection between our number ring and the continued fraction expansion of $\sqrt{d}$.

We look more generally at all integer solutions of

$$x^2 - dy^2 = N \tag{7}$$

where the continued fraction expansion of $\sqrt{d}$ is known.

It is well-known that if $|N| < \sqrt{d}$, then the relatively prime solutions to the variant of Pell's Equation listed above are $x = A_k$ and $y = B_k$ where $\frac{A_k}{B_k}$ is a convergent of $\sqrt{d}$ [6][pp.64-69]. This result essentially relies on the fact that the convergents are the best rational approximations of $\sqrt{d}$.

Not all values of N can be represented by (7) however. We wish to characterize those values that can be so represented. This requires a bit of work. To answer this we consider real quadratic surds and their continued fraction expansions in more detail.

Any real quadratic surd t can be written in the form $\frac{P_0+\sqrt{D}}{Q_0}$ by the quadratic formula where P_0, Q_0, and D are integers, $D > 0$, and Q_0 divides $D - P_0^2$. We use the complete quotients to develop t as a continued fraction [6][pp.65-66]:

$$\begin{aligned}\zeta_1 &= \frac{1}{t-a_0}\\ &= \frac{Q_0}{(P_0-a_0Q_0)+\sqrt{d}}\\ &= \frac{P_1+\sqrt{D}}{Q_1}.\end{aligned}$$

In the last equality we have set $P_1 = a_0Q_0 - P_0$ and $Q_1 = \frac{D-P_1^2}{Q_0}$.

We continue this process to find

$$\zeta_{k+1} = \frac{P_{k+1}+\sqrt{d}}{Q_{k+1}}$$

where $P_{k+1} = a_kQ_k - P_k$ and $Q_{k+1} = \frac{(D-P_{k+1}^2)}{Q_{k+1}}$.

Combining this representation of ζ_k with the result given in (2) we see that for $\sqrt{d}$ we must have

$$\sqrt{d} = \frac{A_k(P_{k+1}+\sqrt{d})+A_{k-1}Q_{k+1}}{B_k(P_{k+1}+\sqrt{d})+B_{k-1}Q_{k+1}}.$$

When we compare the integer and irrational parts of the above equality, we find that

$$A_k = B_kP_{k+1}+B_{k-1}Q_{k+1} \quad \text{and} \quad dB_k = A_kP_{k+1}+A_{k-1}Q_{k+1}.$$

So

$$\begin{aligned}A_k^2-dB_k^2 &= A_k(B_kP_{k+1}+B_{k-1}Q_{k+1})-B_k(A_kP_{k+1}+A_{k-1}Q_{k+1})\\ &= (A_kB_{k-1}-A_{k-1}B_k)Q_{k+1}\\ &= (-1)^{k+1}Q_{k+1}.\end{aligned}$$

So, the potential values for $|N| < \sqrt{d}$ that yield solutions to (7) are given by these Q_k. These turn out to be periodic. For the case of period three, the values of Q_k are given by:

k	0	1	2	3	4	5	6
Q_k	1	$4\ell n + 1$	$4\ell n + 1$	1	$4\ell n + 1$	$4\ell n + 1$	1

so that for $k \equiv 0 \pmod 3$ $Q_k = 1$; otherwise, $Q_k = 4\ell n + 1$.

Thus we have shown:

Theorem 5.1 *For $|N| < \sqrt{d}$ where $\sqrt{d}$ has period three, the only values for N that give rise to relatively prime integer solutions of $x^2 - dy^2 = N$ are ± 1 and $\pm(4\ell n + 1)$. In this case, the relatively prime solutions are given by $x = A_k$ and $y = B_k$ where $\frac{A_k}{B_k}$ is a convergent of $\sqrt{d}$.*

6 BASIC RESULTS ON QUADRATIC NUMBER FIELDS

By *number field*, we mean any subfield of $\mathbb{C}$ that is a finite extension of $\mathbb{Q}$. Any such field is obtained from $\mathbb{Q}$ by adjoining a root (α) of some finite degree polynomial [5][pp.46-49]. Thus, every number field has the form $\mathbb{Q}(\alpha)$ for some algebraic element α of $\mathbb{C}$. If the minimal polynomial of α is of degree n, then $\mathbb{Q}(\alpha)$ has degree n over $\mathbb{Q}$ and the elements $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ form a basis for this field over $\mathbb{Q}$. It can be shown that for every number field, we can choose α to be an *algebraic integer* (i.e. an algebraic number whose minimal polynomial is monic and all coefficients are rational integers) [5][p.77].

By *quadratic number field* we mean a number field of the form $\mathbb{Q}(\sqrt{d})$ where d is a rational number that is assumed to be squarefree. If $d > 0$, we say that $\mathbb{Q}(\sqrt{d})$ is a *real quadratic number field* while if $d < 0$ we call $\mathbb{Q}(\sqrt{d})$ an *imaginary quadratic number field.* These fields are of degree 2 over $\mathbb{Q}$, and so they have the form

$$\mathbb{Q}(\sqrt{d}) \quad = \quad \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

In addition, these fields are normal extensions of $\mathbb{Q}$ with abelian Galois groups (which are isomorphic to $\mathbb{Z}_2$).

We will be interested in the set of algebraic integers contained in these number fields. We typically let $\mathbb{A}$ represent the set of all algebraic integers in $\mathbb{C}$ (this set is actually a ring). So, the set of algebraic integers in $\mathbb{Q}(\sqrt{d})$ is given by

$$\mathrm{R} \quad = \quad \mathbb{A} \cap \mathbb{Q}(\sqrt{d}).$$

It can be shown that R is in fact a ring and is referred to as the *quadratic number ring* associated with $\mathbb{Q}(\sqrt{d})$ (this is true for number fields in general). In fact, these number rings have more structure than that of rings in general - they are ***Dedekind***

Domains [4][pp.55-57].

A Dedekind Domain is any integral domain R satisfying the following conditions:

(1) Every ideal in R is finitely generated.

(2) Every non-zero prime ideal is a maximal ideal.

(3) R is integrally closed in its field of fractions.

We can actually say more about the ideals of a number ring; they are generated by at most two elements - one of which may be chosen arbitrarily [4][pp.61-62]. Since each non-zero ideal must contain some element from $\mathbb{Z}^+$ (as $\alpha \in$ I implies that $N(\alpha) \in$ I) we can choose one generator to be the smallest positive rational integer in the ideal.

We say that a ring is a *Principal Ideal Domain* (or PID) if every ideal is generated by a single element (i.e every ideal is principal). A ring is called a *Unique Factorization Domain* (or UFD) if every element in the ring can be factored uniquely into a product of irreducibles. In general, every PID is a UFD, but not vice versa. With Dedekind Domains, we get the equivalence of the two [4][p.62]. So, one way of determining whether a given number ring is a UFD is to determine whether all the ideals are principal.

Though not every number ring we encounter will be a UFD, there is a type of unique factorization that every number ring will possess (by virtue of being a Dedekind Domain). Namely, every ideal in a number ring can be factored uniquely as a product of prime ideals [4][pp.59-60]. So, even though a number ring may fail to have unique factorization at the element level, we do have unique factorization at the ideal level.

We have been sketching very broad details about number rings in general; we need to focus specifically on the case of quadratic number rings. If $\beta \in \mathbb{Q}(\sqrt{d})$, then it has the form $\beta = a + b\sqrt{d}$. The monic polynomial having this as a root is $x^2 - 2ax + a^2 - db^2$. Thus, β is an algebraic integer if and only if $2a$ and $a^2 - db^2$

are rational integers. Thus a is either a rational integer or half a rational integer - say $a = \frac{c}{2}$ where c is an integer. Then we must have $(\frac{c}{2})^2 - db^2 = \frac{c^2}{4} - db^2$ be an integer. This is equivalent to $c^2 - 4db^2 \equiv 0 \pmod{4}$. Since d is squarefree, it cannot be congruent to zero modulo 4. If $d \equiv 1 \pmod{4}$ then we have $c^2 \equiv 4b^2 \pmod{4}$. If c is odd, then we must have $4b^2 \equiv 1 \pmod{4}$ which can only occur if $b = \frac{e}{2}$ where e is odd. If c is even, then we must have $4b^2 \equiv 0 \pmod{4}$ which says that b is an integer. So, for $d \equiv 1 \pmod{4}$ we have that

$$\mathbb{Q}(\sqrt{d}) \quad = \quad \left\{ \frac{c + e\sqrt{d}}{2} \mid c, e \in \mathbb{Z},\ c \equiv e \pmod{2} \right\}.$$

If $d \equiv 2, 3 \pmod{4}$ then we cannot have half rational integers for our coefficients. Thus, for $d \equiv 2, 3 \pmod{4}$

$$\mathbb{Q}(\sqrt{d}) \quad = \quad \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

We now define some familiar terms and give their form in the case of quadratic number rings. Given any algebraic element β in an algebraic extension $K = \mathbb{Q}(\alpha)$ we can define two functions from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}$. Recall that an embedding of $\mathbb{Q}(\alpha)$ is a ring homomorphism from $\mathbb{Q}(\alpha)$ to $\mathbb{C}$ that fixes $\mathbb{Q}$ point-wise. Such an embedding is completely determined by its action on the element α.

Each embedding of K in $\mathbb{C}$ can only send α to one of its conjugates. We let $\{\alpha = \alpha_1, \ldots, \alpha_n\}$ denote the conjugates of α. Since the minimal polynomial for α has degree n (α has n conjugates) then the dimension of $K = \mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is n. Hence, there are n embeddings of K in $\mathbb{C}$. We denote these embeddings $\{\sigma_1, \ldots, \sigma_n\}$ where $\sigma_i(\alpha) = \alpha_i$.

We now define the trace and norm of β.

Definition 6.1 *The* ***trace*** *of $\beta \in K$ is given by*

$$T_{\mathbb{Q}}^{K}(\beta) = \sum_{i=1}^{n} \sigma_i(\beta)$$

and the ***norm*** *of β is given by*

$$N_{\mathbb{Q}}^{K}(\beta) = \prod_{i=1}^{n} \sigma_i(\beta).$$

It follows easily from the definition that for $\beta, \gamma \in K$

$$\begin{aligned} T_{\mathbb{Q}}^{K}(\beta + \gamma) &= T_{\mathbb{Q}}^{K}(\beta) + T_{\mathbb{Q}}^{K}(\gamma) \\ N_{\mathbb{Q}}^{K}(\beta \cdot \gamma) &= N_{\mathbb{Q}}^{K}(\beta) N_{\mathbb{Q}}^{K}(\gamma) \end{aligned}$$

If β is an element of $K = \mathbb{Q}(\alpha)$ and the degree of β over $\mathbb{Q}$ is m, then m divides n in $\mathbb{Z}$. This gives us an easy way to calculate the trace and norm.

Let $t(\beta) = \beta_1 + \cdots + \beta_m$ and $n(\beta) = \beta_1 \cdots \beta_m$ where $\{\beta = \beta_1, \ldots, \beta_m\}$ are the m conjugates of β. Then

$$\begin{aligned} T_{\mathbb{Q}}^{K}(\beta) &= \left(\frac{n}{m}\right) t(\beta) \\ N_{\mathbb{Q}}^{K}(\beta) &= [n(\beta)]^{\frac{n}{m}} \end{aligned}$$

If the minimal polynomial for β over $\mathbb{Q}$ is

$$x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

where $a_{m-1}, \ldots, a_0$ are in $\mathbb{Q}$ then $t(\beta) = -a_{m-1}$ and $n(\beta) = (-1)^m a_0$. (To see this, note that the minimal polynomial for β is

$$\prod_{i=1}^{m}(x-\beta_i) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0.)$$

This shows that both $t(\beta)$ and $n(\beta)$ (and hence $T_{\mathbb{Q}}^{K}(\beta)$ and $N_{\mathbb{Q}}^{K}(\beta)$) are in $\mathbb{Q}$. If β is an algebraic integer, then both of these are in $\mathbb{Z}$.

In the specific case of real quadratic number rings, we have two embeddings: $\sigma_1(a+b\sqrt{d}) = a+b\sqrt{d}$ and $\sigma_2(a+b\sqrt{d}) = a-b\sqrt{d}$. The norm and trace of an element β in such a ring (which we abbreviate $N(\beta)$ and $T(\beta)$) are given by:

$$\begin{aligned} N(\beta) &= a^2 - db^2 \\ T(\beta) &= 2a. \end{aligned}$$

Another concept that we will have occasion to use is the ***discriminant*** of a number ring. We have shown above that every quadratic number ring can be described as $\mathbb{Z}$-linear combinations of two elements: 1 and $\sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ or 1 and $\frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$. Such a representation is called an integral basis for our ring. It can be shown that every number ring has an integral basis [4][pp.28 - 30].

For our quadratic number rings R, the discriminant is defined to be

$$\text{disc}(R) = \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) \end{vmatrix}^2$$

where $\{\alpha_1, \alpha_2\}$ is an integral basis for R. This quantity can be shown to be independent of the choice of integral basis for a particular R (by considering a change-of-basis matrix) and simple calculation shows that

$$\operatorname{disc}(R) = \quad \operatorname{disc}(\mathbb{A} \cap \mathbb{Q}(\sqrt{d})) = \quad \begin{cases} 4d & \text{if} \quad d \equiv 2, 3 \pmod 4 \\ d & \text{if} \quad d \equiv 1 \pmod 4 \end{cases}$$

Now that we know something about the rings and their elements, let us examine the ideals. Specifically, we will want to know how to find the prime ideals in our number ring. If all the prime ideals are principal, then every ideal is principal (as every ideal factors uniquely into a product of prime ideals). It turns out that we can find all the prime ideals by looking at the ideal factorization of pR where p is a rational prime. To see this, we first make a definition:

Definition 6.2 *If P is a prime ideal of $\mathbb{Q}$ and Q is a prime ideal of $\mathbb{Q}(\sqrt{d})$, then Q is said to lie over P (or P lies under Q) if $Q \cap \mathbb{Z} = P$ where R is the ring of algebraic integers inside $\mathbb{Q}(\sqrt{d})$.*

This condition is equivalent to several others:

Theorem 6.1 *If P is a prime ideal of $\mathbb{Q}$ and and Q is a prime ideal of $\mathbb{Q}(\sqrt{d})$, then the following conditions are equivalent:*
(1) $Q|PR$
(2) $Q \supset PR$
(3) $Q \supset P$
(4) $Q \cap \mathbb{Z} = P$
(5) $Q \cap \mathbb{Q}(\sqrt{d}) = P$.

Proof:

(1)⇒(2) is trivial since $PR = QS$ (for some ideal S in our number field) implies that every element of PR is a combination of elements of the form $q_i s_j$ where q_i

and s_j are generators of the respective ideals. But then ever element of PR can be written as a combination of elements in Q. Hence, we have the containment indicated.

(2)⇒(1) follows from the fact that for every ideal Q, there is an ideal J such that $QJ = (\alpha)$ (i.e., QJ is principal) [4][pp.57-58]. Letting $C = \frac{1}{\alpha}J(PR)$ we see that $QC = PR$. We need only show that C is an ideal in R. We first note that $C \subset R$ since $B \subset Q$ implies that $JB \subset QJ = (\alpha)$. If c is an element of C then αc is an element of JB. Since JB is an ideal $r\alpha c$ is in JB for any r in R. Hence, rc is in C for all r in R and so, C is an ideal of R.

(2)⇒(3) trivially as $P \subset PR$.

(3)⇒(2) trivially as Q is an ideal of R (and so is closed with respect to multiplication by elements in R).

(3)⇒(4) follows from the observation that since $Q \supset P$ (by supposition) and $\mathbb{Z} \supset P$, then $Q \cap \mathbb{Z}$ must contain P. $Q \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$ and since P is a prime ideal of $\mathbb{Z}$ (and hence maximal) it follows that $Q \cap \mathbb{Z}$ is either P or $\mathbb{Z}$. If it were $\mathbb{Z}$ then Q would contain 1 which would give us that $Q = R$. Since we are assuming that Q is a prime ideal, this is a contradiction.

(4)⇒(3) trivially.

(4)⇔(5) trivially since $Q \subset \mathbb{A}$. **QED**

Theorem 6.2 *Every prime ideal Q of $\mathbb{Q}(\sqrt{d})$ lies over a unique prime ideal of $\mathbb{Z}$. Every prime ideal of $\mathbb{Z}$ lies under at least one prime ideal of R.*

Proof:

The first statement is equivalent to showing that $Q \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. Clearly, $Q \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$. We must show that it is prime. If a, b are rational integers and ab is in $Q \cap \mathbb{Z}$, then one of a or b must be in Q (as Q is a prime ideal). Then one of a or b must be in $Q \cap \mathbb{Z}$. Thus, $Q \cap \mathbb{Z}$ is either $\mathbb{Z}$, (0), or a prime ideal in $\mathbb{Z}$. Since 1 is not in Q, it follows that 1 is not in $Q \cap \mathbb{Z}$ and hence, $Q \cap \mathbb{Z}$ is a proper ideal of $\mathbb{Z}$. All that remains is to show that $Q \cap \mathbb{Z}$ is non-zero. Let α be any non-zero element of Q (which must exist since $Q \neq (0)$). Then since $\overline{\alpha}$ (the algebraic conjugate of α) is in R, it follows that $N(\alpha) = (\alpha)(\overline{\alpha})$ is an element of Q (since it is an ideal). Hence $N(\alpha)$ is both in Q and in $\mathbb{Z}$ (being the norm of an algebraic integer). Thus $Q \cap \mathbb{Z}$ is non-zero.

For the second statement, we note that if pR is not all of R, then this ideal must have some prime divisors. Thus, we need only show pR is not R. This is equivalent to showing that 1 is not an element of pR. If 1 were in pR this would imply that $\frac{1}{p}$ was in R. But this is impossible as $\frac{1}{p}$ is clearly not an algebraic integer. Thus every prime ideal of $\mathbb{Z}$ lies over at least one prime ideal of R. **QED**

The principal ideals pR are not necessarily prime in our number ring R and we seek to determine how they factor. This is a difficult problem in general and depends heavily on the form of the number ring. We summarize the results for quadratic number rings below [4][pp.74-75]:

if $p|d$, then

$$pR \;=\; (p, \sqrt{d})^2 \tag{8}$$

if d is odd, then

$$2R \;=\; \begin{cases} (2, 1+\sqrt{d})^2 & \text{if} \quad d \equiv 3(\text{mod } 4) \\ (2, \frac{1+\sqrt{d}}{2})(2, \frac{1-\sqrt{d}}{2}) & \text{if} \quad d \equiv 1 \pmod 8 \\ \text{prime} & \text{if} \quad d \equiv 5 \pmod 8 \end{cases} \tag{9}$$

if p is odd and p does not divide d, then

$$pR \;=\; \begin{cases} (p, n+\sqrt{d})(p, n-\sqrt{d}) & \text{if} \quad d \equiv n^2 \text{ (mod p)} \\ \text{prime} & \text{if} \quad (\frac{d}{p}) = -1 \end{cases} \tag{10}$$

where we have employed the Legendre symbol in the last case of (10). Furthermore, the ideals in the second case of (9) and the first case of (10) are guaranteed to be distinct. A word of caution though - the ideals above may be listed with two generators but can still be principal (one of the generators may be redundant). When we use the factorizations above, a good deal of our time will be spent deciding whether the factors are principal.

Just as we have a norm defined at the element level, we also have a norm on ideals. The norm of an ideal I, denoted $N(I)$, is the index of I in R (the number ring containing I) or equivalently the cardinality of the quotient ring R/I. If we think of our number ring R as a $\mathbb{Z}$-module of rank n (which is justified since any such ring has an integral basis), then any ideal in our ring must be a submodule of the same rank. Hence, the index above must be finite. This also guarantees that every ideal also has an integral basis.

We now wish to develop the ***Class Group*** of a number ring. We construct the group by creating equivalence classes among the ideals. Given ideals I and J of R, we say that I and J are equivalent (denoted by $I \sim J$) if

$$\alpha I = \beta J$$

for some pair of elements α and β in R. Since any number ring is integrally closed in its field of fractions, this is equivalent to the classes determined by $I = \gamma J$ for some non-zero γ in the *number field* $\mathbb{Q}(\sqrt{d})$. We denote the equivalence classes of $\sim$ by C_i. The set of equivalence classes forms a multiplicative abelian group (denoted $H(\mathrm{R})$) called the *class group* of R, and the identity element of $H(\mathrm{R})$ is the class of all principal ideals - C_0 [4][pp.55-58].

The order of the class group $h(R) = |H(R)|$ is called the class number of R. If $h = 1$, then R is a PID and so is a UFD. If $h > 1$ then there exist non-principal ideals of R (as all principal ideals are equivalent under $\sim$) and so R cannot be a UFD. Thus, h is one measure of how far an integer ring misses being a UFD. If $h \leq 2$ then R is said to be a Half-Factorial Domain (HFD). Though the factorization of an element in an HFD is not necessarily unique, any two factorizations of the same element will have the same length.

Our first concern will be to consider the class number one problem for quadratic number rings where d has a continued fraction expansion of period three. This discussion will rely heavily on the known factorization of pR where p is a prime, the divisibility properties of d, and the results on Pell's Equations we have discussed above.

7 A NECESSARY CONDITION FOR $\mathbb{Q}(\sqrt{d})$ TO HAVE CLASS NUMBER ONE

Now that we have characterized all integers d such that $\sqrt{d}$ has a continued fraction expansion of period length 3, we wish to determine to what extent the quadratic integer rings $\mathrm{R} = \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ (where d is square-free) are unique factorization domains (or equivalently, have class number one). We will see that relatively few of these rings can have class number one.

First we consider the case that $d \equiv 2 \pmod 4$. Since d is an even number, 2 divides d. We consider how 2R factors in $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$. We know that

$$2\mathrm{R} \quad = \quad (2, \sqrt{d})^2$$

but we are not guaranteed in general that the factor on the right is non-principal. Suppose that it were principal. Then there would exist an α in $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ such that for some β and γ in $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ we would have

$$\begin{aligned} 2 &= \alpha\beta \\ &\text{and} \\ \sqrt{d} &= \alpha\gamma. \end{aligned}$$

Taking norms, we find that

$$\begin{aligned} 4 &= N(\alpha)N(\beta) \\ &\text{and} \\ -d &= N(\alpha)N(\gamma). \end{aligned}$$

From the first of these equations we find that the norm of α must be ± 2 or ± 4 (± 1 is ruled out as 2R is not all of $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$).

From the second equation we find that since $-d \equiv 2 \pmod 4$, the norm of α can only be ± 2. Thus, if $\alpha = x + y\sqrt{d}$ then we must have

$$x^2 - dy^2 \;\;=\;\; \pm 2.$$

Notice that x and y must be relatively prime (since if $gcd(x, y) > 1$ then $x^2 - dy^2$ certainly cannot be ± 2). Also note that for any pair of parameters ℓ and n, $2 < \sqrt{d}$ (as the smallest such d is 41).

From our results in Theorem 5.1, we see that this equation can have no integer solutions. Thus, in the case that d has the form given in (4) and ℓ and n have opposite parity (so that d is congruent to 2 (mod 4)) the class number of R is greater than one (equivalently, R is not a UFD).

We have actually shown slightly more! Since the ideal $(2, \sqrt{d})$ is of order two (which follows since $(2, \sqrt{d})^2 = 2R$ which is principal), the class group has an element of order two. Hence, the class number of these rings must be even. So, when d has the form given in (4) and ℓ and n have opposite parity (so that d is congruent to 2 (mod 4)) the class number of R must be even.

We now consider the case that $d \equiv 1 \pmod 4$. From the known factorization of 2R given in (9), it will behoove us to subdivide this class. If $\ell \equiv n \pmod 4$, then $d \equiv 1 \pmod 8$.

In this case, we must have that

$$2\mathrm{R} \;\;=\;\; \left(2, \frac{1+\sqrt{d}}{2}\right)\left(2, \frac{1-\sqrt{d}}{2}\right)$$

and as before, we determine whether the factors on the right are principal.

If $(2, \frac{1+\sqrt{d}}{2})$ were principal, then there would exist an α in $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ such that for some β and γ in $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ we would have

$$\begin{aligned} 2 &= \alpha\beta \\ &\text{and} \\ \frac{1+\sqrt{d}}{2} &= \alpha\gamma. \end{aligned}$$

Taking norms, we find that

$$\begin{aligned} 4 &= N(\alpha)N(\beta) \\ &\text{and} \\ \frac{1}{4}(1-d) &= N(\alpha)N(\gamma). \end{aligned}$$

From the first of these equations, we find that $N(\alpha)$ must be equal to ±2 or ±4. Looking at the left term in the second equation, we find that

$$\frac{1}{4}(1-d) \equiv \begin{cases} 0 \pmod 4 & \text{when } \ell, n \text{ are even} \\ 2 \pmod 4 & \text{when } \ell, n \text{ are odd} \end{cases}$$

which can be verified by direct computation.

Considering first the case that ℓ and n are odd, we must have $N(\alpha) = \pm 2$. Letting

$$\alpha = \frac{a+b\sqrt{d}}{2}$$

where $a \equiv b \pmod{2}$ we see that

$$\begin{array}{rcl} \frac{1}{4}(a^2 - db^2) & = & \pm 2 \\ & \text{so that} & \\ a^2 - db^2 & = & \pm 8. \end{array}$$

When a and b are both odd, then we must have $\gcd(a, b) = 1$ (since otherwise $a^2 - db^2$ would have an odd factor). For $8 < \sqrt{d}$ (which is true for all d except 41) we find that this equation can have no solutions by our results on Pell's Equation.

If a and b are even, then our equation reduces to $m^2 - dn^2 = \pm 2$ where $a = 2m$ and $b = 2n$. Since for every d under consideration $2 < \sqrt{d}$, we find that this equation can have no solutions by our results on Pell's Equation. This accounts for all such numbers except $d = 41$ which happens to have class number 1 (we will discuss the computation of this below).

For the case that ℓ and n are both even, then we have that $N(\alpha) = \pm 2, \pm 4$. Using the same parameters for α we have that

$$\begin{array}{rcl} \frac{1}{4}(a^2 - db^2) & = & \pm 2, \pm 4 \\ & \text{so that} & \\ a^2 - db^2 & = & \pm 8, \pm 16. \end{array}$$

In this case, our smallest value of d is 1313 ($\ell = n = 2$) and so $16 < \sqrt{d}$. As before, if a and b are both odd, then our results on Pell's Equation show that there can be no solution to our equation. If $a = 2m$ and $b = 2n$, then the above equation reduces to $m^2 - dn^2 = \pm 2, \pm 4$. We can immediately throw out ± 2 as we have already shown it has no solutions. If m and n are odd, then we can have no solutions to $m^2 - dn^2 = \pm 4$. What if they are both even? Removing the common factor of 2, we have an equation of the form $f^2 - dg^2 = \pm 1$. This tells us that $f + g\sqrt{d}$ is a unit in our number ring. Tracing our steps back to α, we find that

$$\begin{aligned} \alpha &= \frac{1}{4}(a + b\sqrt{d}) \\ &= \frac{1}{4}(2m + 2n\sqrt{d}) \\ &= \frac{1}{4}(4f + 4g\sqrt{d}) \\ &= f + g\sqrt{d}. \end{aligned}$$

But then α is a unit in our number ring - which cannot be as 2R $\neq$ R. So, the original ideal cannot be principal in this case. Thus, no value of d in this case has class number 1.

So, when $d \equiv 1 \pmod 8$ where the continued fraction expansion of d has period 3, the class number of R $= \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ is greater than one except in the case that $d = 41$.

We have shown:

Theorem 7.1 *If d is of the form given in (4) and $d \equiv 2 \pmod 4$ or $d \equiv 1 \pmod 8$ then the class number of $R = \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ is greater than one (or equivalently, R is not a UFD) unless $d = 41$.*

We turn finally to the case that $d \equiv 5 \pmod 8$ (which occurs when $\ell \equiv n \pmod 2$ but $\ell \equiv (n+2) \pmod 4$). In this case, the ideal generated by 2 is prime and cannot give us information about the class number of d.

We consider first the factorization of 3R. Since 3 does not divide any d, we know that

$$3\text{R} = \begin{cases} (3, 1 + \sqrt{d})(3, 1 - \sqrt{d}) & \text{if } \ d \equiv 1 \pmod 3 \\ \text{prime} & \text{if } \ d \equiv 2 \pmod 3 \end{cases}$$

In the case that $d \equiv 1 \pmod 3$, we seek to determine whether the ideals on the right in the equality above are principal. We note that the smallest such d congruent to 5 (mod 8) and congruent to 1 (mod 3) is 4933 (with $\ell = 4$ and $n = 2$). If the ideals are principal, then there exists some α, β, and γ in R such that

$$\begin{aligned} \alpha\beta &= 3 \\ &\text{and} \\ \alpha\gamma &= 1 + \sqrt{d}. \end{aligned}$$

The first of these conditions gives $N(\alpha) = \pm 3, \pm 9$. Letting

$$\alpha = \frac{a + b\sqrt{d}}{2}$$

where $a \equiv b \pmod 2$ we see that $a^2 - db^2 = \pm 12, \pm 36$. Since $36 < \sqrt{4933}$, we can again appeal to our results on Pell's Equation. If $\gcd(a, b) = 1$ then we can have no solutions to $a^2 - db^2 = \pm 12, \pm 36$. If $\gcd(a, b) \neq 1$ then the gcd can only be 2, 3, or 6. If $\gcd(a, b) = 3$, then our equation for the norm of α reduces to $m^2 - dn^2 = \pm 4$ (where $a = 3m$ and $b = 3n$) which can have no solutions. If $\gcd(a, b) = 2$ then our equation for the norm of α reduces to $m^2 - dn^2 = \pm 3, \pm 9$. Since ± 3 is not equal to $\pm(4\ell n + 1)$ for any choice of ℓ or n, this choice is ruled out. We can also rule out ± 9 since the only choice of ℓ and n leading to a solution of Pell's Equation is $\ell = n = 1$, but this choice gives $d = 41$ which is smaller than 4933. If $\gcd(a, b) = 6$ then our equation for the norm of α reduces to $m^2 - dn^2 = \pm 1$ (where $a = 6m$ and $b = 6n$). In this case, $\alpha = 3u$ where u is a unit in R. If this were the case, then $(3, 1 + \sqrt{d}) = (3, 1 - \sqrt{d}) = 3\text{R}$. This is impossible since it would give

$$3\text{R} = (3\text{R})(3\text{R})$$

which cannot be.

Thus, we have shown that of the values of d congruent to 5 (mod 8), the ones congruent to 1 (mod 3) have class number greater than one. Thus, if any of the remaining d are to have class number one, then they must be congruent to 2 modulo 3. By the Chinese Remainder Theorem, then we must have $d \equiv 5 \pmod{24}$.

When we examine the case that $d \equiv 5 \pmod{24}$, both 2R and 3R are prime; thus, we turn to 5R to find out information about the class number. We are supposing that $d \equiv 5 \pmod{24}$ (which occurs when $\ell \equiv 5n + 2 \pmod{12}$ or $\ell \equiv 5n + 10 \pmod{12}$). Using (8) and (10) we see that 5R factors as

$$5\mathrm{R} \;=\; \begin{cases} (5,\sqrt{d})^2 & \text{if} \quad d \equiv 0 \pmod 5 \\ (5, 1+\sqrt{d})(5, 1-\sqrt{d}) & \text{if} \quad d \equiv 1 \pmod 5 \\ (5, 2+\sqrt{d})(5, 2-\sqrt{d}) & \text{if} \quad d \equiv 4 \pmod 5 \\ \text{prime} & \text{if} \quad d \equiv 2, 3 \pmod 5 \end{cases}$$

Since we are also assuming that $d \equiv 5 \pmod{24}$, we have that $d \equiv 5, 101$, and $29 \pmod{120}$ for the first three cases respectively while $d \equiv 77$ or $53 \pmod{120}$ if 5R is prime. For each of the three cases where 5R splits, if the resulting ideals are to be principal, then there must exist an α in R such that one of the ideals is given by (α). If this is to be the case, then we must have $N(\alpha) = \pm 5, \pm 25$. Letting $\alpha = \frac{a+b\sqrt{d}}{2}$ we have the equation

$$a^2 - db^2 \;=\; \pm 20, \pm 100.$$

We must assume that $d > 10000$ to use our results on Pell's Equation. We will look at the finite number of exceptional cases where this does not hold at the end. We know that for $d > 10000$ the only relatively prime solutions to the equation above are ± 1 and $\pm(4\ell n + 1)$. Looking at the equation, we can have that the $\gcd(a, b) = 1, 2, 5$ or

10. If $\gcd(a, b) = 1$, then there are no solutions to the equation. If the $\gcd(a, b) = 2$ then letting $a = 2m$ and $b = 2n$ we arrive at the equation $m^2 - dn^2 = \pm 5, \pm 25$. This can only occur if $4\ell n + 1 = 5, 25$. This produces a finite list of possible values for ℓ and n, and each of these possible combinations yields a value of d already shown to have class number larger than one. So, we have no solutions in this case. If $\gcd(a, b) = 5$, then letting $a = 5m$ and $b = 5n$ we have $m^2 - dn^2 = \pm 4$ which can have no solutions. If $\gcd(a, b) = 10$, then letting $a = 10m$ and $b = 10n$ we have $m^2 - dn^2 = \pm 1$ which gives that $\alpha = 5u$ where u is a unit in R. But then we would have $(\alpha) = 5\mathrm{R}$ which gives a contradiction by the unique factorization property of ideals. So, except for the finite number of possible exceptions, the ideals that 5R splits into are non-principal. We will examine the class number of these exceptional cases in what follows.

In the case that $d \equiv 5 \pmod{120}$ (so $d \equiv 0 \pmod 5$), the only value of d less than 10000 is $d(7, 1) = 1325$. This case is ruled out in any event since 1325 is not square-free. In the case that $d \equiv 101 \pmod{120}$ (so $d \equiv 1 \pmod 5$), the smallest value of d is $d(31, 1) = 24461 > 10000$ so that there are no exceptions. In the case that $d \equiv 29 \pmod{120}$ (so $d \equiv 4 \pmod{120}$), the only value of d less than 10000 is $d(3, 1) = 269$. It turns out that $h(\mathbb{Q}\sqrt{269}) = 1$ (which we show later).

So, in the case that $d \equiv 5 \pmod{24}$, if $\mathbb{Q}(\sqrt{d})$ has class number one, then $d = 269$ or $d \equiv 53, 77 \pmod{120}$.

We consider 7R before generalizing this process. We now assume $d \equiv 53$ or $77 \pmod{120}$ and ask how 7R factors in these number rings. Since none of these numbers is divisible by 7 we have

$$\mathtt{7R} \;=\; \begin{cases} (7,1+\sqrt{d})(7,1-\sqrt{d}) & \text{if} \quad d \equiv 1 \pmod{7} \\ (7,3+\sqrt{d})(7,3-\sqrt{d}) & \text{if} \quad d \equiv 2 \pmod{7} \\ (7,2+\sqrt{d})(7,2-\sqrt{d}) & \text{if} \quad d \equiv 4 \pmod{7} \\ \text{prime} & \text{if} \quad d \equiv 3, 5 \text{ or } 6 \pmod{7} \end{cases}$$

If any of the ideals in the cases where 7R splits are to be principal, then we must have $N(\alpha) = \pm 7, \pm 49$ for some α in R. Again letting $\alpha = \frac{a+b\sqrt{d}}{2}$ we have the equation. $a^2 - db^2 = \pm 28, \pm 196$. In order to use our results on Pell's Equations, we must assume that $d > 196^2 = 38416$. We make this assumption and revisit the finite number of exceptions at the end.

The only possible values for $\gcd(a, b)$ are 1, 2, 7, or 14. If the $\gcd(a, b) = 1$, then there are no solutions to the equation above. If $\gcd(a, b) = 2$, then letting $a = 2m$ and $b = 2n$ we have $m^2 - dn^2 = \pm 7, \pm 49$. There can be no solutions for ± 7, but there are possible solutions to $m^2 - dn^2 = \pm 49$. In this case, we must have $4\ell n + 1 = 49$. This leads to a finite number of possible values for ℓ and n. When we examine these cases, all have already been ruled out. If $\gcd(a, b) = 7$, then letting $a = 7m$ and $b = 7n$ we have $m^2 - dn^2 = \pm 4$ which has no solutions. If $\gcd(a, b) = 14$, then letting $a = 14m$ and $b = 14n$ we have $m^2 - dn^2 = \pm 1$. This gives that $\alpha = 7u$ where u is a unit in R. But then $(\alpha) = 7\text{R}$ which cannot be by the unique factorization of ideals. So, except for the finite number of possible exceptions, the ideals that 7R splits into above are indeed non-principal.

Looking at the first case where $d \equiv 1 \pmod{7}$ and $d \equiv 53$ or $77 \pmod{120}$ gives a smallest value of $d(12, 2) = 42533 > 38416$ so that there are no possible exceptions in this case. The case that $d \equiv 2 \pmod{7}$ and satisfies one of the congruences modulo 120 yields a smallest value of $d(10, 4) = 427877 > 38416$ so that there are no possible exceptions in this case as well. The case that $d \equiv 4 \pmod{7}$ and meets the congruences modulo 120 yields a smallest value of $d(19,1) = 9293$. It turns out that $h(\mathbb{Q}(\sqrt{9293})) = 3$. All values after this are larger than 38416.

So we have shown that if $h(\mathbb{Q}(\sqrt{d})) = 1$ where $\sqrt{d}$ has a continued fraction expansion of period three, then $d = 41, 269$ or $d \equiv 173, 293, 437, 677, 773$, or $797 \pmod{840}$.

We now give a generalization of the procedure that we have been using.

Theorem 7.2 *Let d be a square-free integer of the form given in (4) and let p be an odd prime such that $4p^2 < \sqrt{d}$. If d is a square modulo p and neither p nor p^2 equals $4\ell n + 1$, then $h(\mathbb{Q}(\sqrt{d})) > 1$.*

In other words, for a given value d, if we can find a prime meeting the criteria of the theorem, then the number ring $\mathrm{R} = \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ is not a unique factorization domain.

Proof:

The proof goes through much as the previous arguments did. We consider the factorization of $p\mathrm{R}$:

$$p\mathtt{R} \;=\; \begin{cases} (p, \sqrt{d})^2 & \text{if} \quad p \text{ divides } d \\ (p, n+\sqrt{d})(p, n-\sqrt{d}) & \text{if} \quad d \equiv n^2 \text{ (mod p)} \\ \text{prime} & \text{if} \quad (\frac{d}{p}) = -1 \end{cases}$$

Since we are assuming that d is a square modulo p, we know that $p\mathrm{R}$ is not prime. We need only verify that none of the ideals listed in the first two cases are principal. As before, we suppose that an ideal in question is equal to (α). Looking at norms, we must have that $N(\alpha) = \pm p, \pm p^2$. Letting $\alpha = \frac{a+b\sqrt{d}}{2}$ where $a \equiv b \pmod 2$ we arrive at the equation

$$a^2 - db^2 \;=\; \pm 4p, \pm 4p^2.$$

From the equation above, the gcd of a and b can be $1, 2, p$, or $2p$. Since $4p^2 < \sqrt{d}$ our results on Pell's Equation apply. We look at each of the possible divisors in turn.

If $\gcd(a, b) = 1$, then there can be no solutions to $a^2 - db^2 = \pm 4p, \pm 4p^2$.

If $\gcd(a, b) = 2$, then letting $a = 2m$ and $b = 2n$ we have $m^2 - dn^2 = \pm p, \pm p^2$. Since we are assuming for our particular value of d that $4\ell n + 1 \neq p, p^2$, this equation can have no solutions.

If $\gcd(a, b) = p$, then letting $a = pm$ and $b = pn$ we have $m^2 - dn^2 = \pm 4$ which has no solutions.

If $\gcd(a, b) = 2p$, then letting $a = 2pm$ and $b = 2pn$ we have that $m^2 - dn^2 = \pm 1$. This gives that $\alpha = \frac{a+b\sqrt{d}}{2} = p(m + n\sqrt{d}) = pu$ where u is a unit in R. If this is the case, then we must have $(\alpha) = p\mathrm{R}$ which cannot be by the unique factorization of ideals.

In all cases, we arrive at a contradiction; so the ideals listed cannot be principal. Thus, $h(\mathbb{Q}(\sqrt{d})) > 1$ since we have shown the existence of a non-principal ideal. **QED**

This theorem encapsulates the process we have been using thus far to search for possible number rings having class number one. We illustrate its use by considering the prime 11.

Since $4(11)^2 = 484$, we must have $\sqrt{d} > 484$ or $d > 234256$ for our results to be valid. We must consider the possibility that either 11 or 121 equals $4\ell n+1$. We know that this equation cannot hold for 11, but it could hold for 121. If $4\ell n + 1 = 121$ then we must have $\ell n = 30$. We need to check all possible combinations of positive integers ℓ and n that meet this criterion. There are only eight possible combinations. In addition, since $30 = (2)(3)(5)$, then one of ℓ or n must be even while the other odd. This tells us that these values of d are congruent to 2 (mod 4). We have already shown that these number rings have class number larger than one.

If we run a search for the values of $d \leq 234256$ that have not already been excluded by previous arguments, we come up with the following list of possible exceptional values:

$$\begin{gathered} \mathrm{d}(1,3) = 1613 \\ \mathrm{d}(15,1) = 5837 \\ \mathrm{d}(39,1) = 38573 \\ \mathrm{d}(55,1) = 76397 \\ \mathrm{d}(6,4) = 155333 \\ \mathrm{d}(24,2) = 168293. \end{gathered}$$

Setting these cases aside for the time being (along with the others we have come across), we have that in order for $h(\mathbb{Q}(\sqrt{d})) = 1$ that $d \equiv 2, 6, 7, 8$, or 10 (mod 11). Combining this with our previous results (which said that in order to have class number one $d \equiv 173, 293, 437, 677, 773$, or 797 (mod 840)) we come up with a list of 30 possible congruence classes modulo 9240.

Running through the possible combinations of ℓ and n (mod 9240) and counting the number of these that yield one of the values in this list show that they account for roughly 2.05% of all the values of d. Thus, we have eliminated virtually 98% of all the possible values of d that could have class number one. This shows that Theorem 7.2 severely limits the possible number of rings with class number one and gives credence to our earlier assertion that relatively few of these rings are unique factorization domains. We will show in a later section that the number is actually finite.

8 THE MINKOWSKI BOUND

Thus far, we have only concentrated on trying to determine which of the number rings we have been studying have class number one. Theorem 7.2 gives us the impression that relatively few of them can have class number one.

We would like to find a means of calculating the class number of our rings directly. In fact, there is a formula that calculates it exactly. This formula, though it solves our problem in theory, is very unwieldy, and for rings with even moderate values of d, it can be difficult to evaluate. We will come to this formula in due course. In addition, we will explore other means of calculating class numbers.

The first problem to tackle is showing that the class number is finite. In the process, we will come up with a bound that will give us an indication of how many ideals we need to consider in order to completely describe the class group.

The construction we give is a special case of the more general ***Minkowski Bound*** which proves that the class number of any number ring is finite.

Since we are working over real quadratic number fields, there are exactly two embeddings for each field. If α is in $\mathbb{Q}(\sqrt{d})$, then

$$\alpha \quad = \quad a + b\sqrt{d}.$$

We let σ_1 be the identity embedding and σ_2 be the embedding sending each α to its algebraic conjugate. That is:

$$\sigma_1(\alpha) = \quad \sigma_1(a + b\sqrt{d}) = \quad a + b\sqrt{d}$$

and

$$\sigma_2(\alpha) = \quad \sigma_2(a + b\sqrt{d}) = \quad a - b\sqrt{d}.$$

Note that since any quadratic extension of the rationals is normal, these embeddings are in fact automorphisms. We will not need the full weight of this consequence, only that both of these embeddings have range in $\mathbb{R}$.

We now create a mapping from our number field into $\mathbb{R}^2$ by sending α to the point $(\sigma_1(\alpha), \sigma_2(\alpha)) = (\alpha, \overline{\alpha})$ (where we have used the bar to represent the algebraic conjugate). This mapping is an additive homomorphism since

$$\begin{aligned}(\sigma_1(\alpha+\beta), \sigma_2(\alpha+\beta)) &= (\alpha+\beta, \overline{\alpha+\beta}) \\ &= (\alpha, \overline{\alpha}) + (\beta, \overline{\beta}) \\ &= (\sigma_1(\alpha), \sigma_2(\alpha)) + (\sigma_1(\beta), \sigma_2(\beta)).\end{aligned}$$

It also has trivial kernel, since the only element of our field mapping to $(0, 0)$ is 0. Thus, this mapping is an embedding of our real quadratic number field into $\mathbb{R}^2$ with respect to the additive structure of our field.

Now that we have established a mapping, we want to see how our number ring R $= \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ maps under this operation. If we take an integral basis for our number ring (say α_1 and α_2), then every element of our ring can be written as $m\alpha_1 + n\alpha_2$ where m and n are integers. Mapping this general element into the plane, we get the point $m(\alpha_1, \overline{\alpha_1}) + n(\alpha_2, \overline{\alpha_2})$. Thus, the image of our ring is the integer span of the two vectors $(\alpha_1, \overline{\alpha_1})$ and $(\alpha_2, \overline{\alpha_2})$ in the plane. The image of the integral basis consists of two linearly independent vectors in the plane. To see this, we note that

$$\begin{vmatrix} \alpha_1 & \overline{\alpha_1} \\ \alpha_2 & \overline{\alpha_2} \end{vmatrix} = \pm\sqrt{|\text{disc}(\mathtt{R})|}$$

which is non-zero. Thus, the image of our ring under the mapping in question is a two-dimensional subspace spanned by integer combinations of two vectors in the plane. Such a subspace is commonly referred to as a two-dimensional lattice.

Let v_1 be the image of α_1 under our mapping. Define v_2 similarly. Consider the set

$$F \quad = \quad \{a_1 v_1 + a_2 v_2 \mid 0 \leq a_i < 1\}.$$

Graphically, this set is a parallelogram in the plane - often called the *fundamental parallelotope* of the lattice. From basic geometric considerations, we can see that the area of this parallelogram(which we call vol(Λ_R)) is $\sqrt{|\text{disc(R)}|}$. In Figure 1, we give a graphic representation of a typical lattice with its fundamental parallelotope.

What about the image of a proper ideal I of R? We can find an integral basis for any such I - say I = (β_1, β_2). Since we can represent β_i as a linear combination of our integral basis for R, it follows that the lattice in the plane determined by the ideal I has a fundamental parallelotope with volume

$$\text{vol}(\Lambda_I) \quad = \quad \left|\frac{\text{R}}{\text{I}}\right| \sqrt{|\text{disc(R)}|}$$

where |R/I| is the index of I in R.

We now define a norm on the plane by setting $N(x, y) = xy$. Note that for points mapped from our field, this agrees with the field norm. To see this recall that α from our field is mapped to the point $(\alpha, \overline{\alpha})$. We will show that every lattice in the plane must contain a point whose norm is less than or equal to $\frac{1}{2}\sqrt{|\text{disc(R)}|}$.

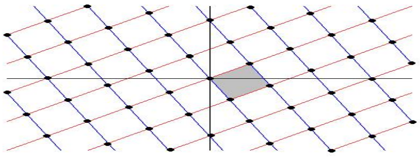

Figure 1: Typical Lattice in R^2

In order to prove this result, we need a theorem due to Minkowski:

Theorem 8.1 *Let $\wedge$ be an n-dimensional lattice in $\mathbb{R}^n$ and let E be a convex, measurable, centrally symmetric subset of $\mathbb{R}^n$ such that*

$$\mathrm{vol}(E) \quad > \quad 2^n \mathrm{vol}(\wedge).$$

Then E contains some non-zero point of $\wedge$. If E is compact, then the inequality can be weakened to $\geq$.

By convex, we mean that if two points are in E, so is the line segment joining them. By measurable, we refer to Lebesgue measure. The details of Lebesgue measure will not concern us much. Suffice it to say that typical sets are measurable and that their measure coincides reasonably with the idea of volume in n-dimensions. We have used $\mathrm{vol}(E)$ to refer to the measure of the set E and $\mathrm{vol}(\wedge)$ to refer to the measure of the fundamental parallelotope of $\wedge$. By centrally symmetric, we imply that if x is in E, then so is $-x$. For a proof, see [4][pp.137-138].

Corollary 8.1 *Suppose there is a compact, convex, centrally symmetric set A of $\mathbb{R}^n$ with $\mathrm{vol}(A) > 0$ and the property that $|N(a)| \leq 1$ for all a in A. Then every n-dimensional lattice $\wedge$ contains a nonzero point x with*

$$|N(x)| \quad \leq \quad \frac{2^n}{\mathrm{vol}(A)} \mathrm{vol}(\wedge).$$

Proof:

Consider the set E= tA $= \{ta \mid a \in A\}$ where

$$t^n \quad = \quad \frac{2^n}{\mathrm{vol}(A)} \mathrm{vol}(\wedge).$$

The set E meets the requirements of the theorem above since

$$\mathrm{vol}(E) = \quad t^n \mathrm{vol}(A) = \quad \frac{2^n \mathrm{vol}(\wedge)}{\mathrm{vol}(A)}.$$

So, E contains a non-zero point x of the lattice $\wedge$. Since $x = ta$ for some a in A, $N(x) = t^n N(a) \leq t^n$. **QED**

To come up with a bound, we need to consider an appropriate set in the plane. We look at the set determined by

$$|x| + |y| \quad \leq \quad 2.$$

This set is compact (being closed and bounded)and centrally symmetric (since if the point (x, y) is in the set, so is $(-x, -y)$). It is also easy to see that this set is convex; graphically, it is a diamond in the plane.

To see that every point in this set has norm less than 1 we first note that the arithmetic mean of the coefficients in this set at most one. Thus, the geometric mean $\sqrt{|xy|}$ is at most the arithmetic mean which is at most one. Since

$$0 \leq \sqrt{|N(x,y)|} \leq 1$$

we can conclude that the norm of every element in this set is less than or equal to one.

The volume of this set (or area since we are in the plane) is 8. Hence, the corollary to Minkowski's Theorem promises us that every lattice in the plane contains a non-zero point whose norm is less than or equal to $\frac{1}{2}\mathrm{vol}(\Lambda_R)$.

Translating this back in terms of ideals we have that

Corollary 8.2 *Every non-zero ideal I of a quadratic number ring R contains a non-*

zero element α with

$$|N(\alpha)| \;\; \leq \;\; \frac{1}{2}\sqrt{|\mathrm{disc}(R)|}\left|\frac{R}{I}\right|.$$

We are now in a position to give bounds for the class number. Our primary result is

Theorem 8.2 *Every ideal class of R contains an ideal J with*

$$\|J\| \;\; \leq \;\; \frac{1}{2}\sqrt{|\mathrm{disc}(R)|}.$$

Proof:

We are using the short-hand $\|J\|$ to stand for the index of J in R. Given a particular class C, we consider its inverse class C^{-1}. Let I be an ideal in the inverse class and obtain the element α in I as in the corollary above. Since the principal ideal (α) is contained in I, there exists an ideal J in C such that $IJ = (\alpha)$. Since $|N(\alpha)| = \|(\alpha)\| = \|I\|\|J\|$ [4][pp.65-69] and

$$|N(\alpha)| \;\; \leq \;\; \frac{1}{2}\sqrt{|\mathrm{disc}(R)|} \;\; \|I\|.$$

we have that

$$\|J\| \;\; \leq \;\; \frac{1}{2}\sqrt{|\mathrm{disc}(R)|}. \;\; \textbf{QED}$$

This is a powerful result. First, it proves that the class number is indeed finite for any quadratic number ring. To see this, recall that every ideal can be factored uniquely in terms of prime ideals. So, if $J = P_1^m P_2^n \dots P_r^q$ then $\|J\| = \|P_1\|^m \|P_2\|^n \dots \|P_r\|^q$. In addition every prime ideal P lies over a unique pR for some rational prime p, and for quadratic number rings $\|P\|$ is either p or p^2. Hence, only a finite number of ideals can satisfy the criterion of Theorem 8.2 and so the class group must itself be finite.

Since the index of a prime ideal P is either p or p^2, it also follows that we need only consider prime ideals lying over primes satisfying

$$p \;\leq\; \frac{1}{2}\sqrt{|\mathrm{disc}(R)|}.$$

So, in order to calculate the class number (and determine the structure of the class group) we need only consider the prime ideals obtained by factoring pR for primes less than the bound given above, form all possible ideals with index less than the same bound whose factorizations are comprised of these ideals, and then determine from this finite set of ideals the ideal classes. This last step is typically the most cumbersome since it involves multiplying the ideals and trying to find which are in the same class.

We note that since the discriminant is either d or $4d$ for quadratic number rings, we need only consider primes up to $\sqrt{d}$. To demonstrate this process, we consider the first of our exceptional cases, $d = 41$.

Example 8.1

For $d = 41$, the Minkowski Bound implies that every ideal class must have an ideal with index less than or equal to $\frac{1}{2}\sqrt{41}$ (here we have used the the fact that the discriminant of R is d when $d \equiv 1 \pmod 4$). This in turn implies that we need only find the prime ideals lying over 2 and 3. Since $41 \equiv 2 \pmod 3$ and since 2 is not a square modulo 3, it follows that 3R is prime in this number ring. Thus, we need only consider the primes lying over 2.

$$2\mathrm{R} \;=\; \left(2, \frac{1+\sqrt{41}}{2}\right)\left(2, \frac{1-\sqrt{41}}{2}\right)$$

A little work will show that both of these ideals are principal. To be specific,

$$\begin{aligned}\left(2, \frac{1+\sqrt{41}}{2}\right) &= \left(\frac{7-\sqrt{41}}{2}\right)\\ &\text{and}\\ \left(2, \frac{1-\sqrt{41}}{2}\right) &= \left(\frac{7+\sqrt{41}}{2}\right).\end{aligned}$$

Since every prime ideal we need to consider is principal, it follows that there can be at most one class in the class group. Thus, $\mathrm{R} = \mathbb{A} \cap \mathbb{Q}(\sqrt{41})$ has class number one and so is a principal ideal domain. □

For a less trivial example, we consider the case $d = 130$.

Example 8.2

Since $\mathrm{R} = \mathbb{A} \cap \mathbb{Q}(\sqrt{130})$ has discriminant 520, we must check all primes less than $\frac{1}{2}\sqrt{520}$. This leads us to consider the prime ideals lying over $2, 3, 5, 7$ and 11.

$$\begin{aligned}2R &= (2, \sqrt{130})^2\\ 3R &= (3, 1+\sqrt{130})(3, 1-\sqrt{130})\\ 5R &= (5, \sqrt{130})^2\\ 7R &= (7, 2+\sqrt{130})(7, 2-\sqrt{130})\\ 11R &= (11, 3+\sqrt{130})(11, 3-\sqrt{130})\end{aligned}$$

Elementary norm arguments show that none of these ideals are principal. We first investigate which of these lie in the same class before considering possible combinations of these primes.

We denote the class of an ideal I by $\overline{I}$. We note that the classes $\overline{(2, \sqrt{130})}$ and $\overline{(5, \sqrt{130})}$ are of order two. Thus, they are their own inverses. We can also show that they are in different classes. To see this, we suppose that they are in the same class. If this were the case, the ideal $(2, \sqrt{130})(5, \sqrt{130})$ would be principal (since the class has order two). This is the ideal generated by $(10, \sqrt{130})$ If this ideal were principal, then $N(\alpha) = \|(10, \sqrt{130})\| = 10$. From our results on Pell's Equation, we know that no element in this ring can have norm 10. Thus, these two classes are distinct.

So far, we have found four distinct classes: C_0 (the class of principal ideals), $\overline{(2, \sqrt{130})}, \overline{(5, \sqrt{130})}$, and $\overline{(10, \sqrt{130})}$. We note that this last ideal class also has order two - since $(10, \sqrt{130})(10, \sqrt{130}) = 10R$. Thus, the class number is at least four.

If we consider the ideal $(12 + \sqrt{130})$, we find that since $N(12 + \sqrt{130}) = 14 = (2)(7)$, the prime factors of this ideal must lie over 2 and 7. Thus $\overline{(2, \sqrt{130})}$ must be the inverse class of either $\overline{(7, 2 + \sqrt{130})}$ or $\overline{(7, 2 - \sqrt{130})}$. Suppose it were the inverse class of the second ideal. Then $\overline{(2, \sqrt{130})} = \overline{(7, 2 - \sqrt{130})}$. But since this class is of order two, it follows that $\overline{(7, 2 + \sqrt{130})} = \overline{(7, 2 - \sqrt{130})} = \overline{(2, \sqrt{130})}$. Since the same result would occur in the other case, we conclude that the ideals lying over 7 are in $\overline{(2, \sqrt{130})}$.

Considering the ideal $(35 + 3\sqrt{130})$, we find that since $N(35 + 3\sqrt{130}) = 55 = (5)(11)$, the prime factors of this ideal must lie over 5 and 11. Mirroring the last argument exactly, we find that $\overline{(7, 2 + \sqrt{130})} = \overline{(7, 2 - \sqrt{130})} = \overline{(5, \sqrt{130})}$.

Multiplication of ideals shows that $(3, 1 + \sqrt{130})(10, \sqrt{130}) = (10 + \sqrt{130})$. Thus, $\overline{(3, 1 + \sqrt{130})} = \overline{(3, 1 - \sqrt{130})} = \overline{(10, \sqrt{130})}$.

So, the all the prime ideals we need to consider have been placed into one of three ideal classes (each of order two). In the process of finding these classes, we have already considered an ideal lying over 2 and 5. The only other way of generating an ideal with index less than or equal to 11 is by finding an ideal lying over 2 and 3. Looking at $(3, 1+\sqrt{130})(2, \sqrt{130})$, we first note that this ideal is non-principal (by basic norm arguments). Using basic reduction techniques to find the generators of this ideal, we find that it reduces to $(6, 2-\sqrt{130})$. Since $(6, 2-\sqrt{130})(5, \sqrt{130}) = (10+\sqrt{130})$, we see that $\overline{(6, 2-\sqrt{130})} = \overline{(5, \sqrt{130})}$.

So, after much effort, we find that the class number of $\mathrm{R} = \mathbb{A} \cap \mathbb{Q}(\sqrt{130})$ is four and the class group is isomorphic to the Klein 4-Group. $\square$

9 FUNDAMENTAL UNITS

As the last section plainly shows, computing class numbers can be laborious at best. We would like to find some process whereby the class number can be calculated and the structure of the class group specified. The first of these problems can be handled by the class number formula. Before we can develop this concept, we must say something about the group of units inside our quadratic number rings.

The Unit Theorem for the multiplicative group of units U in a number ring R states that U is the direct product of a finite cyclic group (composed of the roots of unity in R) and a free abelian group. If our number field is of extension $n = r + 2s$ over $\mathbb{Q}$ (where r is the number of real embeddings and $2s$ the number of complex embeddings), then the free abelian group has rank $r + s - 1$ [4][pp.141-146].

For real quadratic number rings, the only roots of unity contained in R are ± 1. Since $s = 0$ (there are no complex embeddings), it follows that the free abelian group has rank 1. Thus, the multiplicative group of units is of the form:

$$U \quad = \quad \{\pm u^k \mid k \in \mathbb{Z}\}.$$

The generator u for the free abelian group of rank 1 is called the ***fundamental unit*** for the number ring and is uniquely determined if we further specify that $u > 1$.

Knowing the continued fraction expansion for d can greatly simplify the process of finding these fundamental units. We recall that if u is a unit in our number ring, then its norm is necessarily one. Thus, one way of finding the units is to find all the elements with norm one. Our results on Pell's Equation do exactly this! We will be assuming throughout that $\sqrt{d} > 4$.

If $d \equiv 2 \pmod 4$, then we are looking for solutions to

$$x^2 - dy^2 \quad = \quad \pm 1.$$

Except for the case $x = \pm 1$ and $y = 0$, the other solutions to this equation must be the convergents of the continued fraction expression for $\sqrt{d}$.

If $d \equiv 1 \pmod 4$, then the fundamental unit must be of the form

$$u \quad = \quad \frac{x + y\sqrt{d}}{2}$$

where $x \equiv y \pmod 2$. Taking norms, we find that

$$x^2 - dy^2 \quad = \quad \pm 4.$$

If x and y are relatively prime, then ± 4 cannot be a represented by any integers x and y (from our knowledge of the solutions to Pell's Equation when $\sqrt{d}$ has period three). Thus, we find that x and y must be congruent to zero modulo 2. If $x = 2w$ and $y = 2z$, we must have

$$w^2 - dz^2 \quad = \quad \pm 1.$$

Once again, the fundamental unit must be given by the convergents of $\sqrt{d}$.

So, the units of any real quadratic number ring with period three are particular convergents of the continued fraction expansion of $\sqrt{d}$. To find the fundamental unit, we need only find the first convergent pair $(A_n\ ,\ B_n)$ not $(A_0, B_0) = (1, 0)$ that gives $A_n^2 - dB_n^2 = \pm 1$.

In the case where d has continued fraction expansion of period three, the fundamental unit will be $A_2 + B_2\sqrt{d}$ which has norm -1. Using the recursive definitions for the convergents, we find that the fundamental unit for $\mathrm{R} = \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ is

$$(16n^4\ell + 4n^3 + 8n^2\ell + 3n + \ell) + (4n^2 + 1)\sqrt{d}.$$

10 THE CLASS NUMBER FORMULA

Now that we have the notion of fundamental unit, we can develop the class number formula for quadratic number rings. In fact, a class number formula for arbitrary number rings can be given! This would seem to solve our attempts to determine the number of such rings with class number one. Unfortunately, the class number formula (even for quadratic number rings) becomes incredibly difficult to work with as the size of the discriminant increases.

Before we can state the class number formula, we need to make a few definitions and state some fundamental results. Throughout, we will be working with a number ring of discriminant D. The first definition is that of a ***character of a finite abelian group***.

Definition 10.1 *A complex-valued function f defined on an abelian group G is called a* ***character*** *of G if for all a and b in G*

$$f(ab) \quad = \quad f(a)f(b)$$

and if $f(c) \neq 0$ for some c in G.

Since $f(a) = f(ea) = f(e)f(a)$ where e is the identity of G, we must have $f(e) = 1$. Since G is a finite group (say with order n), then $a^n = e$ and so $f(a)^n = 1$. Hence, every character defined on G must map G into the nth roots of unity. There are many other useful results about characters; we only list those pertinent to a discussion of the class number formula. The interested reader is referred to [1][pp. 133-143].

Theorem 10.1 *A finite abelian group G of order n has exactly n distinct characters.*

Before proving this theorem, we need a lemma.

Lemma 10.1 *Let G' be a subgroup of a finite abelian group G, where $G' \neq G$. For any element a in G with indicator $h \neq 1$ in G' (i.e., the smallest positive integer h such that a^h is in G') the set of products*

$$G'' \quad = \quad \{xa^k \mid x \in G' \text{ and } k = 0, 1, \ldots, h-1\}$$

is a subgroup of G containing G'. Moreover, the order of G'' is h times the order of G'.

Proof:

G'' is non-empty as it contains the identity element of G. Suppose $b = xa^k$ and $c = ya^j$ are elements of G'', we must show bc^{-1} is also in G''. Since $c^{-1} = (ya^j)^{-1} = y^{-1}a^{-j}$ we have that $bc^{-1} = (xy^{-1})a^{k-j}$. Using the division algorithm, we can write $k - j = qh + r$ where $0 \leq r < h$. Then $bc^{-1} = (xy^{-1})a^{qh}a^r$, and since a has indicator h in G', we must have $a^{qh} = z \in G'$. Thus $bc^{-1} = (xy^{-1}z)a^r \in G''$.

For the order of G'', we first assume that for some $x, y \in G'$ and some k, j for which $0 \leq j \leq k < h$ that

$$xa^k \quad = \quad ya^j.$$

If this were the case, we would have

$$a^{k-j} \quad = \quad x^{-1}y$$

But since $0 \leq k - j < h$, we would have that the indicator of a in G' is less than h. Thus, xa^k is unique for each x in G' and each k between 0 and $h - 1$. Hence, the order of G' is h times the order of G'. **QED**

Proof of Theorem 10.1:

We let $\langle G', a\rangle$ denote the subgroup G'' from the lemma above. We construct a chain of subgroups inside G and prove the theorem by induction. Let $G_1 = \{e\}$ be the trivial subgroup of G. If $G_1 \neq$ G, pick an element a_1 of G that is not the identity of G and define $G_2 = \langle G_1, a_1\rangle$. If $G_2 \neq$ G, then pick an element a_2 not in G_2 and define $G_3 = \langle G_2, a_2\rangle$. If we continue this process, we get a chain of nested subgroups

$$G_1 \subset G_2 \subset \cdots \subset G_{t+1} = G$$

where the final equality is justified by the fact that we have an increasing sequence of nested subgroups inside a finite group. We note that the only character that can be defined on G_1 (the trivial group) is the one assigning e to 1.

We assume that the theorem holds for G_r (having order m). We will show that we can extend each character on G_r to G_{r+1} in exactly h distinct ways (where h is the indicator of a_r in G_r). Thus, the number of characters for G_{r+1} will be mh which is the order of G_r.

Since a typical element of G_{r+1} is xa_r^k where x is in G_r and $0 \leq k < h$, then if we can extend a character f of G_r to a character $\tilde{f}$ on G_{r+1} we must have

$$\begin{aligned} \tilde{f}(xa_r^k) &= \tilde{f}(x)\tilde{f}(a_r^k) \\ &= f(x)\tilde{f}(a_r)^k. \end{aligned}$$

So, once we determine $\tilde{f}(a_r)$, then the extension of f has been completely specified.

Since the indicator of a_r in G_r is h, we know that $a_r^h = c$ which is an element of G_r. Thus, the only possible values for $\tilde{f}(a_r)$ are the hth roots of f(c). Since each of these roots is distinct, we have h distinct extensions of f to G_{r+1}. Thus, the number of characters of G_{r+1} is at least mh.

To show equality, we need only observe that if we have any character on G_{r+1}, its restriction to G_r must be a character on G_r. Thus, we have produced all the possible characters on G_{r+1} by the extension process. Hence, the number of character on G_{r+1} is the order of G_{r+1}. **QED**

Theorem 10.2 *Under point-wise multiplication, the characters of G form a multiplicative group $\widehat{G}$ of order n. The identity element of $\widehat{G}$ is the character f_1 defined by*

$$f_1(g) \quad = \quad 1 \textit{ for all } g \textit{ in } G$$

and $\widehat{G}$ is isomorphic to G.

Proof:

Verifying that the set of characters is a group is merely an exercise in confirming the group axioms (which we shall omit). To show that the character group is isomorphic to G, we first decompose G into its invariant factors

$$G = \mathbb{Z}_{h_0} \bigotimes \mathbb{Z}_{h_1} \bigotimes \cdots \bigotimes \mathbb{Z}_{h_s}.$$

Then each element a of G can be written as

$$a \quad = \quad a_0^{t_0} a_1^{t_1} \cdots a_s^{t_s} \tag{11}$$

for $0 \leq t_i < h_i - 1$. If b is another element of G where

$$b \quad = \quad a_0^{u_0} a_1^{u_1} \cdots a_s^{u_s} \tag{12}$$

(with similar limits on the u_i) then the mapping

$$\phi : G \to \widehat{G} \tag{13}$$

given by $\phi(a) = f_a$ where f_a is given by

$$f_a(b) = \exp\ 2\pi i \left(\frac{t_0 u_0}{h_0} + \frac{t_1 u_1}{h_1} + \cdots + \frac{t_s u_s}{h_s} \right).$$

This mapping can be shown to be an isomorphism between G and $\widehat{G}$ (and interestingly enough, a non-canonical one) [3][pp.25-27]. **QED**

Throughout the following, we will be assuming that our number field is an abelian extension of $\mathbb{Q}$ (i.e. it is a normal extension with abelian Galois group). In particular, we note that quadratic number rings are abelian extensions (since their Galois group is isomorphic to $\mathbb{Z}_2$). With the notion of characters, we can define the Dirichlet L function (which is a generalization of the Riemann Zeta function).

Definition 10.2 *The Dirichlet L function $L(s, \chi)$ is a two parameter function defined for s in the complex plane and for some character χ defined on $\mathbb{Z}$ by*

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

This function converges to an analytic function on $\Re(s) > 0$ except when χ is the trivial character [4][pp.193-196]. Now that we have the necessary tools in place, we can give a formula for the class number of quadratic number fields. Since such fields are of degree two over the rationals, their Galois groups have only two members. To get a character on the integers, we first extend our number field to a cyclotomic field containing it (which is guaranteed to exist for any abelian extension of $\mathbb{Q}$ by the Kronecker-Weber Theorem). Then we choose the characters corresponding to the elements of the Galois group of this field (which is isomorphic to $\mathbb{Z}_m^*$ for the mth cyclotomic field) which fix our real quadratic number field. These characters (which are now characters on the integers) will be the ones we use. The two corresponding characters on our number fields are the trivial character (which assigns 1 to everything relatively prime to d) and the character determined by:

$$\begin{aligned}\chi(p) &= (\frac{d}{p}) \quad \text{for odd primes not dividing D} \\ \chi(2) &= \begin{cases} 1 & \text{if } d \equiv 1 \pmod 8 \\ \text{-1} & \text{if } d \equiv 5 \pmod 8 \end{cases} \\ \chi(n) &= 0 \quad \text{if } \ (n, D) \neq 1\end{aligned}$$

and extended multiplicatively for all integers relatively prime to D. For odd n, this character equals the Jacobi symbol $(\frac{d}{n})$.

Theorem 10.3 *For a real quadratic number ring $R = \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ with discriminant D, the class number $h(D)$ is given by*

$$h(D) = \frac{\sqrt{D}}{2\log{(u)}} L(1, \chi)$$

where u is the fundamental unit of the number ring and χ is the character described above.

For a proof of this important theorem, see Appendix II. We will have occasion to use this form in later arguments, but for the purpose of calculation, it is rather cumbersome. It so happens that for real quadratic number rings with discriminant $D \geq 3$ that

$$|L(1, \chi)| = \frac{2}{\sqrt{D}} \left| \sum_{k \in \mathbb{Z}_D^*}^{k < D/2} \chi(k) \log \sin \left(\frac{k\pi}{D} \right) \right| \text{(see [4][}p\text{.201]).}$$

Putting this result together with our previous one (and the fact that the class number is positive) gives

Theorem 10.4 *For a quadratic number ring $R = \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ with discriminant D, the class number $h(D)$ is given by*

$$h(D) \quad = \quad \frac{1}{\log{(u)}} \left| \sum_{k \in \mathbb{Z}_D^*}^{k<D/2} \chi(k) \log \sin\left(\frac{k\pi}{D}\right) \right|$$

where u is the fundamental unit of the number ring and χ is the character described above.

This formula is much easier to work with computationally. We will demonstrate its use by calculating the class number for the field $\mathbb{Q}(\sqrt{5})$ with discriminant 5.

Example 10.1

The number ring $\mathbb{A} \cap \mathbb{Q}(\sqrt{5})$ has class number given by

$$h(5) \quad = \quad \frac{1}{\log\left(\frac{1+\sqrt{5}}{2}\right)} \left| \sum_{k \in \mathbb{Z}_5^*}^{k<5/2} \chi(k) \log \sin\left(\frac{k\pi}{5}\right) \right|.$$

We note that the fundamental unit for this ring was computed directly from the equation $t^2 - 5u^2 = \pm 4$ and taking the smallest values of t and u such that $u > 1$. This sum reduces to

$$\begin{aligned} h(5) \quad &= \quad \frac{\left|\chi(1)\log\sin\left(\frac{\pi}{5}\right) + \chi(2)\log\sin(\frac{2\pi}{5})\right|}{\log{(\frac{1+\sqrt{5}}{2})}} \\ &= \quad \frac{\left|\log\sin(\frac{\pi}{5}) - \log\sin(\frac{2\pi}{5})\right|}{\log{(\frac{1+\sqrt{5}}{2})}} \\ &= \quad \frac{\left|\log\left(\frac{\sin(\frac{\pi}{5})}{\sin(\frac{2\pi}{5})}\right)\right|}{\log{(\frac{1+\sqrt{5}}{2})}} \\ &= \quad \frac{\log(2\cos(\frac{\pi}{5}))}{\log{(\frac{1+\sqrt{5}}{2})}}. \end{aligned}$$

After some clever trigonometric manipulation, we find that

$$\cos\left(\frac{\pi}{5}\right) \quad = \quad \frac{1+\sqrt{5}}{4}.$$

Thus $h(5) = 1$. □

In the absence of having exact values for the trigonometric functions, reasonable approximations can be employed to evaluate the class number (as it is an integer). However, for large discriminants, it is easily seen that this formula is still unwieldy. We will examine algorithms for computing the class number in later sections (these methods also have the advantage of determining the structure of the class group).

11 APPROXIMATIONS FOR CLASS NUMBERS

We still have not answered the question which we raised at the beginning of the paper. Is the number of quadratic number rings $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ where $\sqrt{d}$ has a continued fraction expansion of period three with class number one finite? The class number formula 10.3 gives us a means of answering this if we can find a reasonable approximation of $L(1, \chi)$. Such an approximation exists.

According to a result by Tatuzawa [10], we have (with at most one exception)

$$L(1, \chi) \quad > \quad 0.655\eta D^{-\eta}$$

$$\text{for}$$

$$0 < \eta < \frac{1}{2} \quad \text{and} \quad D \geq \max\{e^{\frac{1}{\eta}}, e^{22}\}.$$

Since we have already shown that our rings cannot have class number one unless d is congruent to 1 modulo 4, it suffices to consider this case alone. In particular, $d = D$. Utilizing the approximation above, we find that

$$\begin{aligned} h(D) &= \frac{\sqrt{D}}{2\log{(u)}}L(1, \chi) \\ &> \frac{\sqrt{D}}{2\log{(u)}}0.655\eta D^{-\eta} \\ &= \frac{0.655\eta D^{-\eta+0.5}}{2\log u} \end{aligned}$$

with the appropriate restrictions on D and η.

In order to use this result, we must first find a suitable approximation of the fundamental unit in terms of D. We have already given the form of this unit earlier as

$$u \quad = \quad (16n^4\ell + 4n^3 + 8n^2\ell + 3n + \ell) + (4n^2 + 1)\sqrt{d}.$$

We desire an upper bound on this unit in terms of D. To determine this upper bound, we note that this unit can be written as

$$\begin{aligned} u &= \lambda\left(\frac{(\sqrt{D}+a_0)^2}{4\ell n+1}\right) \\ &\text{where} \\ \lambda &= \frac{\ell(4n^2-1)+n+\sqrt{D}}{4\ell n+1} \end{aligned}$$

and a_0 is the first coefficient in the continued fraction expansion for $\sqrt{D}$.

Since $a_0 = \ell(4n^2+1)+n$ and $a_0 < \sqrt{D}$ we have that

$$\begin{aligned} \lambda &= \frac{\ell(4n^2-1)+n+\sqrt{D}}{4\ell n+1} \\ &< \frac{a_0+\sqrt{D}}{4\ell n+1} \\ &< \frac{2\sqrt{D}}{4\ell n+1} \\ &< \sqrt{D}. \end{aligned}$$

In similar fashion,

$$\begin{aligned} \frac{(\sqrt{D}+a_0)^2}{4\ell n+1} &< \frac{4D}{4\ell n+1} \\ &< D \end{aligned}$$

which gives us

$$u < D^{3/2}.$$

These estimates for u in terms of D seem rather severe. The upper bound on D given in Tatuzawa's approximation of $L(1,\chi)$ will justify making these estimates.

Returning to our approximation for the class number,

$$\begin{aligned} h(D) &> \frac{0.655\eta D^{-\eta+0.5}}{2\log u} \\ &> \frac{0.655\eta D^{-\eta+0.5}}{3\log D}. \end{aligned}$$

If we can find η between 0 and 0.5 such that when $D > \max\{e^{22}, e^{1/\eta}\}$

$$\frac{0.655\eta D^{-\eta+0.5}}{3\log D} > 1$$

then we will have found a bound for D after which none of our quadratic number rings can have class number one. Choosing $\eta = 0.21$, since $e^{1/0.21} < e^{22}$ and since

$$\frac{0.655(0.21)D^{-0.21+0.5}}{3\log D} > 1$$

when $D > e^{22}$ we have that the number of our rings with class number one must be finite. In addition, we have an upper bound with which to work! For $D \geq 3,600,000,000$, $h(D) > 1$.

Thus, we have proven

Theorem 11.1 *The number of quadratic number rings $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ where $\sqrt{d}$ has a continued fraction expansion of period three having class number one is finite. Any such ring with class number one must have discriminant less than* $3,600,000,000$ *(with at most one exception).*

We can actually prove something stronger. The smallest value of η we can use and retain e^{22} as an upper bound on D is obviously $\frac{1}{22}$. Using this value as a lower bound for η proves that with at most one exception, all the number rings under consideration with class number less than or equal to 9 must have discriminants less than $3,600,000,000$.

Theorem 11.2 *The number of quadratic number rings $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ where $\sqrt{d}$ has a continued fraction expansion of period three having class number less than or equal to 9 is finite. Any such ring must have discriminant less than 3,600,000,000 (with at most one exception).*

Running a search using Maple shows that there are exactly 21198 values of d less than 3,600,000,000. We can reduce this number slightly by retaining only the ones which are squarefree (which can easily be tested on Maple with the Möbius function). Of the remaining 19549 values of d, we find that only 3 have class number one. Thus, the maximum number of unique factorization domains we could have is four. Tables 3 and 4 in Appendix A list all values of d having class number less than 10 (with at most one exception). We will consider the means by which these tables were compiled in the following section.

12 ALGORITHMS FOR COMPUTING CLASS NUMBER

We have shown that the number of unique factorization domains among our number rings is finite. In addition, we have an upper bound on the discriminant for such rings. The next logical step in our treatment is to attempt a search for these rings. Thus, we need an efficient algorithm for computing the class number.

In theory, we already have a formula suitable for such an algorithm - the class number formula (as given in 10.4). However, a close inspection of this formula shows that it would be terribly inefficient for discriminants of the size we will need to consider. Since we already have a closed form for the fundamental unit (which can be a problem in general), all the major computation time will be spent evaluating the sum in 10.4. In evaluating this sum, we will first need to determine whether each k less than $\lfloor \frac{D}{2} \rfloor$ is relatively prime to D. The value of $\log \sin$ can be approximated rather quickly using appropriate series representations. The major difficulty in evaluating the individual summands is computing the Jacobi symbol $\chi(k)$ (which requires its own separate algorithm).

Running this algorithm on Maple (which has the Jacobi symbol preprogrammed) is effective only for discriminants on the order of one thousand or so. There are known improvements for prime discriminants using Bernoulli numbers. This is only a slight improvement since evaluating the appropriate Bernoulli number becomes increasingly difficult as the discriminant increases; the $2n$th Bernoulli number depends on each of the $n-1$ Bernoulli numbers preceding it (recall that the mth Bernoulli number is 0 if m is odd).

An alternative method for computing class numbers exists and has been programmed into the computer package PARI. We examine the fundamental aspects of this algorithm without delving too deeply into the specifics. One rather amazing aspect of this algorithm is that computing the structure of the class group (which gives us the class number) is *more* efficient than computing the class number alone [2][p.235].

To avoid making case distinctions, we let D be the discriminant of our number ring (which is equal to d if d is congruent to 1 modulo 4 and $4d$ otherwise). Then our number ring can be represented succinctly as $\mathbb{Z}[\omega]$ where

$$\omega = \frac{D + \sqrt{D}}{2}.$$

Instead of working with the ideals directly, we use binary quadratic forms.

Definition 12.1 *A binary quadratic form f is a function $f(x, y) = ax^2 + bxy + cy^2$ where a, b, and c are integers. We denote this form more briefly as (a, b, c). We say that a form (a, b, c) is primitive if $\gcd(a, b, c) = 1$. The discriminant D of a quadratic form (a, b, c) is given by $D = b^2 - 4ac$.*

We let a matrix act on a form f by:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \bullet f(x, y) = f(\alpha x + \beta y, \gamma x + \delta y)$$

We also define an equivalence relation on forms as follows:

Definition 12.2 *If f and g are two quadratic forms, then we say f and g are equivalent if there exists a matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ in $SL_2(\mathbb{Z})$ such that*

$$g(x, y) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \bullet f(x, y) = f(\alpha x + \beta y, \gamma x + \delta y)$$

Recall that $\mathrm{SL}_2(\mathbb{Z})$ is the set of two-by-two matrices with entries in $\mathbb{Z}$ having determinant equal to one.

This equivalence relation preserves the discriminant of our form (which can be checked by expanding the resulting form and checking the discriminant remembering that $\alpha\delta - \beta\gamma = 1$). Since we will be interested in forms with discriminants that are discriminants of number rings (which implies that D is squarefree or divisible by four and no other perfect square), it follows that all of the forms we will be interested in are primitive. If such a form were not primitive, then $\gcd(a, b, c)$ would be greater than or equal to two. If the gcd is larger than 2, we have a contradiction since then D would be divisible by a square larger than four. If $g = 2$ then d must be congruent to 2 or 3 (mod 4). In this case we would have $d = (b')^2 - 4(a')(c')$ (where the primed coefficients are the ones remaining from $D = b^2 - 4ac$ after dividing through by four). This is clearly impossible. Hence $\gcd(a, b, c) = 1$.

Since the matrices A and $-A$ in $\mathrm{SL}_2(\mathbb{Z})$ determine the same action on a form f, the natural group to act on quadratic forms is $\mathrm{PSL}_2(\mathbb{Z})$ where the matrices A and $-A$ are identified. We will treat members of $\mathrm{PSL}_2(\mathbb{Z})$ as matrices instead of equivalence classes of matrices to avoid unnecessary notational difficulties. Let us denote by $\mathcal{F}(D)$ the set of equivalence classes of primitive forms with discriminant D modulo the action of $\mathrm{PSL}_2(\mathbb{Z})$.

Using these equivalence classes of forms we can establish a correspondence between ideal classes in our number rings and classes of forms. Since the forms are easier to work with computationally, we will have a nice set of objects from which to construct our algorithm.

It will be convenient in what follows to consider the *narrow class number* of a number ring.

Definition 12.3 *Two ideals I and J are said to be equivalent in the narrow sense (denoted $\sim_n$) if there exists an element α in the number field with positive norm such that $I = \alpha\ J$.*

Recall that two ideals I and J are said to be equivalent in the general sense if there exists an element α in our number field such that I $= \alpha$J (this is a trivial modification of our original definition). So, every narrow ideal class is a subset of an ideal class. In addition, it is clear that each ideal splits into exactly two narrow ideal classes. Thus, if we denote by $H^+(D)$ and $h^+(D)$ the narrow class group and narrow class number of our number ring respectively, then we must have

$$h^+(D) \;\; = \;\; 2h(D).$$

We mentioned in the earlier section on number rings that every ideal I in a number ring can be given by an integral basis. In fact, we can choose the integral basis as follows:

$$I \;\; = \;\; a\mathbb{Z} + (b + c\omega)\mathbb{Z}$$

where a is the smallest positive integer in I, $0 \leq b < a$ and $0 < c$ divides a and b [2][p.220]. In this case, $N(I) = ac$.

We are now ready to give the correspondence between the narrow ideal classes and the set $\mathcal{F}(D)$ of primitive forms with discriminant D modulo $\mathrm{PSL}_2(\mathbb{Z})$.

Theorem 12.1 *Let D be the discriminant of a real quadratic number ring, and let the maps*

$$\psi_{FI} : \mathcal{F}(D) \to H^+(D)$$

$$\text{and}$$

$$\psi_{IF} : H^+(D) \to \mathcal{F}(D)$$

be given by

$$\begin{aligned}\psi_{FI}(a,b,c) &= \left(a\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z}\right) q \\ &\textit{and} \\ \psi_{IF}(\omega_1\mathbb{Z}+\omega_2\mathbb{Z}) &= \frac{N(x\omega_1 - y\omega_2)}{N(\omega_1\mathbb{Z}+\omega_2\mathbb{Z})}\end{aligned}$$

respectively, where q is any non-zero element of the number field $\mathbb{Q}(\sqrt{D})$ such that $sign(N(q)) = sign(a)$, and $\{\omega_1, \omega_2\}$ is any integral basis for the ideal I such that

$$\frac{\omega_2\overline{\omega_1} - \omega_1\overline{\omega_2}}{\sqrt{D}} > 0$$

(where $\overline{\omega_i}$ represents the algebraic conjugate of ω_i). Then ψ_{FI} and ψ_{IF} are inverse bijections.

Proof of Theorem 12.1:

We prove the theorem in three parts. We first show ψ_{FI} is well-defined on $\mathcal{F}(D)$ (i.e. that equivalent forms map to the same ideal class). We then do the same for ψ_{IF}. Once we have established that these maps are well-defined, we show that they are inverses of each other. This automatically guarantees the bijection.

ψ_{FI} **is well-defined:**

We suppose that $(a,b,c) \sim (d,e,f)$ and that $D = b^2 - 4ac = e^2 - 4df$. We can also suppose without loss of generality that a is positive. By definition, there is some matrix in $\mathrm{PSL}_2(\mathbb{Z})$ such that

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \bullet (a,b,c) = (d,e,f)$$

where $\alpha\delta - \beta\gamma = 1$. Remembering the definition of the action of $\mathrm{PSL}_2(\mathbb{Z})$ on a quadratic form gives the following relations:

$$\begin{aligned} d &= a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ e &= 2a\alpha\beta + b\alpha\delta + b\beta\gamma + 2c\gamma\delta \\ f &= a\beta^2 + b\beta\delta + c\delta^2. \end{aligned}$$

These prove a bit cumbersome, so we will develop more convenient notation as we progress. We are interested in how the ideal class

$$\left(a\mathbb{Z} + \tfrac{-b+\sqrt{D}}{2}\mathbb{Z}\right) q$$

behaves when we apply an element of $\mathrm{PSL}_2(\mathbb{Z})$. Since we are only interested in the ideal up to a multiple of $\mathbb{Q}(\sqrt{D})$, we choose to factor out a and absorb it into q:

$$(\mathbb{Z} + \tau\mathbb{Z})\, q$$

where

$$\tau = \frac{-b + \sqrt{D}}{2a}$$

The resulting set (ignoring the q) is no longer an ideal but a fractional ideal (i.e. a set that becomes an ideal when it is multiplied by an appropriate element of the field). The details of fractional ideals will not concern us too much.

After some lengthy algebra, we find that d can be written as

$$d = aN(-\gamma\tau + \alpha)$$

which in turn gives that τ becomes

$$\tau \quad \longrightarrow \quad \frac{\delta\tau - \beta}{-\gamma\tau + \alpha}$$

(which we call τ') under the action of $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Thus, the ideal class becomes

$$(\mathbb{Z} + \tau\mathbb{Z})\, q \quad \longrightarrow \quad (\mathbb{Z} + \tau'\mathbb{Z})\, q'$$

under this action. If we can show for an appropriate element q of $\mathbb{Q}(\sqrt{D})$ that

$$(\mathbb{Z} + \tau'\mathbb{Z}) \quad = \quad (\mathbb{Z} + \tau\mathbb{Z})\, q$$

then these two ideal classes are equivalent and ψ_{FI} will be well-defined. We will show that

$$(\mathbb{Z} + \tau'\mathbb{Z}) \quad = \quad \frac{(\mathbb{Z} + \tau\mathbb{Z})}{-\gamma\tau + \alpha}.$$

We begin by first observing that the relation $\alpha\delta - \beta\gamma = 1$ ensures that α and β are relatively prime. In fact, every element of $\mathrm{PSL}_2(\mathbb{Z})$ can be determined by specifying α, β, and an arbitrary integer n (since $\gamma = \gamma_0 + n\alpha$ and $\delta = \delta_0 + n\beta$ where γ_0 and δ_0 are determined by the Euclidean Algorithm).

Let $x = \ell + m\tau'$ be an arbitrary element of $\mathbb{Z} + \tau'\mathbb{Z}$. Then by simple rearrangement we see that

$$\begin{aligned} x &= \ell + m\tau' \\ &= \frac{\ell(-\gamma\tau + \alpha) + m(\delta\tau - \beta)}{-\gamma\tau + \alpha} \\ &= \frac{(\ell\alpha - m\beta) + (m\delta - \ell\gamma)\tau}{-\gamma\tau + \alpha}. \end{aligned}$$

Hence, x is also in $\frac{(\mathbb{Z}+\tau\mathbb{Z})}{-\gamma\tau+\alpha}$. Thus, we have

$$(\mathbb{Z}+\tau'\mathbb{Z}) \;\subseteq\; \frac{(\mathbb{Z}+\tau\mathbb{Z})}{-\gamma\tau+\alpha}.$$

To show the reverse containment, it suffices to show that a general element x of $\mathbb{Z}+\tau\mathbb{Z}$ is in $(-\gamma\tau+\alpha)(\mathbb{Z}+\tau'\mathbb{Z})$. Let $x = \ell\,' + m'\tau$ where $\ell\,'$ and m' are integers. We find integers ℓ and m such that $x = (-\gamma\tau+\alpha)(\ell+m\tau')$. Since

$$\begin{aligned} x &= (-\gamma\tau+\alpha)(\ell+m\tau') \\ &= -\ell\gamma\tau+\alpha\ell+m(\delta\tau-\beta) \\ &= (\alpha\ell-\beta m)+(\delta m-\gamma\ell)\tau \end{aligned}$$

we must have

$$\ell\,' \;=\; \alpha\ell-\beta m$$

and

$$m' \;=\; \delta m-\gamma\ell.$$

These equations give that

$$\ell \;=\; \frac{\ell\,'(1+\beta\gamma)+\alpha\beta m'}{\alpha}$$

and

$$m \;=\; \alpha m'+\gamma\ell\,'$$

where ℓ is guaranteed to be an integer since $\alpha\delta-\beta\gamma=1$ implies that $1+\beta\gamma\equiv 0$

(mod α). Having shown the reverse containment, we have immediately that

$$(\mathbb{Z} + \tau'\mathbb{Z}) = \frac{(\mathbb{Z} + \tau\mathbb{Z})}{-\gamma\tau + \alpha}.$$

Note also that

$$\begin{aligned} N\left(\frac{1}{-\gamma\tau + \alpha}\right) &= \frac{1}{N\left(-\gamma\tau + \alpha\right)} \\ &= \frac{a}{d} > 0 \end{aligned}$$

as required.

ψ_{IF} **is well-defined:**

We can think of an ideal class in $H^+(D)$ as given by an ideal I (with integral basis $\{\omega_1, \omega_2\}$ as described in the theorem) times an element q of the field $\mathbb{Q}(\sqrt{D})$ with positive norm (which is arbitrary except for the requirement that αI be an ideal of the number ring). We note that the integral basis described immediately before the theorem meets the condition given by the theorem.

Then

$$\psi_{IF}(qI) = \frac{N(x\omega_1' - y\omega_2')}{N(qI)}$$

where $\{\omega_1', \omega_2'\}$ is the corresponding integral basis for qI. It is clear that $\omega_i' = q\omega_i$ and using the fact that the norm is multiplicative (for both elements and ideals) we have that

$$\begin{aligned} \psi_{IF}(qI) &= \frac{N(xq\omega_1 - yq\omega_2)}{N(qI)} \\ &= \frac{N(q)N(x\omega_1 - y\omega_2)}{N((q))N(I)} \\ &= \frac{N(x\omega_1 - y\omega_2)}{N(I)} \end{aligned}$$

$$= \quad \psi_{IF}(I).$$

Technically, $N((q)) = |N(q)|$ (where the norm on the left is on a principal ideal while the one on the right is on an element). Since we restricted ourselves to elements of positive norm, we get equality, and the cancellation is justified. Thus, ψ_{IF} is well-defined on the ideal classes of $H^+(D)$.

ψ_{IF} and ψ_{FI} are inverse bijections:

By using an appropriate element of $\mathrm{PSL}_2(\mathbb{Z})$, we can assume that a form (a, b, c) has $a > 0$.

$$\begin{aligned}
\psi_{IF}(\psi_{FI}(a,b,c)) &= \psi_{IF}\left(a\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z}\right) \\
&= \frac{N(xa - y(\frac{-b+\sqrt{D}}{2}))}{N\left(a\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z}\right)} \\
&= \frac{\left(xa + \frac{by}{2}\right)^2 - D\frac{y^2}{4}}{N\left(a\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z}\right)} \\
&= \frac{a^2x^2 + abxy + \frac{b^2-D}{4}y^2}{N\left(a\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z}\right)} \\
&= \frac{a^2x^2 + abxy + acy^2}{N\left(a\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z}\right)} \\
&= \frac{a^2x^2 + abxy + acy^2}{a} \\
&= (a, b, c)
\end{aligned}$$

We have used the fact that $N\left(a\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z}\right) = a$ which can be shown by several different means. Perhaps the easiest is by comparing fundamental parallelotopes under the mapping sending the ring into $\mathbb{R}^2$.

$$\psi_{FI}(\psi_{IF}(qI)) \;=\; \psi_{FI}\left(q[a'\mathbb{Z} + (b' + \ell\omega)\mathbb{Z}]\right)$$

where we have used an integral basis for I as described above. Since ℓ must divide a' and b' we can factor it out and absorb it into the element q. By renaming constants appropriately, our representative for the ideal class becomes

$$a\mathbb{Z} + \tfrac{-b+\sqrt{D}}{2}\mathbb{Z}.$$

Thus,

$$\begin{aligned}
\psi_{FI}(\psi_{IF}(qI)) &= \psi_{FI}\left(q\frac{N(ax - \frac{-b+\sqrt{D}}{2}y)}{a}\right) \\
&= \psi_{FI}(q(ax^2 + bxy + cy^2)) \\
&= \psi_{FI}(q(a,b,c)) \\
&= qI
\end{aligned}$$

Hence, ψ_{IF} and ψ_{FI} are inverse bijections. **QED**

We can represent an ideal class by a class of quadratic forms. The key advantage to this approach is that we can easily identify a special type of form in each class (which we call *reduced*). Unfortunately, for real quadratic number rings (as opposed to imaginary) the reduced forms are not unique in each class but are cyclic. Thus, we must identify the reduced forms for a given discriminant D and then determine the cycle structures among these to determine the narrow class number.

Definition 12.4 *Let $f = (a,b,c)$ be a quadratic form with positive discriminant D.*

We say that f is reduced if we have

$$\left|\sqrt{D} - 2|a|\right| < b < \sqrt{D}.$$

We have as an easy proposition the following results [2][pp.257-258]:

Proposition 12.1 *Let (a, b, c) be a reduced form with positive discriminant D. Then:*

(1) $|a|$, b, and $|c|$ are less than $\sqrt{D}$ and a and c are of opposite signs

(2) $|a| + |c| < \sqrt{D}$

(3) (a, b, c) is reduced if and only if $\left|\sqrt{D} - 2|c|\right| < b < \sqrt{D}$.

We now give a means of reducing an arbitrary form with discriminant D.

Definition 12.5 *Let $D > 0$ be a discriminant. If $a \neq 0$ and b are integers, we define $r(b, a)$ to be the unique integer r such that $r \equiv b \pmod{2a}$ and $-|a| < r \leq |a|$ if $|a| > \sqrt{D}$, $\sqrt{D} - 2|a| < r < \sqrt{D}$ if $|a| < \sqrt{D}$.*

We define the reduction operator ρ on a form (a, b, c) with discriminant $D > 0$ by

$$\rho(a, b, c) = \left(c, r(-b, c), \frac{r(-b, c)^2 - D}{4c}\right).$$

To find a reduced form equivalent to a given one, we just repeatedly apply the reduction operator until we arrive at a reduced form. To show that this is effective we look at the action of ρ on a reduced form and then on forms in general.

If (a, b, c) is reduced, then $|c| < \sqrt{D}$. Thus the action of ρ on (a, b, c) gives the form (c, r, c') where $\sqrt{D} - 2|c| < r < \sqrt{D}$ and c' is number given in the definition. This is clearly reduced, but not the same form. Hence, there are multiple reduced forms in each class.

If we restrict ourselves to the reduced forms in a given class, then ρ acts as a permutation with inverse

$$\rho^{-1}(a,b,c) \;=\; \left(\frac{r(-b,a)^2-D}{4a}, r(-b,a), a\right)$$

which can be verified by direct computation. Since we can have only a finite number of reduced forms in a given class we must have that every form (a,b,c) is equivalent to a cycle of reduced forms. Hence, (a,b,c) is equivalent to a reduced form given by $\rho^n(a,b,c)$ for n sufficiently large.

So, to determine the narrow class number of a given real quadratic number ring $R = \mathbb{A} \cap \mathbb{Q}(\sqrt{D})$, we need only list all the possible reduced quadratic forms with discriminant D and apply the reduction operator to determine the cycle structures among them. The number of orbits under the action of ρ will be the narrow class number (which is twice the class number). We illustrate with an example.

Example 12.1

We consider $R = \mathbb{A} \cap \mathbb{Q}(\sqrt{60})$. Our first task is to find all of the possible reduced forms. Since $b^2 - 4ac = 60$ this is equivalent to finding all pairs (a,b) that meet the following conditions:

(1) $|a| < \sqrt{60}$

(2) $|\sqrt{60} - 2|a|| < b < \sqrt{60}$

(3) $b \equiv 0 \pmod 2$

(4) $4a|b^2 - 60$.

The first two conditions are a direct consequence of the definition of reduced form. Condition (3) comes from the observation that $b^2 \equiv 60 \pmod 4$. Condition (4) ensures that c in the quadratic form is integral.

The possible values of a with the potential values of b are:

a	±1	±2	±3	±4	±5	±6	±7
b	6	4,6	2,4,6	2,4,6	2,4,6	4,6	6

Checking condition (4) gives us the following list of reduced forms for $D = 60$:

$$(1, 6, -6); (-1, 6, 6); (2, 6, -3); (-2, 6, 3);$$
$$(3, 6, -2); (-3, 6, 2); (6, 6, -1); (-6, 6, 1).$$

The only thing left to check are the orbits under ρ. We can easily verify that:

$$\begin{aligned} \rho(1, 6, -6) &= (-6, 6, 1) & \rho(-6, 6, 1) &= (1, 6, -6) \\ \rho(-1, 6, 6) &= (6, 6, -1) & \rho(6, 6, -1) &= (-1, 6, 6) \\ \rho(2, 6, -3) &= (-3, 6, 2) & \rho(-3, 6, 2) &= (2, 6, -3) \\ \rho(-2, 6, 3) &= (3, 6, -2) & \rho(3, 6, -2) &= (-2, 6, 3). \end{aligned}$$

Hence, the narrow class number is 4. Recalling that the class number is always one-half the narrow class number we can see that the class number of $R = \mathbb{A} \cap \mathbb{Q}(\sqrt{60})$ must be 2. □

This method can easily be made into an effective algorithm for computing the class number. In its current form, it is still rather inefficient. Many improvements have been made to this algorithm that bear mentioning.

In our example, we were only concerned with the class number, not the structure of the class group. To deal with class structure, it is possible to define a composition of forms that mimics the multiplication of ideals [2][pp. 241-242]. Using such a composition, we can examine the group structure of the reduced forms which will give us the structure of the narrow class group. We pass to the structure of the class group by identifying the forms (a, b, c) and $(-a, b, -c)$.

One of the more original ideas used to improve the efficiency of the computation is the introduction of a distance function defined on equivalent forms [2][pp. 274-278]. This distance function allows for a more rapid reduction of the forms. Even though we can count the reduced forms directly, the composition of two reduced forms is not guaranteed to be reduced. Thus, the introduction of a distance between forms greatly increases the efficiency of determining the class structure.

This algorithm has been programmed into a number theoretic software package called PARI by Henri Cohen, et al. Tables 3 though 6 in Appendix A were obtained by using PARI to determine the class number of real quadratic rings $R = \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ (where $\sqrt{d}$ has period three) with discriminant less than 3,600,000,000. From our results in the previous section we know that for discriminants larger than 3,600,000,000, the class number must be at least ten (with at most one omission).

If we were just interested in the rings with class number one, we could have reduced the number of discriminants we need to check (which is about 19,550) to around 400 entries using our results on the divisibility of d obtained in Section 7. We opted to determine all 19,550 (which took approximately 6 hours). Interestingly enough, every possible class number up to 150 appears in this list except for five (43, 51, 79, 101, and 145). Of course, to verify that these are actually omitted, we would need to check all discriminants up to 2.125 trillion.

13 CONCLUSION

We have shown conclusively that the number of UFDs for real quadratic number rings $\mathbb{Q}(\sqrt{d})$ where d has continued fraction expansion of period three is at most four. Using analytic results coupled with computational algorithms, we have given a list of these rings along with all rings having class number less than ten (with at most one exception).

There are several interesting unanswered questions that we have raised along the way. The first is whether any prime congruent to three modulo four divides the values of d given by the parametrization we found in Section 3. We did find a sufficient condition guaranteeing that a prime congruent to three modulo four does not divide any given d. This condition is not necessary however.

The second deals with bounds on the class number. The Tatuzawa result gives a rough lower bound for the class number. It seems to be a rather poor one however since the three values of d leading to UFDs have discriminant much less than 3,600,000,000. Are better approximations possible?

Looking at the 19,550 rings for which we know the class number, it would appear that when $d \equiv 1 \pmod 4$, $h(d)$ has a lower bound of about $0.007\sqrt{D}$ ($d = D$ in this case). For $d \equiv 2 \pmod 4$, we see that $h(d)$ has a lower bound of about $0.011\sqrt{D}$ ($D = 4d$ in this case).

Third, are any class numbers omitted for our number rings $\mathbb{Q}(\sqrt{d})$? We have stated that all the class numbers up to 150 except for five appear in our current list. Tatuzawa's lower bound on the L-function gives us an upper bound on the discriminant size we have to check, but the upper bound we obtain is large enough to cause serious computational problems.

Finally, the question of whether the number of arbitrary real quadratic number rings with class number one is infinite is still open (as it has been since the time of

Gauss). Our results seem to indicate that while looking at a particular case is useful in many respects, it is unlikely that there are an infinite number of UFDs for a given period length.

A related question that might be of interest is whether there is a UFD for each period length. This combined with the fact that there is always a d such that $\sqrt{d}$ has a given period length would prove that there are an infinite number of real quadratic number rings with class number one. The paper by Mollin [9] listed in the references provides results along this line (for period lengths up to 24).

APPENDIX A - TABLES

Table 2: d for Small Values of ℓ and n

ℓ	n	d	$[a_0; \overline{a_1, a_1, 2a_0}]$
1	1	41	$[6; \overline{2, 2, 12}]$
2	1	130	$[11; \overline{2, 2, 22}]$
3	1	269	$[16; \overline{2, 2, 32}]$
1	2	370	$[19; \overline{4, 4, 38}]$
2	2	1313	$[36; \overline{4, 4, 72}]$
3	2	2834	$[53; \overline{4, 4, 106}]$
1	3	1613	$[40; \overline{6, 6, 80}]$
2	3	5954	$[77; \overline{6, 6, 154}]$
3	3	13033	$[114; \overline{6, 6, 228}]$

Table 3: Discriminants with Class Number less than 10[1]

ℓ	n	d	D	**h(D)**	**H(D)**
1	1	41	41	1	$\{0\}$
3	1	269	269	1	$\{0\}$
1	3	1613	1613	1	$\{0\}$
4	1	458	1832	2	$\mathbb{Z}_2$
15	1	5837	5837	2	$\mathbb{Z}_2$
4	2	4933	4933	3	$\mathbb{Z}_3$
19	1	9293	9293	3	$\mathbb{Z}_3$
2	1	130	520	4	$\mathbb{Z}_2 \otimes \mathbb{Z}_2$
1	2	370	1480	4	$\mathbb{Z}_2 \otimes \mathbb{Z}_2$
6	1	986	3944	4	$\mathbb{Z}_2 \otimes \mathbb{Z}_2$
2	2	1313	1313	4	$\mathbb{Z}_4$
10	1	2642	10568	4	$\mathbb{Z}_4$
3	2	2834	11336	4	$\mathbb{Z}_2 \otimes \mathbb{Z}_2$
8	2	19109	19109	4	$\mathbb{Z}_4$
5	3	35405	35405	4	$\mathbb{Z}_2 \otimes \mathbb{Z}_2$
39	1	38573	38573	4	$\mathbb{Z}_4$
1	7	41645	41645	4	$\mathbb{Z}_4$
9	1	2153	2153	5	$\mathbb{Z}_5$

[1] This table omits at most one discriminant.

Table 4: Discriminants with Class Number less than 10 (continued)

ℓ	n	d	D	**h(D)**	**H(D)**
11	1	3181	3181	5	$\mathbb{Z}_5$
5	1	697	697	6	$\mathbb{Z}_6$
1	4	4778	19112	6	$\mathbb{Z}_6$
31	1	24461	24461	6	$\mathbb{Z}_6$
55	1	76397	76397	6	$\mathbb{Z}_6$
12	2	42533	42533	7	$\mathbb{Z}_7$
43	1	46829	46829	7	$\mathbb{Z}_7$
6	4	155333	155333	7	$\mathbb{Z}_7$
24	2	168293	168293	7	$\mathbb{Z}_7$
12	1	3770	15080	8	$\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$
5	2	7610	30440	8	$\mathbb{Z}_4 \otimes \mathbb{Z}_2$
18	1	8354	33416	8	$\mathbb{Z}_8$
22	1	12410	49640	8	$\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$
67	1	113165	113165	8	$\mathbb{Z}_4 \otimes \mathbb{Z}_2$
87	1	190445	190445	8	$\mathbb{Z}_4 \otimes \mathbb{Z}_2$
4	6	343493	343493	8	$\mathbb{Z}_8$
13	1	4409	4409	9	$\mathbb{Z}_9$
2	4	17989	17989	9	$\mathbb{Z}_9$

Table 5: Class Numbers for small d

ℓ	n	d	D	**h(D)**	**H(D)**
1	1	41	41	1	$\{0\}$
2	1	130	520	4	$\mathbb{Z}_2 \otimes \mathbb{Z}_2$
3	1	269	269	1	$\{0\}$
1	2	370	1480	4	$\mathbb{Z}_2 \otimes \mathbb{Z}_2$
4	1	458	1832	2	$\mathbb{Z}_2$
5	1	697	697	6	$\mathbb{Z}_6$
6	1	986	3944	4	$\mathbb{Z}_2 \otimes \mathbb{Z}_2$
2	2	1313	1313	4	$\mathbb{Z}_4$
1	3	1613	1613	1	$\{0\}$
8	1	1714	6856	12	$\mathbb{Z}_{12}$
9	1	2153	2153	5	$\mathbb{Z}_5$
10	1	2642	10568	4	$\mathbb{Z}_4$
3	2	2834	11336	4	$\mathbb{Z}_2 \otimes \mathbb{Z}_2$
11	1	3181	3181	5	$\mathbb{Z}_5$
12	1	3770	15080	8	$\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$
13	1	4409	4409	9	$\mathbb{Z}_9$
1	4	4778	19112	6	$\mathbb{Z}_6$
4	2	4933	4933	3	$\mathbb{Z}_3$
14	1	5098	20392	18	$\mathbb{Z}_{18}$
15	1	5837	5837	2	$\mathbb{Z}_2$

Table 6: Class Numbers for small d (continued)

ℓ	n	d	D	**h(D)**	**H(D)**
2	3	5954	23816	12	$\mathbb{Z}_6 \otimes \mathbb{Z}_2$
16	1	6626	26504	16	$\mathbb{Z}_{16}$
17	1	7465	7465	18	$\mathbb{Z}_{18}$
5	2	7610	30440	8	$\mathbb{Z}_4 \otimes \mathbb{Z}_2$
18	1	8354	33416	8	$\mathbb{Z}_8$
19	1	9293	9293	3	$\mathbb{Z}_3$
20	1	10282	41128	16	$\mathbb{Z}_8 \otimes \mathbb{Z}_2$
6	2	10865	10865	12	$\mathbb{Z}_6 \otimes \mathbb{Z}_2$
1	5	11257	11257	17	$\mathbb{Z}_{17}$
21	1	11321	11321	15	$\mathbb{Z}_{15}$
22	1	12410	49640	8	$\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$
3	3	13033	13033	13	$\mathbb{Z}_{13}$
23	1	13549	13549	12	$\mathbb{Z}_{12}$
7	2	14698	58792	18	$\mathbb{Z}_{18}$
24	1	14738	58952	12	$\mathbb{Z}_{12}$
25	1	15977	15977	10	$\mathbb{Z}_{10}$
26	1	17266	69064	32	$\mathbb{Z}_8 \otimes \mathbb{Z}_4$
2	4	17989	17989	9	$\mathbb{Z}_9$
8	2	19109	19109	4	$\mathbb{Z}_4$
28	1	19994	79976	20	$\mathbb{Z}_{10} \otimes \mathbb{Z}_2$

APPENDIX B - PROOF OF THE CLASS NUMBER FORMULA

We prove the class number formula in stages. We first examine the Riemann zeta function $\zeta(s)$ and calculate its residue at $s = 1$. We then define the Dedekind zeta function $\zeta_K(s)$ and expand it in terms of $\zeta(s)$ and appropriate Dirichlet L-functions. We then find the residue of the Dedekind zeta function at $s = 1$ using this expansion. Finally, we use a geometric argument to find the residue of the Dedekind zeta function in a second way (which will involve the class number of the field K). Combining these results will give us a formula for the class number in terms of L-functions.

Recall that the Riemann zeta function is defined to be

$$\zeta(s) \quad = \quad \sum_{n=1}^{\infty} \frac{1}{n^s}$$

where $s = \sigma + it$ is a complex variable. This function is analytic on the half-plane $\sigma > 1$. The Riemann zeta function also admits a nice product form due to Euler:

$$\zeta(s) \quad = \quad \prod_p \left(1 - p^{-s}\right)^{-1}.$$

We can actually say more about the zeta function. On the half-plane $\sigma > 0$, $\zeta(s)$ is analytic except for a simple pole at $s = 1$. To see this, we first consider the function

$$S(s, m, k) \quad = \quad \sum_{n=m+1}^{k} n^{-s}.$$

It can be easily verified that

$$S(s, m, k) \quad = \quad \sum_{n=m}^{k-1} n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) - m^{1-s} + k^{1-s}$$

and

$$n\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) \;=\; s\int_n^{n+1} \frac{\lfloor x\rfloor}{x^{s+1}}\,dx.$$

Since the sum of these terms becomes a sequence of abutting integrals, we can write

$$S(s,m,k) \;=\; s\int_m^k \frac{\lfloor x\rfloor}{x^{s+1}}\,dx - m^{1-s} + k^{1-s}$$

which we change slightly to assure convergence of the integral by

$$S(s,m,k) \;=\; -s\int_m^k \frac{x-\lfloor x\rfloor}{x^{s+1}}\,dx + \frac{1}{s-1}(m^{1-s} - k^{1-s}).$$

Letting $m = 1$ and $k \to \infty$ we see that $S(s,m,k) \to \zeta(s) - 1$ and so we have for $\sigma > 1$

$$\zeta(s) \;=\; \frac{1}{s-1} + 1 - s\int_1^\infty \frac{\lfloor x\rfloor - x}{x^{s+1}}\,dx. \tag{14}$$

This form can be shown to be the analytic continuation for $\zeta(s)$ on $\sigma > 0$. Since $0 \le x - \lfloor x\rfloor \le 1$, it follows that the integral in (14) is bounded. Hence, $\zeta(s)$ has a simple pole at $s = 1$ with residue 1.

We now consider the Dedekind zeta function $\zeta_K(s)$ for a given number field K:

$$\zeta_K(s) \;=\; \sum_{n=1}^{\infty} \frac{j_n}{n^s}$$

where j_n denotes the number of ideals I of the number ring $R = \mathbb{A} \cap K$ with $\|I\| = n$. By the unique factorization of ideals, we know that for each n, j_n must be finite. So, this function is analytic on $\sigma > 1$ and can be extended to a function analytic on $\sigma > 0$ in much the same way that the Riemann zeta function was extended. We do this in two different ways and compare the residues at $s = 1$.

We begin by noting that we can also represent the Dedekind zeta function in two additional ways. The first merely changes the sum from one over n to one over the ideals of R:

$$\zeta(s) \ = \ \sum_{I \in R} \frac{1}{\|I\|^s}.$$

Since we have unique factorization of ideals, this sum can be rewritten as a product exactly as the Riemann zeta function:

$$\zeta(s) \ = \ \prod_{P \in R} \left(1 - \frac{1}{\|P\|^s}\right)^{-1}$$

where P represents a prime ideal in R. This product can be recast into a product over the rational primes by recalling that each prime ideal in R lies over a unique prime p in $\mathbb{Z}$. Since we are dealing with normal extensions of $\mathbb{Q}$ it follows that every prime ideal lying over p must have the same norm

$$\|P\| \ = \ p^{f_p}$$

where f_p is a constant for each p (called the inertial degree of P over p). If there are r_p primes lying over the rational prime p we must have

$$\zeta_K(s) \ = \ \prod_p \left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p}$$

where the product is taken over all rational primes.

Next, we discuss some basic results for arbitrary number fields K which are *abelian extensions* of $\mathbb{Q}$. We will quickly specialize to the case of real quadratic number fields to make the arguments more tractable. Since we are dealing with abelian extensions, the famous theorem of Kronecker and Weber tells us that K is a subfield of a cyclotomic field. Since the Galois group of the cyclotomic field of degree m over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}_m^*$, we can assume that the character group of our field are characters modulo m (sometimes called Dirichlet Characters). So, if $\widehat{G}$ are the characters corresponding to the Galois group of our field K, then we can consider $\widehat{G}$ to be a subgroup of $\widehat{\mathbb{Z}_m^*}$. In the case of real quadratic number fields, we know that $\mathbb{Q}(\sqrt{d})$ is a subfield of the Dth cyclotomic field where D is the discriminant of $\mathbb{Q}(\sqrt{d})$. Hence, the Galois group G of $\mathbb{Q}(\sqrt{d})$ is the subgroup of $\mathbb{Z}_D^*$ of order two that fixes $\mathbb{Q}(\sqrt{d})$. Hence, the character group $\widehat{G}$ of $\mathbb{Q}(\sqrt{d})$ is the corresponding subgroup of $\widehat{\mathbb{Z}_D^*}$. This group contains the trivial character (which assigns one to every integer relatively prime to D and zero to any other integer). And the character given by:

$$\begin{aligned}
\chi(p) &= (\frac{d}{p}) \quad \text{for odd primes not dividing D} \\
\chi(2) &= \begin{cases} 1 & \text{if } d \equiv 1 \pmod 8 \\ \text{-1} & \text{if } d \equiv 5 \pmod 8 \end{cases} \\
\chi(n) &= 0 \quad \text{if} \ \ (n, D) \neq 1
\end{aligned}$$

and extended multiplicatively for all integers relatively prime to D. For odd n, this character equals the Jacobi symbol $(\frac{d}{n})$.

The Dirichlet L-function

$$L(s,\chi) \;=\; \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

also admits a product representation

$$L(s,\chi) \;=\; \prod_{p \not| D} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

It can be shown that taking the product of all L-functions over the character group gives [4][pp.194-195]

$$\prod_{\chi\in\widehat{G}} L(s,\chi) \;=\; \prod_{p\not| D}\left(1-\frac{1}{p^{f_p s}}\right)^{-r_p}$$

which gives us that

$$\zeta_K(s) \;=\; \prod_{p|D}\left(1-\frac{1}{p^{f_p s}}\right)^{-r_p}\prod_{\chi\in\widehat{G}} L(s,\chi).$$

Separating out the trivial character and noting that

$$L(s,1) \;=\; \zeta(s)\prod_{p|D}\left(1-\frac{1}{p^s}\right)$$

we see that

$$\zeta_K(s) \;=\; \zeta(s)\prod_{p|D}\left(1-\frac{1}{p^s}\right)\left(1-\frac{1}{p^{f_p s}}\right)^{-r_p}\prod_{\chi\in\,\widehat{G}-\{1\}} L(s,\chi).$$

In the special case of real quadratic number fields, there is only one non-trivial character. In addition, when $p|D$, we can see from our results on prime ideals that $f_p = 1$ and $r_p = 1$. Hence, we see that

$$\zeta_K(s) \;=\; \zeta(s)L(s,\chi)$$

where χ is the non-trivial character described above. We wish to characterize the pole of the Dedekind zeta function at $s = 1$. To that end, we note that for any non-trivial character, $L(s,\chi)$ is analytic on $\sigma > 0$ [4][pp.195-196]. Hence, $\zeta_K(s)$ has a simple pole at $s = 1$ (since $\zeta(s)$ has one there) and the residue of $\zeta_K(s)$ at $s = 1$ is given by $L(1,\chi)$.

We now compute the residue of $\zeta_K(s)$ in a different fashion. Equating these two forms for the residue will yield the class number formula. To that end, we try to estimate the number j_n appearing in the original definition of the Dedekind zeta function.

We begin by counting the number of ideals in a particular ideal class C with norm less than or equal to a given n. Denote this quantity by $i_C(n)$. To estimate this number, we fix an ideal J in C^{-1} (the inverse class of C) and note that for any ideal I in C, $IJ = (\alpha)$ for some α in R. Since $\|I\| \leq n$ if and only if $|N(\alpha)| \leq n\|J\|$, counting ideals in R with norm less than or equal to n is nearly equivalent to counting elements in R whose norm is less than or equal to $n\|J\|$. The one problem with this approach is that the principle ideal (α) equals the principle ideal $(u\alpha)$ where u is any unit in R. Thus, when we count at the element level, we must ensure that we do not count any associates. If there were only a finite number of units, this would not be an issue (since we could count all elements and then divide by the number of units). Unfortunately, we know that for real quadratic number rings, there are an infinite number of units. Thus, we must find a way of excluding associates from our counts.

To avoid over-counting, we construct a subset D of R in which no two members differ by a unit and such that every non-zero element of R has a unit multiple in D. This can be done by letting D be a set of coset representatives for U (the unit group) in $R - \{0\}$ (which is a multiplicative monoid). To make the arguments more concrete, we discuss the real quadratic case only.

For real quadratic number rings, U is the direct product of the group $\{-1, 1\}$ with the infinite cyclic group $\{u^k \mid k \in \mathbb{Z}\}$ where u is the fundamental unit. We map our number ring into $\mathbb{R}^2$ by $r \rightarrow (r, \sigma(r))$ where σ is the automorphism of the corresponding number field taking each element to its algebraic conjugate (this is the same map we employed when proving the Minkowski Bound). We let Λ_R denote the image of R under this mapping (which is a two-dimensional lattice in $\mathbb{R}^2$.

We now re-map $\Lambda_R - \{0\}$ into $\mathbb{R}^2$ by $(r, \sigma(r)) \to (\ln|r|, \ln|\sigma(r)|)$. In total, we have the following mappings:

$$R - \{0\} \stackrel{(r,\sigma(r))}{\longrightarrow} \Lambda_R - \{0\} \stackrel{(\ln|r|,\ln|\sigma(r)|)}{\longrightarrow} \Phi_{log}(\Lambda_R - \{0\})$$

where $\Phi_{log}(\Lambda_R - \{0\})$ denotes the image of $\Lambda_R - \{0\}$ under the log map defined above. The first mapping is a multiplicative isomorphism. The second mapping is a multiplicative-to-additive isomorphism if we restrict ourselves to the elements of $\Lambda_R - \{0\}$ with positive abscissas.

Since we want to construct a set of coset representatives for $R - \{0\}$ modulo U, we need only consider elements in R^+ since any negative element r is associated with $|r|$. This restricts us to the portion of Λ_R lying in the first and fourth quadrants of $\mathbb{R}^2$. To find the appropriate regions in these quadrants, we first find the coset representatives in $\Phi_{log}(\Lambda_R - \{0\})$ (which will be easier than in $\Lambda_R - \{0\}$). We then pull this region back to its pre-image restricted to the first and fourth quadrants. We then attempt to count the appropriate elements of $\Lambda_R - \{0\}$ in these regions.

Under the action of the log map, all units are sent to the line $x + y = 0$ in $\mathbb{R}^2$ (since the norm of a unit is ±1). We wish to find a region of the plane where all the elements of R^+ (under the composite map) are unassociated. Such a region is shown in Figure 2.

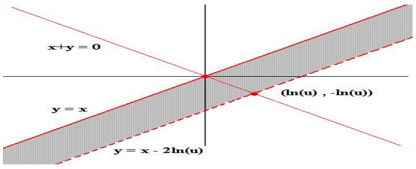

Figure 2: Coset Representatives in $\Phi_{log}(\Lambda_R - \{0\})$

The quantity u in this diagram is the fundamental unit. This region pulls back to the one shown in Figure 3.

Recall that we need only consider the portions of this region in the first and fourth quadrants. Our job now is to estimate the number of points in the lattice Λ_J (the image of the ideal J in $\mathbb{R}^2$) with $|N(r)| = |r\sigma(r)| \leq n\|J\|$. We give a graphical representation of this region in Figure 4 for concreteness.

The area enclosed by these boundaries is obviously

$$\begin{aligned}
\frac{Area}{2} &= \int_0^{\sqrt{n\|J\|}} \left(x - \frac{1}{u^2}x\right)\, dx + \int_{\sqrt{n\|J\|}}^{u\sqrt{n\|J\|}} \left(\frac{n\|J\|}{x} - \frac{1}{u^2}x\right)\, dx \\
&= n\|J\|\ln(u).
\end{aligned}$$

Recall that we used $\mathrm{vol}(\Lambda_R)$ to represent the area of the fundamental parallelotope for the lattice Λ_R (which is essentially the smallest parallelogram making up the lattice). Similarly, we let $\mathrm{vol}(\Lambda_J)$ represent the area of the fundamental parallelotope of the sublattice Λ_J determined by the ideal J. This area is related to $\mathrm{vol}(\Lambda_R)$:

$$\begin{aligned}
\mathrm{vol}(\Lambda_J) &= \|J\|\mathrm{vol}(\Lambda_R) \\
&= \|J\|\sqrt{|\mathrm{disc}(R)|}.
\end{aligned}$$

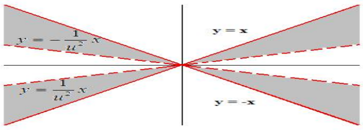

Figure 3: Coset Representatives in $\Lambda_R - \{0\}$

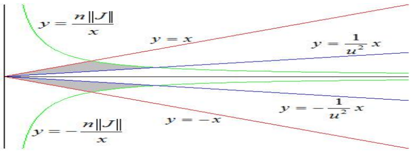

Figure 4: Region Containing Appropriate Lattice Points

We can obtain a rough estimate of the number of points of Λ_J in the specified region of the plane simply by dividing the area of this region by $\mathrm{vol}(\Lambda_J)$. So, we find that

$$\begin{aligned} i_C(n) &= \frac{2n\|J\|\ln(u)}{\mathrm{vol}(\Lambda_J)} + \delta(n) \\ &= \frac{2\ln(u)}{\sqrt{|\mathrm{disc}(R)|}} n + \delta(n) \end{aligned}$$

where $\delta(n)$ is a measure of the error we have incurred by the estimation. We need to give a bound on this error. As $n \to \infty$ the error should be bounded by the number of fundamental parallelotopes of Λ_J intersecting the boundary of our region. We can estimate this number by taking the arc-length of this region and dividing by the length of the smaller side of the parallelotope.

The arc-length is given by

$$\begin{aligned} L &= 2\int_0^{\sqrt{n\|J\|}} (\sqrt{2})\,dx + 2\int_0^{u\sqrt{n\|J\|}} \left(\sqrt{1+\frac{1}{u^2}}\right)\,dx \\ &\quad +2\int_{\sqrt{n\|J\|}}^{u\sqrt{n\|J\|}} \left(\sqrt{1+\left(\frac{n\|J\|}{x^2}\right)^2}\right)\,dx \\ &= 2\sqrt{\|J\|}\left(\sqrt{2}+\sqrt{u^2+\frac{1}{u^2}}\right)\sqrt{n} \;+\; 2\int_{\sqrt{n\|J\|}}^{u\sqrt{n\|J\|}} \left(\sqrt{1+\left(\frac{n\|J\|}{x^2}\right)^2}\right)\,dx. \end{aligned}$$

Since we are only interested in giving an order approximation for the error, we do not need to evaluate the last integral explicitly. We simply note that for

$$\sqrt{n\|J\|} \le x \le u\sqrt{n\|J\|}$$

the integrand is at most $\sqrt{2}$ and approximate accordingly. Hence, the arc-length is bounded by:

$$L \;\leq\; 2\sqrt{\|J\|}\left(\sqrt{2}u+\sqrt{u^2+\frac{1}{u^2}}\right)\sqrt{n}$$

Since $\mathrm{vol}(\Lambda_J) = \|J\|\ \mathrm{vol}(\Lambda_R)$, we know that the smaller side of the fundamental parallelotope for Λ_J is approximately $\sqrt{\|J\|}c$ where c is the smaller side of the fundamental parallelotope for Λ_R. Thus, as $n \to \infty$ we expect the error term in our approximation to grow as

$$\delta(n) \;\approx\; f\sqrt{n}$$

where f is some constant independent of the ideal class C. Hence

$$i_C(n) \;=\; \frac{2\ln(u)}{\sqrt{|\mathrm{disc}(R)|}}n+\delta(n)$$

where $\delta(n)$ is $O(n^{1/2})$ for all ideal classes.

If we now add up the ideals in all ideal classes with norm less than or equal to n (which we denote $i(n)$) we see that

$$i(n) \;=\; h\frac{2\ln(u)}{\sqrt{|\mathrm{disc}(R)|}}n+\delta(n)$$

where h is the class number of our number ring and $\delta(n)$ is $O(n^{1/2})$.

We are interested in the quantity j_n which is the number of ideals with norm equal to n. This quantity should be given by

$$\begin{aligned} j_n &= i(n)-i(n-1) \\ &= h\frac{2\ln(u)}{\sqrt{|\mathrm{disc}(R)|}}+\delta(n)-\delta(n-1). \end{aligned}$$

Hence $j_n - h\frac{2\ln(u)}{\sqrt{|\mathrm{disc}(R)|}}$ is $O(n^{-1/2})$ (since $\sqrt{n} - \sqrt{n-1}$ is $O(n^{-1/2})$). This will help us determine the residue of the Dedekind zeta function at $s = 1$.

By subtracting the term $h\frac{2\ln(u)}{\sqrt{|\mathrm{disc}(R)|}}\zeta(s)$ from the summand of the Dedekind zeta function and compensating appropriately, we see that

$$\zeta_K(s) \;=\; \sum_{n=1}^{\infty} \left(\frac{j_n - h\frac{2\ln(u)}{\sqrt{|\mathrm{disc}(R)|}}}{n^s} \right) + h\frac{2\ln(u)}{\sqrt{|\mathrm{disc}(R)|}}\zeta(s),$$

and since we know the numerator of the summand is $O(n^{-1/2})$, it follows that the sum converges for $s = 1$. Hence, the pole at $s = 1$ must be contained in the remainder term. Consequently, the residue must be $h\frac{2\ln(u)}{\sqrt{|\mathrm{disc}(R)|}}$ (since the residue of the Riemann zeta function at $s = 1$ is one). Equating the two forms for the residue of the Dedekind zeta function gives that

$$h \;=\; \frac{\sqrt{\mathrm{disc}(R)}}{2\ln(u)}L(1,\chi)$$

where we have dropped the absolute value on the discriminant of R since we are dealing with real quadratic number rings. This is precisely the formula given by Theorem 10.3.

REFERENCES

[1] Apostol, T.M. 1976. "Introduction to Analytic Number Theory." *Springer-Verlag, New York, Inc.*

[2] Cohen, H. 1993. "A Course in Computational Algebraic Number Theory." *Springer-Verlag, New York, Inc.*

[3] Cohn, H. 1962. "A Second Course in Number Theory." *John Wiley and Sons, Inc.*

[4] Marcus, D.A. 1977. "Number Fields." *Springer-Verlag, New York, Inc.*

[5] Pollard, H., Diamond, H.G. 1998. "The Theory of Algebraic Numbers." *Dover Publications, Inc.*

[6] Rockett, A., Szusz, P. 1992. "Continued Fractions." *World Scientific.*

[7] Biro, A. 2003. Yokoi's Conjecture. *Acta Arithmetica*, 106, pp.85-104.

[8] Biro, A. 2003. Chowla's Conjecture. *Acta Arithmetica*, 107, pp.179-194.

[9] Mollin, R.A., Williams, H.C. 1992. On Real Quadratic Fields of Class Number Two. *Mathematics of Computation*, 59, pp.625-632.

[10] Tatuzawa, T. 1951. On a theorem of Siegel. *Japan J. Math*, 21, pp.163-178.