The Length of the Continued Fraction of $p\sqrt{3}$

Michael Hofmann

January 14, 2004

Contents

Abstract

I really need to write an abstract

1 Introduction

This paper grew out of a conjecture by Benedict H. Gross in his paper 'An elliptic curve test for Mersenne Primes.' On page five of this paper he states "Corollary 1.4[1] implies that when $p = 2^l - 1$ is prime, the continued fraction of the quadratic irrationality $p\sqrt{3}$ has an unusually long period. It might be interesting to make this more precise." I began investigating the period length of continued fractions of the form $z\sqrt{3}$ and this paper is the result. For the sake of simplicity I concentrated mainly on the case when z is prime, and I assume p is a prime for remainder of this paper.

2 Continued Fractions

Definition 1. *A simple continued fraction is an expression of the form*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}}$$

with $a_0 \in \mathbb{Z}$ *and* $a_n \in \mathbb{N}$ *for* $n \geq 1$.

For the remainder of this paper the phrase continued fraction will represent simple continued fractions unless other wise stated. In order to represent continued fractions in a more concise way we will use the following notation

$$a_0 + \frac{1}{a_1+}\,\frac{1}{a_2+}\,\frac{1}{a_3+}\dots$$

The expression for a continued fraction can be either finite (the expession stops after some number of terms), or the expression can have an infinite number of terms. This leads to the following theorem which will be presented without proof.

Theorem 2.1. *A number represented by continued fraction is rational iff the continued fraction is finite.*

2.1 Definitions

We make the following definintions to help construct the theory of continued fractions. These theorems are presented without proof.

Definition 2. *A convergent is a partial quotient of continued fraction. Let* $\frac{A_n}{B_n}$ *represent the nth convergent.*

[1] Corollary 1.4 states "Assume that p $= 2^l - 1$ is prime. Then the order B $= \mathbb{Z} + p\mathbb{Z}\sqrt{3}$ of the index p in $\mathbb{Z} + \mathbb{Z}\sqrt{3}$ has class number 2 and fundamental unit $\eta = \epsilon^{2^{l-1}}$." The fact that the class number is 2 will be very important later.

Theorem 2.2. *Let $\frac{A_m}{B_m}$ be the nth convergent of a continued fraction and suppose the convergents converge to D then*
$\frac{A_0}{B_0}, \frac{A_2}{B_2}, \frac{A_4}{B_4}$ *...forms an increasing sequence less than D and*
$\frac{A_1}{B_1}, \frac{A_3}{B_3}, \frac{A_5}{B_5}$ *...forms a decreasing sequence greater than D.*

We also need to make sure that the idea of an infinite actually makes sense. In other words if we define a sequence of convergents of an infinite continued fraction, will the sequence converge. Lucky for us it will, the theorem is stated without proof.

Theorem 2.3. *All infinite continued fractions converge to some value in $\mathbb{R}$. This is a result of Theorem 2.2.*

In this paper we will be more concerned with infinite continued fractions and particularly with the continued fractions that representing quadratic irrationals, that is numbers of the form $\frac{P\pm\sqrt{D}}{Q}$, where P, Q are integers and D is a nonsquare positive number. The following important theorem is due to Lagrange.

Theorem 2.4. *Any quadratic irrational has a continued fraction which is periodic after a certain number of terms.*

The proof is stated in the next section.

2.2 Continued Fraction Algorithm

As of yet we have not yet defined a way to find the continued fraction of a given number. In this section we define such an algorithm and in the process show that a simple continued fraction can be constructed uniquely for any real number.

Algorithm 1. *Let α be a real number. We construct our continued fraction as follows. To begin let $r=\alpha$. Then follow these steps repeatedly:*

1. *set a_n equal to $\lfloor r \rfloor$, where $\lfloor r \rfloor$ is the floor function of r*
2. *$s=r - \lfloor r \rfloor$*
3. *$r=s^{-1}$*

This process stops if $s = 0$ and in this case the continued fraction is finite and D is rational. For irrational numbers this process continues indefinitely, but may be periodic as noted in Theorem 2.4.

A simple example will illustrate this process. Lets find the continued fraction representation of $\sqrt{3}$. We begin using the Continued Fraction Algorithm to

compute the continued fraction of $\sqrt{3}$

$$\begin{aligned} r &= \sqrt{3} && (1)\\ a_0 &= \lfloor r \rfloor = 1 && (2)\\ s &= r - \lfloor r \rfloor = \sqrt{3} - 1 && (3)\\ r &= s^{-1} = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} && (4)\\ a_1 &= \lfloor r \rfloor = 1 && (5)\\ s &= r - \lfloor r \rfloor = \frac{\sqrt{3}+1}{2} - 1 = \frac{\sqrt{3}-1}{2} && (6)\\ r &= s^{-1} = \frac{2}{\sqrt{3}-1} = \frac{2(\sqrt{3}+1)}{2} = \sqrt{3}+1 && (7)\\ a_2 &= \lfloor r \rfloor = 2 && (8)\\ s &= r - \lfloor r \rfloor = \sqrt{3} - 1 && (9) \end{aligned}$$

Notice now that (9) is the exact same as (3). From this point forward the terms of the continued fraction will just keep repeating. Thus

$$\sqrt{3} = 1 + \frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{2+}\cdots$$

Remark 1. *The Continued fraction Algorithm can be thought of in terms of groups in $GL_2(\mathbb{Z})$. Consider the matrix $\begin{pmatrix} \alpha \\ 1 \end{pmatrix}$ which represents $\frac{\alpha}{1}$.*

1. *Multiply on the left by $\begin{pmatrix} 1 & -\lfloor \alpha \rfloor \\ 0 & 1 \end{pmatrix}$ This gives $\begin{pmatrix} \alpha - \lfloor \alpha \rfloor \\ 1 \end{pmatrix}$*
2. *Multiply on the left by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ This sends $\begin{pmatrix} \beta \\ 1 \end{pmatrix}$ to $\begin{pmatrix} 1 \\ \beta \end{pmatrix}$*
3. *At the end of each loop the resulting matrix is $\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$*

   The expression $\frac{b_{22}}{b_{21}}$ is the nth convergent of the continued fraction. The expression $\frac{b_{12}}{b_{11}}$ is the (n-1)th convergent.

There is another algorithm that uses r=$-s^{-1}$ as the last step. This is equivalent to $SL_2(\mathbb{Z})$ group action where the second matrix would be $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

We can now use this to give a proof of Theorem 2.4, that a continued fraction is periodic if and only if it represents a quadratic irrational

In Theorem 2.4 we stated that quadratic irrationals have a continued fraction that is periodic after a certain point. This leads to the following definition.

Definition 3. *The length of the period of a continued fraction is the number of terms in each period of a periodic infinite continued fraction. It is only defined when the number represented is a quadratic irrational.*

For the remainder of this paper, whenever length is mentioned it is assumed to be the length of the period of a continued fraction. We need to make sure that the length is well-defined. We do that by showing that a number has only a single representation as a continued fraction.

Definition 4. *A quadratic irrational is called purely periodic if the point where it starts to be periodic is the first term.*

For example we saw that $\sqrt{3} = 1 + \frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{2+}\ldots$ so $\sqrt{3}$ is periodic, but not pure periodic. Whereas $\sqrt{3} - 1 = \frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{2+}\ldots$ is pure periodic.

Definition 5. *A quadratic irrational β is called reduced if $\beta > 1$ and $-1 < \overline{\beta} < 0$, where $\overline{\beta}$ is the conjugate of β.*

Theorem 2.5. *A quadratic irrational is purely periodic iff it is reduced.*

The proof is omitted. Refer to [Davenport] for a complete proof.

Proof of Theorem 2.4. Suppose that a continued fraction is periodic after a certain number point. In terms of matrices this means that after acting on $\begin{pmatrix} \beta \\ 1 \end{pmatrix}$ we get $\begin{pmatrix} \beta \\ 1 \end{pmatrix}$ back again. So $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \beta \\ 1 \end{pmatrix} = \begin{pmatrix} \beta \\ 1 \end{pmatrix}$ After multiplying this out and remembering what the definitions mean we get $\frac{a\beta+b}{c\beta+d} = \frac{\beta}{1}$ This implies that $c\beta^2 + (d-a)\beta - b = 0$. We know that β is irrational since having a periodic continued fraction implies that the continued fraction is not finite, so β must be a quadratic irrational.

If β is a quadratic irrational, all that we need to complete the proof is show that after enough steps using the Continued Fraction Algorithm we get a number r_n that satisfies Theorem 2.5. This portion of the proof is also omitted and the reader is again invited to read further in [Davenport].

□

Theorem 2.6. *If two simple continued fractions represent the same number iff each term in the continued fraction is equal. (This is not true if the continued fractions are not simple.)*

Proof. The if and only if part of this proof is clear. What we need to show for the other direction is that there is only one unique way of expressing a real number as a simple continued fraction. We will do this by showing that Algorithm 1 is the unique algorithm to find a simple continued fraction.

Lets take a closer look at the algorithm. Notice that $0 < \frac{1}{a_n+}\frac{1}{a_{n+1}+}\ldots < 1$ where $a_i \in \mathbb{N}$, so it is clear that in order for the algorithm to work steps 1 and 2 are correct and unique. So for instance after the first two steps we have $r = \lfloor r \rfloor + s$ where $0 < s < 1$ and we need something of the form $r = \lfloor r \rfloor + 1/r_1$ so clearly $r_1 = s^{-1}$ where $1 < r_1$ so $\lfloor r_1 \rfloor \in \mathbb{N}$ and step 3 is correct and unique. This shows that this algorithm is the only way to get a simple continued fraction and that the simple continued fraction for a number is unique. □

2.3 The Pell Equation

Definition 6. *The Pell equation is an equation of the form $x^2 - Dy^2 = 1$ where D is a positive-nonsquare integer greater than one.*

Theorem 2.7. *Every Pell equation has an infinite number of solutions in the integers.*

Proof. Pell's equation is very closely related to continued fractions. Suppose we have the equation $x^2 - Dy^2 = 1$, it is easy to find the continued fraction of $\sqrt{D}$ through the first period. Now using matrices as we defined earlier we have some element in the group $GL_2(\mathbb{Z})$ such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \sqrt{D} \\ 1 \end{pmatrix} = \begin{pmatrix} \sqrt{D} \\ 1 \end{pmatrix}$ This means that $\frac{a\sqrt{D}+b}{c\sqrt{D}+d} = \frac{\sqrt{D}}{1}$ or that $a\sqrt{D}+b = cD+d\sqrt{D}$. Since $\sqrt{D}$ is irrational we now have two equaitons, $a = d$ and $b = cD$. Substituting this back into our original matrix we get $\begin{pmatrix} d & cD \\ c & d \end{pmatrix}$ This matrix is in $GL_2(\mathbb{Z})$ so its determinant is ± 1, so $d^2 - Dc^2 = \pm 1$. If it is 1 then we have constructed a solution (c, d) to the Pell equation. If it is $d^2 - Dc^2 = -1$ then $(d - \sqrt{D}c)(d + \sqrt{D}c) = -1$ now squaring both sides we get $(d^2 + Dc^2 - 2cd\sqrt{D})(d^2 + Dc^2 + 2cd\sqrt{D}) = 1$ so $(d^2 + Dc^2)^2 - D(2cd)^2 = 1$ thus $(d^2 + Dc^2, 2cd)$ is a solution to the Pell equation.

Now supposing we have a solution (x_1, y_1) such that $x_1 \neq 0$ and $y_1 \neq 0$, we will show how to construct an infinite number of solutions.

if (x_1, y_1) is a solution this means

$$x_1{}^2 - Dy_1{}^2 = 1$$

$$(x_1 + \sqrt{D}y_1)(x_1 - \sqrt{D}y_1) = 1$$

$$(x_1 + \sqrt{D}y_1)^n(x_1 - \sqrt{D}y_1)^n = 1$$

let $(x_1 + \sqrt{D}y_1)^n = x_n + \sqrt{D}y_n$ then (x_n, y_n) also solves the Pell equation and (x_n, y_n) is clearly distinct from (x_1, y_1). □

Here is an example of how we can use continued fractions to find solutions to the Pell equation. Consider the equation $x^2 - 3y^2 = \pm 1$. We found earlier that the continued fraction representation of $\sqrt{3} = 1 + \frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{2+}\ldots$. Now let's use the GL_2 action we defined earlier (Remark 1).

According to our algorithm we get

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$$

Now the convergents we are interested in are in the top row, 1 and 2. This implies the fundamental solution to the Pell equation $x^2 - 3y^2 = \pm 1$ is x=2 and y=1. which we can check: $2^2 - 3 * 1^2 = 1$. To find all other solutions we can either use matrices or we can take powers of $2 + \sqrt{3}$.

2.3.1 Considering the Pell Equation Modulo Four

By looking at the Pell equation modulo four we can determine something about the nature of the solutions.

The Pell equation we are interested in is $x^2 - 3p^2y^2 = \pm 1$ with p prime and x,y integers. Now by taking everything modulo 4 we have

$$x^2 - 3p^2y^2 \equiv \pm 1 \pmod 4$$

Theorem 2.8. *The solutions of the equation $x^2 - 3p^2y^2 = \pm 1$ are of the form x even and y odd, or x odd y even and $x^2 - 3p^2y^2$ is never equal to -1.*

Proof. Assuming p is an odd prime, we now have four cases depending on if x and y are even or odd.

CASE 1. *If x and y are even then our equation $x^2 - 3p^2y^2 \equiv \pm 1 \pmod 4$ simplifies to $0 - 0 \equiv \pm 1 \pmod 4$ which is a contradiction.*

CASE 2. *If x is even and y is odd our equation simplifies to $0 - 3 \equiv \pm 1 \pmod 4$ or $1 \equiv \pm 1 \pmod 4$.*

CASE 3. *If x is odd and y is even our equation simplifies to $1 - 0 \equiv \pm 1 \pmod 4$ or $1 \equiv \pm 1 \pmod 4$.*

CASE 4. *If x and y are odd then we have $1 - 3 \equiv \pm 1 \pmod 4$ which is a contradiction.*

This shows that we have two possible cases, either x is even and y is odd (CASE 2), or y is even and x is odd (CASE 3). In both these cases the equation is equal to 1, and never -1. □

2.3.2 The Parity of the Length of Continued Fractions of $p\sqrt{3}$

In the last section we showed that the Pell equation $x^2 - 3p^2y^2$ is never equal to -1 for the special case $D = 3p^2$, this has ramifications on the parity of the length of continued fractions representing $\sqrt{3p^2}$.

Theorem 2.9. *The length of continued fractions representing numbers of the form $3p^2$ is always even.*

Proof. We know there exists a matrix in $GL_2(\mathbb{Z})$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \sqrt{3p^2} \\ 1 \end{pmatrix} = \begin{pmatrix} \sqrt{3p^2} \\ 1 \end{pmatrix}.$$

Using a method similar to Theorem 2.3 we find that our matrix becomes

$$\begin{pmatrix} d & 3p^2c \\ c & d \end{pmatrix}$$

and we know that the determinant of this matrix is ± 1 and it it's determinant is a solution to the equation $d^2 - 3p^2c^2$. But we know from the previous section

that the only possibility is +1. So the determinant of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is 1. Let look at how this matrix is constructed. Remark 1 tells us that this matrix is a product of matrices of the form

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -\lfloor \alpha_i \rfloor \\ 0 & 1 \end{pmatrix}$$

and we have a pair of these matrices for each element in the period of the continued fraction. Now the determinant of this each individual pair of matrices is -1 and the determinant of there product, the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, is 1, so this implies there must be an even number of element is the period of the continued fraction, so the length must be even. □

2.4 Units

Definition 7. *A real quadratic ring is* $\mathbb{Z}[\sqrt{D}]$ *with* $D > 0$ *and* D *nonsquare. This is the ring of algebraic integers when* $D \equiv 2$ *or* $3 \pmod 4$

Definition 8. *The Norm of an element* $a+b\sqrt{D}$ *in* $\mathbb{Z}[\sqrt{D}]$ *is* $a^2 - Db^2$.

Definition 9. *A unit in a real quadratic field is an element* α *such that Norm(*α*)* $= \pm 1$.

Notice that if (x,y) is any solution to the Pell equation $x^2 - Dy^2 = \pm 1$ then $x + y\sqrt{D}$ is a unit in $\mathbb{Q}[\sqrt{D}]$.

Definition 10. *A fundamental unit of a real quadratic field is an element* η *such that all other units in the field can be formed as powers of* η.

Theorem 2.10. *In the ring* $\mathbb{Z}[\sqrt{D}]$ *where* $D > 0$ *and* $D \equiv$ *2 or 3 (mod 4) the fundamental unit is* $x+y\sqrt{D}$ *where (x,y) is the first solution to the Pell equation* $x^2 - Dy^2 = 1$. *Where by first solution it is meant the solution first found by the continued fraction method.*

2.4.1 Finding the Fundamental Unit in $\mathbb{Z}[\sqrt{3}]$

The fundamental unit of the ring $\mathbb{Z}[\sqrt{3}]$ will be very important to later calculations and this calculation also shows a concrete example of continued fractions, Pell's equation and units.

Theorem 2.11. *The fundamental unit in* $\mathbb{Z}[\sqrt{3}]$ *is* $2 + \sqrt{3}$.

Proof. We calculated earlier that

$$\sqrt{3} = 1 + \frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{2+}\cdots$$

and we used that knowledge to find a solution to the Pell Equation $x^2 - 3y^2 = 1$, namely $2 + \sqrt{3}$, thus the fundamental unit of $\mathbb{Z}[\sqrt{3}]$ is $2 + \sqrt{3}$. □

3 Binary Quadratic Forms

Definition 11. *A binary quadratic form is an expression* $ax^2 + bxy + cy^2$ *with* $a, b, c \in \mathbb{Z}$. *To save space we also write (a,b,c).*

The theory of quadratic froms revolves around the question of which numbers can be represented by a quadratic form.

Definition 12. *Two binary quadratic forms* $ax^2+bxy+cy^2$ *and* $a'x^2+'bxy+c'y^2$ *are equivalent if there is a transformation* $x = pX + qY$, $y = rX + sY$ *with* $ps-qr = \pm 1$ *such that* $a(pX + qY)^2 + b(pX + qY)(rX + sY) + c(rX + sY)^2 = a'X^2 + b'XY + c'Y^2$. *We express this as (a,b,c)* $\sim$ *(a',b',c').*

Remark 2. *Note also that the matrix* $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ *is in* $GL_2(\mathbb{Z})$.

Theorem 3.1. $\sim$ *forms an equivalence relation.*

Proof. Let x,y,z $\in Q$ We need to show three things.

1. That x $\sim$ x for any quadratic form x. This is trivial since the identity matrix is in $GL_2(\mathbb{Z})$.

2. If x $\sim$ y then y $\sim$ x. If x $\sim$ y this means there is a element in $GL_2(\mathbb{Z})$ that transforms x into y. Since $GL_2(\mathbb{Z})$ is a group, the inverse of this element is also in $GL_2(\mathbb{Z})$ and it transforms y back to x so y $\sim$ x.

3. If x $\sim$ y and y $\sim$ z then x $\sim$ z. Again this just follows from the nature of $GL_2(\mathbb{Z})$. Since x $\sim$ y and y $\sim$ z this implies there are two elements in $GL_2(\mathbb{Z})$ that send x to y and y to z respectively. The composition of these two operations which is just their product in $GL_2(\mathbb{Z})$ (Which is also in $GL_2(\mathbb{Z})$) will send x to z, so x $\sim$ z.

These three criterion show that $\sim$ is an equivalence relation. □

Since we have an equivlance relation, it now makes sense to split quadratic forms into equivalence classes bases on the following definition.

Definition 13. *The equivalence class of a given quadratic form x:* $\mathcal{C}_x = \{y \in Q$ *such that* $y \sim x\}$.

3.1 Discriminant

Definition 14. *The discriminant D of the binary quadratic form* $ax^2+bxy+cy^2$ *is defined as* $b^2 - 4ac$.

Corollary 1. *Consider the discriminant modulo 4.*

$$D \equiv b^2 - 4ac \pmod 4$$

$$D \equiv b^2 \pmod 4$$

$$D \equiv 0 \text{ or } 1 \pmod 4 \textit{ depending on if b is even or odd respectively}$$

So the Discriminant must be congruent to 0 or 1 modulo 4 and is never congruent to 2 or 3. Also $D \equiv b^2 \pmod 4$.

Corollary 2. *The discriminants of two equivalent quadratic forms are equal.*

Proof. We can express the quadratic form $ax^2 + bxy + cy^2$ as $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$. Suppose (a',b',c') $\sim$ (a,b,c) then this implies there is a matrix $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ in $GL_2(\mathbb{Z})$ such that

$$\begin{pmatrix} a' & b'/2 \\ b'/2 & c' \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix}^{-1}$$

Since $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ is in $GL_2(\mathbb{Z})$ this implies that

$$\begin{vmatrix} a' & b'/2 \\ b'/2 & c' \end{vmatrix} = \begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix}$$

Which implies that $a'c' - \frac{(b')^2}{4} = ac - \frac{b^2}{4}$ which implies that the discriminants of equivalent forms are equal. □

3.2 Reduced Forms

Definition 15. *A quadratic form $ax^2+bxy+cy^2$ is called definite if it's discriminant is less than 0. If it's discriminant is greater than 0 it is called indefinite. When the discriminant is 0 it is called the degenerate case.*

This paper is concerned with quadratic forms whose determinants are $12p^2$. This is always a positive number, and hence all such forms are indefinite forms.

Definition 16. *An indefinite quadratic form $ax^2 + bxy + cy^2$ is called reduced if $0 < b < \sqrt{D}$ and $-b + \sqrt{D} < 2a < b + \sqrt{D}$, where D is the discriminant of the quadratic form.*

There is also another notion of reduced where a is replaced by $|a|$. The relationship between these two notions is similar to the comments after Remark 1. The way we defined it is called GL_2-equivalence, whereas using $|a|$ is called SL_2-equivalence.

Algorithm 2. *In order to prove that a binary quadratic form has a reduced form we use an algorithm to find that reduced form. (INCORRECT)*

1. *If (a,b,c) is not reduced then choose δ such that $\sqrt{D} - 2|c| < -b + 2c\delta < \sqrt{D}$.*
2. *We have (a,b,c) $\sim (c, -b + 2c\delta, a - b\delta + c\delta^2)$*
3. *if $|a - b\delta + c\delta^2| < |c|$ then repeat the process.*

This is a finite process and for any quadratic form will always give an equivlalent reduced form.

Corollary 3. *Each quadratic form has a reduced form.*

Theorem 3.2. *The number of reduced forms of a given discriminant is always finite.*

Proof. The conditions that $D = b^2 - 4ac$ and $0 < b < \sqrt{D}$ is very restrictive. This limits the possibilities for b to a finite number and there are also only a finite number of ways to factor $D - b^2$ into $-4ac$. This implies that the number of reduced forms for each D is also finite. □

3.2.1 Primitive Reduced Forms

Definition 17. *A binary quadratic form $ax^2 + bxy + cy^2$ is called primitive if a,b and c have no common factor.*

Which quadratic forms with Discriminant equal to $12p^2$ with p prime are not primitive?

Theorem 3.3. *if $D = 12p^2$ then all the reduced forms of D are primitive except 2.*

We'll first need a lemma to prove this.

Lemma 1. *The only reduced forms of quadratic forms with discriminant 12 are (1,2,-2) and (2,2,-1).*

Proof. We know $12 = D = b^2 - 4ac$, this implies that 4 divides b^2 or that 2 divides b. Since (a,b,c) is a reduced quadratic form this also means that $0 < b < \sqrt{D} = \sqrt{12}$, so b must be 2. Now $12 = 4 - 4ac$, this reduces to $-2 = ac$, since we also know $-2 + \sqrt{12} < 2a < 2 + \sqrt{12}$ which means a is 1 or 2, this implies that c is -2 or -1 respectably, so (1,2,-2), (2,2,-1) are the only reduced forms of discriminant 12. □

Proof. Theorem 3.3 Let $12p^2 = D = b^2 - 4ac$, if $g = GCD(a, b, c)$ then g^2 divides $12p^2$. If g is greater than 1, this implies either g=2 or g=p or g=2p since p is prime. Lets consider the three cases.

CASE 1. *g=2*

Lets factor g out. $3p^2 = D' = \left(\frac{b}{2}\right)^2 - 4\left(\frac{a}{2}\right)\left(\frac{c}{2}\right)$ *Corollary 1 showed D' is always congruent to 0 or 1 modulo 4 so this implies that in this case p=2. Since p=2 we get D'=12 which has reduced quadratic forms (1,2,-2) and (2,2,-1) from the lemma, so our original discriminant $D = 12p^2$ or D=48 has only the nonprimitive reduced form (2,4,-4) and (4,4,-2) or, written another way, (p,2p,-2p) (2p,2p,-p).*

CASE 2. *g=p*

Lets factor p out. $D' = \left(\frac{b}{p}\right)^2 - 4\left(\frac{a}{p}\right)\left(\frac{c}{p}\right) = 12$. *So again we have the case D'=12. So $D = 12p^2$ has the nonprimitive reduced forms (p,2p,-2p) and (2p,2p,-p).*

CASE 3. *g=2p*

Lets factor 2p out. $D' = \left(\frac{b}{2p}\right)^2 - 4\left(\frac{a}{2p}\right)\left(\frac{c}{2p}\right) = 3$. *Here we have the case that D'=3, but this is a contradiction since* $D' \equiv 0$ *or* $1 \pmod 4$.

So there are only four non-primitive equivalence classes reduced forms with discriminant $12p^2$, namely (p,2p,-2p) and (2p,2p,-p). □

These examples also show an interesting property of reduced forms. It appears for any reduced form (a,b,c) then (-c,b,-a) is also a reduced form. This fact is stated in the following theorem.

Theorem 3.4. *If a quadratic form (a,b,c) with discriminant* $D = 12p^2$ *is reduced then there is another distinct reduced form associated with it, namely (-c,b,-a).*

Proof. First we want to show that that (-a,b,-c) is also a reduced form, then we need to show that it is also distinct from (a,b,c).

Clearly this quadratic form still has discriminant D, since $D - b^2 = -4ac$ this implies $(\sqrt{D} - b)(\sqrt{D} + b) = -4ac$. Since $0 < b < \sqrt{D}$ this implies that $-4ac$ is positive and since a is positive $(0 < \sqrt{D} - b < 2a)$ its clear c must be negative. So $(\sqrt{D} - b)(\sqrt{D} + b) = (2a)(2(-c))$. Since $\sqrt{D} - b < 2a < \sqrt{D} + b$ this implies that $\sqrt{D} - b < 2(-c) < \sqrt{D} + b$. This implies that (-c,b,-a) is a reduced form.

In order to check the that the forms are all distinct we need to show that $a \neq -c$. If a = -c then $b^2 + 4a^2 = D = 12p^2$. This implies $(\frac{b}{2})^2 + a^2 = 3p^2$ So $3p^2$ is the sum of two squares, but an integer with a power of 3 in it's square free part can never be a sum of two squares which implies $a \neq -c$, completing the proof. □

Corollary 4. *This theorem yields the obvious corollary: The number of reduced forms of a given discriminant of the form* $12p^2$ *is always divisible by 2.*

4 The Class Number

4.1 What is the Class Number?

Definition 18. *For the purposes of our dicussion we define the class number h(D) to be the number of equivalence classes of primitive binary quadratic forms of a given discriminant D. Since each quadratic form is equivalent to a reduced form we can look at the number of equivalence classes of reduded forms.*

Corollary 5. *The Class number of a given discriminant is always finite.*

Proof. Theorem 3.2 states the there are only a finite number of reduced forms of any discriminant. It immediately follows that the class number of any discriminant is finite. □

4.2 The Underlying Structure

The structure of real quadratic fields is much more complex and beautiful than that of imaginary quadratic fields. In imaginary quadratic fields each reduced form is in its own equivalence class (with a couple of exceptions), but in real quadratic fields this is not true. Instead the reduced forms form cycles, and the class number is the number of such cycles. First a couple of definitions

Definition 19. *Two reduced forms (a, b, c) and $(-c, b', c')$ are called adjacent if $b + b' \equiv 0 \pmod{2(-c)}$.*

Theorem 4.1. *For any reduced form β there is always exactly one adjacent reduced form distinct from β on either side.*

Proof. The method of cycling between reduced forms is very similar to the continued fraction algorithm (Algorithm 1). Starting from our reduced form $ax^2 + bxy + cy^2$ we set it equal to 0 and perform the substitution $z = x/y$ to get $az^2 + bz + c$. $\frac{-b+\sqrt{D}}{2a}$ is a solution to this equation, where $D = b^2 - 4ac$, and will represent the reduced form. Now we perform the continued fraction algorithm on this number by first inverting it

$$\left(\frac{-b+\sqrt{D}}{2a}\right)^{-1} = \frac{2a}{-b+\sqrt{D}} * \frac{-b-\sqrt{D}}{-b-\sqrt{D}}$$

$$= \frac{(-2a)(b+\sqrt{D})}{b^2-(b^2-4ac)} = \frac{b+\sqrt{D}}{-2c}$$

and then subtracting it by its floor $F \in \mathbb{Z}, F = \lfloor \frac{b+\sqrt{D}}{-2c} \rfloor$

$$\frac{b+\sqrt{D}}{-2c} - F = \frac{-b'+\sqrt{D}}{2(-c)}$$

Now we can see that we have completely determined the first two spots in our new reduced form namely $(-c, b', \bullet)$ and that

$$\frac{b+\sqrt{D}}{-2c} - \frac{-b'+\sqrt{D}}{-2c} = F$$

which implies $\frac{b+b'}{-2c} \in \mathbb{Z}$ so $b + b' \equiv 0 \pmod{2(-c)}$. c' is now also determined since $c' = \frac{D-(b')^2}{4c}$. This is always an integer since $D = b^2 - 4ac$ and $b + b' \equiv 0 \pmod{2(-c)}$ implies $D - (b')^2 \equiv 0 \pmod{4c}$.

Finally we need to show that $(-c, b', c')$ is actually a reduced form. We know $0 < \frac{-b'+\sqrt{D}}{2(-c)} < 1$ which implies $0 < -b' + \sqrt{D} < 2(-c)$and $b' < \sqrt{D}$. So we still need to show that $0 < b'$ and $2(-c) < b' + sqrtD???$.

Finally the uniqueness assertion, suppose that we had (a, b, c) and $(-c, \bullet, \bullet)$, is there another choice for b'? If there were it would have to be at least $2|c|$ more or less than our choice from the algorithm. This means that $\frac{-b''+\sqrt{D}}{2(-c)} > 1$

which implies $-b'' + \sqrt{D} > 2(-c)$. Or that $\frac{-b''+\sqrt{D}}{2(-c)} < 0$ which would imply that $\sqrt{D} < b''$. Both of these options contradict the requirements for reduced forms, thus we only have one possibility for b' and thus c' is also fixed by D. This completes the proof of the theorem for one side, the other direction is similar. □

Theorem 4.2. *Reduced forms in real quadratic fields can be partitioned into cycles.*

Proof. Pick a reduced form, the next in the cycle is simply the next adjacent reduced form. Since there are only a finite number of reduced forms eventually come back to the original reduced form and have formed a cycle. If there is a reduced forms we haven't used yet then continued the process for another cycle with this reduced form, otherwise we are done. □

Corollary 6. *If $D = 12p^2$ the two nonprimitive reduced forms, $(p, 2p, -2p)$ and $(2p, 2p, -p)$, form there own cycles.*

Proof. Clearly they are both adjacent to each other since p and $2p \mid (2p+2p) = b + b'$. We write this as $(p, 2p, -2p) \sim (2p, 2p, -p) \sim (p, 2p, -2p)$. □

A couple examples of the cycle structure will also be elucidating. First consider $D = 12$. We already found that there are only two reduced forms namely $(1, 2, -2)$ and $(2, 2, -1)$. By Theorem 4.1 we see that $(1, 2, -2)$ is adjacent to $(2, 2, -1)$ which is again adjacent to $(1, 2, -2)$ so we have a 2-cycle.

Now for a more complicated case, consider $D = 300 = 12(5)^2$ Using an implementation of Algorithm 4 we find there are 10 reduced forms, (6,6,-11), (11,6,-6), (5,10,-10), (10,10,-5), (3,12,-13), (13,12,-3), (2,14,-13), (13,14,-2), (1,16,-11) and (11,16,-1). Firstly we can take out the nonprimitive reduced forms which form their own 2-cycle as in Corollary 6.

Now lets pick an element, for example (6,6,-11). The next reduced form in the cycle must begin with an 11 so we have two choices, but only (11,16,-1) gives the condition that $6 + 16 \equiv 0 \pmod{2(11)}$. (1,16,-11) and (11,6,-6) then clearly follow. At this point we are again back to our original choice so we have a 4-cycle.

We still have four reduced forms left, consider (13,12,-3). (3,12,-13) is clearly adjacent to it, but then we have two choices which begin with 13, but only one satisfies the second condition, namely (13,14,-2) followed by (2,14,-13) which brings us back to our first choice. So we have a 4-cycle. Since there are no more reduced forms left to choose from we are done.

So we have 3 cycles, a nonprimitive 2-cycle
(5,10,-10)∼(10,10,-5))∼(5,10,-10) and two 4-cycles
(6,6,-11)∼(11,16,-1)∼(1,16,-11)∼(11,6,-6)∼(6,6,-11) and
(13,12,-3)∼(3,12,-13)∼(13,14,-2)∼(2,14,-13)∼(13,12,-3)

4.3 Calculating the Class Number

Let $R = \mathbb{Z} + \mathbb{Z}\sqrt{3}$ and let $\eta = 2 + \sqrt{3}$ which is the fundamental unit in this ring. Assume $p > 3$ then $h(12p^2) = h(12)\frac{\Phi_R(p)}{i\Phi_{\mathbb{Z}}(p)}$ where Φ is the Euler Totient function over a specific ring defined by $\Phi_R(p) = |(R/pR)^\times|$, and i is the smallest integer such that $\eta^i \in \mathbb{Z} + p\mathbb{Z}\sqrt{3}$. Since p is prime we know that $\Phi_{\mathbb{Z}}(p) = p - 1$, in order to calculate $\Phi_R(p)$ we need to investigate if 3 splits over $\mathbb{Z}\sqrt{3}$. If p does not split then $\Phi_R(p) = p^2 - 1$, if p does split then $\Phi_R(p) = (p-1)^2$. It is fairly easy to calculate the $h(12)$ and how p splits over $\mathbb{Z}\sqrt{3}$. Calculating i is considerably more difficult, but an effective algorithm exists for calculating it using a computer.

4.3.1 What is $h(12)$?

This question is most easily answered using quadratic reduced forms. As an example in Subsection 4.2 we found out that the reduced forms of discriminant 12 form a single cycle (1,2,-2)~(2,2,-1)~(1,2,-2). Thus by definition of the class number h(12) = 1.

4.3.2 How does $\sqrt{3}$ split over different fields?

In order to determine the class number we need to determine over what fields $\mathbb{Z}_p$ the $\sqrt{3}$ splits into different factors. This is equivalent to asking over what if 3 is a square over different fields. We can calcuate this using quadratic reciprocity.

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}*\frac{2}{2}}$$
$$= \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$$

Now we have a couple of possibilities. Since p is prime, $p \equiv 1, 5, 7$ or $11 \pmod{12}$

If $p \equiv 1 \pmod{12}$

$$\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{1}{3}\right) = 1$$

so 3 is a square.

If $p \equiv 5 \pmod{12}$

$$\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{2}{3}\right) = -1$$

so 3 is not a square.

If $p \equiv 7 \pmod{12}$

$$\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = -\left(\frac{1}{3}\right) = -1$$

so 3 is not a square.

If $p \equiv 11 \pmod{12}$

$$\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = -\left(\frac{2}{3}\right) = 1$$

so 3 is a square.

This calculation show that $\sqrt{3}$ splits in the field $\mathbb{Z}_p$ iff $p \equiv 1$ or $11 \pmod{12}$. Now using we state the class number formula in its full simplicity

$$h(12p^2) = h(12)\frac{\Phi_R(p)}{i\Phi_{\mathbb{Z}}(p)}$$

$$= \frac{p-1}{i} if p \equiv 1 \text{ or } 11 \pmod{12}$$

$$= \frac{p+1}{i} if p \equiv 5 \text{ or } 7 \pmod{12}$$

Since h(z) is always a positive integer this leads to the following corollary

Corollary 7. *i divides $p-1$ if $p \equiv 1$ or 11 (mod 12) and i divides $p+1$ if $p \equiv 5$ or 7 (mod 12).*

Now that we understand how to calculate the class number using this method lets do a quick example. In Subsection 4.2 we found that for $D = 300 = 12(5)^2$ there are two non-primitive cycles so the class number h(300)=2. Now lets try the other method.

$$h(12p^2) = \frac{h(12)(p \pm 1)}{i}$$

Now $p = 5$, $h(12) = 1$ and $p \equiv 5 \pmod{12}$ so we have

$$h(12p^2) = \frac{p+1}{/} i = \frac{6}{i}$$

Now we need to calculate i. Recall i is the smallest integer such that

$$(2+\sqrt{3})^i \in \mathbb{Z} + p\sqrt{3}\mathbb{Z} = \mathbb{Z} + 5\sqrt{3}\mathbb{Z}$$

Clearly $i \neq 1$ so by Corollary 7 i = 2,3 or 6. $(2+\sqrt{3})^2 = 7 + 4\sqrt{3} \notin \mathbb{Z} + 5\sqrt{3}\mathbb{Z}$ $(2+\sqrt{3})^3 = 26 + 15\sqrt{3} \in \mathbb{Z} + 5\sqrt{3}\mathbb{Z}$ so $i = 3$, thus h(300) = 2.

5 Bounds on the Length of Continued Fractions

5.1 An Upper Bound on the Period of our Continued Fraction

If D is quadratic irrational let p(D) denote the length of its period. In [pacific journal] it is shown that $p(D) < \frac{\mu log \eta}{log \alpha}$ where $\eta = \frac{u_0 + v_0\sqrt{D}}{2}$ is the fundamental

unit in $\mathbb{Z}\sqrt{D}$, $\alpha = \frac{1+\sqrt{5}}{2}$, and $\mu = 3$ if $2 \nmid u_0$ or $\mu = 1$ if $2 \mid u_0$. Now to apply this to $D = 12p^2$ in the order $\mathbb{Z} + p\sqrt{3}\mathbb{Z}$. We get $\eta = \frac{4+2\sqrt{3}}{2}^i$ and $\mu = 1$ (See section 4.3 for an explanation of i. Now applying the theorem we find that $p(12p^2) = \frac{log\eta^i}{log\alpha} = i\frac{log\eta}{log\alpha}$ We know $h(12p^2) = \frac{p\pm1}{i}$ so $p(12p^2) = \frac{p\pm1}{h(12p^2)}\frac{log\eta}{log\alpha}$. Thus $p(12p^2)$ is approximately bounded by p/h.

5.2 A Lower Bound

Some notation:

$$\eta = 2 + \sqrt{3}, \quad \gamma = (1 + \sqrt{5})/2.$$

Let ℓ be a prime greater then 3. Let $\{a_0 = [\ell\sqrt{3}], a_1, a_2, \ldots\}$ be the elements of the continued fraction of $\ell\sqrt{3}$ as in Definition 1, and define

$$\begin{cases} p_k = a_k p_{k-1} + p_{k-2} \\ q_k = a_k q_{k-1} + q_{k-2}. \end{cases}$$

In particular, if p is the period of the said continued fraction, then

$$\eta_\ell = p_{p-1} + \ell\sqrt{3}q_{p-1}$$

is the fundamental unit in the order of discriminant $12\ell^2$. Recall that the class number of that order is given by

$$h(\ell) = (\ell \pm 1)/o(\ell),$$

where $o(\ell)$ is the integer such that $\eta_\ell = \eta^{o(\ell)}$.

We shall now relate the period p with the class number. We need the following theorem:

Theorem 5.1. *(Liouville) There exists a positive real number c such that for every pair of integers p and $q > 0$,*

$$|\sqrt{3} - \frac{p}{q}| \geq \frac{c}{q^2}.$$

Now let $a_0 = [\ell\sqrt{3}], a_1, a_2, \ldots$ be the elements of the continued fraction of $\ell\sqrt{3}$. Let p_k/q_k be the corresponding convergents, defined above. Then it is well known ([K; page 36]) that

$$|\ell\sqrt{3} - \frac{p_k}{q_k}| \leq \frac{1}{a_{k+1}q_k^2}.$$

After dividing both sides by ℓ we arrive to

$$|\sqrt{3} - \frac{p_k}{\ell q_k}| \leq \frac{\ell}{a_{k+1}(q_k\ell)^2}.$$

It follows that ℓ/a_k must be bigger then the costant c in the theorem. In fact this can be made explict, and it follows that $a_k \leq 4\ell$. By replacing a_k by 1 and

4ℓ, in the defining requations for p_k and q_k, we can obtain a lower and upper bound on η_ℓ, respectively:

$$\alpha^p \leq \eta_\ell \leq (4\ell)^p$$

Taking log of all three terms, and dividing by $\log(\eta)$ it follows that

$$p\frac{\log(\alpha)}{\log(\eta)} \leq o(\ell) \leq p\frac{\log(4p)}{\log(\eta)}$$

and

$$\frac{(\ell \pm 1)\log(\eta)}{h(\ell)\log(4p)} \leq p \leq \frac{(\ell \pm 1)\log(\eta)}{h(\ell)\log(\alpha)}$$

6 Algorithms and Experimental Results

This section explains the algorithms I used to calculate different results like the continued fraction of $p\sqrt{3}$, the Class number, or the number of reduced forms of a given discriminant. These results, especially those for continued fraction helped me to see interesting patterns that led me to study this topic more in-depth.

6.1 Length of Continued Fraction Period

As referenced in the introduction, I began looking into this topic after a reading a paper by Benedict H. Gross concerning the relative length of a continued fraction of the type $p\sqrt{3}$ where p is a Mersenne prime. In order to be able to quantify and understand what this really means I saw that it was necessary to understand the length of continued fractions for other values for p. Since I have already explained the method for finding the continued fraction of a given number in Algorithm 1, I will go straight to the Results. n is integer, n prime, n congruent to mod 24

6.2 The Class Number

Algorithm 3. *Recall the method from Subsection 4.3.*

$$h(12p^2) = \frac{h(12)(p \pm 1)}{i}$$

In Subsection 4.3.1 we found that h(12) = 1, and to determine the sign we need to know if 3 splits in $\mathbb{F}_p$. *It was shown in Subsection 4.3.2 that if* $p \equiv 1$ *or* $11 \pmod{12}$ *then 3 splits, otherwise it doesn't.*

let q=p-1 if $p \equiv 1$ *or* $11 \pmod{12}$ *otherwise let q=p+1.*

Now we need to calculate i which is defined to be the smallest integer such that $(2+\sqrt{3})^i \in \mathbb{Z} + p\mathbb{Z}\sqrt{3}$. *In Corollary 7 we saw that* $i \mid q$, *calculate the factors of q and test each, starting with the smallest factor bigger than 1, and see if the factor satisfies the property required for i. This number can get very*

large very quickly requiring very large precision. It is often effective to perform the operations needed modulo p and check that the solution is 0.

Once i is found then h(p) = q / i

6.3 Calculating the Number of Reduced Forms

Algorithm 4. *We have already given a way to find the reduced form of any given binary quadratic form (Algorithm 2). This algorithm computes the number of reduced forms of a given discrimant. It is specifically for $D = 12p^2$, but can easily be adjusted.*

1. *Fix the Discriminant D*
2. *let $r = 0$*
3. *let $b = 0$ (since $12p^2 = D \equiv 0 \pmod 4$)*
4. *let $s = (D - b^2)/4$ (This is always a positive integer)*
5. *Consider all the factors of s. Let r_b be the number of positive factors a such that $-b + \sqrt{D} < 2a < b + \sqrt{D}$ Because of Theorem 3.4, we can actually just consider the number of positive factors less than $\sqrt{D}$ and them multiply this number by two.*
6. *let $r = r + r_b$*
7. *let $b = b + 2$ (Recall from Corollary 1 that $D \equiv b^2 \pmod 4$)*
8. *if $b < \sqrt{D}$ repeat the process.*

r is the total number of reduced forms of a given discriminant $D = 12p^2$ In order to get the number of primitive reduced forms we need to subtract by two because of Theorem 3.3. It also was shown in Theorem 3.2 that this number is always finite, the fact that this is a finite algorithm is basically the reason this quantity is finite.

References

[1] Z. I. Borevich, I. R. Shafarevich: Number Theory (1966)

[2] H. Davenport: The Higher Arithmatic (1999)

[3] essay

[4] Computational number theory

[5] german

[6] Mathworld