GENUS THEORY AND CONVENIENT NUMBERS

SHAMAUL DILMOHAMED

Abstract. We will study genera of quadratic forms as well as convenient numbers in this paper. This discussion requires an exposition of quadratic reciprocity and creating an equivalence relation between quadratic forms, which we will touch upon before our main discussion.

Contents

1. Introduction

In this paper, we will use genus theory to study Euler's convenient numbers. These numbers were used by Euler in order to discover prime numbers much larger than those found by his contemporaries. The organization of this paper is as follows: in Section 2 we will discuss quadratic reciprocity and introduce a homomorphism for $D \equiv 0, 1 \bmod 4, D \neq 0$, $\chi : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$. In Section 3 we will study binary quadratic forms and define an equivalence relation on them. We then will define a representative for classes of these forms, reduced forms. In Section 4 we will study genus theory in order to classify forms that represent certain groups of numbers and in Section 5 we will study a specific type of composition of forms called Dirichlet composition, as well as convenient numbers and their properties.

2. Quadratic Reciprocity

First we will need to define the Legendre symbol, as it will be essential in the discussion of quadratic reciprocity.

Definition 2.1. Let a be an integer and p be a odd prime. The Legendre symbol (a/p) is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & p \nmid a, a \text{ is a quadratic residue modulo } p \\ -1 & p \nmid a, a \text{ is not a quadratic residue modulo } p \end{cases}$$

Euler discovered an equivalent definition of the Legendre symbol, which we will prove.

Lemma 2.2. *(Euler's criterion) Given the above definition of the Legendre symbol, this is equivalent to*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{(p-1)}{2}} \mod p.$$

Proof. Applying Fermat's little theorem, we know that $a^{p-1} \equiv 1 \mod p$. We can factor the left side to receive

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \mod p$$

As p is prime, we know at least one factor must be 0. If a is a quadratic residue modulo p, then there exists an x such that $x^2 \equiv a \mod p$. Applying this to the above equation, it is clear that all quadratic residues modulo p make the first factor 0. Applying Lagrange's theorem, there are at most $\frac{p-1}{2}$ residues that make the first factor 0. Now consider the equation

$$x^2 \equiv a \mod p$$

There are at most 2 roots for each a, which implies there are at least $\frac{p-1}{2}$ quadratic residues. Therefore exactly $\frac{p-1}{2}$ residues modulo p are quadratic residues modulo p. Additionally, the quadratic nonresidues must make the second factor 0, and the lemma is shown. □

Although we will not prove it, Euler's criterion and the Chinese Remainder Theorem are sufficient to prove the Law of Quadratic Reciprocity:

Theorem 2.3. *(Law of Quadratic Reciprocity) Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

We suggest the interested reader to read [1] for more details.

Using Euler's criterion, we can prove the two supplements to the law of quadratic reciprocity.

Theorem 2.4. *(First Supplement to the Law of Quadratic Reciprocity) Using the above definition of the Legendre symbol,*

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p$$

Proof. We get the desired result by direct substitution of -1 into Euler's criterion. □

Theorem 2.5. *(Second Supplement to the Law of Quadratic Reciprocity) Using the above definition of the Legendre symbol,*

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \mod p$$

Proof. Consider the following set of equations:

$$\begin{aligned}1 &= (-1)(-1)^1\\ 2 &= (2)(-1)^2\\ 3 &= (-3)(-1)^3\\ &\dots\\ \frac{p-1}{2} &= \left(\pm\frac{p-1}{2}\right)(-1)^{\frac{p-1}{2}}\end{aligned}$$

where the sign on $\frac{p-1}{2}$ depends on its parity. Observe that if we consider each equation modulo p, the negative odd terms in ascending order are equivalent to the positive even ones in descending order. Then we see that when we multiply all of the equations and take the residue modulo p, we receive

$$\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!\, 2^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{p+1}{2}\frac{1}{2}} \mod p$$

which we can then simplify to

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \mod p$$

Using Euler's criterion then finishes the proof. □

While the Legendre symbol has intriguing characteristics, one major drawback of it is its limitations; it is only defined for odd primes. Our homomorphism is a more generalized version of this symbol. Before that, however, we will need to define the Jacobi symbol, which is another generalization of the Legendre symbol.

Definition 2.6. Let M be an integer and m a positive odd integer coprime to M. Consider the prime factorization of $m = p_1 \cdot \ldots \cdot p_k$. The Jacobi symbol (M/m) is defined

$$\left(\frac{M}{m}\right) = \prod_{i=1}^{k}\left(\frac{M}{p_i}\right)$$

It is simple to show that the Jacobi symbol has the following properties:

$$\begin{aligned}\left(\frac{M}{m}\right) &= \left(\frac{N}{m}\right) \text{ for } M \equiv N \mod m\\ \left(\frac{MN}{m}\right) &= \left(\frac{M}{m}\right)\left(\frac{N}{m}\right)\\ \left(\frac{M}{mn}\right) &= \left(\frac{M}{m}\right)\left(\frac{M}{n}\right)\end{aligned}$$

Additionally, it is not difficult to prove that the Jacobi symbol satisfies a corresponding law of quadratic reciprocity and its supplements as above, and is left as an exercise.

We will need Dirichlet's theorem on primes in arithmetic progressions before proving the main theorem of this section. We will not prove it in this text, but the reader with experience in class field theory should read Chapter 8 of [2].

Theorem 2.7. *(Dirichlet's theorem on primes in arithmetic progression) Let a and d be two coprime integers. Consider the sequence*

$$a+d, a+2d, a+3d, \ldots, a+nd, \ldots$$

Then this sequence contains infinitely many primes.

We are now able to prove the main result of this section.

Theorem 2.8. *Let $D \equiv 0, 1 \mod 4$ be a nonzero integer. There exists a unique homomorphism $\chi : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$ such that $\chi([p]) = (D/p)$ for odd primes p not dividing D.*

Remark 2.9. We use the notation $(\mathbb{Z}/D\mathbb{Z})^*$ to denote the multiplicative group of integers modulo D, which consists of the positive integers coprime to D and less than D.

Proof. We claim that

$$\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right)$$

for $m \equiv n \mod D$ where m and n are positive odd integers and $D \equiv 0, 1 \mod 4$. We will omit the case when $D \equiv 1 \mod 4$, and assume it is true.
When $D \equiv 0 \mod 4, D \neq 0$, we can write the above expression as

$$\left(\frac{4^c k}{m}\right) = \left(\frac{4^c k}{n}\right)$$

where c is a positive integer, which is equivalent to

$$\left(\frac{k}{m}\right) = \left(\frac{k}{n}\right)$$

If k is odd, then we have already assumed the case when $k \equiv 1 \mod 4$ is true, and so we consider the case when $k \equiv 3 \mod 4$. Using a similar argument from above we find that the Jacobi symbols are equal and the exponents on each of the -1 terms are odd, so the statement is proven in this case. If $k \equiv 2 \mod 4$, we can write this as

$$\left(\frac{2}{m}\right)\left(\frac{a}{m}\right) = \left(\frac{2}{n}\right)\left(\frac{a}{n}\right)$$

where a is odd. Evaluating this using quadratic reciprocity and its supplements results in the following equivalent equation

$$(-1)^{\frac{m^2-1}{8}}\left(\frac{a}{m}\right) = (-1)^{\frac{n^2-1}{8}}\left(\frac{a}{n}\right)$$

The Jacobi symbols are equal for the same reasons as above, so we consider the exponents on the -1 term. We can write $n = m + xD$, and so on the left hand side we have

$$\frac{m^2-1}{8}$$

and on the right hand side we get

$$\frac{m^2-1}{8} + \frac{x^2D^2 + 2mxD}{8}$$

The second fraction on the right hand side can be written as

$$\frac{xD(xD+2m)}{8}$$

or

$$\frac{x4^c 2a(x4^c 2a + 2m)}{8}$$

due to the assumptions above. As c is positive this is just

$$x4^{c-1}a(x4^c2a+2m)$$

and because the last term is even we have that the two exponents have the same sign and the equation is true in this case. So we have proven

$$\left(\frac{D}{m}\right)=\left(\frac{D}{n}\right)$$

for $m\equiv n \mod D$ where m and n are positive odd integers and $D\equiv 0,1 \mod 4$. Now we will show that any class in $(\mathbb{Z}/D\mathbb{Z})^*$ contains an odd positive integer. Take $[x]\in(\mathbb{Z}/D\mathbb{Z})^*$ such that x is positive. If x is odd, then we are done. If x is even, then if $D\equiv 1 \mod 4$ we have $x+D$ is odd and in $[x]$, and we are done. If $D\equiv 0$ mod 4 then we have a contradiction as x and D are not coprime as they are both even. So any class in $(\mathbb{Z}/D\mathbb{Z})^*$ can be written as $[m]$ where m is an odd positive integer.
Take $\chi([m])=\left(\frac{D}{m}\right)$. Finally, the properties of the Jacobi symbol imply χ is a homomorphism, as

$$\chi([mn])=\left(\frac{D}{mn}\right)=\left(\frac{D}{m}\right)\left(\frac{D}{n}\right)=\chi([m])\chi([n])$$

Lastly, this homomorphism is unique as every class in $(\mathbb{Z}/D\mathbb{Z})^*$ contains a prime, which follows from Dirichlet's theorem. □

3. Quadratic Forms

As we will see later in the paper, Euler's convenient numbers are numbers that can be written in the form x^2+ny^2 for certain values of n. This expression is an example of a quadratic form, and we will spend the rest of this paper understanding the characteristics of these forms and their relationship to prime numbers.

We will first need to define some terms in order to begin a discussion of quadratic forms.

Definition 3.1. A binary integral quadratic form is a function

$$f(x,y)=ax^2+bxy+cy^2$$

where a,b,c are integers.

Definition 3.2. A binary integral quadratic form is primitive if its coefficients a,b,c are coprime.

In this paper, we will exclusively use primitive binary integral quadratic forms. We still need a way to reference integer solutions of these forms, which is necessary in our conversation of convenient numbers. The following definitions will assist us in that manner.

Definition 3.3. An integer m is said to be represented by a quadratic form $f(x,y)$ if there exist integers a,b such that $m=f(a,b)$. If a,b are coprime, we say m is properly represented by $f(x,y)$.

Definition 3.4. Two quadratic forms $f(x,y)$ and $g(x,y)$ are said to be equivalent if there exist integers p,q,r and s such that

$$f(x,y)=g(px+qy,rx+sy),\quad ps-qr=\pm1$$

If $ps - qr = 1$, we say that the two forms are properly equivalent.

The set of matrices of the form

$$\left\{ \begin{pmatrix} p & q \\ r & s \end{pmatrix} \mid \quad ps - qr = \pm 1 \right\}$$

can be shown to form a group, and this easily implies that equivalence is an equivalence relation. Similarly, proper equivalence is a equivalence relation as well. Now we will show that properly equivalent forms properly represent the same numbers.

Lemma 3.5. *Properly equivalent forms properly represent the same numbers.*

Proof. Let $f(x, y)$ and $g(x, y)$ be properly equivalent quadratic forms, and let m be properly represented by $f(x, y)$. So there exist x', y' coprime such that $m = f(x', y')$. There exist integers p, q, r, s such that $f(x, y) = g(px + qy, rx + sy), ps - qr = 1$. We have the matrix

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

transforms representations from $f(x, y)$ to $g(x, y)$; it follows that the inverse matrix

$$\begin{pmatrix} s & -q \\ -r & p \end{pmatrix}$$

transforms representations from $g(x, y)$ to $f(x, y)$. So $g(x, y) = f(sx-qy, -rx+py)$. Note that $ps - (-qr) = 1$. Then there exist x, y such that $x' = sx - qy$ and $y' = -rx + py$. Now if x and y have a common factor greater than 1 then so does x' and y'; so x and y are coprime and m is properly represented by $g(x, y)$.
Now let n be properly represented by $g(x, y)$. Using the same argument above, we have n is properly represented by $f(x, y)$, and the lemma is shown.

□

The proof for the statement that equivalent forms represent the same numbers is similar to the proof above, and is left as an exercise to the reader. We now have a method to determine if two quadratic forms represent or properly represent the same group of numbers. It may be helpful for our discussion to refer to a representative form. The following definitions will assist us in that goal.

Definition 3.6. The discriminant of a quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is defined to be $D = b^2 - 4ac$.

One may ask why we define the discriminant as such. To understand why, we must consider two quadratic forms $f(x, y)$ and $g(x, y)$, with discriminant D and D' respectively. Suppose that there exist integers p, q, r, s such that

$$f(x, y) = g(px + qy, rx + sy)$$

Then it can be shown that $D = (ps - qr)^2 D'$. This implies that forms that are equivalent to each other share the same discriminant.

Definition 3.7. A quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is said to be indefinite if its discriminant D is positive. If D is negative, then if a is positive we call the form positive definite, and if a is negative we call the form negative definite.

Definition 3.8. A primitive positive definite quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is said to be reduced if

$$|b| \leq a \leq c, \quad b \geq 0 \text{ if either } |b| = a \text{ or } a = c$$

Reduced forms are quite useful as a representative quadratic form; in fact, it is clear that the quadratic form x^2+ny^2 is reduced in the way above. However, there are other forms that are reduced not in this form, such as $2x^2+2xy+3y^2$.

Theorem 3.9. *Every primitive positive definite quadratic form is properly equivalent to a unique reduced form.*

Proof. Let $f(x,y)$ be a primitive positive definite quadratic form. Take $g(x,y) = ax^2+bxy+cy^2$ such that $g(x,y)$ is properly equivalent to $f(x,y)$ and $|b|$ is as small as possible. Observe that

$$g(x+dy,y) = ax^2+(2ad+b)xy+(ad^2+bd+c)y^2$$

is properly equivalent to $g(x,y)$; then if $a<|b|$ we can choose an integer d such that $2ad+b<|b|$; we then have a contradiction with our choice of b. So we have $a \geq |b|$. We obtain $c \geq |b|$ using a similar argument to the one above using the expression $g(x,ex+y)$. Now if $a>c$, we can use the quadratic form $g(-y,x)$ instead of $g(x,y)$; this form is properly equivalent to the latter and exchanges the coefficients a and c. We shall refer to this form as $r(x,y) = Ax^2+Bxy+Cy^2$, which now satisfies $|B| \leq A \leq C$. We have that $r(x,y)$ is reduced unless $B<0$ and either $|B|=A$ or $A=C$. In this case, we have $r'(x,y) = Ax^2-Bxy+Cy^2$ is reduced. Now we have to show that $r(x,y)$ and $r'(x,y)$ are properly equivalent to each other; if $|B|=A$ then $A=-B$ and $r(x+y,y)=r'(x,y)$, so the forms are properly equivalent, and if $A=C$ then $r(-y,x)=r'(x,y)$, thus the forms are properly equivalent and so $f(x,y)$ is properly equivalent to a reduced form.
We leave the proof of uniqueness to the reader. □

Genus theory is essential for distinguishing reduced forms from each other, as we will see in the next section.

4. Genus Theory

Definition 4.1. Two quadratic forms with discriminant D are in the same genus if they represent the same values in $(\mathbb{Z}/D\mathbb{Z})^*$. Similarly, the genus with respect to discriminant D of a set of numbers A consists of all quadratic forms with discriminant D that represent the values of $A \mod D$.

We will need to prove some lemmas regarding representations, as our discussion with convenient numbers is based on this fact.

Lemma 4.2. *Let $f(x,y)$ be a quadratic form, and m be an integer that $f(x,y)$ represents. Then m can be written as $m=n^2m'$, where n is an integer and m' is properly represented by $f(x,y)$.*

Proof. There exist x',y' such that $m=f(x',y')$. Let $g=\gcd(x',y')$. Then $m=f(ga,gb)$ where a and b are coprime. Then we have that $m=g^2f(a,b)$, and by defining $m'=f(a,b)$, the proof is shown. □

Lemma 4.3. *A quadratic form $f(x,y)$ properly represents an integer m if and only if $f(x,y)$ is properly equivalent to the form $mx^2+bxy+cy^2$.*

Proof. Assume m is properly represented by $f(x,y)$. Then there exist coprime integers p,r such that $f(p,r)=m$. There exist q,s such that $ps-qr=1$ as p and r are coprime, and we have that

$$f(px+qy,rx+sy) = f(p,r)x^2+(2apq+bps+bqr+2crs)xy+f(q,s)y^2$$

which is of the desired form. The converse is shown when we observe that $(1,0)$ properly represents m with the form $mx^2+bxy+cy^2$. □

Lemma 4.4. *Let $D \equiv 0,1 \mod 4$ be an integer and m be an odd integer coprime to D. Then m is properly represented by a primitive form of discriminant D if and only if D is a quadratic residue mod m.*

Proof. Let m be properly represented by a primitive form of discriminant D. Then by the above lemma the form is properly equivalent to $mx^2+bxy+cy^2$. Then we have

$$D = b^2 - 4mc$$

which implies

$$D \equiv b^2 \mod m$$

Now if D is a quadratic residue modulo m then there exists an integer b such that $D \equiv b^2 \mod m$. As m is odd assume b and D have the same parity (if they do not, replace b with $b+m$ above). As $D \equiv 0,1 \mod 4$ then $D \equiv b^2 \mod 4m$. There exists c such that $D = b^2 - 4mc$, thus $mx^2+bxy+cy^2$ represents m. As m is coprime to D we have b is coprime to m because of the statement above, so the quadratic form above is primitive and the proof is shown. □

The utility of our homomorphism $(\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$ will be shown if we define a certain type of reduced form, called the principal form. We will show that this form is connected to the kernel of our homomorphism.

Definition 4.5. Given a negative integer $D \equiv 0,1 \mod 4$, the principal form is defined to be

$$x^2 - \frac{D}{4}y^2 \quad D \equiv 0 \mod 4$$
$$x^2 + xy + \frac{1-D}{4}y^2 \quad D \equiv 1 \mod 4$$

Notice that when $D \equiv 0 \mod 4$, the principal form is x^2+ny^2, which is the form we will need to continue our conversation about convenient numbers.

Lemma 4.6. *Given $D \equiv 0,1 \mod 4$ is a negative integer, let $\chi : (\mathbb{Z}/D\mathbb{Z})^*$ be the homomorphism defined in Theorem 2.8, and let $f(x,y)$ be a quadratic form of discriminant D. Then the following statements are true:*

a) The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by the principal form of discriminant D form a subgroup $G \subset \ker(\chi)$.

b) The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by $f(x,y)$ form a coset of G in $\ker(\chi)$.

Proof. We will prove the case for when $D \equiv 0 \mod 4$, as our discussion depends on this case. The case when $D \equiv 1 \mod 4$ is left to the reader if they please.
First, we will show that for n represented by a quadratic form of discriminant D coprime to D, $[n] \in \ker(\chi)$. We can assume n is properly represented by a form of discriminant D, as we know $n = d^2n'$ where n' is properly represented by a quadratic form of discriminant D, and

$$\chi([n]) = \chi([d^2n']) = (\chi([d]))^2\chi([n']) = \chi([n'])$$

Then we know by Lemma 4.4 n is a quadratic residue modulo m. So there exists a such that $D \equiv a^2 \mod m$, and integer k such that $D = a^2 + km$. We know m is odd as it is coprime to D, so we have

$$\chi([m]) = \left(\frac{D}{m}\right) = \left(\frac{a^2 + km}{m}\right) = \left(\frac{a^2}{m}\right) = 1$$

From above, we know that $G \subset \ker(\chi)$, and the identity

$$(x^2 + ny^2)(z^2 + nw^2) = (xz \pm nyw)^2 + n(xw \mp yz)^2$$

shows closure under multiplication, and so G is a subgroup.
Before showing b), we claim that given any integer q, $f(x, y) = ax^2+bxy+cy^2$ properly represents numbers coprime to q. Let $q = p_1p_2...p_n$ be the prime factorization of q. We will partition the primes into three different sets:

$$\begin{aligned} A &= \{p_i \mid \gcd(p_i, a) = 1\} \\ C &= \{p_j \mid \gcd(p_i, c) = 1, p_j \notin A\} \\ B &= \{p_1, p_2, ...p_n\} \setminus (A \cup C) \end{aligned}$$

Then using the Chinese Remainder Theorem, we can create the following system of congruences which have solutions (x, y):

$$\begin{aligned} x &\equiv 1 \mod p_i, \quad y \equiv 0 \mod p_i \text{ for all } p_i \in A \\ x &\equiv 0 \mod p_j, \quad y \equiv 1 \mod p_j \text{ for all } p_j \in C \\ x &\equiv 1 \mod p_k, \quad y \equiv 1 \mod p_k \text{ for all } p_k \in B \end{aligned}$$

Now we claim that $f(x, y)$ and q are coprime. This is shown by contradiction: assume they have a common prime divisor p greater than 1. If $p \in A$, then $f(x, y) - bxy - cy^2 = ax^2$ is divided by p, which is a contradiction as $\gcd(a, p) = 1$ and $x \equiv 1 \mod p$. If $p \in C$ similarly we see p must divide $f(x, y) - ax^2 - bxy = cy^2$, which it cannot as $\gcd(c, p) = 1$ and $y \equiv 1 \mod p$. Lastly, if $p \in B$ then p divides both a and c, so it must also divide $f(x, y) - ax^2 - cy^2 = bxy$. As $f(x, y)$ is primitive it cannot divide b, and it cannot divide x and y as $x \equiv 1 \mod p$ and $y \equiv 1 \mod p$, completing the contradiction.
Now we apply this claim when $q = D = -4n$. Then using Lemma 4.3 we can assume $f(x, y) = a'x^2 + b'xy + c'y^2$ where a' is coprime to D. As $D = -4n$ and $D = b'^2 - 4a'c'$, it follows that b' is even and can be written as $b' = 2s$. We then use the identity

$$4af(x, y) = (2ax + by)^2 - Dy^2$$

for general quadratic forms and apply it to this form, which then implies

$$a'f(x, y) = (a'x + sy)^2 + ny^2$$

Using our observation above, we know $[a'] \in \ker(\chi)$, and so the values of $f(x, y)$ lie in the coset $[a']^{-1}G$. On the converse, if $[r] \in [a']^{-1}G$, then we have $a'r = z^2 + nw^2 \mod 4n$ for some z and w. Then from the above identity it is clear that $f(x, y) \equiv r \mod 4n$, or $f(x, y) \equiv r \mod D$, so $[a']^{-1}G$ consists only of the values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by $f(x, y)$, and the proof is shown. □

Theorem 4.7. *Let $D \equiv 0, 1 \mod 4$ be negative, and let $\chi : (\mathbb{Z}/D\mathbb{Z})^*$ be the homomorphism defined in Theorem 2.8. Then for an odd prime p not dividing D, $[p] \in \ker(\chi)$ if and only if p is represented by a reduced form of discriminant D.*

Proof. By definition, $\chi([p]) = 1$ if and only if p is a quadratic residue modulo D. Then p is properly represented by a quadratic form of discriminant D, and by Theorem 3.9, is represented by a reduced form of discriminant D. □

Theorem 4.8. *Let $D \equiv 0, 1 \mod 4$ be a negative integer, and let G be the subgroup defined in Lemma 4.7. If G' is a coset of G in $\ker(\chi)$ and p is an odd prime not dividing D, then $[p] \in G'$ if and only if p is represented by a reduced form of D in the genus of G'.*

Proof. The proof follows directly from Lemma 4.6 and Theorem 4.7. □

This concludes our discussion on genus theory. This framework is necessary in order to talk about convenient numbers as we will see that convenient numbers only have one reduced form per genus.

5. Convenient Numbers

Definition 5.1. A number n is a convenient number if it satisfies the following: Let m be an odd number coprime to n and properly represented by $x^2 + ny^2$. If there is a unique solution (x, y) for nonnegative x, y that represents m, then m is prime.

We now turn to Dirichlet composition, and will need a lemma in order to properly define it, as we will do subsequently. This will allow us to place a group structure on the classes of forms with a given discriminant.

Lemma 5.2. *Let $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = a'x^2 + b'xy + c'y^2$ be quadratic forms with discriminant D that satisfy $\gcd(a, a', \frac{b+b'}{2}) = 1$ (as b and b' have the same parity, $\frac{b+b'}{2}$ is an integer). Then there exists a unique integer $B \mod 2aa'$ such that*

$$B \equiv b \mod 2a$$
$$B \equiv b' \mod 2a'$$
$$B^2 \equiv D \mod 4aa'$$

The proof of the lemma depends on writing the congruences modulo $2aa'$ and, using the fact that the three numbers are coprime, we can find a unique solution. The details can be found in Chapter 3 of [2].

Definition 5.3. Given two quadratic forms $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y)$ with discriminant D that satisfy $\gcd(a, a', \frac{b+b'}{2}) = 1$, their Dirichlet composition is defined as the form

$$F(x,y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2$$

where B is the integer defined in Lemma 5.2 above.

Dirichlet composition is a specific case of composition that Gauss used, where we use integral bilinear forms to relate the product of two forms and a third form. Once again, the reader is suggested to look at Chapter 3 of [2] for more details.

$C(D)$ will represent the set of classes of primitive positive definite forms of discriminant D, and $h(D)$ is the number of classes there are for a given D, referred to as the class number. For reasons that will become clear immediately, $C(D)$ is referred to as the class group.

Theorem 5.4. *Let $D \equiv 0 \mod 4$. Dirichlet composition induces a well defined binary operation on $C(D)$ which makes it a finite Abelian group with order $h(D)$. Furthermore, the identity element is the class containing the principal form.*

Proof. Using the definition of Dirichlet composition, we leave it as an exercise to show that the operation between two classes is well defined, and it is simple to show that it is also commutative.
Now we will show that the identity element of $C(D)$ is the class containing the principal form. Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y)$ be the principal form of discriminant D. If $D \equiv 0 \mod 4$, then we have that $\gcd(a, 1, \frac{b}{2}) = 1$, and Dirichlet composition is defined for these two forms. We have that b satisfies the conditions in Lemma 5.2, and it follows that $f(x, y)$ is the Dirichlet composition of the two forms, and thus the class containing the principal form is the identity element. □

We will not prove it, but the reader is suggested to read page 144 of [3] for the details of the following classical lemma.

Lemma 5.5. *Let m be a positive odd number coprime to $n > 1$. Then the number of ways that m is properly represented by a reduced form of discriminant $-4n$ is*

$$2\prod_{p|m}\left(1 + \left(\frac{-n}{p}\right)\right)$$

Corollary 5.6. *Let m be properly represented by a primitive positive definite form $f(x, y)$ of discriminant $-4n$, where $n > 1$, and assume m is odd and coprime to n. Let r be the number of prime divisors of m. Then m is properly represented in exactly 2^{r+1} ways by a reduced form in the genus of $f(x, y)$.*

Proof. Two forms that represent m must be in the same genus as $f(x, y)$. Furthermore, for each of the prime factors p of m, we have p is coprime to n and therefore $-4n$. By Lemma 4.4, we have that

$$\left(\frac{-4n}{p}\right) = \left(\frac{-n}{p}\right) = 1$$

for all prime factors of m, and therefore by Lemma 5.2 we have that m is properly represented by $2 \cdot 2^r = 2^{r+1}$ ways. □

Lastly, we need one more classical theorem in order to prove our statement regarding convenient numbers.

Theorem 5.7. *Every genus of forms discriminant $-4n$ consists of a single class if and only if every class in $C(D)$ has order ≤ 2.*

The proof of this theorem encompasses a deeper study into genus theory as well as the structure of $C(D)$, so we will not prove it here. The details are given in Chapter 3 of [2].

Now we can prove our main result.

Theorem 5.8. *A positive integer n is a convenient number if and only if for forms of discriminant $-4n$, every genus consists of a single class.*

Proof. Assume that there is only one class per genus. If m is properly represented by x^2+ny^2 and $m=x^2+ny^2$ has a unique solution (x,y) for nonnegative x,y, then by the above corollary we have there are 2^{r+1} proper representations of m by this form. When restricting $x,y\geq 0$, we have 2^{r-1} proper representations of m that satisfy the above condition. If m has a unique representation we have $r=1$, and thus m is a prime power, p^a. If $a\geq 2$, then p^{a-2} has at least 2 proper representations, and it follows that m does not have a unique representation. Thus $a=1$ and m is prime, so n is a convenient number.
Now assume that n is convenient, and let $f(x,y)$ be a form with discriminant $-4n$. Define $g(x,y)$ to be the Dirichlet composition of $f(x,y)$ with itself, and without loss of generality we can assume $g(x,y)$ to be reduced. Assume $g(x,y)\neq x^2+ny^2$. Using class field theory, it can be shown that $f(x,y)$ represents infinitely many primes, the reader with experience in this topic is suggested to read [2]. With this in mind, let p and q be distinct odd primes represented by $f(x,y)$; it follows that pq is represented by $g(x,y)$. The identity

$$(ax^2+2bxy+cy^2)(az^2+2bzw+cw^2)=(axz+bxw+byz+cyw)^2+n(xw-yz)^2$$

which holds for forms with determinant $-4n$ shows that x^2+ny^2 also represents pq; Corollary 5.6 then implies that pq has 8 proper representations by reduced forms with discriminant $-4n$, and because at least 1 representation comes from $g(x,y)$, at most 7 come from x^2+ny^2. As one solution (x,y) where $x,y\geq 0$ is accompanied by 3 others, where the sign on x or y is changed, pq must be uniquely represented by x^2+ny^2 when the above restrictions are applied. But this contradicts n being convenient, so $g(x,y)=x^2+ny^2$. Using Theorem 5.7, the proof of the statement follows. □

There are additional methods to determine if a number is a convenient number, such as studying the structure of the class group, or even the class number. There are 65 convenient numbers that have been found through these various methods; indeed, Euler verified 18, 518, 809 is a prime number using the fact that 1848 is a convenient number and

$$18,518,809=197^2+1848(100)^2$$

This is quite an impressive feat for his time! Moreover, as convenient numbers have been used to find prime numbers, there is an interesting relationship between these numbers and the Riemann hypothesis: the list of 65 convenient numbers is complete if the Riemann hypothesis is true.

Acknowledgments

It is a pleasure to thank my mentor, Ishan Banerjee, for guiding me through this topic. Without his support I would not have been able to complete it. I would also like to thank Peter May for organizing this REU.

References

[1] Rousseau, G. On the Quadratic Reciprocity Law. https://stacky.net/files/115/RousseauQR.pdf
[2] David A. Cox. Primes of the Form x^2+ny^2. John Wiley and Sons. 1989.
[3] Landau, E. Vorlesungen über Zahlentheorie. Hirzel, Leipzig. 1927.