QUADRATIC RECIPROCITY, GENUS THEORY, AND PRIMES OF THE FORM $x^2 + ny^2$

DANIEL CHONG

ABSTRACT. A popular problem in number theory is the question of when a prime p can be written in the form $x^2 + ny^2$, with x, y and n integers and n positive. The full treatment of this problem necessitates an approach using class field theory; however, in this paper, we attempt to approach the problem by using a combination of quadratic reciprocity and Gauss' *genus theory* instead, providing an alternative, albeit admittedly more limited, perspective of this problem.

CONTENTS

1. QUADRATIC RECIPROCITY

Though it may not be apparent, the question of when a prime p can be written in the form $x^2 + ny^2$ is intricately related to the notion of quadratic reciprocity and the Legendre symbol. Thus, we begin this paper by first establishing what quadratic reciprocity is, then demonstrating how it relates to the problem at hand.

1.1. Quadratic Residues.

Definition 1.1 (Quadratic Residue)**.** Let n be an integer. Then, an integer q is called a quadratic residue mod n if there exists a integer x such that

$$x^2 \equiv q \pmod{n}$$

Date: September 7, 2016.

That is, q is a quadratic residue mod n if it is equivalent to a square modulo n.

Looking at the equation $p = x^2 + ny^2$, we note that for there to be integer solutions, we must have that $-n \equiv (x/y)^2 \pmod{p}$ since $\mathbb{Z}/p\mathbb{Z}$ is a field and p cannot possibly divide y. In other words, we require that $-n$ be a quadratic residue modulo p. This definition, in turn, motivates us to define what proves to be a rather useful tool:

Definition 1.2 (Legendre Symbol)**.** Let p be a prime number. Then, for an integer a, we define the Legendre symbol as:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \text{ and } p \nmid a; \\ -1 & \text{if } a \text{ is not a quadratic residue mod } p; \\ 0 & \text{if } p \mid a. \end{cases}$$

Thus, for any prime p to be written in the form $x^2 + ny^2$, we must have that $(-n/p) = 1$. Euler found that the Legendre symbol also satisfied the following criterion:

Lemma 1.3 (Euler's Criterion)**.** *Let p be an odd prime and let a be an integer relatively prime to p. Then,*

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

This lemma enables us to prove a few important facts about the Legendre symbol:

Corollary 1.4. *If p is an odd prime, then:*

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

Proof. This follows by plugging in -1 to Euler's criterion. □

Lemma 1.5. *If p is an odd prime, then:*

$$\left(\frac{2}{p}\right) = \frac{p^2-1}{8}.$$

Proof. Let $P = \frac{p-1}{2}$. Then, we note that:

$$1 = (-1)(-1), \qquad 2 = 2(-1)^2, \qquad 3 = (-3)(-1)^3, \qquad \ldots, \qquad P = (\pm P)(-1)^P.$$

Taking the product of all the equations, the overall LHS is equal to $P!$, while the RHS is a product of alternating positive/negative integers and a $(-1)^{1+2+\ldots+P} = (-1)^{P(P+1)/2}$ term. If we take both sides mod p, then since $2P = p - 1 \equiv -1 \pmod{p}$, $2(P-1) = p - 3 \equiv -3 \pmod{p}$, and so on, the RHS evaluates to $(-1)^{P(P+1)/2} \times 2 \times 4 \times \cdots \times 2(P-1) \times 2P = (-1)^{P(P+1)/2} \times 2^P P!$. Combining this all together:

$$P! \equiv (-1)^{P(P+1)/2} \times 2^P P! \pmod{p} \Leftrightarrow 2^P \equiv (-1)^{P(P+1)/2} \pmod{p},$$

and since $P(P+1)/2 = (p^2-1)/8$, the result follows from Euler's criterion. □

To make our definition of the Legendre symbol more robust, we introduce the following definition:

Definition 1.6 (Jacobi Symbol)**.** For any integer M and odd $m > 0$ relatively prime to it, we define the *Jacobi symbol* to be the product:

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

where $p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorization of m.

The following properties hold true for the Jacobi symbol:

Lemma 1.7. *For integers M, N and odd m, n relatively prime to them:*

$$\left(\frac{MN}{m}\right) = \left(\frac{M}{m}\right)\left(\frac{N}{m}\right), \qquad \text{when } M \equiv N \ (\text{mod } m);$$
$$\left(\frac{M}{mn}\right) = \left(\frac{M}{m}\right)\left(\frac{M}{n}\right).$$

Moreover, if $M \equiv N$ (mod m) then $\left(\frac{M}{m}\right) \equiv \left(\frac{N}{m}\right)$.

Proof. These are straightforward manipulations involving the Legendre symbol. □

Equipped with all of this new machinery, we move on to proving one of the key results in the area of quadratic reciprocity, which is aptly named:

1.2. **The Law of Quadratic Reciprocity.** Before we state exactly what is the law of quadratic reciprocity and prove it, we require a few preliminary results:

Theorem 1.8 (Wilson's Theorem)**.** *If p is an odd prime, then $(p-1)! \equiv -1$ (mod p).*

Proof. Consider the numbers $1, 2, \ldots, p-1$. We note that each of these $p-1$ numbers has an multiplicative inverse in $\mathbb{Z}/p\mathbb{Z}$. A number is equal to its multiplicative inverse if and only if $x^2 \equiv 1 \pmod p \Rightarrow x \equiv \pm 1 \pmod p$. Thus, when each of the other numbers are multiplied, they pair up to form units, meaning that:

$$(p-1)! \equiv 1 \times 2 \times \cdots \times (p-1) \equiv 1 \times (p-1) \equiv -1 \pmod p.$$

□

A natural result of this is the following corollary:

Corollary 1.9. *For any odd prime p, let $P = \frac{p-1}{2}$. Then,*

$$(P!)^2 \equiv (-1)^{P+1} \ (\text{mod } p)$$

Proof. This follows from Wilson's Theorem by:

$$\begin{aligned} -1 \equiv (p-1)! &\equiv P! \times (P+1) \times (P+2) \times \cdots \times (p-1) \\ &\equiv P! \times -P \times (-P+1) \times \cdots \times -1 \\ &\equiv (-1)^P (P!)^2 \pmod p. \end{aligned}$$

□

With these results, we are now able to prove the law of quadratic reciprocity:

Theorem 1.10 (Law of Quadratic Reciprocity)**.** *If p and q are odd primes, then:*

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

Proof. The following proof is due to Rosseau [3]. Let $P = \frac{p-1}{2}$, and let $Q = \frac{q-1}{2}$. Consider the group $((\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times)/U$, where $U = \{(1,1),(-1,-1)\}$. Let π denote the product of *all* elements in this quotient. To calculate the value of π, we must figure out ways to represent the cosets of U. Since taking this quotient group divides $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ into sets containing both of x and $-x$ for all $x \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$, it effectively divides it into two. There are three different ways that do so, splitting it into the cosets $(i,j)U$ such that $(i,j) \in$

(a) $S = \{(i,j) \mid i = 1,2,\ldots,p-1, j = 1,2,\ldots Q\}$.
(b) $T = \{(i,j) \mid i = 1,2,\ldots,P, j = 1,2,\ldots q-1\}$.
(c) $V = \{(k \pmod p), k \pmod q)) \mid k = 1,2,\ldots,\frac{pq-1}{2}$ and $\gcd(k,pq) = 1\}$.

The last result comes from the fact that $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \cong (\mathbb{Z}/pq\mathbb{Z})^\times$ by the Chinese Remainder Theorem.

To determine π, we examine each of these possibilities separately. Using the first representation, it can be easily verified that the product of all $(i,j) \in S$ is equal to

$$\left(((p-1)!)^Q, (Q!)^{p-1}\right).$$

Considering first the x-coordinate, note that by Wilson's Theorem:

$$((p-1)!)^Q \equiv (-1)^Q \pmod p$$

For the y-coordinate, by the corollary to Wilson's Theorem:

$$(Q!)^{p-1} = ((Q!)^2)^P \equiv (-1)^{(Q+1)P} \pmod q.$$

Hence, the product of all $(i,j) \in S$ is equivalent to $\left((-1)^Q, (-1)^{(Q+1)P}\right)$. An identical argument for when $(i,j) \in T$ shows that $\pi = \left((-1)^{(P+1)Q}, (-1)^P\right)U$.

In the case of the last representation, note that the set of all possible k are those such that $\gcd(k,pq) = 1 \Rightarrow \gcd(k,p) = 1$ and $\gcd(k,q) = 1$, with $k \leq \frac{pq-1}{2}$. That is, k can be any one of the first $\frac{pq-1}{2}$ integers excluding all multiples of p and q. Note that we can write this set as some $X \setminus Y$, where

$$X = \{1,2,\ldots,p-1,p+1,p+2,\ldots,2p-1,2p+1,\ldots,Qp+1,\ldots,Qp+P\},$$

and $Y = \{q, 2q, \ldots Pq\}$. Note that X is merely the first $Qp + P = \frac{pq-1}{2}$ integers without the multiples of p, and Y is the set of all multiples of q less than $Qp + P$. Thus, considering one coordinate at a time, the product of all such $k \pmod p$ is equal to:

$$\frac{(Qp+P)!}{(P!)q^P \times (Q!)p^Q} \equiv \frac{((p-1)!)^Q \times P!}{(P!)q^P} = \frac{((p-1)!)^Q}{q^P} \equiv \frac{(-1)^Q}{q^P} \pmod p.$$

By Euler's criterion, $q^P \equiv (q/p) \pmod p$, meaning that the x-coordinate is equivalent to $(-1)^Q(q/p) \pmod p$. We can repeat the same argument for the y-coordinate to demonstrate that it is equivalent to $(-1)^P\left(\frac{p}{q}\right) \pmod q$. Thus, overall, we have that $\pi = \left((-1)^Q\left(\frac{q}{p}\right), (-1)^P\left(\frac{p}{q}\right)\right)U$.

We can now compare how π evaluates for the three different representations. Looking at the first and third in particular, we note that:

$$\left((-1)^Q, (-1)^{(Q+1)P}\right) = \pm\left((-1)^Q\left(\frac{q}{p}\right), (-1)^P\left(\frac{p}{q}\right)\right).$$

If we compare the x-coordinates, we note that this ± is precisely equal to (q/p). The y-coordinate then tells us that:

$$(-1)^{(Q+1)P} = (-1)^P \left(\frac{p}{q}\right)\left(\frac{q}{p}\right),$$

which means that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{PQ} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

which is precisely the law of quadratic reciprocity. □

While the law of quadratic reciprocity itself does not shed much light on the problem of when a prime p can be written in the form $x^2 + ny^2$, it does enable us to prove a few additional facts about the Jacobi symbol that will come into use at a later stage:

Lemma 1.11. *For an integer M and odd m relatively prime to it:*

$$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2};$$
$$\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8};$$
$$\left(\frac{M}{m}\right) = (-1)^{(M-1)(m-1)/4}\left(\frac{m}{M}\right).$$

Proof. Suppose r and s are odd. Then, $r, s \equiv 1, 3 \pmod 4$. It is a straightforward case-by-case calculation to show that if $r \equiv s \pmod 4$, then $r + s \equiv rs + 1 \equiv 2 \pmod 4$, and that if $r \not\equiv s \pmod 4$, then $r + s \equiv rs + 1 \equiv 0 \pmod 4$. Either way, we have that

$$r + s \equiv rs + 1 \pmod 4 \Rightarrow \frac{r-1}{2} + \frac{s-1}{2} \equiv \frac{rs-1}{2} \pmod 2. \tag{1.12}$$

It is also easy to verify that for odd r:

$$r^2 \equiv \begin{cases} 1 \pmod{16} & \text{if } r \equiv \pm 1 \pmod{16}, \\ 9 \pmod{16} & \text{if } r \equiv \pm 3 \pmod{16}, \\ 9 \pmod{16} & \text{if } r \equiv \pm 5 \pmod{16}, \\ 1 \pmod{16} & \text{if } r \equiv \pm 7 \pmod{16}. \end{cases}$$

If $r^2 \equiv s^2 \pmod{16}$, then it can easily be verified that $r^2s^2 + 1 \equiv r^2 + s^2 \equiv 2 \pmod{16}$, whereas if $r^2 \not\equiv s^2 \pmod{16}$, we have $r^2s^2+1 \equiv r^2+s^2 \equiv 10 \pmod{16}$. Thus, either way, we have that:

$$r^2 + s^2 \equiv r^2s^2 + 1 \pmod{16} \Rightarrow \frac{r^2-1}{8} + \frac{s^2-1}{8} \equiv \frac{r^2s^2-1}{8} \pmod 2. \tag{1.13}$$

For the first equation in the lemma, let $m = p_1^{e_1} \cdots p_k^{e_k}$. By Corollary 1.4,

$$\left(\frac{-1}{m}\right) = \prod_{i=1}^{k} \left(\frac{-1}{p_i}\right)^{e_i} = (-1)^{\sum e_i(p_i-1)/2}.$$

Applying (1.12) inductively, the power of the -1 in the above equation is:

$$\sum_{i=1}^{k} \frac{e_i(p_i-1)}{2} \equiv \frac{\prod p_i^{e_i} - 1}{2} = \frac{m-1}{2} \pmod 2.$$

Thus, $(-1/m) = (-1)^{\sum e_i(p_i-1)/2} = (-1)^{(m-1)/2}$, as desired.

The proof for the second equation is identical, except we use Lemma 1.5 and (1.13) instead. To prove the last equation, let $q_1 \cdots q_l$ be the prime factorization of M, and let $p_1 \cdots p_k$ be the prime factorization of m. Then, the last equation is merely a result of the law of quadratic reciprocity, following from:

$$\left(\frac{M}{m}\right)\left(\frac{m}{M}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right) = (-1)^{\sum\sum \frac{p_i-1}{2}\frac{q_j-1}{2}},$$

and hence

$$\sum_{i=1}^{k}\sum_{j=1}^{l}\frac{p_i-1}{2}\frac{q_i-1}{2} \equiv \frac{M-1}{2}\sum_{i=1}^{k}\frac{p_i-1}{2} \equiv \frac{M-1}{2}\frac{m-1}{2} \pmod 2.$$

□

Now that we've established these facts about the Legendre and Jacobi symbols, we can take a step back and re-examine what it means for a prime p to be of the form $x^2 + ny^2$. To do so, we introduce the notion of quadratic forms, which is central to genus theory.

2. Quadratic Forms

We now attempt to generalize the problem of when a prime p can be written in the form $x^2 + ny^2$ in order to look at it from a more distanced, yet nuanced perspective. Doing so requires the introduction of a new concept—quadratic forms.

2.1. Quadratic Forms.

Definition 2.1. A *quadratic form* is a polynomial of the form $ax^2+bxy+cy^2$, where a, b, c, x, y are integers. Its *discriminant* D is defined to be the integer $D = b^2-4ac$. Moreover, if a, b, c are relatively prime, then the form is said to be *primitive.*

Definition 2.2. An integer m is said to be *represented* by a form $f(x, y)$ if $m = f(x, y)$ for some $x, y \in \mathbb{Z}$. If the x, y can be made relatively prime, then we say m is *properly represented* by $f(x, y)$.

Thus, our original problem is simply the question of when a prime p can be properly represented by the form x^2+ny^2. However, these definitions in themselves don't add much to the discussion. Rather, the importance of quadratic forms comes in how they can be divided into different equivalence classes depending on what they represent. This motivates the following definition:

Definition 2.3. We say that two forms $f(x, y)$ and $g(x, y)$ are *equivalent* if there are integers p, q, r, s with

$$ps - qr = \pm 1$$

such that:

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

We say the forms are *properly equivalent* if $ps - qr = 1$.

Note that the $ps-qr$ in Definition 2.3 is the determinant of the matrix $A = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$. Since we require that $ps-qr = \pm 1$, A is an element of $GL(2, \mathbb{Z})$, making this notion of "equivalence" a reflexive, transitive, and symmetric relation.

Whether two forms are equivalent is also strongly related to their discriminants.

If the forms $f(x,y)$ with discriminant D and $g(x,y)$ with discriminant D' are equivalent with $f(x,y)=g(px+qy,rx+sy)$, it is easy to verify that $D=(ps-qr)D'$. Thus, properly equivalent forms have the same discriminant. We now introduce a lemma to demonstrate how useful this notion of equivalence is:

Lemma 2.4. *A form $f(x,y)$ properly represents an integer m if and only if $f(x,y)$ is properly equivalent to the form $mx^2+Bxy+Cy^2$ for some $B,C\in\mathbb{Z}$.*

Proof. First, suppose that $f(x,y)=ax^2+bxy+cy^2$ properly represents m. Then, there are integers p,r relatively prime such that $m=f(p,r)$. We want to identify some $q,s\in\mathbb{Z}$ with $ps-qr=1$ such that $mx^2+Bxy+Cy^2=f(px+qy,rx+sy)$. Note that

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

Since $m=f(p,r)$, if we let $B=2apq+bps+bqr+2rs$ and $C=f(q,s)$, then we are done. Next, suppose that $f(x,y)$ is properly equivalent to the form $mx^2+Bxy+Cy^2$, with $f(px+qy,rx+sy)=mx^2+Bxy+Cy^2$. Note that when $x=1$ and $y=0$, we have that $f(p,r)=m$, and since $ps-qr=1\Rightarrow\gcd(p,r)=1$, we are done. □

While we seem to be moving further and further from our initial question, the following lemma demonstrates the relationship between our previous work on quadratic residues and the representation of numbers by forms:

Lemma 2.5. *Let $D\equiv 0,1\pmod 4$, and let m be an odd number relatively prime to D. Then, m is properly represented by a form with discriminant D if and only if D is a quadratic residue mod m.*

Proof. Suppose that m is properly represented by a form $f(x,y)$ with discriminant D. By Lemma 2.4, we can select this form to be $mx^2+Bxy+Cy^2$, which also has discriminant D. Thus, $D=B^2-4mC\Rightarrow D\equiv B^2\pmod m$.

Now, suppose that D is a quadratic residue mod m (that is, $m\mid D-b^2$ for some $b\in\mathbb{Z}$). Since m is odd, we have that b can be selected to be of the same parity as m (if b is of opposite parity, replace b with $b+m$). If $D\equiv 0\pmod 4$, then $b^2\equiv 0\pmod 4$ for all b, and if $D\equiv 1\pmod 4$, then $b^2\equiv 1\pmod 4$. Thus, in either case, we have that $D\equiv b^2\pmod 4\Rightarrow 4\mid D-b^2$. Since $\gcd(m,4)=1$, we thus have that $4m|D-b^2\Rightarrow D=b^2-4ma$ for some $a\in\mathbb{Z}$. Then, the form $mx^2+bxy+ay^2$ properly represents m and has discriminant D. □

Note that the form x^2+ny^2 is a form with discriminant $-4n$, and since p is an odd prime, then the lemma demonstrates that any p is properly represented by x^2+ny^2 if and only if $-4n$ is a quadratic residue mod p. To simplify matters even further, we note that the lemma gives rise to the following corollary:

Corollary 2.6. *If n is an integer and p is an odd prime that does not divide n, then $\left(\frac{-n}{p}\right)=1$ if and only if p is represented by a form with discriminant $-4n$.*

Proof. Since p is an odd prime, $-4n$ is a quadratic residue mod p if and only if $\left(\frac{-4n}{p}\right)=\left(\frac{-n}{p}\right)=1$. Thus, this is merely the case of Lemma 2.5 when $D=-4n$. □

Thus, we've demonstrated once again that $(-n/p)=1$ is not only a consequence, but also a prerequisite for p to be of the form x^2+ny^2.

We now attempt to narrow down our focus among all the equivalence classes of forms. Let D be the discriminant of the form $f(x,y) = ax^2 + bxy + cy^2$. Then, one can easily verify that:

$$4af(x,y) = (2ax + by)^2 - Dy^2 \tag{2.7}$$

We see that the range of $f(x,y)$ depends on a and D. If D is positive, then $f(x,y)$ will span both the positive and negative integers, whereas if D is negative, then $f(x,y)$ will either span only the positive integers ($a > 0$) or only the negative integers ($a < 0$). This, in turn, motivates the following definition:

Definition 2.8. Let D be the discriminant of a form $f(x,y)$. If $D > 0$, we say that $f(x,y)$ is *indefinite*. If $D < 0$ and its leading coefficient is positive, then we say $f(x,y)$ is *positive definite*. If its leading coefficient is negative, we say it's *negative definite*.

It is clear that the form $x^2 + ny^2$ is a positive definite one. Keeping this in the back of our minds, we conclude this introduction to quadratic forms with an interesting fact that will become of use later on:

Lemma 2.9. *For any primitive form $f(x,y)$ and integer M, $f(x,y)$ represents an infinity of numbers relatively prime to M.*

Proof. Let $f(x,y) = ax^2 + bxy + cy^2$. We first prove that for any given prime p, $f(x,y)$ can represent an infinity of numbers not divisible by p. Since $f(x,y)$ is primitive, no prime p can divide all three of a, b, c, or else $f(x,y)$. There are three possibilities:

1. If $p \nmid a$, then if we select an x not divisible by p and a number y divisible by p, then $f(x,y)$ will represent a number not divisible by p.
2. Likewise, if $p \nmid c$, we select an x divisible by p and a y not divisible by p.
3. In the case where $p \nmid b$ instead, if x and y are not divisible by p, then $f(x,y)$ will represent a number not divisible by p.

Thus, for any prime p, $f(x,y)$ can represent an infinity of numbers not divisible by p. Note that we have reduced this problem to a series of simple congruences—thus, in the case when M is composite, we merely have to solve for these congruences for x and y with respect to all of M's prime factors. By the Chinese Remainder Theorem, there are infinitely many such solutions, meaning that $f(x,y)$ represents an infinite number of integers relatively prime to M. □

The next step in the study of quadratic forms is to classify the different equivalence classes of forms even further. In order to do so, we require the introduction of reduced forms.

2.2. Lagrange's Theory of Reduced Forms.

Definition 2.10. Let $f(x,y) = ax^2 + bxy + cy^2$ be a primitive, positive definite form. Then, if $|b| \leq a \leq c$ and $b \geq 0$ if either $|b| = a$ or $a = c$, then we say $f(x,y)$ is a *reduced* form.

The utility of reduced forms stems from the fact that each of the equivalence classes, as the following proposition demonstrates, contains some reduced form. This enables us to reference the different classes with something more concrete overall.

Proposition 2.11. *Every primitive, positive definite form is properly equivalent to some unique reduced form.*

Proof. First, we show that every primitive, positive definite form is properly equivalent to a reduced form. For any form that we start with, we replace it with a form $f(x, y) = ax^2 + bxy + cy^2$ equivalent to it with the lowest value of $|b|$. Consider the form

$$g(x, y) = f(x + my, y) = ax^2 + (2am + b)xy + (am^2 + c)y^2$$

Suppose $a < |b|$. Note that $g(x, y)$ is properly equivalent to $f(x, y)$. However, since $a < |b|$, it is possible to pick an m such that $|2am + b| < |b|$, leading us to a contradiction. Hence, we must have that $a > |b|$. If $a > |b|$, then $g(x, y)$ shows that $|b| < c$ as well. In order to get that $a \leq c$, note that if $c < a$, we can replace $f(x, y)$ with $f(y, -x)$ if necessary.

Now, suppose that $|b| = a$. If $b < 0$, this means that $b = -a$ and $f(x, y)$ is not reduced. Then, we can substitute it with the form $f(x + y, y)$. Similarly, if $a = c$ but $b < 0$, then we can substitute $f(x, y)$ with the form $f(-y, x)$. Thus, we have that all primitive, positive definite forms are properly equivalent to some reduced form.

The next step we have to perform is to show that this reduced form is unique. Suppose that $f(x, y)$ is properly equivalent to another reduced form, $g(x, y) = dx^2 + exy + fy^2$. WLOG, suppose that $a \geq d$. Clearly, $g(x, y)$ properly represents d, meaning that $f(x, y)$ properly represents d as well. Thus, for some $p, q \in \mathbb{Z}$, we have that:

$$d = f(t, u) \geq a(t^2 + u^2) + btu \geq a(t^2 + u^2) - a|tu| \geq a|tu|.$$

Thus, since $a \geq d$, we must have that $|tu|$ is equal to either 0 or 1.

Before we consider cases, we recall that since $f(x, y)$ and $g(x, y)$ are properly equivalent, we have that $g(x, y) = f(px + qy, rx + sy)$ for some $p, q, r, s \in \mathbb{Z}$ with $ps - qr = 1$. It is easy to verify that:

$$g(x, y) = f(p, r)x^2 + (2apq + bps + bqr + 2crs)xy + f(q, s)y^2. \tag{2.12}$$

First, suppose that u is 0. Then, $d = f(t, 0) = at^2$, meaning that $t^2 = 1$ and, in turn, that $a = d$. Then, by (2.12), the leading coefficient of $g(x, y)$ is $f(p, r) = d = a$. We note that a is represented by $f(x, y)$ precisely when $x = \pm 1, y = 0$. Thus, in this case, we must have that $p = \pm 1, r = 0$, and also that $ps - qr = ps = 1$. Thus, the coefficient of xy in (2.12) is equal to

$$e = 2apq + bps + bqr + 2crs = 2apq + bps = b \pm 2aq.$$

Since $g(x, y)$ is reduced, it is necessary that $|e| \leq d$, but from the previous equation, this can only happen if either $q = 0$, which would imply that $f(x, y) = g(x, y)$, or if $q = \mp 1$ and $b = a$, in which case $e = -a = -d < 0$, which is an impossible result since $g(x, y)$ is reduced. Thus, when $u = 0$, $f(x, y)$ is unique. The proof for when $t = 0$ instead is essentially identical.

The last case that we have to consider is when $|tu| = 1$. Then, the inequality $d \geq a|tu|$ implies that $d = a$, and we once again apply the argument used when $u = 0$ to demonstrate that $f(x, y)$ must be unique. □

Note that for any reduced $f(x, y) = ax^2 + bxy + cy^2$ with discriminant $D = b^2 - 4ac$, we have that $b^2 \leq a^2$ and $a \leq c$, meaning that:

$$-D = 4ac - b^2 \leq 4a^2 - a^2 = 3a^2,$$

which implies that $0 < a < \sqrt{-D}/3$. This means that a can only take on a finite number of values, and since $|b| < a$, this applies to b as well. Holding D fixed, we observe that this also applies to c. Thus, there are only finitely many reduced forms with discriminant D, which, according to Proposition 2.11, means that there are only a finite number of equivalence classes of forms with discriminant D. This motivates the following definition:

Definition 2.13. If two forms are properly equivalent, we say that they are of the same *class*. For any integer D, we let $h(D)$, known as the *class number*, denote the number of classes of primitive positive definite forms with discriminant D.

The following lemma essentially follows by definition:

Lemma 2.14. *Fix $D < 0$. Then, $h(D)$ is finite and equal to the number of reduced forms with discriminant D.*

These results are very powerful in the sense that we've essentially established that there are only finitely many classes of forms with discriminant D. By looking at the interactions between these classes and their relation to each other, we can shed further light on our initial problem. Before we do that, however, we rephrase one of our earlier lemmas in a different light:

Corollary 2.15. *For any positive integer n and odd prime p that does not divide n, we have that $(-n/p) = 1$ if and only if p is represented by one of the $h(-4n)$ reduced forms with discriminant $-4n$.*

Proof. This is merely a restatement of Lemma 2.5 in light of Proposition 2.11. □

We now move on to examining another aspect of quadratic reciprocity.

2.3. The Homomorphism χ and Quadratic Reciprocity.

We take a moment to detach ourselves from the theory of forms and look at another important application of the Legendre symbol (which we will, in fact, show is actually related to the theory of forms.)

Theorem 2.16. *Let $D \equiv 0, 1 \pmod 4$ be a non-zero integer. Then, there is a unique homomorphism $\chi : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ that maps any odd prime p not dividing D to (D/p). Moreover,*

$$\chi([-1]) = \begin{cases} 1 & \text{when } D > 0, \\ -1 & \text{when } D < 0. \end{cases}$$

and if $D \equiv 1 \pmod 4$,

$$\chi([2]) = \begin{cases} 1 & \text{if } D \equiv 1 \pmod 8), \\ -1 & \text{if } D \equiv 5 \pmod 8). \end{cases}$$

Proof. Let m and n be odd and positive integers, and let $m \equiv n \pmod D$. We prove that $(D/m) = (D/n)$ for all such m, n. First, suppose that $D \equiv 1 \pmod 4$ and $D > 0$. Then, by Lemma 1.11, we have that:

$$\left(\frac{D}{m}\right) = (-1)^{(D-1)(m-1)/4}\left(\frac{m}{D}\right)$$

and likewise for n. Since $m \equiv n \pmod D$, we have $(m/D) = (n/D)$. Moreover, since $D \equiv 1 \pmod 4$, it follows that the exponent of -1 is equivalent to $0 \pmod 2$. Thus, when $D \equiv 1 \pmod 4$ and $D > 0$, we have that $(D/m) = (D/n)$. Now, suppose D is negative. We note that $(D/m) = \left(\frac{-1}{m}\right)(|D|/m)$ by Lemma 1.7, and $(D/m) = (D/n)$ follows from part (a) of Lemma 1.11. If $D \equiv 0 \pmod 4$ instead, then we note that $(D/m) = (2/m)(k/m)$ where $D = 2k$. Repeating this until $k \equiv 1 \pmod 4$, $(D/m) = (D/n)$ follows from part (b) of Lemma 1.11 once again.

We note that every class in $(\mathbb{Z}/D\mathbb{Z})^\times$ can be written as $[m]$, where m is some odd, positive integer. This follows from the fact that if D is even, then $\gcd(m, D) \geq 2$, and hence $m \notin (\mathbb{Z}/D\mathbb{Z})^\times$. If D is odd, then we can replace m with $m + D$ if m is even. Thus, we can define χ to be the mapping on $(\mathbb{Z}/D\mathbb{Z})^\times$ to $\{\pm 1\}$ that sends $[m]$ to (D/m). To check that χ is well-defined, note that we have demonstrated that $m \equiv n \pmod D \Rightarrow (D/m) = (D/n)$. Moreover, by Lemma 1.7, we also have that for any m, n that are odd, positive integers, $\chi([mn]) = (D/mn) = (D/m)(D/n) = \chi([m])\chi([n])$, demonstrating that χ is a homomorphism. The fact that $\chi([p]) = (D/p)$ for any odd prime p follows from definition.

Let $D = p_1 \cdots p_k$ be the prime factorization for D. Note that when $D > 0$,

$$\chi([-1]) = \prod_{i=1}^{k} \left(\frac{p_i}{p_i - 1}\right) = 1.$$

On the other hand, when $D < 0$,

$$\chi([-1]) = \left(\frac{-p_1}{p_1 - 1}\right) \prod_{i=2}^{k} \left(\frac{p_i}{-1}\right) = \left(\frac{-1}{p_1 - 1}\right) \prod_{i=2}^{k} \left(\frac{p_i}{-1}\right) = -1$$

as desired. The last equation follows from the fact that since D is odd,

$$\chi([2]) = \left(\frac{D}{D+2}\right) = (-1)^{(D-1)(D+1)/4} \left(\frac{2}{D}\right) = (-1)^{(D^2-1)/4 + (D^2-1)/8}.$$

Evidently, $\frac{D^2-1}{4} \equiv 0 \pmod 4$, meaning that it is equivalent to $0 \pmod 2$. On the other hand,

$$\frac{D^2 - 1}{8} \equiv \begin{cases} 0 \pmod 2 & \text{if } D \equiv 1 \pmod 8, \\ 1 \pmod 2 & \text{if } D \equiv 5 \pmod 8. \end{cases}$$

The statement follows. □

The relationship between the homomorphism χ and the theory of forms is summarized by the following theorem:

Theorem 2.17. *Let D and χ be as in Theorem 2.16, and let $D < 0$. Then, for any odd prime p not dividing D, $[p] \in \ker(\chi)$ if and only if p is represented by one of the $h(D)$ reduced forms with discriminant D.*

Proof. We note that from the previous theorem, a prime p is in the kernel of χ, by definition, if and only if $(D/p) = 1$, which happens if and only if p can be represented by a primitive, positive definite form with discriminant D by Lemma 2.5. This, in turn, happens if and only if the form is properly equivalent one of the $h(D)$ reduced forms with discriminant D by Proposition 2.11. □

We are now well-equipped to move on to Genus theory, which offers a better perspective of how quadratic reciprocity might relate to the problem at hand.

3. Genus Theory

Genus theory, developed by Lagrange, looks more specifically at exactly what forms which represent the same values have in common. The theory derives its name from the following definition.

Definition 3.1. Fix $D < 0$. If two primitive, positive definite forms with discriminant D represent the same values in $(\mathbb{Z}/D\mathbb{Z})^\times$, then we say they are in the same *genus* (plural: *genera*).

Note that as a basic result of this, equivalent forms are all in the same genus since they represent the same numbers. We move on to prove other results in genus theory.

3.1. Fundamentals of Genus Theory.

Definition 3.2. Fix $D < 0$, and let $D \equiv 0, 1 \pmod 4$. Then, we define the *principal form* to be:

$$\begin{cases} x^2 - \frac{D}{4}y^2, & \text{if } D \equiv 0 \pmod 4; \\ x^2 + xy + \frac{1-D}{4}y^2, & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

It is easy to verify that principal forms, as defined above, are reduced forms with discriminant D. It is also easy to verify that the form $x^2 + ny^2$ is, in fact, a principal form with discriminant $D = -4n$. The following lemma investigates the relationship between the previously-introduced homomorphism χ and the genus theory.

Lemma 3.3. *Let D and χ be as defined in Theorem 2.17. Then, all elements in $(\mathbb{Z}/D\mathbb{Z})^\times$ that can be represented by the principal form of discriminant D form a subgroup H in* $\ker(\chi)$.

Proof. We prove that any integer m represented by a form $f(x, y)$ can be written in the form d^2m', where $f(x, y)$ properly represents m'. Let $f(p, q) = m$ for some p and q such that $\gcd(p, q) = d$. Then, we can write $p = kd$, and $q = ld$. Note that since $\gcd(p, q) = d$, we have that $\gcd(k, l) = 1$. It is a straightforward calculation to show that $f(p, q) = d^2 f(k, l)$, and since $f(x, y)$ properly represents $m' = f(k, l)$, we are done.

For any $m \in (\mathbb{Z}/D\mathbb{Z})^\times$, by our earlier result, we have that $\chi([m]) = \chi([d^2m']) = (\chi([d]))^2\chi([m']) = \chi([m'])$. Thus, for the purposes of our proof, we can assume that any $m \in H$ is properly represented by $f(x, y)$, which, in turn, means that D is a quadratic residue mod m by Lemma 2.5. Thus, we can write $D = b^2 - km$, where b and k are integers. When m is odd, by Lemma 1.7 we have that:

$$\chi([m]) = \left(\frac{D}{m}\right) = \left(\frac{b^2 - km}{m}\right) = \left(\frac{b^2}{m}\right) = \left(\frac{b}{m}\right)^2 = 1.$$

The case when m is even is slightly more complicated. We first prove that if m is even, then $D \equiv 1 \pmod 8$. By Lemma 2.4, if a form with discriminant D properly represents an even integer $2k$, then we must have that $D = B^2 - 8kC$. Hence, $D \equiv B^2 \pmod 8$. It is easily verified by checking on a case-by-case basis that $D \equiv 1 \pmod 4$, along with the above fact, implies that $D \equiv 1 \pmod 8$.

Let m be an integer relatively prime to D, and suppose it can be properly represented by a form with discriminant D. If m is even and $m = 2^k m'$ for some odd integer m', then the above shows that $D \equiv 1 \pmod 8$. Thus, by our remark following Theorem 2.16, $\chi([m]) = \chi([2^k m']) = (\chi([2]))^k \chi([m']) = \chi([m'])$. Since m' is odd, our previous argument demonstrates that $[m] \in \ker(\chi)$. Moreover, since any form with discriminant D is properly equivalent to its respective principal form, by Lemma 2.4, we note that the above result also holds true for principal forms. Thus, any element of H is mapped to the identity under χ, meaning that $H \subset \ker(\chi)$.

At this stage, we still need to prove that H is a subgroup. When $D \equiv 0 \pmod 4$, note the identity:

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

Hence, when $D \equiv 0 \pmod 4$, H is closed under multiplication, and since it inherits the rest of the group properties, this shows that H is a subgroup. On the other hand, when $D \equiv 1 \pmod 4$, it is a straightforward calculation to show that:

$$4\left(x^2 + xy + \frac{1-D}{4}y^2\right) \equiv (2x+y)^2 \pmod D.$$

Let $G \subset (\mathbb{Z}/D\mathbb{Z})^\times$ be the subgroup of squares in $(\mathbb{Z}/D\mathbb{Z})^\times$. What the previous equation demonstrates is that any $m = k^2 \in G$ is represented by the form $f(k, 0)$, since $D \equiv 1 \pmod 4$ and $4(f(k,0)) \equiv (2k)^2 \pmod D \Rightarrow f(k,0) \equiv k^2 \pmod D$. Thus, $H = G$, and since the subgroup of squares is closed under multiplication, H is also a subgroup when $D \equiv 1 \pmod 4$. □

This lemma enables us to prove further results regarding the nature of χ.

Lemma 3.4. *Let D, H, and χ be defined as previously, and let $f(x, y)$ be a primitive, positive definite form of discriminant D. Then, the elements in $(\mathbb{Z}/D\mathbb{Z})^\times$ that are represented by $f(x, y)$ form a coset of H in* $\ker(\chi)$.

Proof. Suppose that $D = -4n$. From Lemma 2.9, we note that $f(x, y)$ can represent an infinity of numbers relatively prime to $4n$. Applying Lemma 2.4, this means that we can set $f(x, y) = ax^2 + bxy + cy^2$, where $\gcd(a, 4n) = 1$. Since $f(x, y)$ satisfies $D = b^2 - 4ac = -4n$, this must mean that b is even and can be written as $2b'$. Thus, plugging this into (2.7), we have that:

$$af(x, y) = (ax + b'y)^2 + ny^2.$$

Since $\gcd(a, 4n) = 1$, the above statement shows that the numbers that $f(x, y)$ represents in $(\mathbb{Z}/4n\mathbb{Z})^\times$ are a subset of the coset $[a]^{-1}H$. On the other hand, for any $[c] \in [a]^{-1}H$, we must have that $ac \equiv z^2 + nw^2 \pmod{4n}$, meaning that $[a]^{-1}H$ is a subset of the values represented by $f(x, y)$ in $(\mathbb{Z}/D\mathbb{Z})^\times$. Thus, the two sets are equal.

Now, suppose instead that $D \equiv 1 \pmod 4 \Leftrightarrow D = -4n + 1$. Since $D = b^2 - 4ac$, we must have that $b^2 \equiv 1 \pmod 4$, meaning that b must be odd. Thus, we can write $b = 2m + 1$ for some m. It is easy to verify from (2.7) that:

$$af(x, y) = (ax + my)^2 + (am + my)y + ny^2$$

The remainder of the proof is identical to that of when $D \equiv 0 \pmod 4$ □

What this lemma implies is that the different genera form different and distinct cosets in $(\mathbb{Z}/D\mathbb{Z})^\times$. This motivates the following definition:

Definition 3.5. Let D, χ, H be as defined previously. Let H' be any coset of H. Then, the *genus* of H' consists of all forms with discriminant D that represent the elements of H'.

With this in mind, we can restate Theorem 2.17 in a different form:

Theorem 3.6. *Let D, χ, H be defined as earlier. If H' is a coset of H and p is an odd prime not dividing D, then $[p] \in H'$ if and only if p is represented by a form in the genus of H'.*

We now move on to a discussion of class groups, which will, in conjunction with genus theory, enable us to partially answer the question of when a prime can be written in the form $x^2 + ny^2$.

4. Class Groups

4.1. **Composition of Genera.**

Our objective in this section is to define a group structure on the genera with a fixed discriminant. To do so, we begin by proving a series of useful results:

Lemma 4.1. *Let $p_1, q_1, \dots, p_r, q_r, m$ be numbers with $\gcd(p_1, \dots, p_r, m) = 1$. Then, the congruences*

$$p_i x \equiv q_i \ (mod\ m), \qquad i = 1, \dots, r$$

have a unique solution mod m if and only if for all $i, j = 1, \dots, r$, we have that:

$$p_i q_j \equiv p_j q_i \ (mod\ m).$$

Proof. That the former implies the latter is easily verified by plugging in $q_i \equiv p_i x \pmod{m}$. To prove the opposite direction, since $\gcd(m, p_1, \dots, p_r) = 1$, there exist an $a, a_1, \dots, a_r$ such that for any k, $am + \sum_{i=1}^{r} p_i a_i = 1 \Leftrightarrow q_k \left(\sum_{i=1}^{r} p_i a_i\right) \equiv q_k \pmod{m} \Leftrightarrow p_k \left(\sum_{i=1}^{r} q_i a_i\right) \equiv q_k \pmod{m}$. □

Lemma 4.2. *Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + cy^2$ be forms with discriminant D such that $\gcd(a, a', (b + b')/2) = 1$ (note that $b^2 - 4ac = (b')^2 - 4a'c'$ implies that b and b' have the same parity). Then, there is a unique integer B $(mod\ 2aa')$ that satisfies the following congruences:*

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

Proof. If B satisfies the first two congruences, then $B - b \equiv 0 \pmod{2a}$ and $B - b' \equiv 0 \pmod{2a'}$ imply that $(B - b)(B - b') \equiv 0 \pmod{4aa'}$. Hence, the third congruence can be written as $(b + b')B \equiv bb' + D \pmod{4aa'}$. Thus, we can rephrase the original three congruences as:

$$a'B \equiv a'b \pmod{2aa'}$$
$$aB \equiv ab' \pmod{2aa'}$$
$$(b + b')B/2 \equiv (bb' + D)/2 \pmod{2aa'}.$$

Note that since $\gcd(a, a', (b + b')/2) = 1$ and the pairwise congruence of LHS's and RHS's are easy to verify. By Lemma 4.1, the existence and uniqueness of B follows. □

With these two lemmas, we can define what will be our group operation for the group of genera that we will attempt to construct:

Definition 4.3. For two primitive, positive definite forms $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$, 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 solution of the system of equations in Lemma 4.2.

The following property for $F(x, y)$ holds:

Lemma 4.4. *Let $f(x, y), g(x, y)$, and their Dirichlet composition $F(x, y)$ be defined as above. Then, $F(x, y)$ is a primitive positive definite form with discriminant D.*

Proof. This is the result of straightforward manipulations of the definition. □

With this, we can begin to define a group structure on the genera.

Definition 4.5. Let $D \equiv 0, 1 \pmod 4$ be a negative integer. The *form class group*, $C(D)$, is defined as the set of all primitive positive definite forms with discriminant D. The class that the principal form lies in is called the *principal class*, and the form $ax^2 - bxy + cy^2$ is said to be the *opposite* of the form $ax^2 + bxy + cy^2$.

Through the following theorem, we see that $C(D)$ is indeed a group.

Theorem 4.6. *Let $D \equiv 0, 1$ (mod 4) be a negative integer, and let $C(D)$ denote the set of all primitive, positive definite forms with discriminant D. Then,*

(a) Dirichlet composition induces a well-defined binary operation on $C(D)$ which makes $C(D)$ a finite Abelian group with order $h(D)$;
(b) The identity element of $C(D)$ is the principal class;
(c) The inverse of the class containing any form is the one containing its opposite.

Proof. Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y)$ be primitive, positive definite forms. By Lemma 2.9, $g(x, y)$ represents an infinite number of integers relatively prime to a, which means that by Lemma 2.4, we can write $g(x, y) = a'x^2 + b'xy + c'y^2$, where $\gcd(a, a') = 1$. Thus, the Dirichlet composition of these two forms is defined between classes in $C(D)$, and we can use it as our group operation. That this operation is well-defined and that it makes $C(D)$ an Abelian group can be directly demonstrated from the definition; however, its proof is long, so we omit it here.

To prove that the principal class is the identity, note that the principal form can be composed with a form of any other class, satisfying the prerequisites easily. Moreover, since $B = b$ satisfies the conditions of Lemma 4.2 and subsequently $(B^2 - D)/4aa' = c$, we see that the principal class is indeed the identity.

To prove that classes containing opposite forms are inverses, let $f(x, y) = ax^2 + bxy + cy^2$ be in one class and its inverse $f'(x, y) = ax^2 - bxy + cy^2$ be in another. Note that $g(x, y) = f'(-y, x) = cx^2 + bxy + ay^2$ is properly equivalent to $f'(x, y)$, and hence is in the same class. Since $\gcd(a, c, (b + b)/2) = \gcd(a, b, c) = 1$, Dirichlet composition is defined for $f(x, y)$ and $g(x, y)$. Once again, $B = b$ can be verified to satisfy the conditions of Lemma 4.2, meaning the composition of the two is the form $acx^2 + bxy + y^2$. To show that this form is properly equivalent to its respective principal form, note that the transformations $(x, y) \to (y, -x - by/2)$ for $D \equiv 0 \pmod 4$ and $(x, y) \to (y, -x - (1 + b)y/2)$ for $D \equiv 1 \pmod 4$ map the composition to its respective principal form. Thus, the two classes are inverses. □

We also take note of the following interesting fact about class groups, which will prove very useful later on.

Lemma 4.7. *The class containing a reduced form $f(x, y) = ax^2 + bxy + cy^2$ in $C(D)$ has order ≤ 2 if and only if $b = 0, a = b$, or $a = c$.*

Proof. Let $f'(x, y)$ denote the opposite of $f(x, y)$. By Theorem 4.6, a class has order ≤ 2 if and only if the class containing $f(x, y)$ is equal to its inverse—the class containing $f'(x, y)$, which happens if and only if $f(x, y)$ and $f'(x, y)$ are properly equivalent. Since $f(x, y)$ is reduced, we have that $|b| < a < c$, in which case $f'(x, y)$ is also reduced. Thus, by Proposition 2.11, $b = 0$ if and only the two are properly equivalent, while $a = b$ or $a = c$ also implies they are properly equivalent following the proof of Proposition 2.11. □

With this, we are well-equipped to demonstrate the relationship between class groups and genus theory.

4.2. **The Link with Genus Theory.** We now establish the link between the class groups and genus theory. Since all forms within any class will represent the same numbers, we can define a map $\Phi : C(D) \to \ker(\chi)/H$ where each class is mapped to the coset of $H \in \ker(\chi)$ that it represents.

Lemma 4.8. *The map $\Phi : C(D) \to \ker(\chi)/H$ as defined previously is a group homomorphism.*

Proof. Let $f(x, y)$ and $g(x, y)$ be forms with discriminant D that represent values in cosets H' and H'' of $H \in \ker(\chi)$ respectively. Then, the product of numbers that $f(x, y)$ and $g(x, y)$ represent is represented by their Dirichlet composition, $F(x, y)$, which we can assume is defined (by definition of composition and looking at the coefficient of x^2). Thus, $F(x, y)$ represents the elements in $H'H''$, proving that it is a homomorphism. □

Corollary 4.9. *Let $D \equiv 0, 1 \ (mod\ 4)$ be a negative integer. Then, all genera of forms with discriminant D consist of the same number of classes.*

Proof. We note that the fiber of each coset of H in $\ker(\chi)/H$ will have the same number of elements since Φ is a homomorphism. □

Now that we've established a relationship between the class group and genera, we can begin to explore additional properties of the two. The following theorem contains several useful facts that will help us answer our original problem.

Theorem 4.10. *Let D be as defined previously, and let r be the number of odd primes dividing D. We define the number μ to be r if $D \equiv 1 \ (mod\ 4)$, and if $D = -4n$ (meaning $D \equiv 0 \ (mod\ 4)$) instead, then we define μ to be:*

$$\mu = \begin{cases} r & n \equiv 3 \ (mod\ 4); \\ r + 1 & n \equiv 1, 2 \ (mod\ 4) \ \text{or}\ n \equiv 4 \ (mod\ 8); \\ r + 2 & n \equiv 0 \ (mod\ 8). \end{cases}$$

If μ is defined in this way, then:

(a) The class group $C(D)$ has exactly $2^{\mu-1}$ elements of order ≤ 2;
(b) There are $2^{\mu-1}$ genera of forms with discriminant D;
(c) The principal genus consists of the classes in $C(D)^2$, which denotes the subgroup of squares in $C(D)$.

Proof. The basic idea for the proof of part (a) is that we have to count the number of cases that satisfy the conditions specified in Lemma 4.7. We perform the proof for when $D = -4n$ and $n \equiv 1 \pmod 4$, and note that the proof for the other cases are similar. Since n is odd, note that r is, by definition, the number of prime divisors of n. If $D \equiv 0 \pmod 4$, then a form with discriminant D can be written in the form $ax^2 + 2bxy + cy^2$. Then, Lemma 4.7 implies that we have to count the cases where $2b = 0$, $a = 2b$, or $a = c$.

We first count the forms with $2b = 0$. In this case, $f(x, y) = ax^2 + cy^2$ and $D = -4ac \Rightarrow ac = n$. Since $\gcd(a, c) = 1$ and both a and c have to be positive, we can pick 2^r possible combinations for the both of them. However, since $f(x, y)$ is also reduced, we must have $a < c$, meaning that there are actually only 2^{r-1} reduced forms with $2b = 0$.

Next, we want to count the forms with $a = 2b$ or $a = c$. Let $n = bk$, where b, k are integers such that $\gcd(b, k) = 1$ and $0 < b < k$. Following the logic used previously, there are 2^{r-1} combinations for b and k. Set $c = (b+k)/2$, and consider the form $f(x, y) = 2bx^2 + 2bxy + cy^2$, which has discriminant $-4n$ and relatively prime coefficients. If $2b < c$, then $f(x, y)$ is a reduced form of the first type ($a = 2b$). If $2b > c$, then $f(-y, x+y) = cx^2 + 2(c-b)xy + cy^2$ is a reduced form of the second type ($a = c$) since $2(c - b) < c$. Note that this covers all possibilities, as if $a = 2b$, then $k = 2c - b$ satisfies our initial assumption, whereas if $a = c$, then $f(x, y)$ is properly equivalent to the form $f(x + y, -x)$, which has $a = 2b$. Thus, we have proven (a).

While (b) appears similar to (a), its proof is quite different. To prove it, we need to introduce the notion of *assigned characters*. If $p_1, \ldots, p_r$ are all the distinct odd primes that are factors of D, then, we assign the functions:

$$\begin{aligned} \chi_i(a) &= \left(\frac{a}{p_i}\right) && \text{defined for } a \text{ prime to } p_i,\ i = 1, \ldots, r; \\ \delta(a) &= (-1)^{(a-1)/2} && \text{defined for } a \text{ odd;} \\ \epsilon(a) &= (-1)^{(a^2-1)/8} && \text{defined for } a \text{ odd.} \end{aligned}$$

to different a depending on the discriminant D. If $D \equiv 1 \pmod 4$, then we define the assigned characters to be $\chi_1, \ldots, \chi_r$, and when $D = -4n$, we define the assigned characters to be:

n	Assigned Characters
$n \equiv 3 \pmod 4$	$\chi_1, \ldots, \chi_r$
$n \equiv 1 \pmod 4$	$\chi_1, \ldots, \chi_r, \delta$
$n \equiv 2 \pmod 8$	$\chi_1, \ldots, \chi_r, \delta, \epsilon$
$n \equiv 6 \pmod 8$	$\chi_1, \ldots, \chi_r, \epsilon$
$n \equiv 4 \pmod 8$	$\chi_1, \ldots, \chi_r, \delta$
$n \equiv 3 \pmod 8$	$\chi_1, \ldots, \chi_r, \delta, \epsilon$

Evidently, the number of assigned characters is equal to μ. Thus, the assigned characters give a homomorphism $\Psi : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}^\mu$, which satisfies the following important lemma:

Lemma 4.11. *The homomorphism $\Psi : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}^\mu$ is a surjective mapping with kernel H, where H is the subgroup of values that the principal form represents. In other words, Ψ induces an isomorphism from $(\mathbb{Z}/D\mathbb{Z})^\times/H$ to $\{\pm 1\}^\mu$.*

Proof. If $D \equiv 1 \pmod 4$, since the order of both groups are equal, then for any $e \geq 1$, the Legendre symbol is a homomorphism that maps $(\mathbb{Z}/p^e\mathbb{Z})^\times \to \{\pm 1\}$ by definition. Surjectivity is easily verified, and the fact that the kernel of this homomorphism is the subgroup of squares in $(\mathbb{Z}/p^e\mathbb{Z})^\times$ follows from the definition of the Legendre symbol. If we let $D = -\prod_{i=1}^k p_i^{e_i}$ be D's prime factorization, then the Chinese Remainder Theorem suggests that Ψ can be seen as a mapping from $\prod_{i=1}^k (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ to $\{\pm 1\}^\mu$ instead, with $([a_1], \ldots, [a_\mu]) \mapsto ((a_1/p_1), \ldots, (a_\mu/p_\mu))$. It follows that this map is surjective and has the subgroup of squares in $(\mathbb{Z}/D\mathbb{Z})^\times$ as its kernel. In the proof of Lemma 3.3, we demonstrated that these are precisely the values that the principal form represents, and so we are done.

The proof for when $D \equiv 0 \pmod 4$ is considerably more complex, as the subgroup represented by the principal form may not necessarily be the subgroup of squares. The above approach works when dealing with the odd primes p dividing D, but in order to deal with the factor of two, considerably more work has to be done. Thus, we omit this proof for the purposes of this paper, but further details of it can be found in [1]. □

To prove (b), note that $\ker(\chi)$ has index 2 in $(\mathbb{Z}/D\mathbb{Z})^\times$, meaning that $\ker(\chi)/H$ must have order $2^{\mu-1}$ by the lemma that we have just proven. By Dirichlet's theorem on primes in arithmetic progressions, any class in $\ker(\chi)$ will contain some odd prime p. Note that $[p] \in \ker(\chi)$ means that $(D/p) = 1$, meaning that by Lemma 2.5, p is represented by a form with discriminant D. Hence, every congruence class in $\ker(\chi)$ contains a number represented by a form with discriminant D, meaning that $\Phi(C(D)) = \ker(\chi)$, and since the number of genera is just the order of $\Phi(C(D))$ in $\ker(\chi)/H$, we have that the number of genera of forms with discriminant D is equal to $2^{\mu-1}$.

To prove (c), note that by virtue of $\Phi : C(D) \to \ker(\chi)/H \cong \{\pm 1\}^{\mu-1}$ being a homomorphism, the subgroup of squares $C(D)^2$ lies in $\ker(\Phi)$. This, in turn, induces the map $C(D)/C(D)^2 \to \{\pm 1\}^{\mu-1}$. Let $C(D)'$ denote the subgroup of $C(D)$ with elements of order ≤ 2. Note that since the map $C(D) \to C(D)^2 \subset C(D)$ gives the short exact sequence $0 \to C(D)' \to C(D) \to C(D)^2 \to 0$, we have that the index of $C(D)^2$ in $C(D)$ is equal to the order of $C(D)'$, which is $2^{\mu-1}$ by part (a). Thus, since the map $C(D)/C(D)^2 \to \{\pm 1\}^{\mu-1}$ is a surjective homomorphism, it must be an isomorphism since the order of both groups are equal. Thus, $C(D)^2$ is the kernel of Φ, and since $\ker(\Phi)$ consists of the classes in the principal genus, we are done. □

The most important point about the previous theorem is the fact that there are *exactly* $2^{\mu-1}$ genera of forms with discriminant D. While the importance of this may not be obvious now, it will be in the following theorem, which is the main result of class theory we need to tackle the question of when $p = x^2 + ny^2$.

Theorem 4.12. *Let n be a positive integer. Then, the following statements are equivalent:*

(a) Every genus of forms with discriminant $-4n$ consists of a single class.

(b) If $ax^2 + bxy + cy^2$ is a reduced form of discriminant $-4n$, then either $b = 0$, $a = b$, or $a = c$.

(c) Two forms of discriminant $-4n$ are equivalent if and only if they are properly equivalent.

(d) The class group $C(-4n)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$ for some integer m.

(e) The class number $h(-4n)$ equals $2^{\mu-1}$

Proof. Let C denote the class group $C(D)$. To prove (a) implies (b), note that by Theorem 4.10, the principal genus is C^2, which is $\{1\}$ according to (a), meaning that every element of C has order ≤ 2. As a result, Lemma 4.7 shows that (a) implies (b).

To show (b) implies (c), suppose two forms of discriminant $-4n$ are equivalent, which means that they are either properly equivalent or opposites. Replacing the two forms with reduced forms if necessary, we note that either $b = 0$, $a = b$, or $a = c$. Following our proof of Proposition 2.11, we note that forms of this type are necessarily properly equivalent to their opposites, meaning that in any case, the forms are properly equivalent. Hence, we have (c).

To demonstrate that (c) implies (d), recall that a form $f(x, y)$ is equivalent to its opposite by the transformation $(x, y) \to (x, -y)$. Thus, assuming (c), we have that opposites are properly equivalent and hence in the same class in C. By part (c) of Theorem 4.6, this means that C is its own inverse. The only finite Abelian group structure that satisfies this property is that of $(\mathbb{Z}/2\mathbb{Z})^m$ for for any m. Hence, we have (d).

To prove that (d) implies (e), note that by Theorem 4.10, the number of genera is $2^{\mu-1}$. Thus, $h(-4n) = 2^{\mu-1}|C^2|$ since each genera is of the same order (by virtue of Φ being a homomorphism) and the principal genus is C^2. If (d) holds, then we must have that $C^2 = \{1\}$, and (e) follows immediately.

Lastly, if (e) holds, by Theorem 4.10, the principal genus comprises a single class, and since every genus has the same number of classes, we have (a). □

Of all of the parts of the theorem above, the one that holds the most importance is the last one. What it suggests is that for all n such that $x^2 + ny^2$ is prime for some $x, y \in \mathbb{Z}$, if any of the conditions of Theorem 4.12 hold, then $h(-4n)$ must be a power of two. This gives us a way to search for the possible values of n. In his *Disquistiones Arithmeticae*, Gauss lists the values of n that satisfy the theorem's properties:

$h(-4n)$	Values of n
1	1, 2, 3, 4, 7
2	5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58
4	21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253
8	105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760
16	840, 1320, 1365, 1848

It was proven later on that aside from these 65 numbers, there could only possibly be one more n that satisfies the theorem's properties [1] (whether it actually exists has yet to be determined.) However, this is not to say that these are the only n for which $x^2 + ny^2$ is prime for some integers x and y; it has even been demonstrated by Euler that there are also solutions when $n = 27$ or $n = 64$ instead—only two of the many values of n not listed by Gauss. Unfortunately, the proof of further cases requires class field theory, which lies beyond the scope of this paper.

Acknowledgments. I'd like to thank my mentor, Jingren Chi, for his guidance and patience with me as I wrote this paper. I would also like to thank Professor Peter May for the invaluable time and effort that he devoted to coordinating the entire REU program for the University of Chicago.

References

[1] Cox, D. A. (1989). *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication.* New York: Wiley.

[2] Gauss, C. F. (1966). *Disquisitiones Arithmeticae* (A. A. Clarke, Trans.). New Haven: Yale University Press.

[3] Rousseau, G. (1991, December). *On the quadratic reciprocity law.* Journal of the Australian Mathematical Society, 51(03), 423-425.