Representations of Primes by Quadratic Forms

Senior Thesis
Madhav Chandrasekher
## Table of Contents

I. Introductory Theory and Examples  
   pgs. 3 - 18

II. The Classification of Primes Represented by the Form $x^2 + 17y^2$.  
    pgs. 19 - 29

III. Character Sums in Finite Fields.  
     pgs. 30 - 38

IV. The Class Number Formula  
    pgs. 39 - 45
When we consider an equation with integer coefficients of the form \( f(x, y) = c \) for some constant \( c \), the questions that usually spring to mind are: Are there any solutions over the integers? Is there a way to determine those \( c \) for which solutions exist? In this paper, we will give an exposition of some of the methods that have been developed to answer both of these questions. However, we will add one more question to this list: Are there any solutions to the equation over finite fields? There are two reasons for investigating this additional question. The first is that one can obtain many elegant formulas for the number of solutions to certain equations over finite fields by various methods. Secondly, it turns out that these techniques can be applied to the first question regarding representations of forms over the integers to obtain further insights.

Instead of trying to develop answers for the general polynomial \( f(x, y) \) we shall restrict our attention to the special cases of positive definite quadratic forms. We hope to give an exposition of the variety and depth of the various tools that have been developed to tackle the fundamental questions. In treating quadratic forms, we will consider solutions to: \( ax^2 + bxy + cy^2 = n \), where all coefficients are integers. Following the arguments given in [Cox 1989] we will consider cases where \( n \) is prime. The reason for this is that in many cases, through the use of various algebraic identities discovered by Euler, Lagrange, or Gauss, once we know that a prime can be represented by a certain form, it will follow that the products of such primes will also be represented by a form of the same type. The theory of these forms that we describe is taken from the treatments given in [Cox 1982], [Ireland and Rosen 1992], and [LeVeque 1956]. At the next stage we will bring finite fields into the picture. After giving a brief exposition of some of the methods used to count solutions to equations, following the methods described in [Ireland and Rosen 1992], we will apply them to study certain forms.

**NOTE**: We recall that the discriminant \( D \) of a quadratic form \( f(x, y) = ax^2 + bxy + cy^2 \) is defined to be \( D = b^2 - 4ac \). Since we are dealing with positive definite forms we assume that \( D < 0 \) and
$a > 0$. Since we will only deal with positive definite quadratic forms, from now on this is what we shall mean when we refer to a form.

We will organize our study by looking at forms of a fixed discriminant. Then we will try to find what primes are represented by the forms with this discriminant. Unless stated otherwise we shall assume that the gcd of the coefficients of any given form is 1 since we are interested in what primes can be represented by the form (such forms are called primitive). Let $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = a_1x^2 + b_1xy + c_1y^2$ be two forms. We say that $f$ and $g$ are equivalent forms if there exists a $2 \times 2$ matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with integer entries and with $\text{det}(A) = 1$ that satisfies $f(ax + by, cx + dy) = g(x,y)$. It is clear that this induces an equivalence relation on the set of all forms of a given discriminant. Since equivalent forms represent the same integers, it suffices to investigate one form from each equivalence class. However, this in itself is a daunting task because for any given discriminant there are many forms in each equivalence class. In order to organize our study we wish to ascertain the existence of a certain type of form such that for any value of $D$ there is a form of this type in each equivalence class. Then, we can devote our attention to studying this special class of forms. However, it is not obvious that such a class should exist. For example, if we set some arbitrary constraints on the coefficients of a form, can we say that for each value of $D$ there will be a form in each equivalence class that satisfies these constraints? It is a truly beautiful aspect of this theory that we can in fact find a set of forms with this property. In what follows we will find this set of constraints and describe this set of forms. The arguments are taken from [LeVeque 1956] and [Serre 1973].

We will first require some groundwork before prescribing our set of constraints. Let $\Gamma$ denote the group of all $2 \times 2$ matrices with integer entries that have determinant 1. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of $\Gamma$. With this matrix we associate the following transformation of the complex plane: $A(z) = \frac{az + b}{cz + d}$. It is easy to see that $A$ maps the complex upper half plane into itself. We say that
two points \( z \) and \( z_1 \) of the upper half plane are equivalent if there is an element \( A \) of \( \Gamma \) such that \( A(z) = z_1 \). This induces an equivalence relation on points in the complex upper half plane. Now if we chose one element from each equivalence class and called the resulting set \( S \), every point in the complex upper half plane would be equivalent to a point of \( S \). Furthermore, no two points of \( S \) would be equivalent to each other. However, there are many possible such sets \( S \). We can see right away that any reasonable choice of \( S \) should be a subset of an infinite strip:

\[
(1) \{ z : \Im z > 0 \text{ and } a \leq \Re z < a + 1 \}.
\]

This follows since the matrix \( A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) is an element of \( \Gamma \). The map associated with \( A \) is horizontal translation by 1 unit. Therefore, it is clear that \( S \) can be chosen to be a subset of a strip of unit width. Furthermore, since all strips of the type specified in (1) are equivalent we can choose our strip, call it \( S_0 \), to be \( S_0 \overset{\text{def}}{=} \{ z : \Im z > 0, -\frac{1}{2} \leq \Re z < \frac{1}{2} \} \). Is it true that \( S = S_0 \)? Clearly \( S \) is smaller since the point \( \frac{i}{2} \) is mapped to \( 2i \) under the map \( A(z) = -\frac{1}{z} \), where \( A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \).

Therefore we know that \( S \subset S_0 \). However, we can say much more. The following theorem from [LeVeque 1956] describes \( S \) explicitly:

**Theorem:** \( S \overset{\text{def}}{=} \{ z : -\frac{1}{2} \leq \Re z < \frac{1}{2} \text{ and } |z| > 1 \text{ or } |z| = 1 \text{ and } -\frac{1}{2} \leq \Re z \leq 0 \} \).

**Proof:** We must show two things: (i) no two points of \( S \) are equivalent to one another under any element of \( \Gamma \) and (ii) every point of the complex upper half plane is equivalent to a point of \( S \).

The following arguments are taken from [Serre 1973]. Let \( A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \), so that \( A(z) = -\frac{1}{z} \), and \( T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \), so that \( T(z) = z + 1 \). We shall first prove that every point of the complex upper half plane is equivalent to a point of \( S \) under \( \Gamma \). For notational convenience we shall denote the complex upper half plane by \( H \). We observe that for \( z \in H \) and \( g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, \ Im(g(z)) = \frac{Im(z)}{|c+\bar{d}|^2} \). Pick some number \( K > 0 \). Since \( c, d \) are integers and \( Im(z) > 0 \), there are only finitely many pairs \((c,d)\) that are solutions to the inequality \( 0 < |cz+d|^2 < K \). Pick the solution pair \((c,d)\) for which the quantity \( |cz+d|^2 \) is smallest. We claim that we can then find integers \( a, b \) such that \( ad - bc = 1 \).
only way this could fail is if \( c \) and \( d \) shared a common factor. This would contradict the minimality of \( |cz + d|^2 \). Therefore, for a given \( z \in H \), we can find an element \( g \in \Gamma \) such that \( \text{Im}(g(z)) \) is maximum. There exists an integer \( n \) such that \( T^n(g(z)) \) has real part in the interval \( [-\frac{1}{2}, \frac{1}{2}] \). Let \( z' = T^n(g(z)) \). We wish to claim that in fact \( T^n(g(z)) \in S \). Assume that this was not the case.

Then we must have one of the two possibilities: (1) \( |z'| < 1 \) or (2) \( |z'| = 1 \) and \( 0 < \text{Re}(z') \leq \frac{1}{2} \). If the first possibility held we would obtain that \( \frac{1}{z'} > \text{Im}(g(z)) \). Since \( \frac{1}{z'} \) is the image of \( z \) under \( \text{AT}g \in \Gamma \), this would contradict the maximality of \( \text{Im}(g(z)) \). Therefore, we can rule out (1). If (2) held, then \( A(z') \in S \). Therefore, we have shown that every element \( z \in H \) is equivalent to a point of \( S \) under \( \Gamma \). We will now show that no two points of \( S \) are equivalent to one another under \( \Gamma \).

Assume that there exists a point \( z \in S \) such that \( g(z) \in S \), for \( g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \). Since \( g^{-1}(g(z)) = z \in S \), we may assume without loss of generality that \( \text{Im}(g(z)) \geq \text{Im}(z) \). Since \( \text{Im}(g(z)) = \frac{\text{Im}(z)}{|cz + d|^2} \), we obtain that \( |cz + d| \leq 1 \). If \( c \geq 2 \), this inequality is impossible. To see this note that \( \text{Im}(z) \geq \frac{\sqrt{3}}{2} \). Therefore, if \( c \geq 2 \), \( |cz + d| \geq \sqrt{3} > 1 \). This leaves us with the three cases:

1. \( c = 0 \),
2. \( c = 1 \), or
3. \( c = -1 \).

If \( c = 0 \), then \( d = 1 \). This implies that \( a = 1 \) and \( b = \pm 1 \). Since \( g = \pm T \) it is impossible for \( g(z) \) to be in \( S \). If \( c = 1 \), then the fact that \( |z + d| \leq 1 \) implies that \( d = 0 \) or \( 1 \). To see this note that since \( z \in S \) we must have \( |d| < 2 \). If \( d = 2 \), then we would obtain \( |z + 2| > |2 - 1/2| > 1 \). If \( d = -2 \), then \( |z - 2| > |2 - 1/2| > 1 \). If \( d = -1 \), then \( |z - 1| > |\frac{\sqrt{3}}{2} - 1| \).

Therefore, when \( c = 1 \) the only possibilities are \( d = 0 \) or \( 1 \). If \( d = 0 \), then \( b = -1 \). Furthermore, \( |z| \leq 1 \) implies that \( |z| = 1 \) since \( z \in S \). Since \( g(z) = \frac{az - 1}{z} = a - \frac{1}{z} \) and \( |\frac{1}{z}| = 1 \) we obtain that \( a = 0 \), in which case \( z = g(z) = i \). If \( d = 1 \), then the inequality \( |z + 1| \leq 1 \) could only hold (for \( z \in S \)) if \( z = e^{\frac{2\pi i}{3}} \). In this case, \( g(z) = \frac{az + b}{z + 1} = \frac{az + (a - 1)}{z + 1} = a - \frac{1}{1 + z} = a - \frac{1}{(1/2 + i\sqrt{3}/2)} = a + (-1/2 + i\sqrt{3}/2) = a + z \). This implies that \( a = 0 \), showing that \( g(z) = z \). This takes care of the case where \( c = 1 \). If \( c = -1 \), then the fact that \( |z + d| = |z - d| \leq 1 \) implies that \( d = 0, -1 \). Dealing with these cases as before we find that \( z = i \) and \( z = e^{\frac{2\pi i}{3}} \) are the only possibilities, and that in each of these cases \( g(z) = z \). Therefore, no two points of \( S \) are equivalent to one another under \( \Gamma \). This completes the
proof of the Theorem.

The region $S$ is referred to as the fundamental domain of the group $\Gamma$.

We now have the information required to help us in classifying forms. For each form $f(x, y) = ax^2 + bxy + cy^2$ with real coefficients consider the polynomial $f(z) = az^2 + bz + c$. Since $D = b^2 - 4ac < 0$, both roots of this polynomial are complex. Pick the root with positive imaginary part and call it $\omega$. Then to each form we can associate a point $\omega$ in the complex upper half plane. Conversely, given a point $\omega$ we can associate the polynomial $h(z) = C(z - \omega)(z - \overline{\omega}) = C(z^2 - 2Re(\omega)z + \omega \overline{\omega})$. For each value of $D$, there is a unique value of $C$ such that $h(z)$ has discriminant $D$. Therefore, for each value of $D$ there is a one-to-one correspondence between points in the upper half plane and forms with real coefficients and discriminant $D$. This implies that that two forms $f_1$ and $f_2$ are equivalent if and only if their associated points in the upper half plane, $\omega_{f_1}$ and $\omega_{f_2}$, are equivalent. We will now prove this:

**Claim:** Let $f_1$ and $f_2$ be two forms with discriminant $D$. Then, $f_1$ is equivalent to $f_2$ if and only if their associated points in the upper half plane are equivalent.

**Proof:** Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Let $f_1(x, y) = a_1x^2 + b_1xy + c_1y^2$. If $f_1(x, y)$ is equivalent to $f_2(x, y)$ under $A$, then, by definition, $f_1(ax + by, cx + dy) = f_2(x, y)$. Let $\omega_{f_1}$ and $\omega_{f_2}$ denote the roots in the complex upper half plane of $f_1$ and $f_2$, respectively. Then we find that $\omega_{f_2} = A^{-1}(\omega_{f_1})$, where $A^{-1}(z) = \frac{dz - b}{cz + a}$. Therefore, $\omega_{f_1}$ and $\omega_{f_2}$ are equivalent under $A^{-1} \in \Gamma$. Conversely, assume that $\omega_{f_1}$ and $\omega_{f_2}$ are equivalent under some matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. This means that $\omega_{f_2} = A(\omega_{f_1})$. Consider the form $f(x, y) = f_1(dx - by, -cx + ay)$. The point $\omega_f$ associated with this form satisfies: $\omega_f = A(\omega_{f_1}) = \omega_{f_2}$. By the comments preceding the claim, there is a one-to-one correspondence between points in the complex upper half plane and forms with real coefficients and discriminant $D$. This implies that $f = f_2$, showing that $f_1$ and $f_2$ are equivalent under $\Gamma$. This concludes the proof.
If $f_1$ and $f_2$ are equivalent, then both of the points $\omega_{f_1}$ and $\omega_{f_2}$ are equivalent to some point in the fundamental domain $S$; and since no two points of $S$ are equivalent to each other we have that $\omega_{f_1}$ and $\omega_{f_2}$ are both equivalent to the same point in the fundamental domain. It follows that there is a unique form $f$ of discriminant $D$ which is in the equivalence class of $f_1$ and whose representative $\omega_f$ lies in the fundamental domain. This unique form is called reduced. Since we will be considering forms with integer coefficients we can see that the reduced form in each equivalence class also has integer coefficients because matrices in $\Gamma$ have integer entries. Therefore, from now on we shall switch back to our assumption that the forms we are dealing with have integer coefficients. We will now find a set of constraints that the coefficients of a reduced form must satisfy.

Let $f(x, y) = ax^2 + bxy + cy^2$ be reduced. Then $\omega = \frac{-b + \sqrt{b^2 - 4ac}}{2a}$ is in $S$. Therefore, since $S = \{ z : -\frac{1}{2} \leq \Re z \leq \frac{1}{2}$ and $|z| > 1$ or $-\frac{1}{2} \leq \Re z \leq 0$ and $|z| = 1 \}$, we must have $|\omega|^2 = \frac{b^2}{4a^2} + \frac{4ac - b^2}{4a^2} = \frac{c}{a} > 1$ and $-\frac{b}{2a} < \frac{1}{2}$ or $\frac{c}{a} = 1$ and $-\frac{1}{2} \leq -\frac{b}{2a} \leq 0$. In the latter case, after simplifying the inequalities, we obtain $a = c$ and $0 \leq b \leq a$. In the former case we have $c > a$ and $-a < b \leq a$. Therefore, if a form is reduced its coefficients must satisfy these conditions. Conversely, if a form's coefficients satisfy these inequalities its representative is in the fundamental domain which implies that it is reduced. We now have an answer to the question that we asked at the beginning of this section. For a fixed discriminant we can pick the reduced form from each equivalence class.

We shall now state some facts about the set of reduced forms for a fixed discriminant that will be useful in our investigations. Unless stated otherwise these facts and definitions are taken from [Cox 1982]:

(1) **Proposition 1**: Assume that $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a_1x^2 + b_1xy + c_1y^2$ are two reduced forms of discriminant $D$ that satisfy $\gcd(a, a_1, \frac{(b+b_1)}{2}) = 1$. Then there is an integer $B$
which is unique mod \((2aa_1)\) and satisfies the following congruences: \(B \equiv b \ (2a), \ B \equiv b_1 \ (2a_1),\) and 
\(B^2 \equiv D \ (4aa_1)\).

(2) **Definition:** Let \(f(x, y) = ax^2 + bxy + cy^2\) and \(g(x, y) = a_1x^2 + b_1xy + c_1y^2\) be two reduced forms that satisfy the hypotheses of the above Proposition. Then the **Dirichlet composition** of \(f\) and \(g\) is defined as: 
\[fg = F(x, y) = a_1x^2 + Bxy + \frac{B^2-D}{4aa_1}y^2,\]
where \(B\) is as in the Proposition above.

(3) Let \(F\) be the Dirichlet composition of two reduced forms \(f\) and \(g\). Then \(F\) represents all numbers of the form \(f(x, y)g(z, w)\).

It is clear that \(F(x, y)\), the Dirichlet composition of \(f\) and \(g\), is a primitive positive definite form of discriminant \(D\). The proof of the fact that \(F\) is positive definite and has discriminant \(D\) follows easily from the definition of \(F\). To prove that \(F\) is also primitive we proceed via contradiction. Assume that \(p\) is a prime number which divides all numbers represented by \(F\). Then \(p\) divides all numbers of the form \(f(x, y)g(z, w)\). Find \(z, w\) such that \((p, g(z, w)) = 1\). Then for this fixed choice of \(z, w\) we have that \(p\) divides all numbers of the form \(f(x, y)g(z, w)\) for any choice of \((x, y)\). This contradicts the fact that \(f(x, y)\) is primitive, thereby proving that \(F(x, y)\) is primitive. We shall now proceed with our list of required facts.

(4) Under the composition operation described in (2), the set \(C(D)\) of equivalence classes of forms of discriminant \(D\) form a finite Abelian group.

(5) The form \(I(x, y) = \begin{cases} x^2 - \frac{D}{4}y^2 & \text{if } D \equiv 0 \ (4); \\ x^2 + xy + \frac{(1-D)}{4}y^2 & \text{if } D \equiv 1 \ (4). \end{cases}\) lies in the identity class of \(C(D)\).

**Proof:** Let \(f(x, y) = ax^2 + bxy + cy^2\) and \(I(x, y)\) have discriminant \(D\). The gcd condition specified in Proposition 1 is satisfied. Choose \(B = b\). Then, \(B\) satisfies the three congruences in Proposition 1.

Letting \(F\) denote the Dirichlet composition of \(f\) and \(I\), we obtain \(F(x, y) = ax^2 + Bxy + \frac{B^2-D}{4}y^2 = \)
\[ ax^2 + bxy + cy^2. \] This shows that the form \( I \) lies in the identity class.

(6) If \( f(x, y) = ax^2 + bxy + cy^2 \in C(D) \), then the class that the form \( g(x, y) = ax^2 - bxy + cy^2 \) belongs in is the inverse of the class which contains \( f \) (the form \( g(x, y) \) is referred to as the opposite of \( f \)).

**Proof:** Let \( C = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \). Then \( g(x, y) = ax^2 - bxy + cy^2 \) is equivalent to the form \( h(x, y) = cy^2 + bxy + ay^2 \) under \( C \). We will compose \( f \) with \( h \). Since \( \gcd(a, b, c) = 1 \), the \( \gcd \) condition in Proposition 1 is satisfied. Furthermore, as in the proof of (5), we can choose \( B = b \). The congruence conditions of the proposition are then satisfied. Letting \( F(x, y) \) denote the Dirichlet composition of \( f \) and \( h \), we obtain \( F(x, y) = acx^2 + bxy + y^2 \). When \( D \equiv 0 \pmod{4} \), \( F(x, y) \) is equivalent to \( I(x, y) \) under the matrix \( K = \begin{pmatrix} 0 & -1 \\ 1 & \frac{b}{2} \end{pmatrix} \). When \( D \equiv 1 \pmod{4} \), \( F \) and \( I \) can similarly be shown to be equivalent. This proves (6).

(7) A reduced form \( f(x, y) = ax^2 + bxy + cy^2 \) of discriminant \( D \) has order \( \leq 2 \) in \( C(D) \) if and only if \( b = 0 \), \( a = b \), or \( a = c \).

**Proof:** This proof is taken from [Cox 1982]. By (6) we know that a reduced form \( ax^2 + bxy + cy^2 \) has order \( \leq 2 \) if and only if it is equivalent to the form \( ax^2 - bxy + cy^2 \). Since \( ax^2 + bxy + cy^2 \) is reduced, we have one of the two possibilities: (i) \( |b| < a < c \) (ii) \( b = a \) or \( a = c \). If (i) holds, then the form \( ax^2 - bxy + cy^2 \) is also reduced. By uniqueness this implies that \( b = 0 \). If (ii) holds and \( a = b \), then \( ax^2 - axy + cy^2 \) is equivalent to \( ax^2 + axy + cy^2 \) under the matrix \( T_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \). If (ii) holds and \( a = c \), then \( ax^2 + bxy + ay^2 \) is equivalent to \( ax^2 - bxy + ay^2 \) under the matrix \( T_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \). This proves (7).

(8) **Definition:** For a given \( D \), the order of the form class group \( C(D) \) is called the *class number* and is denoted \( h(D) \).
It is easily seen that the class number $h(D)$ is finite (a proof is given in [Cox 1982]). Since we will only be dealing with reduced forms, the constraints on the coefficients in fact imply that $a \leq \sqrt{\frac{-D}{3}}$. This inequality allows us to explicitly determine the reduced forms of any fixed discriminant. For example, consider the four cases: (1) $h(-28)$, (2) $h(-16)$, (3) $h(-36)$, and (4) $h(-68)$.

Note: in all of these cases the fact that $b^2 - 4ac$ equals an even number implies that $b$ must be even. This will reduce the following computations.

Case 1: $h(-28)$

By the inequality $a \leq \sqrt{\frac{-D}{3}}$, we obtain that $a \leq 3$. If $a = 3$, then $b$ must be either 0 or ±2. If $b = 0$ we obtain that $-12c = -28$, which is impossible. The other possibilities can similarly be ruled out. If $a = 2$, we must have $b$ equal to either 0 or ±2. The only case that could possibly work is when $b = 2$, in which case we obtain $c = 4$. However, the form with these coefficients is not primitive. If $a = 1$ we obtain $b = 0$ as the only possibility, in which case $c = 7$. Thus, the only reduced form of discriminant -28 is $f(x, y) = x^2 + 7y^2$.

Case 2: $h(-16)$

We must have that $a \leq 2$. Working through the possibilities we obtain that the only reduced form is $f(x, y) = x^2 + 4y^2$.

Case 3: $h(-36)$

We must have $a \leq 3$. This inequality implies that the only possibilities are $3x^2 + 3y^2$, $2x^2 + 2xy + 5y^2$, and $x^2 + 9y^2$. However, (1) is not primitive. Thus, we only have the following two reduced forms: (1) $2x^2 + 2xy + 5y^2$ (2) $x^2 + 9y^2$. We note that this is consistent with the group structure of $C(D)$ as discussed earlier. Form (1) composed with itself yields a form equivalent to (1) and (2) is in the identity class.
Case 4: $h(-68)$

In this case we shall use two methods to find all the forms. The first method we shall use will provide us with the value of $h(-68)$ but it will not tell us what forms correspond to this discriminant. However, it provides a striking example of the deep relation between the class number and finite fields. The following definitions and formulae are taken from [Cox 1982]:

**Definition:** For $p$ a prime define the **Kronecker symbol** $(\frac{D}{p})$ as follows:

$$(\frac{D}{p}) = \begin{cases} 
(D/p) & \text{if } p \text{ is an odd prime;} \\
0 & \text{if } p = 2 \text{ and } 2|D; \\
1 & \text{if } p = 2 \text{ and } D \equiv 1 \pmod{8}; \\
-1 & \text{if } p = 2 \text{ and } D \equiv 5 \pmod{8}.
\end{cases}$$

The Kronecker symbol is defined for composite integers as follows:

**Definition:** Let $n = p_1^{l_1}p_2^{l_2} \cdots p_m^{l_m}$. We define:

$$(D/n) = (D/p_1)^{l_1}(D/p_2)^{l_2} \cdots (D/p_m)^{l_m}.$$ 

Using the Kronecker symbol, we have the following formula for the class number of a given discriminant $D$,

$$h(D) = \frac{1}{|D|} \sum_{n=1}^{|D|-1} (\frac{D}{n}) \cdot n.$$ 

**NOTE:** we will describe where this formula comes from a little later.

Now for odd $n$, $(\frac{-68}{n}) = (\frac{-1}{n})(\frac{17}{n}) = (-1)^{\frac{n-1}{2}}(\frac{n}{17})$, by quadratic reciprocity. The squares modulo 17 are 1, 2, 4, 8, 9, 13, 15, 16 and we know that $(\frac{D}{2m}) = 0$. Therefore all that is left to do is to substitute these values back into the formula in order to evaluate the sum. After doing so we obtain that $h(-68) = 4$.

We will now explicitly determine the forms with $D = -68$ using the same methods as in the previous cases. Since $a \leq 4$, computing the possibilities we obtain the following four forms: (1) $2x^2 +$
2xy + 9y^2, (2) x^2 + 17y^2, (3) 3x^2 + 2xy + 6y^2, and (4) 3x^2 - 2xy + 6y^2. We note that the group
C(-68) is cyclic of order 4. This follows from the fact that forms (1) and (2) have order less than 2
in C(-68) and forms (3) and (4) are opposites.

Now, having determined the forms for the given discriminants, we will proceed to investigate
what integers are representable by them.

If a prime p is represented by a form of discriminant D \equiv 0 \mod 4, then we must have \left(\frac{D}{p}\right) = 1.
Namely, suppose that \( f(P,Q) = aP^2 + bPQ + cQ^2 = p \) for some \( P, Q \). Dividing the equation by
\((Q^{-1})^2\), where \( Q^{-1} \) is the multiplicative inverse of \([Q] \) in the ring of integers modulo \( p \), we obtain
that \( f(PQ^{-1}, 1) = 0 \) in \( \mathbb{Z}_p \). So the quadratic equation \( f(x, 1) \) is solvable modulo \( p \). Thus, by the
quadratic formula \( D \equiv b^2 \mod p \), for some \( b \).

Starting with the case \( h(-16) \), we wish to decide what primes can be represented by the form
\( x^2 + 4y^2 \). By the above argument, if \( p = x^2 + 4y^2 \) we must have \( \left(\frac{-1}{p}\right) = 1 \). Since \( \left(\frac{-1}{p}\right) = 1 \) we
must have that \( p \equiv 1 \mod 4 \). However, this argument does not give any indication as to whether this
condition is sufficient. What we need is the following result, taken from [Cox 1982]:

**Definition**: A form \( f(x, y) \) is said to properly represent an integer \( m \) if there exists a pair of
relatively prime integers \( p, q \) such that \( f(p, q) = m \).

**Lemma**: A form \( f(x, y) \) properly represents an integer \( n \) if and only if it is equivalent to the form
\( nx^2 + bxy + cy^2 \), where \( b, c \) are integers.

**Proof**: Let \( f(x, y) = Ax^2 + Bxy + Cy^2 \) for some integers \( A, B, \) and \( C \). By hypothesis \( f(p, q) = n \), for
\( (p, q) = 1 \). Then, there exists integers \( k \) and \( l \) such that \( kp - lq = 1 \). Expanding \( f(px + ly, qx + ky) \),
we obtain \( f(px + ly, qx + ky) = A(px + ly)^2 + B(px + ly)(qx + ky) + C(qx + ky)^2 = nx^2 + bxy + cy^2 \)
for some integers \( b, c \). Conversely, if \( f(x, y) \) is equivalent to the form \( nx^2 + bxy + cy^2 \) there exists a
matrix $A = \begin{pmatrix} p & 1 \\ q & k \end{pmatrix} \in \Gamma$ such that $f(px + ly, qx + ky) = nx^2 + bxy + cy^2$. The fact that $\text{det}(A) = 1$ implies that $(p, q) = 1$, from which we obtain that $f(p, q) = n$ is a proper representation. This concludes the proof of the Lemma.

This result allows us to prove that the condition $p \equiv 1 \pmod{4}$ is in fact sufficient for $p$ to be represented by $x^2 + 4y^2$. Assuming that $\left( \frac{-1}{p} \right) = 1$, since $D = -16$ we obtain $D = c^2 \pmod{p}$ for some $c$. Now, by definition, $D \equiv 0$ or $1 \pmod{4}$, both of which are squares mod 4. Since $p$ is an odd prime, by the Chinese Remainder Theorem we obtain $D \equiv b^2 \pmod{4p}$ for some $b$. Thus, $D = b^2 - 4pk$, for some integer $k$. Therefore, $p$ is represented by the form $f(x, y) = px^2 + bxy + ky^2$ of discriminant $D$. However, by our previous computations, all forms of discriminant $D = -16$ are equivalent to $x^2 + 4y^2$. This implies that $p = x^2 + 4y^2$ for some integers $x$ and $y$, proving that the condition $p \equiv 1 \pmod{4}$ is both necessary and sufficient. This completely determines what primes are represented by those forms in the group $C(-16)$.

The methods in the above proof clearly generalize to cases where $h(D) = 1$. However, in some of our examples $h(D) > 1$. For example, $h(-36) = 2$. The list of forms we obtained were:

1. $f(x, y) = x^2 + 9y^2$
2. $f(x, y) = 2x^2 + 2xy + 5y^2$.

The first question that springs to mind is: Could there be primes that are represented by both these forms? The answer to this question is no. However, to prove it we will use the following results which are taken from [Cox 1982]:

**Note:** The proofs for most of these results are taken from [Cox 1982].

(1) **Lemma:** Let $D \equiv 0 \pmod{4}$ and $m$ be an integer relatively prime to $D$. Then $m$ is properly represented by one of the $h(D)$ reduced forms of discriminant $D$ if and only if $D$ is a quadratic residue modulo $m$.

**Proof:** Assume $f(x, y) \in C(D)$ and properly represents $m$. We have shown earlier that $f(x, y)$ is
equivalent to the form \( mx^2 + 2bxy + cy^2 \), for some integers \( b \) and \( c \) which satisfy \( D = 4b^2 - 4mc \).

Therefore \( D \equiv 4b^2 \ (m) \), showing that \( D \) is a quadratic residue modulo \( m \). Conversely, assume that \( D \) is a quadratic residue mod \( m \). Then \( D \equiv b^2 \ (m) \), for some \( b \). Since \( m \) is relatively prime to \( D \), we can assume that \( b \) is even (otherwise we could replace \( b \) by \( b + m \)). Then \( D - b^2 = mc \), for some integer \( c \). Since \( D - b^2 \equiv 0 \ (4) \), we obtain that \( 4|c \). Letting \( c = 4c' \), we obtain that \( m \) is properly represented by the form \( g(x, y) = mx^2 + bxy - c'y^2 \in C(D) \). This proves the lemma.

(2) **Theorem 1:** Let \( p, q \) be odd primes and \( D \equiv 0 \ (4) \). Then, if \( p \equiv q \ (D) \) either both primes are represented by one of the reduced forms in \( C(D) \) or neither of them are.

**Proof:** By the properties of the Jacobi symbol we know that \( \left( \frac{D}{p} \right) = \left( \frac{D}{q} \right) \) when \( p \equiv q \ (D) \) (this property is proved in [Cox 1982]). Therefore, \( D \) is either a quadratic residue mod \( p \) and mod \( q \) or a quadratic non-residue mod \( p \) and mod \( q \). By the above lemma, it follows that either both \( p \) and \( q \) are represented by a reduced form in \( C(D) \) or neither of them are.

Theorem 1 allows us to determine which primes are represented by forms in \( C(D) \). We need only choose one prime from each of the \( \phi(D) \) arithmetic progressions \( a + Dk \), where \( a \in (\mathbb{Z}/D\mathbb{Z})^* \), and check if \( D \) is a quadratic residue modulo this prime. This procedure only gives us those primes that are represented by forms in \( C(D) \). It does not tell us anything about which forms in \( C(D) \) represent these primes. For example, Theorem 1 does not tell us if \( p \) and \( q \) are represented by the same reduced form in \( C(D) \) when \( p \equiv q \ (D) \). The following results allow us to determine the answers to such questions so that we may complete our classification for \( D = -36 \).

**Definition:** We shall say that a form \( f(x, y) \) represents a congruence class \( a \in (\mathbb{Z}/D\mathbb{Z})^* \) if the congruence \( f(x, y) \equiv a \ (D) \) is solvable. We stress that this does not mean that \( f(x, y) \) represents every integer in the sequence \( a + Dk \), only that it represents at least one integer in the sequence.

(3) Let \( D \equiv 0 \ (\text{mod } 4) \), \( (\mathbb{Z}/D\mathbb{Z})^* \) denote the multiplicative group of \( \mathbb{Z}/D\mathbb{Z} \), and \( f(x, y) \) be any form.
with discriminant $D$. Then the map $\chi : (\mathbb{Z}/D\mathbb{Z})^* \mapsto \{\pm 1\}$ defined as $\chi(m) = \left(\frac{D}{m}\right)$ is a well-defined homomorphism.

(4) **Theorem 2**: Let $D \equiv 0 \pmod{4}$. If a form $f(x, y)$ is in the identity class of $C(D)$, the congruence classes in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by $f(x, y)$ form a subgroup $H$ of the kernel of $\chi$.

**Proof**: Since $f$ lies in the identity class we can assume that $f(x, y) = x^2 + ny^2$, where $n = -D/4$. The lemma shows that the set of values properly represented by $f(x, y)$ lie in the kernel of the homomorphism $\chi$ described in (1). If $m$ is any number represented by $f(x, y)$, then we can write $m = d^2m'$, where $m'$ is properly represented by $f(x, y)$. Since $\chi(m) = \chi(m')$, it follows from the lemma that $[m] \in ker(\chi)$. Letting $H$ denote the congruence classes in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by $f(x, y)$, we obtain that $H \subseteq ker(\chi)$. It remains to show that $H$ is a subgroup of $ker(\chi)$. This follows from the following identity, which is taken from [Cox 1982]:

$$\text{(I) } (x^2 + ny^2)(x^2 + nw^2) = (xz + nyw)^2 + n(xw - yz)^2.$$  

This identity shows that $H$ is closed under multiplication. Let $m \in H$. Since $mx \in H$ for any $x \in H$, it follows that there exists an $x_0 \in H$ such that $mx_0 = 1$, showing that $H$ is a subgroup of $ker(\chi)$. This proves the Theorem.

(5) **Corollary**: If $f(x, y)$ is not in the identity class of $C(D)$, then the congruence classes it represents in $(\mathbb{Z}/D\mathbb{Z})^*$ form a coset of $H$ in the quotient group $ker(\chi)/H$, where $H$ is as described in Theorem 1.

**Proof**: Let $D = -4N$ and $f(x, y) \in C(D)$ be a form not in the identity class. The key to the proof of the Corollary is the fact that $f(x, y)$ properly represents some integers which are relatively prime to $D$ (this is an exercise in [Cox 1982]). Let $w$ be an integer relatively prime to $D$ that is properly represented by $f(x, y)$. Then, by a previous result we can assume without loss of generality that
\[ f(x, y) = w^2 + bxy + c^2, \] where \( b \) is even since \( D \equiv 0 (4) \). We then have the identity:

\[ (II) \quad 4wf(x, y) = (2wx + by)^2 - Dy^2. \]

Writing \( b = 2b' \) and recalling that \( D = -4N \), we can simplify (II) to obtain:

\[ (III) \quad wf(x, y) = (wx + b'y)^2 + Ny^2. \]

Therefore, if \( f(x, y) \) represents the congruence class \([a] \in (\mathbb{Z}/D\mathbb{Z})^* \), then the form \( x^2 + Ny^2 \) represents the congruence class \([w^2a] \). This implies that the congruence classes in \((\mathbb{Z}/D\mathbb{Z})^* \) represented by \( f(x, y) \) are contained in the coset \([w^{-1}]H \). Conversely, let \( q \in [w^{-1}]H \). Then \( x^2 + Np^2 \equiv wq \ (4N) \) for some integers \( x \) and \( p \). Using (III) and recalling that \( w \) is relatively prime to \( D = -4N \) we obtain that \( f(x, y) \equiv q \ (4N) \) is solvable. This shows that the congruence classes in \((\mathbb{Z}/D\mathbb{Z})^* \) represented by \( f(x, y) \) are exactly those in the coset \([w^{-1}]H \) and concludes the proof of the Corollary.

(6) **Theorem 3**: Let \( D \equiv 0 (4) \) and \( H \) be the subgroup of congruence classes represented by the form \( I(x, y) \). Let \( H_1, H_2, ..., H_l \) denote the different cosets of \( H \) represented by the reduced forms in \( C(D) \), where \( l \leq h(D) \). Then, for an odd prime \( p \) relatively prime to \( D \), we have \([p] \in H_i \) if and only if \( p \) is represented by one of the reduced forms whose representative coset is \( H_i \).

**Note**: By the term **representative coset** we mean the coset of congruence classes in \((\mathbb{Z}/D\mathbb{Z})^* \) represented by a reduced form in \( C(D) \). No form can represent more than one coset, hence we choose the term representative coset.

**Proof**: With notation as in the Theorem assume \( p \) is a prime such that \([p] \in H_i \). Since \( H_i \subseteq ker(\chi) \) it follows that \( D \) is a quadratic residue mod \( p \). Therefore, \( p \) is represented by one of the \( h(D) \) reduced forms in \( C(D) \). Since distinct cosets have trivial intersection it follows that \( p \) can't be represented by those reduced forms whose representative cosets do not contain \([p] \). Therefore, \( p \) is represented by one of the reduced forms whose representative coset is \( H_i \). Conversely, assume \( p \) is represented
by one of the reduced forms in \( C(D) \) whose representative coset is \( H_i \). Then it follows that \([p] \in H_i\). This proves the Theorem.

Theorems 1 and 2 show that the two reduced forms in \( C(-68) \) could not represent the same prime. If this was the case the cosets in \( ker(\chi)/H \) that correspond to these two forms would have non-empty intersection which would imply that they were identical. It is easily checked that \([5] \) is represented by the form \( 2x^2 + 2xy + 5y^2 \) but not by the form \( x^2 + 9y^2 \). With these facts in hand we can complete our classification problem. The Theorems above tells us exactly what congruence classes in \((\mathbb{Z}/36\mathbb{Z})^*\) the two reduced forms, \( x^2 + 9y^2 \) and \( 2x^2 + 2xy + 5y^2 \), could possibly represent. At best, they could represent all values in \( ker(\chi) \). Computing those \( m \in (\mathbb{Z}/36\mathbb{Z})^* \) for which \((\frac{-36}{m}) = 1\), we obtain the following set: \( \{1, 5, 13, 17, 25, 29\} \).

When we reduce \( x^2 + 9y^2 \) (mod 36) for any integer pair \((x, y)\) we will obtain \( x^2 \) if \( y \) is even. When \( y \) is odd we obtain \( x^2 + 9 \). This follows by expanding \( x^2 + 9(2k+1)^2 \) and reducing (mod 36). Therefore, a prime \( p \) is represented by the form \( x^2 + 9y^2 \) if and only if at least one of the congruences \( p \equiv x^2 + 9 \) (36) or \( p \equiv x^2 \) (36) is solvable. This follows since all elements in \( H \) are of the form \([x^2 + 9]\) or \([x^2]\). Using this fact we obtain that the only elements of \((\mathbb{Z}/36\mathbb{Z})^*\) that are of the form \( x^2 \) or \( x^2 + 9 \) and in \( ker(\chi) \) are 1,13, and 25. Since \([5] \) is represented by the form \( 2x^2 + 2xy + 5y^2 \), if we denote the coset of values represented by this form as \( H' \), we know that \( H \cap H' = \emptyset \). Therefore, we obtain the following classification for the case where \( D = -36 \):

\[
p = x^2 + 9y^2 \text{ iff } p = 1, 13, 25 \text{ (36)} \quad \text{and} \quad p = 2x^2 + 2xy + 5y^2 \text{ iff } p = 5, 17, 29 \text{ (36)}.
\]
The Classification of Primes Represented by $x^2 + 17y^2$

We have not yet run into the problem where two reduced forms represent the same coset of $H$ in the group $\ker(\chi)/H$. In the example where $D = -36$ it was easy to show that this was not the case by a simple computation. Furthermore, once we had determined the subgroup $H$ of congruence classes represented by the form $x^2 + 9y^2$ we were almost completely done with our classification. As we proceed to deal with the case where $D = -68$ we will see that significant difficulties arise using our previous methods.

Recall that the four reduced forms of discriminant $D = -68$ are: (1) $2x^2 + 2xy + 9y^2$ (2) $x^2 + 17y^2$ (3) $3x^2 + 2xy + 6y^2$ and (4) $3x^2 - 2xy + 6y^2$. One can see right away that forms (3) and (4) will represent the same congruence classes in $(\mathbb{Z}/68\mathbb{Z})^*$. Therefore the previous methods of classification will not work in this case. Furthermore, since $[21]$ is represented by both forms (1) and (2), we can see that the best we can do is separate forms (1) and (2) from forms (3) and (4). This is not a very satisfying classification because there are primes that are represented by form (1) and not by form (2) and vice-versa. For example, 13 is represented by form (1) and not by form (2) and 149 is represented by form (2) but not by form (1). We will therefore try another approach to classify what primes are represented by the form $x^2 + 17y^2$. Since the methods that will be developed deal specifically with the form $x^2 + 17y^2$, it is with the classification of primes represented by this form that we shall concern ourselves. The following definitions and facts are taken from [Cox 1982]:

**Note:** When we refer to ideals in a ring it will be assumed that we are speaking of non-zero proper ideals.

(1) **Definition:** Let $I_K$ denote the set of all fractional ideals of a number field $K$ and $P_K$ the subgroup of all principal ideals. The quotient group $I_K/P_K$ is called the ideal class group and is denoted $C(O_K)$.
(2) **Definition:** The Hilbert class field $L$ is defined to be the finite Galois extension of an imaginary quadratic extension $K$ which is the maximal unramified Abelian extension of $K$.

(3) Let $K$ be a number field and $O_K$ the algebraic integers of $K$. If $a$ is a prime ideal of $O_K$, the quotient ring $O_K/a$ is a finite field.

(4) If $K = \mathbb{Q}(\sqrt{-N})$ is an imaginary quadratic field, where $N$ is positive and square-free, then the discriminant $d_K$ of $K$ is defined to be: $d_K = \begin{cases} -N, & \text{if } N \equiv 3 \pmod{4}; \\ -4N, & \text{otherwise}. \end{cases}$

(5) If $K = \mathbb{Q}(\sqrt{-N})$, then $O_K = \begin{cases} \mathbb{Z}[\sqrt{-N}] & \text{if } -N \not\equiv 1 \pmod{4}; \\ \mathbb{Z}[\frac{1+\sqrt{-N}}{2}] & \text{otherwise}. \end{cases}$

(6) If $K$ is an imaginary quadratic field, the ideal class group $C(O_K)$ and the form class group $C(d_K)$ are isomorphic.

(7) If $L$ is a finite Galois extension of $K$ and $p$ is a prime ideal of $K$, the Galois group $\text{Gal}(L/K)$ acts transitively on prime ideals of $L$ containing $p$.

(8) If $L \supset K$ is the Hilbert Class Field, where $K$ is an imaginary quadratic field, then $C(O_K) \simeq \text{Gal}(L/K)$.

(9) Given a number field $K$, there is a one-to-one correspondence between unramified Abelian extensions $M$ of $K$ and subgroups $H$ of the ideal class group $C(O_K)$.

(10) Let $K$ be an imaginary quadratic field with discriminant $d_K$ and let $p \in \mathbb{Z}$ be a prime ideal. Then $p$ splits completely in $K$ iff $\left(\frac{d_K}{p}\right) = 1$. Furthermore, $p$ ramifies in $K$ iff $p$ divides $d_K$. In this case $pO_K = \beta^2$ for some prime ideal $\beta$ of $O_K$.

**NOTE:** $\left(\frac{\cdot}{p}\right)$ refers to the Kronecker symbol mentioned earlier in the paper.

Using fact (7) we obtain the following result which is an exercise in [Cox 1982]:

20
Corollary: If $L \supset K$ is Galois and $p$ is a prime ideal of $K$ which factors as: $pO_L = \beta_1^{e_1} \beta_2^{e_2} \cdots \beta_m^{e_m}$ in $O_L$, then we have $e_i = e_j$ for all $i, j \in \{1, 2, \ldots, m\}$. Furthermore, if $f_i$ denotes the inertial degree of $p$ in $\beta_i$, we also have $f_i = f_j$ for all $i, j \in \{1, 2, \ldots, m\}$.

Proof: We wish to show that $e_i = e_j$ for $i \neq j$. Choose $\sigma \in \text{Gal}(L/K)$ such that $\sigma(\beta_i) = \beta_j$. Since $\sigma(\beta_i^{e_i}) = \sigma(\beta_i)^{e_i} = \beta_j^{e_i}$, by the unique factorization of prime ideals in $O_L$ and the fact that $\sigma(p) = p$, we obtain that $e_i = e_j$. Next we want to show that $f_i = f_j$ for $i \neq j$. Define $\phi: O_L \mapsto O_L/\beta_j$ as $\phi(a) = \sigma(a) + \beta_j O_L$, where $\sigma \in \text{Gal}(L/K)$ is such that $\sigma(\beta_i) = \beta_j$. Then $\phi$ is a surjective homomorphism whose kernel is $\beta_i$. The fact that $\phi$ is a homomorphism is clear. Surjectivity follows from the fact that $\sigma$ is an automorphism of $L$. To see that $\ker(\phi) = \beta_i$, note that by our choice of $\sigma$ we clearly have $\beta_i \subset \ker(\phi)$. To show the reverse containment let $a \in \ker(\phi)$. The fact that $\sigma(a) \in \beta_j$ implies that $a \in \beta_i$ since $\sigma^{-1}(\beta_j) = \beta_i$. Therefore we obtain that $\ker(\phi) = \beta_i$, which implies that $O_L/\beta_i \simeq O_L/\beta_j$. This implies that $f_i = f_j$ for $i \neq j$, concluding the proof of the corollary.

The following result from [Cox 1982] shows the relevance of these results to our classification problem:

Theorem 1: Let $L$ be the Hilbert class field of $K = \mathbb{Q}(\sqrt{-n})$ where $n$ is positive, square-free, and $n \neq 3 (4)$. If $p$ is an odd prime not dividing $n$, then $p = x^2 + ny^2$ iff $p$ splits completely in $L$.

This theorem is the key result in our classification because it provides us with a necessary and sufficient condition to check whether a prime $p$ is represented by the form $x^2 + 17y^2$. However, we are far from finished with this case. Although the above theorem allows us to see the relevance of the algebraic machinery introduced, it does not have very much practical computational use. The condition that $p$ splits completely in $L$ is very abstract. What we need is a concrete practical procedure that will allow us to check if this condition holds or fails. The following result from [Cox
1982] is what we require:

**Theorem 2**: Let $K$ be an imaginary quadratic field, and let $L \supset K$ be finite and Galois over $K$ and $\mathbb{Q}$. Then:

(i) $L = K(\alpha)$, where $\alpha$ is a real algebraic integer.

(ii) Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of $\alpha$. If $p$ is a prime not dividing the discriminant of $f(x)$, then $p$ splits completely in $L$ iff \( (\frac{\alpha}{p}) = 1 \) and $f(x) = 0$ (mod $p$) has an integer solution.

Before proceeding to prove Theorem 2 we will need the following results, which are exercises in [Cox 1982]:

**Lemma 1**: If $K = \mathbb{Q}(\sqrt{-N})$, where $N$ is positive and square-free, and $L$ is a finite Galois extension of $K$, then $L$ is Galois over $\mathbb{Q}$ if and only if $\tau(L) = L$, where $\tau$ denotes complex conjugation.

**Proof**: Assume that $\tau(L) = L$. Denote the group of automorphisms of $L$ that fix $K$ as $G(L/\mathbb{Q})$, we obtain that $\tau \in G(L/K)$. Since $L \supset K$ is Galois we obtain $o(G(L/K)) = [L : K]$. Furthermore, for each $\sigma \in G(L/K)$ the map $\tau \circ \sigma \in G(L/\mathbb{Q})$. Doing this for each element of $G(L/K)$ we obtain $o(G(L/\mathbb{Q})) \geq [L: \mathbb{Q}]$. Since the reverse inequality always holds given the hypotheses, we obtain $o(G(L/\mathbb{Q})) = [L: \mathbb{Q}]$. This implies that $L$ is Galois over $\mathbb{Q}$. Conversely, assume that $L \supset \mathbb{Q}$ is Galois. Then, by definition, $\tau(L) = L$. This concludes the proof of the lemma.

**Lemma 2**: With the hypotheses as in Lemma 1, assume in addition that $L \supset \mathbb{Q}$ is Galois. Then:

1. $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$

2. For $\alpha \in L \cap \mathbb{R}$, $L \cap \mathbb{R} = \mathbb{Q}(\alpha)$ iff $L = K(\alpha)$.

**Proof**: By Lemma 1 we obtain that $\tau(L) = L$. We observe that $L \cap \mathbb{R}$ is the fixed field of
Therefore, if we let $S = <\tau>$ be the subgroup of $\text{Gal}(L/\mathbb{Q})$ generated by $\tau$, Galois Theory tells us that $[L \cap R : \mathbb{Q}] = |\text{Gal}(L/\mathbb{Q}) : S| = \frac{|L : \mathbb{Q}|}{2} = [L : K]$. This proves the first part of the lemma. We will now prove (2). Assume $L \cap R = \mathbb{Q}(\alpha)$, where $\alpha \in L \cap R$. Then we obtain $(L \cap R)(\sqrt{-N}) = (\mathbb{Q}(\alpha))(\sqrt{-N}) = K(\alpha)$. By (1) we know that $[L : \mathbb{Q}] = [L : L \cap R][-L \cap R : \mathbb{Q}] = [L : K][-K : \mathbb{Q}] = [L \cap R : \mathbb{Q}][K : \mathbb{Q}]$. It follows that $(L \cap R)(\sqrt{-N}) = L$. Therefore we obtain $L = K(\alpha)$. Conversely, assume that $L = K(\alpha)$, where $\alpha \in L \cap R$. Then we obtain $L \cap R = K(\alpha) \cap R$. From the definition of $K$ it follows that $L \cap R = \mathbb{Q}(\alpha)$. This concludes the proof of the lemma.

**Lemma 3:** Let $\mathbb{Q} \subset K \subset L$, where $K$ is an imaginary quadratic field and $L$ is Galois over $K$ and $\mathbb{Q}$. A prime ideal $p$ of $\mathbb{Z}$ splits completely in $L$ if and only if it splits completely in $K$ and some prime ideal $\beta$ of $O_K$ containing $p$ splits completely in $L$.

**Proof:** Assume that $p$ splits completely in $L$. If $\beta$ was a prime ideal of $O_K$ that contained $p$ and $e_{\beta|p} > 1$, we would obtain a contradiction to the fact that $p$ is unramified in $L$. To show that $f_{\beta|p} = 1$ for any prime ideal $\beta$ of $O_K$ containing $p$, let $\beta'$ denote a prime ideal of $O_L$ that contains $\beta$. We know that $\mathbb{Z}/p\mathbb{Z} \subset O_K/\beta \subset O_L/\beta'$. Since $\mathbb{Z}/p\mathbb{Z} \simeq O_{L/\beta'}$ we obtain that $f_{\beta|p} = 1$. We also obtain that every prime ideal $\beta$ of $O_K$ containing $p$ splits completely in $L$. This follows from the preceding arguments and from the product formula: $e_{\beta'|p} = e_{\beta'|\beta}e_{\beta|p}$. Conversely, assume that $p$ is a prime ideal of $\mathbb{Z}$ that splits completely in $K$ and that some prime ideal $\beta$ of $O_K$ containing $p$ splits completely in $L$. By the fact that $K$ is Galois over $\mathbb{Q}$ we know that if $pO_K = \beta_1\beta_2 \cdots \beta_m$ and $f_{\beta_i|p} = 1$ for some $i$, then $f_{\beta_i|p} = 1$ for all $i \in \{1, 2, ..., m\}$. By hypothesis, one of these $\beta_i$'s, say $\beta_1$, splits in $L$. For any prime $\beta'$ of $O_L$ that contains $\beta_1$, we obtain that $O_K/\beta_1 \simeq O_{L/\beta'}$. Since $L$ is Galois over $\mathbb{Q}$ we obtain that $\mathbb{Z}/p\mathbb{Z} \simeq O_L/\beta'$, for any prime $\beta'$ of $O_L$ containing $p$. The proof that the ramification indices are all 1 follows by an application of the product formula that we used in the first part of the proof. This proves that $p$ splits completely in $L$ and concludes the proof of the lemma.
We can now proceed to prove Theorem 2. The proof that is presented here is mostly taken from [Cox 1982]. We simply fill in the parts that have been left as exercises.

**Proof**: We first wish to show that there exists a real algebraic integer $\alpha$ that satisfies $L = K(\alpha)$.

By Lemma 1 we know that $[L \cap \mathbb{R} : \mathbb{Q}]$ is a finite algebraic extension of $\mathbb{Q}$. By the Primitive Element Theorem there exists a real algebraic integer $\alpha$ such that $L \cap \mathbb{R} = \mathbb{Q}(\alpha)$. By Lemma 2 we obtain that $L = K(\alpha)$. To prove the second part of the Theorem we will use the following scheme:

1. $p$ splits completely in $L$

$\iff$ (2) $p$ splits in $K$ and some prime ideal $\beta$ of $O_K$ containing $p$ splits in $L$

$\iff$ (3) $(\frac{d_K}{p}) = 1$ and $f(x) = 0 \ (\beta)$ is solvable in $O_K$

Before proceeding we note that if $f(x)$ is the minimal polynomial of $\alpha$ over $\mathbb{Q}$, then $f(x) \in \mathbb{Z}[x]$. This fact is proven in [Ireland and Rosen 1992]. Let $p$ be a prime not dividing the discriminant of $f(x)$. Then, by the definition of the discriminant, the roots of $f(x)$ are distinct modulo $p$. Therefore $f(x)$ is separable mod $p$. Since $K$ is an imaginary quadratic field we know that $pO_K = \beta_1 \beta_2$ for $\beta_1 \neq \beta_2$ iff $(\frac{d_K}{p}) = 1$. By Lemma 3, $p$ splitting in $L$ is equivalent to $p$ splitting in $K$ and one of the $\beta_i$'s, say $\beta_1$, splitting completely in $L$. This shows that (1) and (2) are equivalent. Now we must show that (2) and (3) are equivalent. Since we already know that $(\frac{d_K}{p}) = 1$ iff $p$ splits completely in $K$, we need only show that $f(x) = 0 \ (\beta_1)$ is solvable in $O_K$ iff $\beta_1$ splits completely in $L$. This is the content of the following result which we will prove now:

**Claim**: Let $J \supset M$ be Galois, where $J = M(u)$ for some $u \in O_J$. Let $g(x) \in O_M[x]$ be the monic minimal polynomial of $u$ over $M$. If $p$ is prime ideal in $O_M$ and $g(x)$ is separable modulo $p$, then we obtain:

(i) $p$ is unramified in $J$.  

24
(ii) $p$ splits completely in $J$ if and only if $g(x) = 0 \pmod p$ has a solution in $O_M$.

**Proof**: The proof of (i) is contained in [Lang 1994]. Since $g(x)$ is separable mod $p$ we can write $g(x) = g_1(x)g_2(x)\cdots g_m(x)$ where the $g_i(x)$ are distinct and irreducible mod $p$. Let $pO_J = \rho_1\rho_2\cdots\rho_m$.

It can be shown (see [Lang 1995]) that $\rho_i = pO_J + g_i(u)O_J$, $g_i(u) \in \rho_i$ for each $i$, and that the degrees of the $g_i$'s are all the same with common value $f_{\rho_i\mid p}$. If $p$ splits completely in $J$, all the degrees of the $g_i(x)$'s are 1. Since $g_i(x) = 0 \pmod {\rho_i}$ has a solution in $O_J$, the fact that $O_M/p \approx O_J/\rho_i$ implies that $g_i(x) = 0 \pmod p$ has a solution in $O_M$. This shows that $g(x) = 0 \pmod p$ has a solution in $O_M$.

Conversely, if $g(x) = 0 \pmod p$ has a solution $a$ in $O_M$, some $g_i$ satisfies $g_i(a) = 0 \pmod p$. Since all the $g_i$'s are irreducible mod $p$ we must have that all the $g_i$'s have degree 1. By the preceding arguments this shows that the inertial degree of $p$ in any of the $\rho_i$'s is 1, thereby proving that $p$ splits completely in $J$. This proves the claim.

Since we have proved that (1) and (2) are equivalent and that (2) and (3) are equivalent, we obtain that (1) and (3) are equivalent. So we know that $p$ splits completely in $L$ if and only if $(d_K/p) = 1$ and $f(x) = 0 \pmod {\beta_1}$ has a solution in $O_K$, where $\beta_1$ is a prime of $O_K$ which contains $p$. This is equivalent to the statement: $p$ splits completely in $L$ if and only if $(d_K/p) = 1$ and $f(x) = 0 \pmod p$ has an integer solution, which completes the proof of the Theorem.

We are now ready to classify primes that are represented by the form $x^2 + 17y^2$. The arguments presented here are analogous to those used in [Cox 1982], where the same problem is solved for the form $x^2 + 14y^2$. The first step will be to find a primitive element $\alpha$ such that the Hilbert class field $L$ of $K = \mathbb{Q}(\sqrt{-17})$ is of the form $L = K(\alpha)$. Then, letting $f_\alpha(x)$ denote the minimal polynomial of $\alpha$ in $\mathbb{Z}[x]$, we obtain that $p = x^2 + 17y^2$ iff $(-17/p) = 1$ and $f_\alpha(x) = 0 \pmod p$ has a solution in $\mathbb{Z}$.

**Claim**: Let $K = \mathbb{Q}(\sqrt{-17})$. For $\alpha = \sqrt{1+\sqrt{17}}/2$, $L = K(\alpha)$ is an extension of degree 4 and $f_\alpha(x) = x^4 - x^2 - 4$ is the minimal polynomial of $\alpha$. 

25
Proof: We shall prove that $x^4 - x^2 - 4$ is the minimal polynomial of $\alpha$. Since $\alpha = \sqrt{1 + \sqrt{17}}$ we obtain that $\alpha^2 = \frac{1 + \sqrt{17}}{2}$ from which we get $\alpha^4 = \frac{1}{4} + \frac{\sqrt{17}}{2} + \frac{17}{4}$. Since $\alpha^4 - \alpha^2 = 4$ we obtain that $\alpha$ is a root of $x^4 - x^2 - 4$. Using the quadratic formula we obtain that the 4 roots of this polynomial are: $\pm \sqrt{\frac{1 + \sqrt{17}}{2}}, \pm \sqrt{\frac{1 - \sqrt{17}}{2}}$. Since $\sqrt{17} \notin K$ we obtain that $f(x)$ is irreducible in $O_K[x]$. Let $\alpha' = \sqrt{\frac{1 - \sqrt{17}}{2}}$. Since $\alpha \alpha' = \sqrt{-4}$ and $\frac{\sqrt{-17}}{\sqrt{17}} \in L$ it follows that $\alpha \alpha' \in L$ and that all the 4 distinct roots of $f(x)$ lie in $L$. Therefore, $[L : K] = 4$ and $f_\alpha(x) = x^4 - x^2 - 4$. This concludes the proof of the claim.

Note that $L$ is Galois over $K$ and $\mathbb{Q}$ since all the 4 distinct roots of $f_\alpha(x)$ lie in $L$ and $L$ is closed under complex conjugation. Furthermore, since $[L : K] = o(\text{Gal}(L/K)) = 4$, we obtain that $L$ is an Abelian extension of $K$ because any finite group of order less than 6 is Abelian. If we show that all finite prime ideals $p$ in $K$ are unramified in $L$ we will have shown that $L$ is the Hilbert class field of $K$. This is because $h(-68) = 4 = o(\text{Gal}(L/K)) = o(C(O_K))$, which implies that $L$ is the maximal unramified Abelian extension of $K$. We do not need to bother with infinite primes because $K$ is an imaginary quadratic extension and therefore cannot be embedded in $\mathbb{R}$.

To show that $L \supset K$ is unramified we will use the following strategy. Let $K_1 = K(\sqrt{17})$ and $u = \frac{1 + \sqrt{17}}{2}$, so that $L = K_1(\sqrt{u})$. By the product formula quoted earlier it suffices to show that $K \subset K_1$ is unramified and that $K_1 \subset L$ is unramified. Applying the formula to each prime ideal $p$ in $O_K$ which is unramified in $L$ we see that $L$ is an unramified extension of $K$ iff $L$ is unramified over $K_1$ and $K_1$ is unramified over $K$. However, before we proceed with this strategy we need a concrete way to test that a prime ideal $p$ is unramified. The following result which is taken from [Cox 1982] does the job:

**Proposition 2**: Let $M = N(\sqrt{u})$ be a quadratic extension with $u \in O_N$. If $p$ is a prime ideal in $O_N$, then:
(1) If $2u \notin p$ then $p$ is unramified in $M$

(2) If $2 \in p$, $u \notin p$ and $u = b^2 - 4bc$ for some $b, c \in O_K$, then $p$ is unramified in $M$.

This Proposition allows us to prove that $K_1 \supset K$ and $L \supset K_1$ are unramified.

**Step 1**: $K_1 \supset K$ is unramified.

**Proof**: Since $17 = 1(4)$ we know that $O_K = \mathbb{Z}[\sqrt{-17}]$. Let $p$ be a prime ideal of $O_K$ and consider the element $2\sqrt{17}$. If $2\sqrt{17} \notin p$, then $p$ is unramified. Otherwise, if $2\sqrt{17} \in p$ we must have one of the following three possibilities: (i) $2 \notin p$ and $\sqrt{17} \in p$ (ii) $2 \in p$ and $\sqrt{17} \notin p$ (iii) $2 \in p$ and $\sqrt{17} \in p$.

We can see right away that (iii) is impossible. If $2 \in p$ and $\sqrt{17} \in p$ we would obtain that $2$ and $17 \in p$. This would imply that $1 \in p$, contradicting the fact that $p \neq O_K$. If the second possibility held, since $17 = 5^2 - 4 \cdot 2$, Proposition 2 would imply that $p$ is unramified. Therefore we are left to deal with the first possibility. Since $17$ divides $d_k = -68$ we obtain that $17 = \beta^2$ for some prime ideal $\beta$ in $O_K$. However, we are assuming that $\sqrt{17} \in p$. Therefore, by unique factorization, we obtain that $\beta = p$. Since $17O_K = p^2$ we obtain that $17 \in p^2$. This implies that $17$ is a square in $O_K$.

Therefore, there exist $a, b \in \mathbb{Z}$ such that $(a + b\sqrt{-17})^2 = 17$. This implies the following equalities: $2ab\sqrt{-17} = 0$ and $a^2 - 17b^2 = 17$. However, the first equality implies that one of $a$ or $b$ is zero.

Trying out both possibilities we can see that the second equality cannot hold in either case. We are therefore left with (ii) as the only viable possibility in the case where $2\sqrt{17} \in p$. This shows that $K_1 \supset K$ is unramified.

**Step 2**: $L \supset K_1$ is unramified.

**Proof**: Recall that $L = K_1(\sqrt{u})$ where $u = \frac{a + \sqrt{17}}{2}$. If $p$ is a prime of $O_{K_1}$ we must have either $2u \in p$ or $2u \notin p$. In the latter case Proposition 2 tells us that $p$ is unramified in $L$. In the former case we are again left with three possibilities as in Step 1: (i) $2 \in p$ and $u \notin p$ (ii) $2 \notin p$ and $u \in p$ (iii)
2 \in p \text{ and } u \in p. \text{ Assume that (ii) held and let } u' = \frac{1+\sqrt{17}}{2}. \text{ It is clear that } L = K_1(\sqrt{u}) = K_1(\sqrt{u'}).

Since \( u + u' = 1 \), not both of \( u \) and \( u' \in p. \) Otherwise we would obtain that \( p = O_{K_1}. \) Since we are assuming (ii), we obtain that \( u' \notin p. \) By applying Proposition 2 to \( L = K_1(\sqrt{u'}) \) we obtain that \( p \) is unramified. Now by the fact that \( L = K_1(\sqrt{u}) = K_1(\sqrt{u'}) \) we need only consider one of (i) or (iii).

Assume one of (i) or (iii) holds. Since \( u \) and \( u' \) satisfy the equation \( x = x^2 - 4 \), by Proposition 2 we obtain that \( p \) is unramified in \( L \) in either case. This shows that \( L \supset K_1 \) is unramified.

Collecting our results thus far we have shown that \( L \supset K \) is the Hilbert class field of \( K \), where \( K = \mathbb{Q}(\sqrt{-17}) \). Since \( 17 = 1 \times 4 \) and is square-free, the hypotheses of Theorems 1 and 2 are satisfied. Computing the discriminant of \( x^4 - x^2 - 4 \) we find that it is \(-2^9 \cdot 17^2\). This gives us the following criterion for deciding which primes are represented by the form \( x^2 + 17y^2 \):

**Theorem**: Let \( p \) be a prime \( p \neq 2, 17. \) Then \( p = x^2 + 17y^2 \) is solvable if and only if \((-17/p) = 1\) and \( x^4 - x^2 - 4 = 0 \) \( (p) \) has a solution in \( \mathbb{Z} \).

There are clearly limitations in the methods we have described to classify forms. The most obvious one is the problem of separating two forms with discriminant \( D \) whose representative cosets in \( (\mathbb{Z}/D\mathbb{Z})^* \) are identical. For example, this is the problem we encountered in the case where \( D = -68. \) For the most part, the main trick that was used was quadratic reciprocity. When this did not work we had to introduce a lot of new algebraic machinery to classify just one form.

We will next encounter some cases where some new techniques are required. Consider the following form: \( f(x, y) = x^2 + 243y^2 \) (this example is taken from [Ireland and Rosen 1992]). It is known from the theory of cubic residues that for a prime \( p \) congruent to 1 mod 3, \( 4p = x^2 + 243y^2 \) is solvable if and only if \( 3 \) is a cubic residue modulo \( p. \) Furthermore, consider the form \( f(x, y) = x^2 + 64y^2. \) It is known that this form represents a prime \( p \) if and only if \( 2 \) is a biquadratic residue modulo \( p. \) The proofs of these theorems are quite elementary. However they require a
totally different approach from what we have used thus far. In the next section we will introduce
the methods required to derive these results.

In considering a form $f(x, y)$ we were interested in knowing what primes were representable by
this form. In many cases this question, for a given $p$, was dependent on the solvability of certain
congruences in the field $\mathbb{Z}_p$. Therefore, in working over this finite field, we were able to obtain
an answer to one of our main questions. In the following section we will explore this relation more
deeply.
Character Sums in Finite Fields

Let \( \chi \) denote a multiplicative character over \( \mathbb{F}_p \). The following is a list of some of the elementary facts we shall assume about characters.

**Note:** We define \( \chi(0) = \begin{cases} 0, & \text{if } \chi \neq \varepsilon; \\ 1, & \text{if } \chi = \varepsilon, \end{cases} \)

1) \( \chi \) is a \((p-1)\)st root of unity.

2) \( \chi(a^{-1}) = \overline{\chi(a)} \)

3) Let \( N(x^k = a) \) denote the number of solutions in \( \mathbb{F}_p \) of \( x^k = a \). Then, when \( k \mid p-1 \), we have \( N = \sum \chi(a) \), where the sum is over all characters of order dividing \( k \).

4) If \( a \in \mathbb{F}_p^* \) and \( a \neq 1 \), then \( \sum \chi(a) = 0 \), where the sum is over all characters of the field.

5) If \( \chi \neq \varepsilon \), where \( \varepsilon \) denotes the identity character, then \( \sum_{a=0}^{p-1} \chi(a) = 0 \).

**Definition:** The Gauss sum belonging to a given character \( \chi \) is \( g_\chi(\chi) = \sum \chi(t)\zeta^{at} \), where \( a \) is a fixed element of \( \mathbb{F}_p^* \), \( \zeta = e^{2\pi i/p} \), and the sum ranges over all \( t \) in \( \mathbb{F}_p \).

**Definition:** Let \( \chi_1, \ldots, \chi_r \) be characters of the field \( \mathbb{F}_p^* \). Then the Jacobi sum \( J(\chi_1, \chi_2, \ldots, \chi_r) \) is defined as follows: \( J(\chi_1, \chi_2, \ldots, \chi_r) = \sum \chi_1(t_1)\chi_2(t_2) \cdots \chi_r(t_r) \), where the sum extends over all \( r \)-tuples of \( t_i \)'s whose sum is 1.

The proofs of the results preceding the definitions can be found in [Ireland and Rosen 1992]. We shall in addition use the following results on Jacobi and Gauss sums:

1) \( J(\varepsilon, \varepsilon) = p \)

2) \( J(\varepsilon, \chi) = 0 \), if \( \chi \neq \varepsilon \)

3) \( J(\chi, \chi^{-1}) = -\chi(-1) \)

4) \( |g(\chi)| = \sqrt{p} \), provided that \( \chi \neq \varepsilon \)

This concludes the list of preliminary facts which we shall be using.

Let \( a, b, c \neq 0 \) and consider the equation \( ax^2 + by^2 = c \) over \( \mathbb{F}_p \). Then it is easy to see that the equation has a solution. To see this, consider the set of elements of the form \( ax^2 \) and \( c - by^2 \). These two sets are non-disjoint, since each set contains \( \frac{p+1}{2} \) elements by the cyclicity of \( \mathbb{F}_p^* \). This example is taken from a
homework assignment in Mathematics 504.

Let's specialize our situation a little more and choose $a, b, c = 1$. Then, using the above facts, the number of solutions of the equation is

$$N(x^2 + y^2 = 1) = \sum (1 + \chi(a))(1 + \chi(b))$$

where the sum is over all $a, b$ such that $a + b = 1$ and $\chi$ denotes the quadratic character. Then, expanding the summand, we obtain $N = p + J(\chi, \chi)$. Now, since $\chi$ is its own inverse, by the above facts on Jacobi sums, we have $J(\chi, \chi) = -\chi(-1)$. Thus, if $p \equiv 1 \ (4)$, $N = p - 1$, and when $p \equiv 3 \ (4)$, $N = p + 1$.

Now let at least one of $a$ or $b$ be a non-square, since if both were squares we could absorb them into the variables and reduce it to the situation we just dealt with. Thus, consider

$$N(ax^2 + by^2 = c) = \sum (1 + \chi(a^{-1})\chi(A))(1 + \chi(b^{-1})\chi(B))$$

where the sum is over all $A, B$ such that $A + B = c$. Now let $A = cP$, $B = cQ$, where $P + Q = 1$. Then we can rewrite our sum as follows:

$$\sum (1 + \chi(a^{-1}c)\chi(P))(1 + \chi(b^{-1}c)\chi(Q))$$

Expanding we obtain that $N = p + \chi(a^{-1}b^{-1})J(\chi, \chi)$. If $a$ and $b$ are non-squares, then $\chi(a)$ and $\chi(b) = -1$. Therefore, in this case $N = p + J(\chi, \chi)$. Thus, by the same reasoning as above we obtain that $N = p + 1$ if $p \equiv 3 \ (4)$ and $p - 1$ when $p \equiv 1 \ (4)$. If $a$ is a square and $b$ is a non-square, or vice versa, then we have $N = p - J(\chi, \chi)$. So, $N = p - 1$ if $p \equiv 3 \ (4)$ and $p + 1$ if $p \equiv 1 \ (4)$.

As our next example consider the same equation with exponent $n = 3$. We must break up our analysis into two cases $p \equiv 1 \ (3)$ and $p \equiv 2 \ (3)$. If $p \equiv 2 \ (3)$, then $(3, p - 1) = 1$. Thus, the map $x \mapsto x^3$ is an automorphism of $F_p^*$. So the number of solutions to $x^3 + y^3 = 1$ is the same as the number of solutions to $x + y = 1$. However, for the latter equation we can pick $y$ arbitrarily ($p$ choices), and $x$ is then determined. Thus, there are $p$ solutions if $p \equiv 2 \ (3)$. If $p \equiv 1 \ (3)$, the argument is a little more complicated. Using the facts on Jacobi sums we obtain the following equation:

$$N(ax^3 + by^3 = c) = \sum (1 + \chi(a^{-1}A) + \chi^2(a^{-1}A))(1 + \chi(b^{-1}B) + \chi^2(b^{-1}B))$$
where the sum is over all $A, B$ such that $A + B = c$ and $\chi$ denotes a cubic character. Let $A = cM$ and $B = cN$. Then, our sum becomes:

$$N(ax^3 + by^3 = c) = \sum (1 + \chi(a^{-1}cM) + \chi^2(a^{-1}cM))(1 + \chi(b^{-1}cN) + \chi^2(b^{-1}cN))$$

where the sum is over all $M, N$ such that $M + N = 1$. Then, expanding we obtain

$$N = p + \chi((ba)^{-1}c^2)J(\chi, \chi) + \chi^2((ba)^{-1}c^2)J(\chi^2, \chi^2) + \chi(a^{-1}c)\chi^2(b^{-1}c)J(\chi, \chi^2) + \chi(b^{-1}c)\chi^2(a^{-1}c)J(\chi, \chi^2)$$

From the facts on Jacobi sums, we know that $J(\chi, \chi^2) = -\chi(-1)$. Since -1 is a cube we obtain that $J(\chi, \chi^2) = -1$. Now consider the terms with $J(\chi, \chi)$ and $J(\chi^2, \chi^2)$. Since $\chi$ is a cubic character, $J(\chi, \chi) \in \mathbb{Z}[\omega]$, where $\omega = (-1 + \sqrt{-3})/2$. Thus, $J(\chi, \chi) = g + h\omega$, for $g, h \in \mathbb{Z}$. Since $J(\chi^2, \chi^2) = \overline{J(\chi, \chi)}$, this implies that $J(\chi, \chi) + J(\chi^2, \chi^2) = J(\chi, \chi) + \overline{J(\chi, \chi)} = 2\Re J(\chi, \chi) = 2g - h$. So, getting back to our sum, thus far we have determined that:

$$N(ax^3 + by^3 = c) = p - \chi(a^{-1}b) - \chi(ab^{-1}) + (\text{terms with } J(\chi, \chi) \text{ and } \overline{J(\chi, \chi)})$$

Now, the coefficients of each of the latter Jacobi sums are $\chi((ba)^{-1}c^2)$ and $\chi(cba)$ respectively. Let $k = (ba)^{-1}c^2$. Then, the coefficients are $\chi(k)$ and $\chi(k^{-1})$. If $k$ was a cube, both of the latter would be equal to 1. We can further simplify our equation to obtain:

$$(1) \quad N(ax^3 + by^3 = c) = p - \chi(a^{-1}b) - \chi(ab^{-1}) + (2g - h)$$

If $k$ is not a cube then $\chi(k) = \omega$ or $\omega^2$. If the latter holds then:

$$N(ax^3 + by^3 = c) = p - \chi(a^{-1}b) - \chi(ab^{-1}) + \omega^2 \cdot J(\chi, \chi) + \omega \cdot \overline{J(\chi, \chi)}.$$ 

In the other case, we exchange the coefficients of $J(\chi, \chi)$ and $\overline{J(\chi, \chi)}$. Therefore, when $\chi(k) = \omega^2$ we obtain

$$J(\chi, \chi)\chi(k)+\overline{J(\chi, \chi)}\chi(k^{-1}) = (g + h\omega)\omega^2 + (g + h\omega^2)\omega = 2h - g.$$ 

If $\chi(k) = \omega$ we obtain $J(\chi, \chi)\omega + \overline{J(\chi, \chi)}\omega^2 = (g + h\omega)\omega + (g + h\omega^2)\omega^2 = -g - h$. This takes care of the case where $k$ is a non-cube. Consider the term $-(\chi(a^{-1}b) + \chi(ab^{-1}))$ in formula (1) above. We obtain that $\chi(a^{-1}b) = \chi(ba^{-1}) = \chi((ab)^{-1}) = \overline{\chi(ab)}$. Therefore, if $ab^{-1}$ is a cube, we have that $-(\chi(a^{-1}b) + \chi(ab^{-1})) = -2$. Otherwise, using the fact that
\[ \omega^2 + \omega + 1 = 0, \] we obtain that \(- (\chi(a^{-1}b) + \chi(ab^{-1})) = 1.\] We now have enough information to pin down some actual values for \(N\), given a value for \(p\).

Consider \(p = 7\). Since \(|J(\chi, \chi)| = \sqrt{p}\), we obtain \(g^2 - gh + h^2 = 7\) (we are assuming some facts about the norm function on \(Z[\omega]\) which will be formally stated later). In this representation, \(g,h\) must satisfy \(g \equiv 2 (3), \text{ and } h \equiv 0 (3)\). This is also a fact which we shall assume for now and prove later when we are in the process of describing the primary elements of \(Z[\omega]\). The fact that \(g \equiv 2 (3)\) and \(h \equiv 0 (3)\) immediately shows that \(g,h\) have the same sign since if they had opposite sign, all the terms in the representation of \(p\) would be positive. Since \(g,h\) are bounded by 3 in absolute value, this implies that \(h = \pm 3\) and \(g = -1\) or 2.

Now, rewriting the equation as: \(g^2 - gh + h^2 = (g-h)^2 + gh = 7\), we can see that we must have \(g = 2\) and \(h = 3\) or \(g = -1\) and \(h = -3\). Either way, the quantity \(2g - h\) is equal to 1. So now all we need to do is specify coefficients for our equation. Since 5 is a generator of \(F^*_p\), let \(c = 5^3, b = 5^3\), and \(a = 5\). We can now evaluate the equation:

\[ N(5x^3 + 3y^3 = 6) = 7 - \chi(2) - \chi(4) + 1. \]

Since \(a^{-1}b\) is not a cube the number of solutions to this equation is 9.

As a final example consider the case with the exponent \(n = 4\). It will be necessary to split up into cases where \(p \equiv 1 \text{ or } 3 (4)\). If \(p \equiv 3 (4)\) and \(p > 3\) we claim that the map \(\phi(x) = x^4\) takes \(F^*_p\) onto the subgroup \(S\) of squares in \(F^*_p\). Otherwise, we would obtain that \(Im(\phi)\) is a subgroup of \(S\) of index 2. This implies that \(4|p - 1\), which is a contradiction. Therefore, the number of solutions to the equation \(x^4 + y^4 = 1\) is the same as the number of solutions to \(x^2 + y^2 = 1\). We found earlier that this value is \(N = p + 1\). The much more interesting case is when \(p \equiv 1 (4)\). Then, letting \(a,b,c = 1\), we obtain the following equation:

\[ N(x^4 + y^4 = 1) = \sum N(x^4 = a)N(y^4 = b) \]

where the sum is over all \(a,b\) such that \(a + b = 1\). Letting \(\chi\) be a character of order 4 and \(\rho\) be the quadratic character, we rewrite the sum as: \(\sum (1 + \chi(a) + \rho(a) + \chi^3(a))(1 + \chi(b) + \rho(b) + \chi^3(b))\). Expanding this product and summing, we obtain

\[ N = p + J(\chi, \rho) + J(\chi, \chi^{-1}) + J(\chi, \chi) + J(\chi^{-1}, \rho) + J(\chi^{-1}, \chi^{-1}) + J(\chi^{-1}, \chi^{-1}) + J(\rho, \chi) + J(\rho, \chi^{-1}) + J(\rho, \rho) \]
which equals: \( p + 4 \text{Re} J(\chi, \rho) - 2\chi(-1) + J(\rho, \rho) + 2\text{Re} J(\chi, \chi) \). Since \( \chi(-1)^2 = 1 \), we obtain that \( \chi(-1) = \pm 1 \).

If \( \chi(-1) = 1 \), then \( N = p - 3 + 4\text{Re} J(\chi, \rho) + 2\text{Re} J(\chi, \chi) \). Otherwise, \( N = p + 1 + 4\text{Re} J(\chi, \rho) + 2\text{Re} J(\chi, \chi) \).

Since \( \chi \) is a biquadratic character, it is either \( \pm i \) or \( \pm 1 \). Therefore, \( J(\chi, \rho) \in \mathbb{Z}[i] \) which implies that \( J(\chi, \rho) = a + bi \), for some integers \( a, b \). We shall require the following results to deduce further information about \( N \). The lemmas are both taken from exercises in [Ireland and Rosen 1992]:

**Lemma 1**: \( N = p - 3 + 6\text{Re} J(\chi, \rho) \) if \( p \equiv 1 \pmod{8} \), and \( N = p + 1 + 2\text{Re} J(\chi, \rho) \) if \( p \equiv 5 \pmod{8} \).

**Proof**: By a result in [Ireland and Rosen 1992] we know that \( J(\chi, \chi) = \chi(-1)J(\chi, \rho) \). We can also write \( \chi(-1) = (-1)^{(\frac{p-1}{4})} \) (this is a special case of a more general fact which will be stated later). Therefore, if \( p \equiv 1 \pmod{8} \), then \( \chi(-1) = 1 \) and we obtain that \( N = p - 3 + 6\text{Re} J(\chi, \rho) \). If \( p \equiv 5 \pmod{8} \), then \( \chi(-1) = -1 \) which implies that \( N = p + 1 + 2\text{Re} J(\chi, \rho) \). This concludes the proof.

The following two facts are taken from [Ireland and Rosen 1992]:

**Theorem 1**: If \( \chi \) and \( \lambda \) are multiplicative characters of the finite field \( F_p \) and \( \chi \lambda \neq \epsilon \), then \( |J(\chi, \lambda)|^2 = p \).

**Theorem 2**: Let \( \pi = -J(\chi, \rho) = c + di \) where \( c \) is odd and \( d \) be even. If \( 4 | d \), then \( c \equiv 1 \pmod{4} \). If 4 does not divide \( d \), then \( c \equiv 1 \pmod{4} \).

**Proof**: It was stated earlier that \( J(\chi, \chi) = \chi(-1)J(\chi, \rho) \). It is shown in [Ireland and Rosen 1992] that \( \pi = -\chi(-1)J(\chi, \chi) \equiv 1 \pmod{2 + 2i} \). We claim that the Theorem follows from this result. First suppose that \( 4 | d \). Since \( 4 = -2(1 + i)(1 - i) \) we obtain \( \pi = c + di \equiv c (2 + 2i) \equiv 1 (2 + 2i) \). Taking conjugates we obtain \( c \equiv 1 (2 - 2i) \). This implies that \( 8|(c - 1)^2 \), from which it follows that \( c \equiv 1 \pmod{4} \). If 4 does not divide \( d \), then letting \( d = 4k + 2 \) we obtain \( \pi = c + di \equiv c + 2i (2 + 2i) \equiv c - 2 (2 + 2i) \equiv 1 (2 + 2i) \). Therefore, \( c \equiv 3 (2 + 2i) \). Taking conjugates again we obtain \( 8|(c - 3)^2 \), from which it follows that \( c \equiv -1 \pmod{4} \). This proves the Theorem.

By Theorem 1 we know that \( p = \pi \overline{\pi} = c^2 + d^2 \). If we require that \( c \) is odd and \( d \) is even, then unique factorization in \( \mathbb{Z}[i] \) implies that \( c \) and \( d \) are uniquely determined up to sign. Theorem 2 provides the conditions that determine the sign of \( c \).

Using these facts we obtain the following refinement of Lemma 1:

**Lemma 2**: Let \( p \equiv 1 \pmod{4} \), so that \( p = A^2 + B^2 \). If we require that \( A \equiv 1 \pmod{4} \), so that \( A \) is fixed, then \( N = \)
\( p - 3 - 6A \) when \( p \equiv 1 \) (8) and \( N = p + 1 + 2A \) if \( p \equiv 5 \) (8).

**Proof**: By the previous result, \( N = p - 3 - 6Re\pi \) when \( p \equiv 1 \) (8). Since \( \pi = c + di \), we have \( N = p - 3 - 6c \) and \( p-1 \equiv 0 \) (8) implies that \( d \equiv 0 \) (4). This implies \( c = A \) and \( N = p - 3 - 6A \). If \( p \equiv 5 \) (8), then \( p-1 \equiv 4 \) (8). This implies that \( d \equiv 2 \) (4). Thus, \( c \equiv -1 \) (4) which means that \( c = -A \). Then \( N = p + 1 + 2ReJ(\chi, \rho) = p + 1 - 2c = p + 1 + 2A \). This concludes the proof.

Consider the examples \( p = 17, 29 \). Then, since \( 17 = 1^2 + 4^2 \), we obtain \( N = 17 - 3 - 6 = 8 \). And, since \( 29 = 5^2 + 2^2 \), \( N = 29 + 1 + 10 = 40 \).

Before proceeding to the next example, we shall require a few facts about the ring \( \mathbb{Z}[\omega] \), where \( \omega = (-1 + \sqrt{-3})/2 \).

1. **Definition**: The norm in this ring is: \( N(a + b\omega) = a^2 - ab + b^2 \).

2. **Definition**: A prime \( \pi = a + b\omega \) in \( \mathbb{Z}[\omega] \) is called primary if we have \( a \equiv 2 \) (3) and \( b \equiv 0 \) (3), where \( a, b \) are elements of \( \mathbb{Z} \).

3. Let \( G = \mathbb{Z}[\omega] \). For a prime \( \pi \) defined as above, the ring \( G/\pi G \) is a finite field.

4. Let \( \pi \) be a prime in \( G \) and \( \chi_\pi \) a cubic character of the finite field \( G/\pi G \). Then \( J(\chi, \chi) = a + b\omega \) for some \( a \equiv 2 \) (3), \( b \equiv 0 \) (3).

5. Given any prime \( p \equiv 1 \) (mod 3) \( \in \mathbb{Z} \), there exists a prime \( \pi \) in \( \mathbb{Z}[\omega] \) such that \( p = \pi \bar{\pi} \). Conversely, if \( \pi \) is a complex prime in \( G \) its norm is a prime in \( \mathbb{Z} \) which is congruent to 1 (mod 3).

6. If \( \chi_\pi \) is as above, then for \( \alpha \in G/\pi G \) we have \( \alpha^{N_{G/\pi G}^{-1}} \equiv \chi_\pi(\alpha) \) (mod \( \pi \)).

7. (Eisenstein’s Supplement to the Law of Cubic Reciprocity) If \( \pi = a + b\omega \) is a complex primary element of \( D \) so that \( a = 3m - 1 \), then \( \chi_\pi(1 - \omega) = \omega^{2m} \).

These results and their proofs can be found in [Ireland and Rosen 1992].

The above facts and the theorem regarding norms of Jacobi sums then imply the following result:

**Corollary**: Let \( p \equiv 1 \) (mod 3) and \( \chi \) be a cubic character. Then \( J(\chi, \chi) = a + b\omega \), where \( a \equiv 2 \) (3) and \( b \equiv 0 \) (3).

Thus far we have concerned ourselves only with determining the solvability of certain equations over finite fields and finding formulas for the number of solutions to those equations that are solvable. However,
the following examples show that there is a striking link between such investigations and our earlier results concerning representations of primes by quadratic forms over the integers. The first example shows that a prime $p$ is represented by a certain form if and only if a special congruence is solvable in the finite field $\mathbb{F}_p$.

This result is taken from an exercise in [Ireland and Rosen 1992]:

**Proposition 1**: Let $p$ be a prime congruent to 1 mod 3, so that $p = \pi \bar{\pi}$ for some primary prime $\pi = a + b\omega$. Then $x^3 \equiv 3 \pmod{p}$ is solvable in $\mathbb{Z}$ if and only if $p$ satisfies $4p = C^2 + 243B^2$, where $C = 2a - b$ and $B \in \mathbb{Z}$.

**Proof**: Let $\pi = a + b\omega$, where $a = 3m - 1$ and $b = 3n$ for some integers $m$ and $n$. Letting $\chi_\pi$ denote the cubic character, we claim that $\chi_\pi(3) = \omega^{2n}$. This follows since $3 = -\omega^2(1 - \omega)^2$, which implies that $\chi_\pi(3) = \chi_\pi(-\omega^2)\chi_\pi((1 - \omega)^2) = \chi_\pi(\omega)^2\chi_\pi(1 - \omega)^2 = (\omega^{\frac{a^2 + 3b^2 - 1}{3}})^2 \omega^{4m}$. Now $\frac{a^2 - ab + b^2 - 1}{3} = -2m + n (3) = m + n (3)$

Simplifying our results we obtain that $\chi_\pi(3) = \omega^{2n}$. Furthermore, $\omega^{2n} = 1$ if and only if $3|n$. This implies that $b = 9k$ for some integer $k$. Thus, rewriting $p = a^2 - ab + b^2$ as $4p = 4a^2 - 4ab + 4b^2 = (2a - b)^2 + 3b^2$, the fact that $9$ divides $b$ implies, letting $C = 2a - b$ and $B = \frac{b}{3}$, that $4p = C^2 + 243B^2$. This shows that $\chi_\pi(3) = 1$ if and only if $9|b$. Therefore it is clear that if $x^3 \equiv 3 \pmod{p}$ is solvable, then $p$ satisfies $4p = (2a - b)^2 + 243B^2$.

Conversely, assume $p$ satisfies $4p = (2a - b)^2 + 243B^2$. From the definition of the norm we can deduce that $4p = (2a - b)^2 + b^2$. This implies that $243B^2 = b^2$, showing that $9|b$. This concludes the proof of the proposition.

In what follows we give an elegant proof of Gauss' Theorem and show an application of this theorem to counting solutions of equations over finite fields. This proof is taken from [Ireland and Rosen 1992].

**Gauss' Theorem**: If $p \equiv 1 \pmod{3}$ there are integers $A, B$ such that $4p = A^2 + 27B^2$.

**Proof**: Let $\chi$ be a cubic character of $G/\pi G$, where $p = \pi \bar{\pi}$. From our definitions we know that $J(\chi, \chi) = a + b\omega$ is primary. Taking the norm of this quantity and using the fact that $|J(\chi, \chi)|^2 = p$ we obtain, $p = a^2 - ab + b^2$. This implies that $4p = (2a - b)^2 + 3b^2$. Then, letting $A = 2a - b$, and $B = \frac{b}{3}$, we obtain that $4p = A^2 + 27B^2$. This concludes the proof of Gauss' Theorem.

As a further application of this result consider the form $x^3 + y^3$. The following result (taken from [Ireland and Rosen 1992]) provides a stunning application of Gauss' Theorem:

**Proposition 2**: Let $p$ be a prime congruent to 1 modulo 3 so that $4p = A^2 + 27B^2$ for some integers $A$
and \( B \). Then \( A \) is uniquely determined if we require that \( A \equiv 1 \pmod{3} \), and the number \( N \) of solutions to the equation \( x^3 + y^3 = 1 \) in the finite field \( \mathbb{F}_p \) is equal to \( p - 2 + A \).

**Proof**: Let \( A, B \) satisfy \( 4p = A^2 + 27B^2 \). We wish to show that if \( A \equiv 1 \pmod{3} \), then \( A \) is unique. Assume there is another pair \( (C, D) \) such that \( C \equiv 1 \pmod{3} \) and \( 4p = C^2 + 27D^2 \). Then \( 4p(D^2 - B^2) = (A^2 + 27B^2)(C^2 + 27D^2) - (C^2 + 27D^2)B^2 = (AD + CB)(AD - CB) \). It follows that \( p \) divides one of the latter factors. Assume without loss of generality that \( p \) divides \( (AD - CB) \). Then, we have that \( 16p^2 = (A^2 + 27B^2)(C^2 + 27D^2) = A^2C^2 + 27B^2C^2 + 27A^2D^2 + 27B^2D^2 = A^2C^2 + 27B^2C^2 + 27A^2D^2 + 27B^2D^2 + 54AFCD - 54ABC \) \( D = (AC + 27BD)^2 + 27(AD - CB)^2 \). This implies that \( 16p^2 - (AC + 27BD)^2 = 27(AD - CB)^2 \). From this we obtain that \( p | (AC + 27BD) \). Dividing through the last equation by \( p^2 \) we obtain that \( 16 \cdot \frac{(AC + 27BD)^2}{p^2} = \frac{27(AD - CB)^2}{p^2} = 27K^2 \) where \( K = \frac{(AD - CB)}{p} \). This equality can hold only if \( K = 0 \). This implies that \( AD = CB \). From this we obtain that \( A = kC \) for some rational constant \( k \). Then the equation \( 4p = A^2 + 27B^2 = k^2(A^2 + 27B^2) \) implies that \( k = \pm 1 \). Since we assumed that \( A \) and \( C \) are congruent to 1 \( \pmod{3} \) we must have \( k = 1 \). This uniqueness argument is taken from [Silverman-Tate 1992]. By our previous work, we saw that the number of solutions to the equation \( x^3 + y^3 = 1 \) was given by the formula \( N = p - 2 + 2ReJ(\chi, \chi) \), where \( \chi \) denotes a cubic character of the field \( G/\pi G \). Since \( J(\chi, \chi) = a + b\omega \) for some integers \( a, b \), we obtain that \( ReJ(\chi, \chi) = \frac{(2a - b)}{2} \). Since \( J(\chi, \chi) \) is primary we obtain that \( a \equiv 2 \pmod{3} \), which shows that \( 2a - b \equiv 1 \pmod{3} \). Writing \( 4p = (2a - b)^2 + 27B^2 \), where \( B = \frac{b}{3} \), we obtain that \( N = p - 2 + 2ReJ(\chi, \chi) = p - 2 + A \) by the uniqueness of \( A \).

The next result is a proof of the biquadratic character of 2. Before proceeding we will list a few facts that are required for the proof:

1. Let \( p \equiv 1 \pmod{4} \) be a prime in \( \mathbb{Z} \). There exists a prime \( \pi = a + bi \in \mathbb{Z}[i] \) such that \( p = \pi \overline{\pi} \). Conversely, if \( \pi = a + bi \) is a complex prime in \( \mathbb{Z}[i] \), then \( \pi \overline{\pi} = p \), where \( p \equiv 1 \pmod{4} \).

2. Let \( H = \mathbb{Z}[i] \) and \( \pi \) be as above. Then, \( H/\pi H \) is a finite field.

3. If \( \alpha \in H/\pi H \), then \( \left( \frac{\alpha}{\pi} \right)_4 \equiv \alpha^{\frac{N_{\pi}-1}{4}} \pmod{\pi} \).

**Proposition**: \( x^4 = 2 \pmod{p} \) is solvable if and only if \( p = m^2 + 64n^2 \), for some integers \( m, n \).

**Proof**: Since \( p \equiv 1 \pmod{4} \) we know that we can write \( p = a^2 + b^2 \), where \( a \) is odd and \( b \) is even. Choose
π ∈ D such that p = ππ. Furthermore, quadratic reciprocity implies \((\frac{a}{p}) = 1\) since \((\frac{a}{p}) = (\frac{p}{a})\). Now if we denote the biquadratic residue symbol by \((\frac{2}{\pi})_4\) to distinguish it from the Jacobi symbol, we wish to find necessary and sufficient conditions such that \(\(\frac{2}{\pi}\)_4 = 1\). We claim that \((\frac{2}{\pi}) = i^{\frac{3b}{4}}\). To see this note that

\[2p = (a + b)^2 + (a - b)^2\]

therefore, \((\frac{2p}{a+b}) = 1\) which implies that \((\frac{-2}{a+b})(\frac{-p}{a+b}) = (\frac{-2}{a+b})(\frac{a+b}{p}) = 1\) by quadratic reciprocity. Therefore, we obtain that \((\frac{a+b}{p}) = (-1)^{\frac{(a+b)^2-1}{8}}\). However, \((-1)^{(a+b)^2-1} = (-1)^{\frac{1}{2}\cdot \frac{a^2 + b^2 + 2ab - 1}{4}} = i^{\frac{-1}{4}} \cdot i^{\frac{3b}{4}} = (\frac{1}{\pi})_4 \cdot i^{\frac{3b}{4}}\). Now, to relate \((\frac{a+b}{p})\) to \((\frac{2}{\pi})_4\) note that \((a + b)^2 = a^2 + b^2 + 2ab \equiv 2ab (p)\) which implies that \((\frac{a+b}{p}) = (\frac{2ab}{\pi})_4\). Since \(π = a + bi\) we know that \(b \equiv ai (π)\), which implies that \(2ab \equiv (a + ai)^2 (π) \equiv a^2(1 + i)^2 (π) \equiv 2a^2i (π)\). Therefore, \((\frac{a+b}{p}) = (\frac{2ab}{\pi})_4 = (\frac{a^2}{\pi})_4(\frac{i}{\pi})_4(\frac{a^2}{\pi})_4\). Since \((\frac{a}{p}) = 1\), we obtain that \((\frac{a^2}{\pi})_4 = 1\). Therefore, we have: \((\frac{2}{\pi})_4(\frac{1}{\pi})_4 = (\frac{2ab}{\pi})_4 \cdot i^{\frac{3b}{4}}\). This proves the claim that \((\frac{2}{\pi})_4 = i^{\frac{3b}{4}}\). Now, \(x^4 = 2\) is solvable mod \(p\) if and only if \((\frac{2}{\pi})_4 = 1\) which happens if and only if \(8|ab\).

Since \(b\) is odd this happens iff \(8|a\). Therefore, letting \(a = 8m\), we obtain that \(x^4 = 2\) is solvable mod \(p\) if and only if \(p = 64m^2 + b^2\) for some integers \(m\) and \(b\). This concludes the proof of the proposition.
The Class Number Formula

In this last section we will sketch the proof of a special case of Dirichlet’s class number formula which we quoted earlier in the paper. For convenience we shall refer to the Kronecker symbol in this section as \( \chi \). We now restate the formula quoted earlier in the paper:

\[
    h(D) = \frac{1}{|D|} \sum_{n=1}^{|D| - 1} \chi(n)n, \text{ where } D < 0.
\]

We recall that when \( K \) is an imaginary quadratic extension of \( \mathbb{Q} \), the form class group \( C(d_K) \) and the ideal class group \( C(O_K) \) are isomorphic. We used the class number formula to determine \( h(-68) \). Therefore, we shall prove the class number formula for the case where \( K = \mathbb{Q}(\sqrt{-N}) \), \( N > 0 \), and \( N = 1 \) (4) is square-free. In this case we have \( d_K = -4N \). The formula we wish to prove is therefore:

\[
    (I) \quad h(-4N) = \frac{1}{4N} \sum_{n=1}^{4N-1} \chi(n)n.
\]

We shall now state some standard facts and definitions that are required for the proof of this special case of the class number formula:

(1) **Definition:** The Riemann Zeta Function \( \zeta(s) \) is defined by \( \zeta(s) = \sum_{n=1}^{\infty} n^{-s} \), for \( s > 0 \).

**Note:** The series in (1) converges for all \( s > 1 \).

(2) \( \zeta(s) = \prod_p (1 - \frac{1}{p^s})^{-1} \), where the product ranges over all primes \( p \in \mathbb{Z} \).

(3) \( \lim_{s \to 1^+} (s - 1)\zeta(s) = 1 \).

(4) **Definition:** Let \( m > 0 \) be a fixed integer. A function from \( \mathbb{Z} \) to \( \mathbb{C} \) is called a Dirichlet character modulo \( m \) if it satisfies the following three conditions:

   (i) \( \chi(n + m) = \chi(n) \) for all \( n \in \mathbb{Z} \).

   (ii) \( \chi(kn) = \chi(k)\chi(n) \) for all \( k, n \in \mathbb{Z} \).

   (iii) \( \chi(n) \neq 0 \) if and only if \( (n, m) = 1 \).

(5) **Definition:** Let \( \chi \) be a Dirichlet character mod \( m \). We define the Dirichlet \( L \)-function by the formula:

\[
    L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)n^{-s}.
\]
(6) Let $\chi$ be a non-trivial Dirichlet character. Then $L(s, \chi)$ is a continuous function of $s$ for $s > 0$.

(7) If $K$ is a number field and $a$ is a non-zero ideal of $O_K$, then $O_K/a$ is a finite ring.

(8) **Definition:** Let $K$ be a number field. We define the norm of a non-zero ideal $a$ of $O_K$ as: $N(a) = |O_K/a|$. 

(9) (Euler Product Formula) $\sum_a N(a)^s = \prod_p \left(1 - \frac{1}{N(p)^s}\right)$, where the sum is over all non-zero ideals of $O_K$ and the product is over all prime ideals of $O_K$ and $s > 1$.

(10) Let $K$ be a number field. If $\beta$ is a prime ideal of $O_K$, then there is a unique prime $p$ in $\mathbb{Z}$ contained in $\beta$.

(11) Let $\beta$ and $p$ be as above. Then $N(\beta) = p^f$, where $f$ denotes the inertial degree of $p$ in $\beta$.

(12) Let $K = \mathbb{Q}(\sqrt{-N})$, $N > 1$ be an imaginary quadratic field with $\beta$ and $p$ as in (10). Then:

   (i) $N(\beta) = p$ if $p|d_K$;

   (ii) $N(\beta) = p$ if $p$ does not divide $d_K$ and $p$ splits in $K$;

   (iii) $N(\beta) = p^2$ if $pO_K$ remains prime in $O_K$.

(13) Let $K$ be as above and $p$ be a prime in $\mathbb{Z}$. Then $p$ ramifies in $K$ if and only if $p$ divides $d_K$.

The 3 possibilities in (12) account for all prime ideals of $O_K$ when $K$ is an imaginary quadratic extension.

We recall that in a previous section we quoted the fact that an integer prime $p$ splits completely in $K$ if and only if $\chi(p) = 1$, in which case $p = \beta_1 \beta_2$, where $\beta_1 \neq \beta_2$. Putting this fact together with (11) and (12), it can be shown (see [Cox 1982]) that for odd primes $p$ the Kronecker symbol satisfies:

$$\chi(p) = \begin{cases} 0 & \text{if } p \text{ ramifies in } O_K; \\ 1 & \text{if } p \text{ splits completely in } O_K; \\ -1 & \text{if } pO_K \text{ is prime in } O_K. \end{cases}$$

This concludes our list of preliminary facts. The proofs for (2), (6), and (7) are in [Ireland and Rosen 1992]. The proof for (9) is in [Edwards 1977], and (10), (11), (12), and (13) are taken from [Cox 1982].

We will discuss the proof of the class number formula for $K = \mathbb{Q}(\sqrt{-N})$, where $N > 1, N \equiv 1 \pmod{4N}$. In this case the Kronecker symbol, which we are denoting as $\chi$, is a Dirichlet character mod $4N$. The key to the proof is the Euler Product Formula. There will be two main steps in the proof. In the first step the right hand side of Euler’s formula is rearranged to obtain $L(1, \chi)$. The infinite series defined by $L(1, \chi)$ is then reduced to a finite sum by various manipulations. The second step involves a rearrangement of the left
hand side of Euler’s formula. This leads to an expression involving the class number $h(-4N)$. The following
arguments are taken from [Edwards 1977].

**Step 1:** Evaluation of $\prod_P (1 - \frac{1}{N(P)^2})^{-1}$, where it is understood that the product is over all prime
ideals of $O_K$.

**Note:** Assume $s > 1$.

**Part 1a** From the facts in our list we can write:

$$\prod_{\text{all prime ideals } P} (1 - \frac{1}{N(P)^2})^{-1} = \prod_{\text{p ramifies}} (1 - \frac{1}{p^2})^{-1} \prod_{\text{p splits}} (1 - \frac{1}{p^2})^{-2} \prod_{\text{p stays prime}} (1 - \frac{1}{p^2})^{-1}$$

$$= \prod_{\text{all } p} (1 - \frac{1}{p^2})^{-1} \prod_{\text{p splits}} (1 - \frac{1}{p^2})^{-1} \prod_{\text{p stays prime}} (1 + \frac{1}{p^2})^{-1}$$

$$= \zeta(s) \prod_{\text{all } p} (1 - \frac{\chi(p)}{p^s})^{-1}.$$

If we multiply this quantity by $(s-1)$ and expand the product, using the multiplicativity of $\chi$ and item
(2) on our list, we obtain:

$$(s-1) \prod_P (1 - \frac{1}{N(P)^2})^{-1} = (s-1) \zeta(s) \prod_P (1 - \frac{\chi(p)}{p^s})^{-1} = (s-1) \zeta(s) \sum_n \frac{\chi(n)}{n^s},$$

where the sum is over all natural numbers $n$. The rightmost equality is justified since the fact that $s > 1$
allows us to rearrange terms in the infinite series at will without affecting the sum. Taking the limit as $s$
goes to 1, the right hand side of (II) becomes $\sum_n \frac{\chi(n)}{n^s} = L(1, \chi)$.

**Part 1b:** Evaluating $L(1, \chi) = \sum_n \frac{\chi(n)}{n}$, where it is understood that the sum is over all natural numbers
$n$.

Let $L(1, \chi) = 1 + \frac{\chi(2)}{2} + \cdots = c_0(1 + \frac{1}{2} + \frac{1}{3} + \cdots) + c_1(\alpha + \frac{\alpha^2}{2} + \cdots) + c_{4N-1}(\alpha^{4N-1} + \frac{(\alpha^{4N-1})^2}{2} + \cdots)$,

where $\alpha = e^{2\pi i}$ and the $c_n$’s are to be determined. Equating coefficients of $\frac{1}{k}$ on both sides we obtain:

$\chi(k) = \sum_{n=1}^{4N-1} c_n \alpha^{nk}$. After some simplifications it is shown in [Edwards 1977] that each of the $c_n$’s satisfy:

$c_n = \frac{1}{4N} \sum_{j=1}^{4N} \chi(j) \alpha^{-jn}$. This shows that $c_0 = 0$ since $\sum_{j=1}^{4N-1} \chi(j) = 0$. Using the fact that $\log \frac{1}{1-x} = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots$, for $|x| \leq 1, x \neq 1$, it is proved in [Edwards 1977] that $L(1, \chi) = \sum_{n=1}^{4N-1} c_n \cdot \log \frac{1}{1-\alpha^n}$, where $\alpha = e^{2\pi i}$ and
\[ c_n = \frac{1}{4N} [\chi(1)\alpha^{-n} + \chi(2)\alpha^{-2n} + \cdots + \chi(4N)\alpha^{-4Nn}] \]. We shall use this fact as the starting point in our attempt to simplify \( L(1, \chi) \). The following result and its proof are taken from [Edwards 1977]:

**Proposition 1**: \( c_n = c_1 \chi(n) \) for all \( n \in \{1, 2, \ldots, 4N - 1\} \).

**Proof**: For convenience we shall let \( m = 4N \). If \( n \) is relatively prime to \( m \) there exists an integer \( k \) such that \( nk \equiv 1 \mod{m} \). This implies

\[
(\text{III}) \quad c_1 = \frac{1}{m} [\chi(1)\alpha^{-1} + \chi(2)\alpha^{-2} + \cdots + \chi(m)\alpha^{-m}] = \frac{1}{m} [\chi(nk)\alpha^{-nk} + \chi(2nk)\alpha^{-2nk} + \cdots + \chi(mnk)\alpha^{-mnk}]

= \frac{\chi(n)}{m} [\chi(k)\alpha^{-nk} + \chi(2k)\alpha^{-2nk} + \cdots + \chi(mk)\alpha^{-mnk}].
\]

Since \( k \) is relatively prime to \( m \), the integers \( \{k, 2k, 3k, \ldots, mk\} \) form a representative residue class modulo \( m \). Therefore, we can further simplify (III) to obtain:

\[
c_1 = \frac{\chi(n)}{m} [\chi(1)\alpha^{-n} + \chi(2)\alpha^{-2n} + \cdots + \chi(m)\alpha^{-mn}].
\]

This implies that \( c_n = c_1 \chi(n) \) when \( n \) is relatively prime to \( m \). Since \( \chi(n) = 0 \) if \( n \) is not relatively prime to \( m \), it remains to show that \( c_n = 0 \) in this case. Let \( n = pk \) and \( m = pq \). Then we can write

\[
(\text{IV}) \quad c_n = \frac{1}{m} [\chi(1)\alpha^{-pk} + \chi(2)\alpha^{-2pk} + \cdots + \chi(m)\alpha^{-mpk}].
\]

If \( rk \equiv sk \mod{q} \), then \( \alpha^{-prk} = \alpha^{-p\alpha} \). Therefore, we obtain the following simplification of (IV):

\[
(\text{V}) \quad c_n = \frac{1}{m} [\left( \sum_{n \equiv 1 \mod{q}} \chi(n)\alpha^{-pk} \right) + \left( \sum_{n \equiv 2 \mod{q}} \chi(n)\alpha^{-2pk} \right) + \cdots + \left( \sum_{n \equiv 0 \mod{q}} \chi(n)\alpha^{-mpk} \right)].
\]

By the properties of the Kronecker symbol it follows that the sum of the characters in each congruence class of \( q \) in (V) are zero, thereby proving that \( c_n = 0 \) if \( n \) is not relatively prime to \( m \). This concludes the proof of the Proposition.

**Proposition 2**: \( c_1 = \pm \frac{1}{\sqrt{\chi(-1)m}} \), where we have let \( m = 4N \).

**Proof**: We stated earlier that:

\[
(\text{VI}) \quad \chi(j) = \sum_{n=1}^{m-1} c_n \alpha^{jn}.
\]

42
Using Proposition 1 we find:

\[(VII) \chi(j) = c_1 \sum_{n=1}^{m} \chi(n)\alpha^{nj}.\]

Substituting (VII) in (VI) we obtain:

\[(VIII) \chi(j) = c_1 \sum_{n=1}^{m} \left[ c_1 \sum_{k=1}^{m} \chi(k)\alpha^{nk}\right]\alpha^{nj}.\]

Switching the order of summation in (VIII) we get:

\[(IX) \chi(j) = c_1^2 \sum_{k=1}^{m} \left[ \sum_{n=1}^{m} \alpha^{nk}\alpha^{nj}\right]\chi(k).\]

The bracketed sum in (IX) is zero unless \(j + k \equiv 0 \pmod{m}\), in which case the sum is \(m\). Therefore \(\chi(j) = c_1^2 m\chi(-j)\) for \(j \in \{1, 2, ..., m\}\). This implies \(c_1 = \pm \frac{1}{\sqrt{\chi(-1)m}}\) and completes the proof of the proposition.

**Note:** The above proof is taken from [Edwards 1977].

Putting these facts together with the formula for \(L(1, \chi)\) that we started off with, we obtain:

\[(X) L(1, \chi) = \pm \frac{1}{\sqrt{\chi(-1)m}} \sum_{n=1}^{m-1} \chi(n) \log \frac{1}{1 - \alpha^n}.\]

Since \(\alpha\) is a primitive \(m\)-th root of unity we can use the following formula to simplify the sum in (X):

\[
\log \frac{1}{1 - e^{i\theta}} = -\log \left(2 \sin \frac{\theta}{2}\right) + i \left(\pi - \theta\right), \text{ for } 0 < \theta < 2\pi.
\]

Using this formula we obtain the following simplification of \(L(1, \chi)\):

\[L(1, \chi) = \pm \frac{\pi}{m\sqrt{m}}[1 + \chi(2)2 + \cdots + \chi(m)m].\]

We now recall from (II) that \(L(s, \chi) = \frac{1}{\zeta(s)}\prod_p \left(1 - \frac{1}{N(p)^s}\right)^{-1}\), where the product is over all prime ideals of \(O_K\). This implies that \(L(s, \chi) \geq 0\) for all \(s > 1\). By continuity of \(L(s, \chi)\) for positive \(s\) we obtain that

\[
\lim_{s \to 1^+} L(s, \chi) = L(1, \chi) \geq 0.
\]

Therefore, we can write:

\[L(1, \chi) = \frac{\pi}{m\sqrt{m}}[1 + \chi(2)2 + \cdots + \chi(m-1)(m-1)].\]

Aside from the factor of \(\frac{\pi}{m\sqrt{m}}\), the right hand side of this formula for \(L(1, \chi)\) looks exactly like the right hand side of formula (I). We shall now proceed to sketch the second stage of the proof to obtain an expression involving the class number \(h(-4N)\).
Step 2: Evaluation of $\sum_A \frac{1}{N(A)^s}$, where it is understood that the sum is over all non-zero ideals of $O_K$.

Assume that $s > 1$. Since there are only finitely many equivalence classes of ideals which make up the form class group $C(O_K)$ and the sum $\sum_A \frac{1}{N(A)^s}$ is absolutely convergent, we obtain:

$$(XI) \sum_A \frac{1}{N(A)^s} = \sum_{A \sim A_1} \frac{1}{N(A)^s} + \sum_{A \sim A_2} \frac{1}{N(A)^s} + \cdots + \sum_{A \sim A_h} \frac{1}{N(A)^s},$$

where the individual sums are over the $h$ distinct equivalence classes of ideals (here we have let $h = h(-4N)$).

The key step in this part of the proof is that all of the $h$ individual sums in (XI) approach the same value as $s$ approaches 1. This crucial fact is proved in [Edwards 1977]. Therefore, we can simply pick an equivalence class of ideals to sum over and multiply its value by the class number $h(-4N)$ to obtain the value of the sum over all ideal classes as in (XI). The easiest class of ideals over which to compute the sum in (XI) is the class of principal ideals, which we shall denote $A_1$. Since we have chosen $N > 1$ and $N \equiv 1 \pmod{4}$, the only units in the field $K = \mathbb{Q}(\sqrt{-N})$ are $\pm 1$. Using these facts, we can rewrite the sum in (XI) as:

$$(XII) \lim_{s \to 1^+} \sum_A \frac{1}{N(A)^s} = \lim_{s \to 1^+} h(-4N) \cdot \sum_{A \sim A_1} \frac{1}{N(A)^s} = \lim_{s \to 1^+} \frac{1}{2} \sum_{(x,y) \neq (0,0)} (x^2 + Ny^2)^{-s}.$$

It is proven in [Edwards 1977] that the difference between the rightmost sum in (VIII) and the double integral

$$\iint_{x^2 + Ny^2 \geq 1} (x^2 + Ny^2)^{-s} dx \ dy$$

is bounded as $s$ approaches 1. Therefore, it follows that

$$\lim_{s \to 1^+} (s - 1) \sum_A \frac{1}{N(A)^s} = \lim_{s \to 1^+} (s - 1) h(-4N) \cdot \frac{1}{2} \sum_{(x,y) \neq (0,0)} (x^2 + Ny^2)^{-s}$$

$$= \lim_{s \to 1^+} (s - 1) h(-4N) \cdot \frac{1}{2} \iint_{x^2 + Ny^2 \geq 1} (x^2 + Ny^2)^{-s} dx \ dy.$$

After the change of variable $x = \sqrt{N} z$ the double integral can be integrated using polar coordinates. Its value is then found to be $\frac{\pi}{(s - 1)} N^{1 - \frac{1}{2} + s - 1}$. Multiplying this quantity by $(s - 1)$ and taking the limit, we obtain

$$(XIII) \lim_{s \to 1^+} (s - 1) \sum_A \frac{1}{N(A)^s} = \frac{h(-4N)\pi}{2\sqrt{N}}.$$

Equating the two expressions that we found for each side of Euler's Product Formula, we find that

$$\frac{h(-4N)\pi}{2\sqrt{N}} = \frac{\pi}{m\sqrt{m}} |1 + \chi(2)2 + \cdots + \chi(m-1)(m-1)|.$$

44
Since we set $m = 4N$, after cancelling common terms, we obtain the Class Number Formula.

The Class Number Formula forms a fitting end to our investigations. In the first section of this paper we saw that quadratic reciprocity played a big part in determining what primes are represented by a given reduced form. In dealing with finite fields we saw that there is a striking reciprocal relationship between solvability of certain quadratic equations or cubic equations modulo a prime $p$ and representability of this prime by a given quadratic form. The ideas used in the proof of the Class Number Formula form a pleasing blend of these various techniques, thereby underscoring the deep relation between character sums in finite fields and the form class group.
Bibliography


