Binary Quadratic Forms, Genus Theory, and Primes of the Form $p = x^2 + ny^2$

Josh Kaplan

July 28, 2014

Contents

1 Introduction

In this paper, we will develop the theory of binary quadratic forms and elementary genus theory, which together give an interesting and surprisingly powerful elementary technique in algebraic number theory. This is all motivated by a problem in number theory that dates back at least to Fermat: for a given positive integer n, characterizing all the primes which can be written $p = x^2 + ny^2$ for some integers x, y. Euler studied the problem extensively, and was able to solve it for $n = 1, 2, 3, 4$, giving the first rigorous proofs of the following four theorems of Fermat:

$$p = x^2 + y^2 \text{ for some } x, y \in \mathbb{Z} \iff p = 2 \text{ or } p \equiv 1 \mod 4,$$

$$p = x^2 + 2y^2 \text{ for some } x, y \in \mathbb{Z} \iff p = 2 \text{ or } p \equiv 1, 3 \mod 8,$$

$$p = x^2 + 3y^2 \text{ for some } x, y \in \mathbb{Z} \iff p = 3 \text{ or } p \equiv 1 \mod 3,$$

$$p = x^2 + 4y^2 \text{ for some } x, y \in \mathbb{Z} \iff p \equiv 1 \mod 4.$$

For $n > 4$, however, Euler was unsuccessful in giving a proof. He did manage conjectures, though, for many values of n, such as:

$$p = x^2 + 6y^2 \text{ for some } x, y \in \mathbb{Z} \iff p \equiv 1, 7 \mod 24.$$

With the techniques we will develop, these beautiful and, particularly for $n = 6$, otherwise difficult results follow from easy computations (as do similar results

for $n = 5, 7, 9, 10, 12, 13$, and over 50 other values of n). As we will see near the end of the paper, the techniques are not enough for us to characterize primes of the form $p = x^2 + ny^2$ for arbitrary n, but what they are able to achieve is remarkable in its own right. This paper will assume knowledge of basic field theory and group theory.

2 Quadratic Reciprocity

In order to characterize primes of the $p = x^2 + ny^2$ by their congruences, we first need to prove the law of quadratic reciprocity. This law will allow us to easily determine when a number is a square in a finite field (remember that for prime p, $\mathbb{F}_p$ denotes the finite field $\mathbb{Z}/p\mathbb{Z}$). Just how crucial this ability is to our project will not become clear until the next section, but it is a beautiful and important theorem that has many uses outside of the problem we are focusing on and is worth proving for its own sake. To give our proof, we first need the following theorem.

Theorem 2.1. *Let p be an odd prime. Then an element x of $\mathbb{F}_p^*$ is a square if and only if $x^{(p-1)/2} = 1$.*

Proof. From Fermat's Little Theorem, we have:

$$\forall a \in \mathbb{F}_p^*, a^{p-1} = 1.$$

So the $p-1$ roots of $a^{p-1} - 1$ are the distinct elements of $\mathbb{F}_p^*$. This means that there are $(p-1)/2$ distinct roots of $a^{(p-1)/2} - 1$ and of $a^{(p-1)/2} + 1$. If there exists y in $\mathbb{F}_p^*$ such that $y^2 = x$, then $x^{(p-1)/2} = y^{p-1} = 1$, so all squares in $\mathbb{F}_p^*$ are roots of $a^{(p-1)/2} - 1$. Since $\mathbb{F}_p^*$ is cyclic, there exists g in $\mathbb{F}_p^*$ such that $\mathbb{F}_p^* = \{1, g, g^2, ..., g^{p-2}\}$, so there are at least $(p-1)/2$ distinct squares in $\mathbb{F}_p^*$. The theorem follows.

□

Definition 2.2. Let p be an odd prime, and let $x \in \mathbb{F}_p^*$. The *Legendre symbol of x*, denoted by $\left(\frac{x}{p}\right)$, is the integer $x^{(p-1)/2}$.

Note that the Legendre symbol is frequently given the following alternative definition (in $\mathbb{Z}$ rather than $\mathbb{F}_p^*$):

$$\left(\frac{x}{p}\right) = \begin{cases} 1, & \text{if } [x] \in \mathbb{F}_p^{*2}, x \not\equiv 0 \mod p \\ -1, & \text{if } [x] \notin \mathbb{F}_p^{*2} \\ 0, & \text{if } x \equiv 0 \mod p. \end{cases}$$

From Theorem 2.1, it is clear that for $x \not\equiv 0 \mod p$, this definition is equivalent to our own. A few properties of the Legendre symbol also follow immediately from our definition. Obviously, we have $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$. Also, it is clear that $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = 1$ if and only if $p \equiv 1 \mod 4$.

The following useful lemma is often referred to as Gauss's Lemma. It will allow us to prove the law of quadratic reciprocity, but it also will give us a general formula for $\left(\frac{2}{p}\right)$. For the rest of this section, S will denote the subset $\{1, ..., \frac{p-1}{2}\}$ of $\mathbb{F}_p^*$, where p is an odd prime (note that $\mathbb{F}_p^*$ is the disjoint union of S and $-S$). Also, for any s in S, we will define $e_s : \mathbb{F}_p^* \to \{\pm 1\}$ so that for all a in $\mathbb{F}_p^*$, $as = e_s(a)s_a$ for some s_a in S.

Lemma 2.3. *Let p be an odd prime. Then for any a in $\mathbb{F}_p^*$, $\left(\frac{a}{p}\right) = \prod_{s\in S} e_s(a)$.*

Proof. Clearly $s \mapsto s_a$ is a bijection from S onto itself, so we can use $as = e_s(a)s_a$ to get the following:

$$a^{(p-1)/2} \prod_{s\in S} = \left(\prod_{s\in S} e_s(a)\right)\left(\prod_{s\in S} s_a\right) = \left(\prod_{s\in S} e_s(a)\right)\left(\prod_{s\in S} s\right).$$

Therefore

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} = \prod_{s\in S} e_s(a).$$

□

Note that this means $\left(\frac{a}{p}\right) = (-1)^v$ where v is the number of times as falls in $-S$ rather than S. And now, as promised, we can derive the following:

Proposition 2.4. $\left(\frac{2}{p}\right) = 1$ *if and only if* $p \equiv 1, 7 \mod 8$

Proof. Since $e_s(2) = 1$ if and only if $2s \leq \frac{p-1}{2}$, we get $\left(\frac{2}{p}\right) = (-1)^{n(p)}$, where $n(p)$ is the number of integers s such that $\frac{p-1}{4} < s \leq \frac{p-1}{2}$. Clearly p can be written in the form $4k \pm 1$, and we see $n(p) = k$. Then if $p \equiv \pm 1 \mod 8$, k is even, and if $p \equiv \pm 5 \mod 8$, k is odd, so the result is immediate.

□

And we are also ready now to prove the major result of this section. For odd n, define

$$\mathcal{E}(n) = \begin{cases} 0, & n \equiv 1 \mod 4, \\ 1, & n \equiv 3 \mod 4. \end{cases}$$

Theorem 2.5 (Law of Quadratic Reciprocity)**.** *Let l and p be two distinct odd primes. Then $\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)(-1)^{\mathcal{E}(p)\mathcal{E}(l)}$.*

Proof. First, note the following trigonometric fact, which we will not prove here (although the proof is elementary): for any positive, odd integer m,

$$\frac{\sin mx}{\sin x} = (-4)^{(m-1)/2} \prod_{j=1}^{(m-1)/2} \left(\sin^2 x - \sin^2 \frac{2\pi j}{m}\right).$$

Let $S = \{1, ..., (p-1)/2\} \subseteq \mathbb{F}_p^*, T = \{1, ..., (l-1)/2\} \subseteq \mathbb{F}_l^*$. Since $ls = e_s(l)s_l$, of course,

$$\sin \frac{2\pi}{p} ls = e_s(l) \sin \frac{2\pi}{p} s_l.$$

So from Gauss's Lemma, we have:

$$\left(\frac{l}{p}\right) = \prod_{s \in S} e_s(l) = \prod_{s \in S} \sin \frac{2\pi ls}{p} / \sin \frac{2\pi s_l}{p}.$$

Using the fact that $s \mapsto s_l$ is a bijection, and the trigonometric fact we noted at the beginning of the proof, we get the following:

$$\begin{aligned}\left(\frac{l}{p}\right) = \prod_{s \in S} \sin \frac{2\pi ls}{p} / \sin \frac{2\pi s}{p} &= \prod_{s \in S} (-4)^{(l-1)/2} \prod_{t \in T} \left(\sin^2 \frac{2\pi s}{p} - \sin^2 \frac{2\pi t}{l}\right) \\ &= (-4)^{(l-1)(p-1)/4} \prod_{s \in S, t \in T} \left(\sin^2 \frac{2\pi s}{p} - \sin^2 \frac{2\pi t}{l}\right).\end{aligned}$$

If we permute l and p, the same argument gives us

$$\left(\frac{p}{l}\right) = (-4)^{(l-1)(p-1)/4} \prod_{s \in S, t \in T} \left(\sin^2 \frac{2\pi t}{l} - \sin^2 \frac{2\pi s}{p}\right).$$

Therefore

$$\begin{aligned}\left(\frac{l}{p}\right) = (-4)^{(l-1)(p-1)/4} \prod_{s \in S, t \in T} -\left(\sin^2 \frac{2\pi t}{l} - \sin^2 \frac{2\pi s}{p}\right) &= (-1)^{(p-1)(l-1)/4} \left(\frac{p}{l}\right) \\ &= (-1)^{\mathcal{E}(p)\mathcal{E}(l)} \left(\frac{p}{l}\right).\end{aligned}$$

□

The importance of this result for characterizing primes of the form $p = x^2 + ny^2$ will soon become clear. For now, just note that the law of quadratic reciprocity, when combined with the multiplicative property of Legendre symbols, gives us the remarkable ability to determine whether any given element of $\mathbb{F}_p^*$ is a square without having to find its square root. We will give a few examples here of Legendre symbol calculations before returning to our main project in the next section.

Example 2.6.

$$\begin{aligned}\left(\frac{137}{307}\right) = \left(\frac{307}{137}\right) = \left(\frac{33}{137}\right) = \left(\frac{3}{137}\right)\left(\frac{11}{137}\right) = \left(\frac{137}{3}\right)\left(\frac{137}{11}\right) &= \left(\frac{2}{3}\right)\left(\frac{5}{11}\right) \\ &= \left(\frac{2}{3}\right)\left(\frac{11}{5}\right) \\ &= \left(\frac{2}{3}\right)\left(\frac{1}{5}\right) \\ &= -1 * 1 = -1.\end{aligned}$$

Example 2.7. $\left(\frac{89}{509}\right) = \left(\frac{509}{89}\right) = \left(\frac{64}{89}\right) = \left(\frac{2}{89}\right)^8 = 1$, since $(\pm 1)^8 = 1$.

3 Binary Quadratic Forms

At the end of this section, we will be able to use the theory of reduced forms to characterize primes of the form $p = x^2 + ny^2$ for $n = 1, 2, 3, 4, 7$. This theory is elementary but quite powerful, and to develop it, we first must define some concepts which will serve as the foundation for the rest of our discussion.

Definition 3.1. A *binary quadratic form* (hereafter just quadratic form) is a function in two variables $f(x, y) = ax^2 + bxy + cy^2$. Our discussion will be limited to integral quadratic forms (i.e. $a, b, c \in \mathbb{Z}$). We say a quadratic form $f(x, y)$ is *primitive* if a, b and c are relatively prime.

Definition 3.2. An integer m is *represented* by quadratic form f if there exist x, y in $\mathbb{Z}$ such that $f(x, y) = m$. If those x, y are relatively prime, then m is *properly represented* in f.

Definition 3.3. Two quadratic forms $f(x, y)$ and $g(x, y)$ are *equivalent* if there exist p, q, r, s in $\mathbb{Z}$ such that $f(x, y) = g(px + qy, rx + sy)$ and $ps - qr = \pm 1$. If $ps - qr = 1$, we say the equivalence is *proper*. If not, we say it is *improper*. (Note that it is possible for two forms to be both properly equivalent and improperly equivalent. A simple example is that $f(x, y) = x^2 + y^2$ is clearly properly equivalent to itself ($f(x, y) = f(x, y)$), and is also improperly equivalent to itself ($f(x, -y) = f(x, y)$)).

It is easy to see that both equivalence and proper equivalence of quadratic forms are equivalence relations. It also clear that equivalent forms represent the same numbers. The following relation between proper representation and proper equivalence will be more useful to us though.

Lemma 3.4. *A quadratic form $f(x, y)$ properly represents an integer m if and only if $f(x, y)$ is properly equivalent to $mx^2 + bxy + cy^2$ for some integers b, c.*

Proof. ($\Rightarrow$) For $f(x, y) = ax^2 + bxy + cy^2$, suppose $f(p, r) = m$ for p, r relatively prime. Since $\gcd(p, r) = 1$, there exist integers q, s such that $ps - qr = 1$. Then

$$\begin{aligned} f(px + qy, rx + sy) &= f(p, r)x^2 + (2apq + bps + brq + 2crs)xy + f(q, s)y^2 \\ &= mx^2 + b'xy + c'y^2. \end{aligned}$$

($\Leftarrow$) If $f(px + qy, rx + sy) = mx^2 + bxy + cy^2$ for some p, q, r, s such that $ps - qr = 1$, then $f(p, r) = m$, and clearly p and r are relatively prime (since 1 is in the ideal (p, r)).

□

This, of course, means that properly equivalent forms properly represent the same numbers. And now, we have a few more definitions.

Definition 3.5. The *discriminant* of $ax^2+bxy+cy^2$ is defined by $D = b^2-4ac$.

Definition 3.6. If the discriminant D of $f(x,y) = ax^2 + bxy + cy^2$ is negative and $a > 0$ (respectively, $a < 0$), then $f(x,y)$ is *positive definite* (respectively, *negative definite*). If D is positive, we say $f(x,y)$ is *indefinite*.

We get these terms because if $f(x,y)$ is positive definite, $f(x,y)$ only represents positive integers (the analogous statement holds for negative definite forms), and if $f(x,y)$ is indefinite, it represents both positive and negative integers. We will leave these facts to the reader to verify.

It is important to note that the discriminant is invariant for equivalent forms, which can be easily proven as follows.

Proposition 3.7. *If $f(x,y)$ and $g(x,y)$ are equivalent, then their discriminants are equal.*

Proof. Let D and D' be the discriminants of $f(x,y)$ and $g(x,y)$ respectively. Suppose $f(x,y) = g(px+qy, rx+sy)$ for some $p,q,r,s \in \mathbb{Z}$ such that $ps-qr = \pm 1$. Then we can easily calculate that $D = (ps-qr)^2 D' = D'$.

□

Also note that positive and negative definiteness are invariant under equivalence. We also now can prove the following lemma, as well as a corollary which relates the theory of quadratic forms to the previous section of the paper, and will be extremely important in characterizing primes of the form $p = x^2 + ny^2$.

Lemma 3.8. *Let D be an integer congruent to 0 modulo 4, and m be an odd integer relatively prime to D. Then m is properly represented by a primitive form of discriminant D if and only if D is a quadratic residue modulo m.*

Proof. ($\Rightarrow$) Suppose primitive form $f(x,y)$ properly represents m. Then $f(x,y)$ is properly equivalent to $mx^2 + bxy + cy^2$ by Lemma 3.4, so $D = b^2 - 4mc$ for some b, c in $\mathbb{Z}$. Therefore, $D \equiv b^2 \mod m$.

($\Leftarrow$) Suppose $D \equiv b^2 \mod m$. Let

$$b' = \begin{cases} b, & \text{if } b \text{ is even,} \\ b+m, & \text{if not.} \end{cases}$$

Then $D \equiv b'^2 \mod m$, and, since m is odd and D is congruent to 0 modulo 4, D and b' are both even. This means that $D \equiv b'^2 \mod 4m$ (since 4 divides both D and b'^2). Thus $D = b^2 - 4mc$ for some c. So we have the form $f(x,y) = mx^2 + bxy + cy^2$, which is of discriminant D, properly represents m (since $f(1,0) = m$), and is primitive since m is relatively prime to D, finishing the proof of our lemma.

□

Corollary 3.9. *Let n be an integer and p be an odd prime that does not divide n. Then p is represented by a primitive form of discriminant $-4n$ if and only if $\left(\frac{-n}{p}\right) = 1$.*

Proof. First, note that a primitive form represents a prime p if and only if it properly represents p. With this, the corollary is an immediate consequence of Lemma 3.8 and Theorem 2.1 since $\left(\frac{-4n}{p}\right) = \left(\frac{-n}{p}\right)\left(\frac{2}{p}\right)^2 = \left(\frac{-n}{p}\right)$.

□

That should make it a little clearer why quadratic reciprocity was a necessary first step towards our goal. In fact, we are very close to being able to characterizing $p = x^2 + ny^2$ for a few values of n. We will now narrow our discussion to positive definite forms (which include the forms we're most interested in, $x^2 + ny^2$), which have some beautiful and extremely useful properties.

Definition 3.10. A primitive, positive definite quadratic form $ax^2 + bxy + cy^2$ is *reduced* if i) $|b| \leq a \leq c$ and ii) $b \geq 0$ if either $|b| = a$ or $a = c$

Theorem 3.11. *Every primitive, positive definite form is properly equivalent to a unique reduced form.*

Proof. Let $f(x, y)$ be any given primitive, positive definite form. First, we will prove that it is properly equivalent to a form $g(x, y) = ax^2 + bxy + cy^2$ satisfying $|b| \leq a \leq c$. Out of all the forms properly equivalent to $f(x, y)$, let $g(x, y)$ be a form such that $|b|$ minimal. We see that for any integer m, $g(x + my, y) = ax^2 + (2am + b)xy + c'y^2$ is properly equivalent to $g(x, y)$, so if $a < |b|$, we can choose m such that $|2am + b| < |b|$, which contradicts our choice of b. Thus $a \geq |b|$. That c is greater than or equal to $|b|$ can be proved similarly. If $a > c$, we simply need to exchange the outer coefficients, which is done in the properly equivalent form $g(-y, x)$. The resulting form $ax^2 + bxy + cy^2$ satisfies $|b| \leq a \leq c$.

This form will already be reduced unless $b < 0$ and either $a = -b$ or $a = c$. If $ax^2 + bxy + cy^2$ isn't reduced, $ax^2 - bxy + cy^2$ will be reduced, so we just need to prove that the two are properly equivalent if $a = -b$ or $a = c$. If $a = -b$, then $(x, y) \mapsto (x + y, y)$ takes $ax^2 - axy + cy^2$ to $ax^2 + axy + cy^2$. If $a = c$, then $(x, y) \mapsto (-y, x)$ takes $ax^2 - bxy + ay^2$ to $ax^2 + bxy + ay^2$. So we have proven that $f(x, y)$ is properly equivalent to a reduced form.

Now we only need to prove that that reduced form is unique, which we will accomplish by showing that different reduced forms cannot be properly equivalent. Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be properly equivalent reduced forms. It is easy to show that for any reduced form,

$$f(x, y) \geq (a - |b| + c) \min(x^2, y^2). \tag{1}$$

First we will consider the case where $|b| < a < c$. Using (1) and remembering that x and 0 are relatively prime if and only if $x = 1$, , we see

$$a < c < a - |b| + c$$

are the three smallest non-zero values properly represented by $f(x, y)$. From (1), it's also clear that

$$f(x, y) = a,\ \gcd(x, y) = 1 \iff (x, y) = \pm(1, 0),$$
$$f(x, y) = c,\ \gcd(x, y) = 1 \iff (x, y) = \pm(0, 1).$$

Now we turn to $g(x, y)$. From (1), we know that a' is the smallest non-zero value properly represented by $g(x, y)$, which means $a' = a$ since $f(x, y)$ and $g(x, y)$ are properly equivalent. By similar logic, c' must be either the smallest or second smallest value properly represented by $f(x, y)$ (i.e. $c' = a$ or $c' = c$). If $c' = a$, the equation $g(x, y) = a$ has four proper solutions, $\pm(1, 0)$ and $\pm(0, 1)$, which is a contradiction since $f(x, y) = a$ has only two proper solutions. Thus $c' = c$. Since $f(x, y)$ and $g(x, y)$ have the same discriminant, $g(x, y) = ax^2 \pm bxy + cy^2$. Using that $g(x, y) = f(px + qy, rx + sy)$ for $ps - qr = 1$, we easily get a system of equations which show that $f(x, y) = g(x, y)$.

We are two cases away from a complete proof. Now consider if $a = c$ and $a \neq |b|$. We have $a = a'$ for the same reasons as before. Similarly, we again have that c' is either the smallest or second smallest non-zero value properly represented by $f(x, y)$ (i.e. either $c' = a$ or $c' = 2a - |b|$). But if $c' = 2a - |b|$, $g(x, y) = a$ has only two proper solutions, whereas $f(x, y) = a$ has four. This means $c' = a = c$. We know $b, b' \geq 0$, so $f(x, y) = g(x, y)$.

Lastly, consider if $a = |b|$. We again have $a = a'$, so if $a' = |b'|$ as well, clearly $f(x, y) = g(x, y)$ since $b, b' \geq 0$ and the discriminants are equal. And if $a' \neq |b'|$, we only need to reverse the roles of $f(x, y)$ and $g(x, y)$ to reduce this to one of our previous two cases, and so our proof is complete.

□

Theorem 3.12. *Let $D < 0$ be fixed. Then the number $h(D)$ of equivalence classes of primitive positive definite forms of discriminant D is finite, and $h(D)$ is equal to the number of reduced forms of discriminant D.*

Proof. All we need to prove is that the number of reduced of forms of discriminant D is finite, and the rest will follow immediately from Theorem 3.11. We know that for any reduced form $ax^2 + bxy + cy^2$, $b^2 \leq a^2$ and $a \leq c$. So we have

$$-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2.$$

This means

$$|b| \leq a \leq \sqrt{-D/3}.$$

So we have a finite number of possible values for a and b. Remembering that $D = b^2 - 4ac$ (i.e. given values for a, b and D, there is only one possible value for c), we have our result.

□

Let us summarize our main results so far. Corollary 3.9 tells us (with a few conditions) that a prime p is represented by a primitive form of discriminant $-4n$ if and only if $\left(\frac{-n}{p}\right) = 1$ (and quadratic reciprocity gives us a good way to calculate the Legendre symbol). Since a form with a negative discriminant representing positive integers must be positive definite, we can combine this with Theorem 3.11 to get that a prime p is represented by a reduced form of discriminant $-4n$ if and only if $\left(\frac{-n}{p}\right) = 1$. Finally, Theorem 3.12 tells us that the reduced forms of a given discriminant are finite, and actually gives us an

explicit bound on the coefficients.[1] Noting that $x^2 + ny^2$ is a reduced form, it is now clear just how useful these results could be to us. And, in fact, we now have all that we need to characterize primes of the form $p = x^2 + ny^2$ for a few values of n. To demonstrate the power of these theorems and as reward for our efforts so far, we will now prove the four theorems of Fermat given in the introduction, and also characterize primes of the form $p = x^2 + 7y^2$. Amazingly, the proofs now require nothing more than some easy computation.

Theorem 3.13. *For p prime, $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1 \mod 4$.*

Proof. Corollary 3.9 requires that p be odd, so we must handle the case of $p = 2$ separately (which obviously is represented by $x^2 + y^2$). For odd p, though, we know p is represented by a reduced form of discriminant -4 if and only if $\left(\frac{-1}{p}\right) = 1$. Now we must determine all the reduced forms of discriminant -4. We know $|b| \leq a \leq \sqrt{4/3} < 2$, and if $a = b = 0$, the discriminant must be 0, so a must equal 1. $1 - 4c = -4$ has no integer solutions, so b must equal 0. Thus, the only reduced form of discriminant -4 is $x^2 + y^2$. Now we only need to know $\left(\frac{-1}{p}\right)$, and remember we already showed in Section 2 that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \mod 4$, so we have our result.

□

Note that with that result, we can easily prove that a prime p is of the form $p = x^2 + 4y^2$ if and only if $p \equiv 1 \mod 4$. For p odd to be of the form $p = x^2 + y^2$, either x or y must be even, and so our proof is complete.

Theorem 3.14. *For p prime, $p = x^2 + 2y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1, 3 \mod 8$.*

Proof. For odd p, p is represented by a reduced form of discriminant -8 if and only if $\left(\frac{-2}{p}\right) = 1$, so, as in the previous proof, we must determine all the reduced forms of discriminant -8 (these proofs are extremely algorithmic in nature). We know $|b| \leq a \leq \sqrt{8/3} < 2$, so again, a must equal 1. $1 - 4c = -8$ has no integer solutions, so the only reduced form of discriminant -8 is $x^2 + 2y^2$. Recall from Section two that $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1, 7 \mod 8$, so $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1, 3 \mod 8$.

□

[1] For the reader with previous background in algebraic number theory, it is good here to take note of the relationship between reduced forms and the ideal class groups. One can construct a bijection (actually, an isomorphism, which is a sensible statement because the classes of quadratic forms can be made an abelian group with the group action being composition as defined by Gauss [2, §235]) between the equivalence classes of quadratic forms of discriminant $-4n$ and the ideal classes in the ring of integers $\mathcal{O}_{-n}$ [1, Thm 7.7]. So these past two theorems both give an interesting alternative proof of the finiteness of the ideal classes, and provide a nice, elementary method to compute the class number of ideal class groups. The bound on a is very close to Minkowski's, and as we will see in the next few proofs, determining the number of reduced forms of a given discriminant could not be much easier (although with larger discriminants, the calculations would get very lengthy).

Theorem 3.15. *For p prime, $p = x^2 + 3y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p = 3$ or $p \equiv 1 \mod 3$.*

Proof. The other condition of Corollary 3.9 is that p does not divide n, so we also must handle the case of $p = 3$ separately now. And for $p > 3$, p is represented by a reduced form of discriminant -12 if and only if $\left(\frac{-3}{p}\right) = 1$. For such a form, $|b| \leq a \leq \sqrt{12/3} = 2$, so this time, we also have to examine the case where $a = 2$. $-8c = -12$ and $1 - 8c = -12$ have no integer solutions, and while $4 - 8c = -12$ has a solution, $2x^2 + 2xy + 2y^2$ is not primitive, so, again, a must equal 1. $1 - 4c = -12$ also has no integer solutions, so $x^2 + 3y^2$ is the only reduced form of determinant -12. Since the numerator is no longer congruent to 1 modulo 4, from the law of quadratic reciprocity, we have

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right), & p \equiv 1 \mod 4, \\ -\left(\frac{p}{3}\right), & p \equiv 3 \mod 4. \end{cases}$$

This appears uglier than it actually is, because when we combine it with the congruence we know for $\left(\frac{-1}{p}\right)$, we get $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$. Determining $\left(\frac{p}{3}\right)$ just requires us to know the squares in a particular group, $\mathbb{F}_3^*$, and if we didn't already know it, we could easily compute that $\mathbb{F}_3^{*2} = \{1\}$. Thus, $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \mod 3$.

□

Theorem 3.16. *For p prime, $p = x^2 + 7y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p = 7$ or $p \equiv 1, 2, 4 \mod 7$.*

Proof. For $p \neq 2, 7$, p is represented by a form of discriminant -28 if and only if $\left(\frac{-7}{p}\right) = 1$. For such a form, $|b| \leq a \leq \sqrt{28/3} < 4$. $9 - 12c = -28$, $4 - 12c = -28$, $1 - 12c = -28$, and $-12c = 28$ all have no integer solutions, so $a \neq 3$. $1 - 8c = -28$ and $-8c = -28$ have no solutions, and while $4 - 8c = -28$ has a solution, $2x^2 + 2xy + 4y^2$ is not primitive, so a must equal 1. So since $1 - 8c = -28$ has no solutions, $x^2 + 7y^2$ is the only reduced form of discriminant -28. By the same logic as in the previous proof, we get $\left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right)$, and we can easily calculate that $\mathbb{F}_7^{*2} = \{1, 2, 4\}$, so we have our result.

□

The power of our quadratic form theorems should be quite evident now. However, without adding any further theory, this approach suffers from some very serious limitations. All four of the previous proofs were similar in that there was only one reduced form of the given determinant. However, this is not true in the general case. In fact, there are no other values of n where $x^2 + ny^2$ is the only reduced form of discriminant $-4n$ (this can be proven [1, Thm 2.18], although we will not do so here). Trying the same approach on $p = x^2 + 5y^2$, for instance, we get that $\left(\frac{-5}{p}\right) = 1$ if and only if p is of the form $p = x^2 + 5y^2$ *or* of the form $p = 2x^2 + 2xy + 3y^2$. In order to distinguish between these two cases, we will need some elementary genus theory.

4 Elementary Genus Theory

There is a very natural homomorphism related to the Legendre symbol that we will use extensively in this section. Its usefulness to us will become almost immediately apparent, so we will begin this section simply by constructing it.

Lemma 4.1. *Let $D = 4n$ for some integer n. Then there is a unique $\chi : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$ such that $\chi([p]) = \left(\frac{D}{p}\right)$ for all p prime that do not divide D.*

Proof. Before we consider whether or not it is a homomorphism, we first must show that such a function could be well-defined. In particular, we must show that for any two primes x, y not dividing D which are congruent modulo D, $\left(\frac{D}{x}\right) = \left(\frac{D}{y}\right)$. We can write y as $x + mD$ for some m, and let $n = p_1 \cdot ... \cdot p_r$, where $p_1, ..., p_r$ are prime. For now, assume n is odd. We clearly have

$$\left(\frac{D}{x+mD}\right) = \left(\frac{p_1}{x+mD}\right) \cdot ... \cdot \left(\frac{p_r}{x+mD}\right) = \pm \left(\frac{x+mD}{p_1}\right) \cdot ... \cdot \left(\frac{x+mD}{p_r}\right),$$

and since for all i, p_i divides D, $\left(\frac{x+mD}{p_1}\right) \cdot ... \cdot \left(\frac{x+mD}{p_r}\right) = \left(\frac{x}{p_1}\right) \cdot ... \cdot \left(\frac{x}{p_r}\right)$. Since 4 divides D, $x + mD$ and x have the same congruence modulo 4, so

$$\left(\frac{D}{x+mD}\right) = \pm \left(\frac{x}{p_1}\right) \cdot ... \cdot \left(\frac{x}{p_r}\right) = \left(\frac{p_1}{x}\right) \cdot ... \cdot \left(\frac{p_r}{x}\right) = \left(\frac{D}{p}\right).$$

If n is even, x and $x + mD$ have the same congruence modulo 8, so $\left(\frac{2}{x}\right) = \left(\frac{2}{x+mD}\right)$, and the rest of the argument holds.

Every class in $(\mathbb{Z}/D\mathbb{Z})^*$ contains a prime, so χ is uniquely defined. We only need to check that it is a homomorphism. Let x, y be prime, and choose m such that $xy + mD$ is prime. Noting that $xy + mD \equiv 3 \mod 4$ if and only if x and y don't have the same congruence modulo 4, we get

$$\begin{aligned}
\chi([xy]) = \left(\frac{D}{xy+mD}\right) &= \left(\frac{p_1}{xy+mD}\right) \cdot ... \cdot \left(\frac{p_r}{xy+mD}\right) \\
&= \pm \left(\frac{xy+mD}{p_1}\right) \cdot ... \cdot \left(\frac{xy+mD}{p_r}\right) \\
&= \pm \left(\frac{x}{p_1}\right) \cdot ... \cdot \left(\frac{x}{p_r}\right) \left(\frac{y}{p_1}\right) \cdot ... \cdot \left(\frac{y}{p_r}\right) \\
&= \left(\frac{p_1}{x}\right) \cdot ... \cdot \left(\frac{p_r}{x}\right) \left(\frac{p_1}{y}\right) \cdot ... \cdot \left(\frac{p_r}{y}\right) \\
&= \left(\frac{D}{x}\right) \left(\frac{D}{y}\right) \\
&= \chi([x])\chi([y]).
\end{aligned}$$

□

Of course, that gives us the following for primes p that do not divide $-4n$:

$$p \text{ is represented by a form of discriminant } -4n \iff \left(\frac{n}{p}\right) = 1 \iff [p] \in \ker \chi.$$

This seems like it might be useful as $\ker \chi$ is a group, and so we might hope to use the algebraic properties of this group to learn more about the forms of a given discriminant. As we will soon demonstrate, there is a useful relationship between a certain subgroup of $\ker \chi$ and the different reduced forms of discriminant $-4n$. In fact, for quite a few values of n, we get the best result possible: all the different reduced forms of discriminant $-4n$ represent disjoint subsets of $\ker \chi$, and they represent a prime p if and only if $[p]$ is in the corresponding subset. This all falls under genus theory, which, for our purposes, is the characterization of how different forms do or don't intersect in the values that they represent. We really only need one more theorem to be able to characterize primes of the form $p = x^2 + ny^2$ for about 50 more values of n, although it will require a few lemmas and definitions.

Definition 4.2. For a negative integer $D \equiv 0 \mod 4$, the *principal form of discriminant* D is $x^2 - \frac{D}{4}y^2$.

Lemma 4.3. *If $f(x, y)$ represents an integer m, then m can be written as d^2m', where $f(x, y)$ properly represents m'.*

Proof. Choose x, y in $\mathbb{Z}$ such that $f(x, y) = m$. Let $d = \gcd(x, y)$. Then $x = dx', y = dy'$ for x', y' relatively prime. So $m = f(x, y) = f(dx', dy') = a(dx')^2 + b(dx')(dy') + c(dy')^2 = d^2(ax'^2 + bx'y' + cy'^2) = d^2 f(x', y') = d^2m'$. □

Lemma 4.4. *For any primitive form $f(x, y) = ax^2 + bxy + cy^2$ and integer M, $f(x, y)$ properly represents infinitely many integers relatively prime to M.*

Proof. We will begin by finding one value properly represented by $f(x, y)$ that is relatively prime to M. It is clear that every prime is relatively prime to either a, b, or c, because otherwise $\gcd(a, b, c) = p$, which contradicts the fact that $f(x, y)$ is primitive. Let S_a be the set of distinct prime factors of M that are relatively prime to a, S_c be the set of distinct prime factors that are relatively prime to c but not a, and S_b be the set of distinct prime factors that are relatively prime to b but not a or c. Let $X = \prod_{p \in S_c}$ and $Y = \prod_{p \in S_a}$. For p in S_a, p does not divide X or a, but p divides Y, so p is relatively prime to $f(X, Y)$. The analogous argument shows that all p in S_c are relatively prime to $f(X, Y)$. For p in S_b, p divides a and c, but not X, Y, or b, so p is relatively prime to $f(X, Y)$. This, of course, means that $f(X, Y)$ is relatively prime to M.

The same argument shows that for any S, T relatively prime to M, $f(SX, TY)$ is relatively prime to M. So long as S and T are relatively prime, $f(SX, TY)$ is properly represented, and there are clearly infinitely many values for S and T that satisfy those conditions.

□

Lemma 4.5. *Let $D = -4n$ for some positive integer n, and $f(x, y)$ be a primitive form of discriminant D. Then i) the values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by the principal form of discriminant D form a subgroup H of $\ker \chi$, and ii) the values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by $f(x, y)$ form a coset of H in $\ker \chi$.*

Proof. i) Let m be prime to D, and represented by the principal form of discriminant D. From Lemma 4.3, we know that $m = d^2m'$ for some m' that is properly represented by the principal form. We clearly see that

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

We also know from Lemma 3.8 that D is a quadratic residue modulo m', so $D = b^2 - km'$. Let $p_1, ..., p_r$ be the prime factors of m'. Since it is prime to D, m' is odd, so we can use the Legendre symbol without issue to get

$$\begin{aligned}\chi([m']) = \chi([p_1]) \cdot ... \cdot \chi([p_r]) &= \left(\frac{D}{p_1}\right) \cdot ... \cdot \left(\frac{D}{p_r}\right) \\ &= \left(\frac{b^2 - km'}{p_1}\right) \cdot ... \cdot \left(\frac{b^2 - km'}{p_r}\right) \\ &= \left(\frac{b^2}{p_1}\right) \cdot ... \cdot \left(\frac{b^2}{p_r}\right) \\ &= \left(\frac{b}{p_1}\right)^2 \cdot ... \cdot \left(\frac{b}{p_r}\right)^2 = 1.\end{aligned}$$

So $[m]$ is in $\ker \chi$, which implies $H \subseteq \ker \chi$. We easily see that

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

so H is closed under multiplication, and, therefore, is a subgroup.

ii) From Lemma 3.4 and Lemma 4.4, we can assume $f(x, y) = ax^2+bxy+cy^2$ where a is relatively prime to $4n$. Since the discriminant of $f(x, y)$ is $-4n$, b must be even, so we can write b as $2b'$. It is easy to show that for any form $g(x, y) = \alpha x^2 + \beta xy + \gamma y^2$ of discriminant D', $4\alpha g(x, y) = (2\alpha x + \beta y)^2 - D'y^2$. So we get

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

Since a is relatively prime to $4n$, it is now clear that the values of $(\mathbb{Z}/D\mathbb{Z})^*$ represented by $f(x, y)$ lie in $[a]^{-1}H$. Conversely, if $[c]$ is in $[a]^{-1}H$, we know that $[ac]$ is represented by $x^2 + ny^2$. Using the above identity, it is easy to show that $f(x, y)$ represents $[c]$. Therefore the values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by $f(x, y)$ form the coset $[a]^{-1}H$.

□

Definition 4.6. Let $D = -4n$ for positive n, and let H be as in Lemma 4.4. For any coset H' of H, the *genus* of H' is the set of all quadratic forms of discriminant D that represent H' modulo D.

Theorem 4.7. *Let $D = -4n$ for some positive integer n, and let H be as in Lemma 4.4. If H' is a coset of H in $\ker \chi$ and p is an odd prime not dividing D, then p is represented by a reduced form of discriminant D in the genus of H' if and only if $[p]$ is in H'.*

Proof. If we note that distinct cosets of H must be disjoint, this follows immediately from Lemma 4.4 and Theorem 3.11.

□

This theorem allows us (in many cases, at least) to make a distinction between the values represented by some of the different reduced forms of the same discriminant. With it, we are now ready to prove the conjecture of Euler's which we gave in the introduction (we chose $n = 6$ to avoid filling the paper with many more Legendre symbol calculations, which at this point should feel trivial to the reader).

Theorem 4.8. *A prime p is of the form x^2+6y^2 if and only if $p \equiv 1, 7 \mod 24$.*

Proof. Let $p > 3$ be prime. If reduced form $f(x, y) = ax^2 + bxy + cy^2$ is of discriminant $D = -24$, it satisfies $|b| \leq a \leq \sqrt{-24/3} < 3$. If $a = 1$, $1-4c = -24$ has no integer solutions, so $b = 0$ and $f(x, y) = x^2 + 6y^2$. If $a = 2$, $1 - 8c = -24$ and $4 - 8c = -24$ have no integer solutions, so $f(x, y) = 2x^2 + 3y^2$. Thus the reduced forms of discriminant D are $x^2 + 6y^2$ and $2x^2 + 3y^2$.

We showed in our proof of Theorem 3.15 that $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \mod 3$, and Proposition 2.4 tells us that $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1, 3 \mod 8$, so

$$\left(\frac{-6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1, 5, 7, 11 \mod 24.$$

This of course means that $\ker \chi = \{1, 5, 7, 11\}$. We can see quite easily that of those values, $x^2 + 6y^2$ represents only 1 and 7 (i.e. $H = \{1, 7\}$). And since $2x^2 + 3y^2$ represents 5 and 11 and so can't be in the genus of H, the genus of H is simply $x^2 + 6y^2$ and the forms properly equivalent to it. Therefore, p is of the form $x^2 + 6y^2$ if and only if $p \equiv 1, 7 \mod 24$, which also holds for $p = 2, 3$.

□

Again, this technique allows us to prove a quite impressive result in number theory very easily, needing only a simple, very procedural proof. We encourage the reader to try with $p = x^2 + 5y^2$ to get a further feel of genus theory; as in Theorem 4.8, the proof amounts to little more than basic computations. The power of this technique is fairly remarkable. But while the addition of elementary genus theory lets us characterize primes of the form $p = x^2 + ny^2$ for a lot of values n that the theory of reduced forms alone fell short on, it too has serious limitations. It should be clear that our proof of Theorem 4.8 depended on the fact that the principal form of discriminant -24 was the only reduced form in its genus. From a probabilistic standpoint, though, this is almost never the case. And so, to finish our paper, we will use genus theory to prove one

last conjecture of Euler's, which is about primes of the form $p = x^2 + 14y^2$. This is a noteworthy achievement in its own right, but will also clearly illustrate some of the limitations of the technique we've developed. If we wanted a better characterization, we would need some further theory that falls outside the scope of this paper. We encourage the interested reader to study class field theory in order to learn more about this problem.

Theorem 4.9. *For prime $p \neq 2, 7$, either p or $2p$ is of the form $x^2 + 14y^2$ if and only if $p \equiv 1, 9, 15, 23, 25, 39 \mod 56$, and $3p$ is of the form $x^2 + 14y^2$ if and only if $p \equiv 3, 5, 13, 19, 27, 45 \mod 56$. (Note that we easily can show that p is of the form $2x^2 + 7y^2$ if and only if $2p$ is of the form $x^2 + 14y^2$, giving the result a very nice aesthetic composition).*

Proof. Performing the calculations exactly as in previous proofs, we find that the only reduced forms of discriminant $D = -56$ are $x^2 + 14y^2$, $2x^2 + 3y^2$, $3x^2 + 2xy + 5y^2$, and $3x^2 - 2xy + 5y^2$. Since $\left(\frac{-14}{p}\right) = \left(\frac{-7}{p}\right)\left(\frac{2}{p}\right)$, we also have

$$\left(\frac{-14}{p}\right) = 1 \iff p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \mod 56.$$

It is easy to see that $x^2 + 14y^2$ represents only 1, 9, 15, 23, 25, and 39, and since $2x^2 + 7y^2$ obviously represents 9, it must be in the same genus as the principal form. We also see that $3x^2 \pm 2xy + 5y^2$ represent 3, 5, 13, 19, 27, and 45, and so share their own genus. It's quite clear that p is of the form $2x^2 + 14y^2$ if and only if $2p$ is of the form $x^2 + 14y^2$, so all that remains is to show that $3p$ is of the form $x^2 + 14y^2$ if and only if p is either of the form $3x^2 + 2xy + 5y^2$ or the form $3x^2 - 2xy + 5y^2$. We clearly see that if $p = 3x^2 \pm 2xy + 5y^2$, then $3p = (3x + y)^2 + 14y^2$. Conversely, suppose $3p = x^2 + 14y^2$. If y was a multiple of 3, then y^2 and x^2 would be multiples of 9, so p would be divisible by 3, which is a contradiction. This means we can express y as $3y' \pm 1$. Either way, $14y^2 \equiv 2 \mod 3$, so $x^2 \equiv 1 \mod 3$, which means we can express x as $3x' \pm (3y' \pm 1)$. From here, we easily see that $p = 3x'^2 \pm 2x'(3y' \pm 1) + 5(3y' \pm 1)^2$. □

Acknowledgments

I would like to thank my mentor, Daniel Le, both for guiding my study of this problem and for all that he has taught me about algebra and number theory. I also would like to thank Peter May and the University of Chicago Math Department for making this experience possible. It really was wonderful.

References

[1] David A. Cox. Primes of the Form $p = x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication. John Wiley & Sons, Inc. 1989.

[2] Carl Friedrich Gauss. Disquisitiones Arithmeticae. Trans. Arthur A. Clarke, S.J. Yale University Press. 1966.

[3] Daniel A. Marcus. Number Fields. Springer-Verlag New York, Inc. 1977.

[4] Jean-Pierre Serre. A Course in Arithmetic. Springer-Verlag New York, Inc. 1973.