Binary Quadratic Forms and the Ideal Class Group

Seth Viren Neel

August 6, 2012

1 Introduction

We investigate the genus theory of Binary Quadratic Forms. Genus theory is a classification of all the ideals of quadratic fields $k = \mathbb{Q}(\sqrt{m})$. Gauss showed that if we define an equivalence relation on the fractional ideals of a number field k via the principal ideals of k, and denote the set of equivalence classes by $H^+(k)$ that this is a finite abelian group under multiplication of ideals called the *ideal class group*. The connection with knot theory is that this is analogous to the classification of the homology classes of the homology group by linking numbers. We develop the genus theory from the more classical standpoint of quadratic forms. After introducing the basic definitions and equivalence relations between binary quadratic forms, we introduce Lagrange's theory of reduced forms, and then the classification of forms into genus. Along the way we give an alternative proof of the descent step of Fermat's theorem on primes that are the sum of two squares, and solutions to the related problems of which primes can be written as $x^2 + ny^2$ for several values of n. Finally we connect the ideal class group with the group of equivalence classes of binary quadratic forms, under a suitable composition law. For $d < 0$, the ideal class

group of $\mathbb{Q}(\sqrt{d})$ is isomorphic to the class group of integral binary quadratic forms of discriminant d.

2 Binary Quadratic Forms

2.1 Definitions and Discriminant

An integral quadratic form in 2 variables, is a function $f(x, y) = ax^2 + bxy + cy^2$, where $a, b, c \in \mathbb{Z}$. A quadratic form is said to be *primitive* if a, b, c are relatively prime. We will discuss the theory of primitive quadratic forms. An integer is represented by a quadratic form $= f(x, y)$ if the equation $f(x, y) = m$ has a solution in integers.

We now define an equivalence relation on binary quadratic forms. We say that $f(x, y) \equiv g(a, b)$ iff $\exists\ p, q, r, s$ such that $f(x, y) = g(px + qy, rx + sy)$, and $ps - rg = \pm 1$. Two forms are properly equivalent if $ps - rg = 1$.It is immediately clear that two equivalent forms represent the same numbers. The reader may verify that equivalence and proper equivalence does indeed give us an equivalence relation on integral binary quadratic forms. Now let us see an example of a problem we have solved during this course rephrased in the language of binary quadratic forms. Let p be a prime number. What odd primes p are represented by the integral quadratic form $x^2 + y^2$? It was seen that:

$$p \equiv 1 \pmod 4 \leftrightarrow \text{there exists } x, y \in \mathbb{Z} \text{ such that } x^2 + y^2 = p$$

The proof consists of two steps:

1. Descent Step: If $p|x^2 + y^2$ and $gcd(x, y) = 1$, then $p = x^2 + y^2$.

2. Reciprocity Step: If $p \equiv 1 \pmod 4$ then -1 is a quadratic residue modulo p.

The reciprocity step is a consequence of quadratic reciprocity. In this section we build up a basic theory of quadratic forms, and use it to prove the descent step, giving an alternative proof of Fermat's theorem.
We begin with a lemma that makes it immediately clear how our notions of equivalence will help us understand binary quadratic forms.

Lemma 2.1. *Let $a \in \mathbb{Z}$. Then $f(x, y)$ represents a iff $f(x, y)$ is properly equivalent to the form $g(x, y) = ax^2 + bxy + cy^2$ for some $b, c \in \mathbb{Z}$.*

Proof. Suppose $f(z, w) = a$, where $gcd(x, y) = 1$. Then by Bezout's lemma there exists $q, r \in \mathbb{Z}$ such that $qz - rw = 1$. Changing variables to the properly equivalent form $f(zx + ry, wx + qy)$ we see that the coefficient of x^2 is simply $f(z, w) = a$. Conversely, suppose $f(x, y) \equiv g(x, y) = ax^2 + bxy + cy^2$, then $g(1, 0)$ represents a, and so $f(x, y)$ does as well. □

We define the discriminant of a quadratic form $ax^2 + bxy + cy^2$ in the familiar way, as $D = b^2 - 4ac$. A form where $D > 0$ is called indefinite, and a form where $D < 0$ is called definite.

Exercise 1. *Prove that a definite form either represents all positive or all negative integers, according to the sign of a.*

We claim that discriminant is invariant under the equivalence relation defined above, so that we can speak of the discriminant of a class. Let $f(x, y) = ax^2+bx+c$, and suppose that $g(x, y) = f(px + ry, qx + sy)$ where $ps - qr = \pm 1$. Then $D(g) = (2apr + bps + brq + 2cqs)^2 - 4(ap^2 + bpq + cq^2)(ar^2 + brs + cs^2) = (b^2 - 4ac)(ps - qr)^2 = b^2 - 4ac = D(f)$, as desired. Equipped with a notion of discriminant that

is compatible with our equivalence relation, we can immediately see its application our original problem of representing integers with integral binary quadratic forms.

Lemma 2.2. *An odd integer M is properly represented by a primitive form of discriminant D iff $D \equiv x^2 \pmod{m}$ for some $x \in (\mathbb{Z}/m\mathbb{Z})^*, (D, M) = 1$, and D is a quadratic residue* $\pmod{4}$.

Proof. Suppose that $D \equiv t^2 \pmod{m}$, then $D = t^2 + km$, for some $k \in \mathbb{Z}$. Since m is odd we can assume that $t^2 \equiv D \pmod{4}$. Then taking $D = t^2 + km \pmod{4}$ and using $(m, D) = 1$ we deduce that $4|k$, so $k = 4c$. Then $D = b^2 - mc$, and so D is the discriminant of the quadratic form $mx^2 + bxy + cy^2$, which represents m. Conversely if D is the discriminant of a primitive form representing m, then it is the discriminant of a primitive form $mx^2 + kxy + sy^2$, and so $D \equiv k^2 \pmod{m}$. Since the form is primitive we get that $(m, D) = 1$. □

So we have shown that we can determine if a number m is representable by a primitive quadratic form of discriminant D, based on its quadratic residue $\bmod D$. Note that if m is representable then $m + kD$ is as well $\forall k \in \mathbb{Z}$. However, at this stage knowing that a given number is representable by a form of discriminant D is not especially helpful information, as there are many different quadratic forms with a given discriminant. This is where Lagrange's theory of reduced forms comes in; we will show that every form is equivalent to a much simpler form. We will also restrict our attention to forms with $D < 0$, as they are the ones we really care about anyways.

2.2 Lagrange's Theory of Reduced Forms

In this section we state several of the results without proof when the reasoning is lengthy, the interested reader can find these proofs in [1].

Definition 1. *A primitive positive definite quadratic form $ax^2 + bxy + cy^2$ is said to be reduced if $c \geq a \geq |b|$, and when $|b| = a$ or $a = c, b \geq 0$.*

Then we have due to Legendre:

Theorem 2.3. *Every primitive form with $D < 0$ is properly equivalent to a unique reduced form.*

The proof finds the form in each equivalence class minimizing $|b|$, and then shows that if the conditions are not met a form with smaller $|b|$ can be constructed. For details see [1, p.28-29]. As an example, the forms $7x^2 \pm 6xy + 13y^2$ are clearly equivalent via $(x, y) \to (-x, y)$, but since they are reduced, they cannot be properly equivalent (uniqueness).

An important consequence of the theorem is that there are finitely many proper equivalence classes of forms with a given discriminant $D < 0$. Since $b^2 - 4ac = D$, and $c \geq a \geq |b|$, then we have $-D \geq 4a^2 - a^2 \implies a \leq \sqrt{-D/3}$ and since $a \geq |b|$, and $b^2 - 4ac$ is fixed, there are finitely many values of (a, b, c) such that $ax^2 + bxy + cy^2$ is a reduced form of discriminant D, and hence finitely many proper equivalence classes of forms of discriminant D. We are now equipped to give an alternative proof of the descent step in the proof of Fermat's theorem that prime $p \equiv 1 \pmod 4 \iff$ its represented by the form $x^2 + y^2$. We note that $p | x^2 + y^2$ for some $x, y \iff (\frac{-4}{p}) = 1$, which by Lemma 2.2 means that p is represented by

a primitive form of discriminant -4. But then $|b| \leq a \leq \sqrt{4/3}$, so $b = 1, 0$. But if $b = 1$ then $b^2 - 4ac \equiv 1 \pmod 4 \neq -4$. So $b = 0$, and thus $ac = 1 \implies a = c = 1$, since $-x^2 - y^2$ isn't reduced. Thus if $p|y^2 + x^2$ for some x, y then p is representable by $f(x, y) = x^2 + y^2$.

2.3 Genus Theory of Binary Quadratic Forms

Now that we can prove Fermat's theorem with ease we may be feeling quite good about ourselves. However, we have made use of the fact that there was only one reduced form with discriminant -4. In general we will not be able to do this, and so a further classification of reduced forms with discriminant D is necessary. Indeed it is a theorem of Landau that if we let h denote the number of equivalence classes of such forms, $h(-4k) = 1 \iff n = 1, 2, 3, 4, 7$. And indeed there may be more than one form in each equivalence class. Our goal is to describe solutions of $p = x^2 + ny^2$, so we need to get a sense of what other primitive forms of discriminant $-4n$ are out there.

Definition 2. *We say that two reduced forms of discriminant $D < 0$ are in the same genus if they represent the same set of elements in $(Z/D\mathbb{Z})^*$.*

It is immediately clear that equivalent reduced forms are in the same genus. We claim that if f represents $x \in (Z/D\mathbb{Z})^*$, as does g, then f and g are in the same genus. To this end we show that the numbers in $(Z/D\mathbb{Z})^*$ representable by forms f form an equivalence class with respect to the subgroup of representable numbers, and so these equivalence classes are disjoint.

Definition 3. *We define the principal form as $x^2 - \frac{D}{4}y^2$ when $D \equiv 0 \pmod 4$, and $x^2 + xy + \frac{1-D}{4}y^2$ when $D \equiv 1 \pmod 4$.*

Denote by λ the subgroup of $(Z/D\mathbb{Z})^*$ of representable numbers. Then we have the following theorem describing the equivalence relation in $(Z/D\mathbb{Z})^*$:

Theorem 2.4. *The values in (Z/DZ)* represented by the genus of the principal form make up a subgroup $H \subset \lambda$. Then the values in $(Z/D\mathbb{Z})^*$ represented by an arbitrary reduced binary quadratic form of discriminant D consists of a coset $xH, x \in \lambda$.*

Proof. It can be show with relative ease that H is in fact a subgroup. In the case that $D \equiv 1 \pmod 4$ it is simply the subgroup of quadratic residues in $(Z/D\mathbb{Z})^*$ which is seen via the computation:

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

So we focus on showing that the elements in $(Z/D\mathbb{Z})^*$ represented by an arbitrary form $f(x,y)$ are an H coset of λ. To do so we need the following lemma due to none other than Gauss:

Lemma 2.5. *Let $f(x,y)$ an integral quadratic form, and let M be an integer. Then f represents at least one integer that is relatively prime to M.*

Then by the lemma we can say WLOG that $f(x,y) = ax^2 + bxy + cy^2$where $(a, 4n) = 1$. We first address the case $D \equiv 0 \pmod 4$, letting $D = 4n$. Then we can conclude the $b^2 \equiv 0 \pmod 4$, and hence $2|b$. Let $b = 2b'$.So we can write:

$$af(x,y) = a^2x^2 + 2b'axy + b'^2y^2 + (ac - b'^2)(y^2)$$

which since $4b'^2 - 4ac = 4n$, is simply

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

and hence the values represented by $f(x,y) \subset a^{-1}H$, and conversely if $s = a^-1h$ where $h \in H$ then we need only show that $af(x,y)$ represents h, but $af(x,y)$ is simply the principal form, which represents h by definition. Thus each reduced form of discriminant D represents a coset aH of the subgroup $H \subset \lambda$ in $(Z/D\mathbb{Z})^*$. $\square$

Now we apply the corrollary that if p a prime and $p \not| n$ then $p \in H \iff p \equiv x^2 \pmod{4n}$ or $x^2+n \pmod{4n}$ for some $x \in (Z/D\mathbb{Z})^*$, to a few of the principal forms we were interested in. We compute:

$p = x^2 + 6y^2 \iff p \equiv 1, 7 \pmod{24}$

$p = x^2 + 15y^2 \iff p \equiv 1, 19, 31, 49 \pmod{60}$ etc.

...

And so we have solved the problem of representing primes as $x^2 + ny^2$ for several values of n.

3 The Class Group

Earlier we separated forms of discriminant D into equivalence classes, and it is natural to see if a group structure can be defined on these classes. This is where the study of binary quadratic forms, is related to the study of the ideal class group of the number field $\mathbb{Q}(\sqrt{D})$. The ideal class group is the group of fractional ideals modulo the principal ideals. In a principal ideal domain, the ideal class group is trivial.

We describe the correspondence between classes of ideals of $\mathbb{Q}(\sqrt{D})$, and reduced binary quadratic forms of discriminant D, following from [2]. We then describe a composition law on quadratic forms due to Gauss, which turns out to be compatible

with multiplication of fractional ideals. It is then evident that the ideal class group of $\mathbb{Q}(\sqrt{D})$ is equal to the class group of quadratic forms of discriminant D.

Denote the ring of integers of $K = Q(\sqrt{D})$ by O_K. Then the set of fractional ideals of O_K modulo the subring of principal fractional ideals forms a group known as the ideal class group. The group law is multiplication of ideals in the usual way. Then every fractional ideal of O_K can be written in the form $c(ax + (B + \sqrt{D})y)$ for some integers a, B, g, x, y [2]. We say that two ideals are equivalent if they differ by an element of O_K; i.e. $I \equiv T \iff \exists\ \alpha, \beta \in O_K$ such that $\alpha I = \beta T$. Then as in the case of quadratic forms we can *reduce* ideals modulo this equivalence relation to ideals $(2a, b + \sqrt{D})$ where $4a|b^2 - D$. There is a bijection between such reduced forms and quadratic forms with discriminant D. We send this ideal to the form $(ax + \frac{b+\sqrt{D}}{2}y)(ax + \frac{b-\sqrt{D}}{2}y) = a(ax^2 + bxy + cy^2)$, which has discriminant D. We now describe the composition of quadratic forms that corresponds to ideal multiplication.

Definition 4. *Given $f(x, y)$ and $g(x, y)$ primitive forms of discriminant $D < 0$ then $h(x, y)$ is their composition if $f(x, y)g(z, w) = h(B(x, y, z, w), S(x, y, z, w))$ where B, S are bilinear forms $B = axz + bxw + cyz + dyw, S = exz + fxw + gyz + kyw$, where $af - eb = f(1, 0)$ and $ag - ec = g(1, 0)$.*

Then it is an important result of Gauss that this composition respects proper equivalence, and makes the set of classes of forms into a finite abelian group. This is the class group of binary quadratic forms. But then by the above reasoning, the ideal class group is seen to be isomorphic to the class group. This composition is abelian, and because we have shown that there are only finitely many equivalence classes of reduced forms of discriminant D, we have shown that the ideal class group of $\mathbb{Q}(\sqrt{D})$ is thus finite and abelian!

4 References

[1] Cox, David, *Primes of the Form $x^2 + ny^2$ Fermat, Class Field Theory, and Complex Multiplication,* Wiley 1989.

[2] Granville, Andrew, *Binary Quadratic Forms Lecture Notes*, http://www.dms.umontreal.ca/ andrew/Courses/Chapter4.pdf.