

Lectures # 7: The Class Number Formula For Positive Definite Binary Quadratic Forms.

Noah Snyder

July 17, 2002

1 Definitions

Definition 1.1. A binary quadratic form (BQF) is a function $Q(x, y) = ax^2 + bxy + cy^2$ (with $a, b, c \in \mathbb{Z}$) and will be denoted (a, b, c) .

These BQFs were first studied in an attempt to generalize Fermat's theorem that $n = x^2 + y^2$ if and only if when we write $n = \prod p^{a_p}$ the exponent a_p is even for every prime $p \equiv 1 \pmod{4}$.

Definition 1.2. We say that a BQF Q represents a number n when there exist integers x and y such that $Q(x, y) = n$. If x and y are relatively prime then we say that Q properly represents n .

Notice that if $d = \gcd(x, y)$ then $Q(x, y) = n$ if and only if $Q(\frac{x}{d}, \frac{y}{d}) = \frac{n^2}{d}$. Since the latter representation is proper, to find all numbers represented by Q it is enough to find all the numbers it properly represents.

The basic question in the theory of BQF's is to find all numbers represented by a form Q and to find how many different ways there are to represent each of these numbers.

Definition 1.3. If $Q = (a, b, c)$ is a BQF, we define the associated matrix (which by abuse of notation we will denote Q) to be

$$\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

Proposition 1.4. Let $v = \begin{pmatrix} x \\ y \end{pmatrix}$. Then

$$Q(x, y) = v^T Q v.$$

Proof. This simply says that $ax^2 + bxy + cy^2 = ax^2 + \frac{b}{2}xy + \frac{b}{2}yx + cy^2$. □

Notice that this means if we change variables $\begin{pmatrix} x' \\ y' \end{pmatrix} = v' = Av$ (the entries of A are integers) then $Q(x', y') = (Av)^T Q Av = v'^T (A^T Q A) v'$. Therefore, if Q represents a number then so does $A^T Q A$. In particular, if A has an inverse with integer entries, then we get that Q and $A^T Q A$ represent all the same numbers. Clearly if A has an inverse B with integer entries, then $\det A \det B = \det AB = 1$, thus $\det A = \pm 1$. Furthermore one can easily show that if $\det A = \pm 1$ then A has an integer inverse. Lagrange defined two forms Q and Q' to be equivalent if there exists A with determinant ± 1 such that $A^T Q A = Q'$. Gauss strengthened this notion as follows.

Definition 1.5. We say that two forms Q and Q' are properly equivalent if there exists a matrix A such that $A^T Q A = Q'$ and $\det A = 1$. If there exists a matrix A such that $A^T Q A = Q'$ and $\det A = -1$ then we call the two BQFs improperly equivalent. Unless otherwise noted, when we say equivalent we mean properly equivalent.

Notice that two BQFs can be both properly and improperly equivalent, for example $(1, 0, 1)$ is equivalent to itself under the identity transformation and under the transformation $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, thus it is improperly equivalent to itself.

Furthermore notice that proper equivalence is an equivalence relation (while improper equivalence is not).

Notice that if two forms Q and Q' are equivalent, then $\det Q' = \det A^T \det Q \det A = \det Q$. This suggests the following definition.

Definition 1.6. *The discriminant of a form Q is the integer $D_Q = -4 \det Q = b^2 - 4ac$.*

We have already proved that the discriminant is defined up to equivalence.

Notice that $D_Q \equiv b^2 \equiv 0$ or $1 \pmod{4}$. Furthermore, if D_Q is a perfect square then Q factors as the product of two linear forms. Since the theory is trivial in this case we only consider forms Q with D_Q nonsquare.

Henceforth the number D will always denote a non-square integer congruent to 0 or 1 modulo 4.

Proposition 1.7. *Let $D = D_Q$ for some fixed form Q . If $D > 0$ then Q represents both positive and negative numbers. If $d < 0$ and $a > 0$ then Q represents only nonnegative numbers. If $d < 0$ and $a < 0$ then Q represents only nonpositive numbers.*

Proof. If $D > 0$ then $F(1, 0) = a$ and $F(b, -2a) = -Da$. These two numbers have opposite signs. If $D < 0$ notice that $4aQ(x, y) = (2ax + by)^2 - dy^2 \geq 0$, from which the result follows. \square

Definition 1.8. *If $D_Q > 0$ then we call Q indefinite. If $d < 0$ and $a > 0$ then Q is called positive definite. If $d < 0$ and $a < 0$ then Q is called negative definite.*

Since positive and negative definite forms are simply negatives of each other, we can ignore negative definite forms. In this week's lectures we will only be considering positive definite forms, indefinite forms will be dealt with in one of the projects. Many of the following results also hold for indefinite forms, finding which ones will be left as an exercise to the reader.

Finally we call a BQF primitive if a , b , and c are relatively prime. Again, if they weren't we could factor out the common factor and study that quadratic form and recover all the information about the original form. Thus from now on we will only consider

2 Class Number

Suppose we consider one particular equivalence class of BQFs. We would like to be able to pick a particularly nice representative of this class with small coefficients.

Theorem 2.1. *Every class contains a form for which $|b| \leq |a| \leq c$.*

Proof. Choose a form (a_0, b_0, c_0) belonging to the class in question. Let a be a nonzero number represented by (a_0, b_0, c_0) with minimal absolute value. Thus

$$a = a_0 r^2 + b_0 r t + c_0 t^2.$$

We must have $\gcd(r, t) = 1$ or else $\frac{a}{\gcd(r, t)}$ would be represented contradicting minimality. Therefore we can find numbers u and t such that $ru - st = 1$.

A simple computation shows that $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ takes (a_0, b_0, c_0) to (a, b', c') for some integers b' and c' .

Now the transformation $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ takes (a, b', c') to $(a, 2ah + b', c(h))$. Thus for suitably chosen h , the second coefficient can be made smaller in absolute value than b . Therefore, we have found an element of the class (a, b, c) with $|b| \leq |a|$. Since $c \neq 0$ can be represented by Q we get $|a| \leq |c|$ as we had hoped to show. \square

Therefore the number of distinct primary equivalence classes with a given discriminant is finite. This number is called the class number and will be denoted $h(D)$.

If $D \equiv 0 \pmod{4}$ then $(D, 0, 1)$ has discriminant D and if $D \equiv 1 \pmod{4}$ then $(1, 1, \frac{1-D}{4})$ has discriminant D . Thus for any D , $h(D) > 0$.

Letting $\chi(n) = \left(\frac{D}{n}\right)$ Our goal is to give a formula for $h(D)$ in terms of $L(1, \chi)$. As a consequence we will see that $L(1, \chi) \neq 0$.

3 Which Numbers are Represented by Some Form With Discriminant D .

Theorem 3.1. *The numbers properly represented by Q are exactly the numbers a' which appear as the first term of forms equivalent to Q .*

Proof. If $Q = (a, b, c) \sim (a', b', c')$ via the matrix $A = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$, then $n = Q(r, t)$. Since $\det A = 1$, this representation is proper.

In our proof of the finiteness of class number we should that if a number a' was properly represented by Q then Q is equivalent to (a', b', c') for some b' and c' . \square

Theorem 3.2. *If n is properly representable by $Q = (a, b, c)$ with discriminant D , then $D \equiv \square \pmod{4|n|}$.*

Proof. By the last theorem there exist some b' and c' such that $(a, b, c) \sim (n, b', c')$. Thus $b'^2 - 4nc' = D$. The theorem follows. \square

Theorem 3.3. *If $D \equiv \square \pmod{4|n|}$, then n is properly by some form of discriminant D .*

Proof. By assumption there exists some integers ℓ and k such that $\ell^2 = D - 4nk$. Therefore the form (n, ℓ, k) has discriminant D and represents n . \square

Furthermore, for each choice of $\ell^2 \equiv D \pmod{4n}$ with $0 \leq \ell < 2k$, there is only one form written in the form (n, ℓ, k) with discriminant D .

4 An Application

Theorem 4.1. *An odd prime p can be written in the form $x^2 + y^2$ exactly when $p \equiv 1 \pmod{4}$.*

Proof. Let $Q = (1, 0, 1)$. This has discriminant -4 . Suppose (a, b, c) is a reduced representative of some equivalence class with discriminant D . Thus $|b| \leq a \leq |c|$ and $b^2 - 4ac = -4$. Thus $b^2 = 4(ac - 1)$. Since $|ac| \geq b^2$ we must have $ac - 1 = 0$. Thus the only such form is $(1, 0, 1)$. Therefore, $h(-4) = 1$. Hence p is representable by $(1, 0, 1)$ if and only if $-4 \equiv \square \pmod{4p}$. Thus if and only if $\left(\frac{-1}{p}\right) = 1$. By the supplementary law to QR we're done. \square

Similarly one can show that $p = x^2 + 2y^2$ exactly when $p \equiv 1$ or $3 \pmod{8}$.

5 Number of Representations

We want to find the number of ways in which we can properly represent n by some BQF of fixed discriminant $D < 0$. By arguments we have already made it suffices to find every transformation

$A = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ with $\det A = 1$ sending Q to itself. For this to happen we must have

$$a = ar^2 + brt + ct^2,$$

$$b = 2ars + b(1 + 2st) + 2ctu.$$

Therefore we must also have, $0 = ars + bst + ctu$.

We can eliminate b to get, $as = cst^2 - crt u = -ct$. On the other hand we can eliminate c to get, $a(u - r) = bt$. Therefore, $a|ct$ and $a|bt$. If Q is primitive, then $a|t$. Let $t = at'$. Therefore, $s = -ct'$ and $u - r = bt'$. Hence it follows that,

$$(u + r)^2 = (u - r)^2 + 4ur = b^2t'^2 + 4(1 + st) = b^2t'^2 + 4(1 - act'^2) = Dt'^2 + 4.$$

Therefore, $(u + r)^2 - Dt'^2 = 4$. If $D = -3$ then there are 6 solutions. If $D = -4$ there are 4 solutions. If $D < -4$ then there are only 2 solutions. We let w denote this number of solutions.

Theorem 5.1. *Suppose n is an integer relatively prime to D . If n is divisible by μ distinct primes each of which has $\left(\frac{D}{p}\right) = 1$ but by no other primes, then n can be represented in $w2^\mu$ distinct ways by a primitive form of discriminant D . Otherwise n cannot be represented by a primitive form of discriminant D .*

Proof. Recall that each pair of solutions of $\ell^2 \equiv D \pmod{4n}$ gives us exactly w ways of representing n by some form of discriminant K . We factor $4n$ as a product of primes and use the Chinese remainder theorem to reduce to counting the number of square roots of D modulo a prime power p^k .

For each odd prime we can write D as a square modulo p^k in exactly $1 + \left(\frac{D}{p}\right)$ ways.

Now we turn our attention to the prime 2. Suppose n is odd. Then the power of two we are looking at is 4. Since $D \equiv 0$ or $1 \pmod{4}$ it can be written as a square in exactly 2 ways. If n is even then we are looking modulo at least 8. Since n is relatively prime to D , $D \equiv 1 \pmod{4}$. Thus D can be written as a square in $2\left(1 + \left(\frac{D}{2}\right)\right)$ ways.

By only counting one solution from each pair, for the last two cases we should only consider half the solutions. Thus, for each prime with $\left(\frac{D}{p}\right) = 1$ we pick up 2 solutions, and modulo the product we end up with 2^μ pairs of solutions. Thus the total number of representations is $w2^\mu$. \square

It follows that:

Theorem 5.2. *We have*

$$\sum_Q \sum_{x,y} Q(x,y)^{-s} = w \sum_{m=1}^{\infty} \frac{2^\mu}{m^s},$$

where Q runs over each primary class once and x and y run over all relatively prime pairs with $Q(x,y)$ relatively prime to D . \square

The right hand side has an Euler factorization.

$$\sum_{m=1}^{\infty} \frac{2^\mu}{m^s} = \prod_{p: \left(\frac{D}{p}\right)=1} \left(1 + \frac{2}{p^s} + \frac{2}{p^{2s}} + \dots\right) = \prod_{p: \gcd(p,D)=1 \text{ and } \left(\frac{D}{p}\right)=1} \frac{1 + p^{-s}}{1 - p^{-s}}.$$

Therefore,

$$\sum_Q \sum_{x,y} Q(x,y)^{-s} = w \prod_{\gcd(p,D)=1} \frac{1 + p^{-s}}{1 - \left(\frac{D}{p}\right)p^{-s}} = w \frac{L(s, \chi_0)L(s, \chi)}{L(2s, \chi_0)}.$$

If we multiply both sides by $L(2s, \chi_0)$, the left hand side becomes

$$\sum_n \sum_{x,y \text{ relatively prime}} (n^2 Q(x,y))^{-s} = \sum_n \sum_{x,y \text{ relatively prime}} Q(nx, ny)^{-s} = \sum_{x',y'} Q(x', y'),$$

where each of these sums range over all pairs with Q relatively prime to D and where the last sum ranges over *all* such pairs.

Therefore, (still summing over $Q(x,y)$ relatively prime to D),

$$\sum_Q \sum_{x,y} Q(x,y)^{-s} = wL(s, \chi_0)L(s, \chi).$$

Dirichlet noticed that if you multiply both sides by $(s-1)$ and send $s \rightarrow 1^+$ then you get well-defined limit. The righthand side is $\frac{w\varphi(|D|)}{|D|}L(1, \chi)$.

Proposition 5.3. *Suppose a_n is a sequence. Let $f(x) = \sum_{n \leq x} a_n$ such that*

$$\lim_{x \rightarrow \infty} \frac{f(x)}{x} \rightarrow c.$$

Then

$$\lim_{s \rightarrow 1^+} (s-1) \sum_{n=1}^{\infty} \frac{a_n}{n^s} = c.$$

Proof. This proposition states that if some sequence has a well-defined density, then it also has a well-defined Dirichlet density and the two are equal. The converse, however, is not true.

If $f(n-1) < i \leq f(n)$ then let $k_i = n$. Notice that the multiset of all the k_i 's contains the element n exactly a_n times. Thus

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \sum_{i=1}^{\infty} k_i^{-s}.$$

Let $h_n = \frac{n}{k_n}$. We claim $\lim_{n \rightarrow \infty} h_n = c$. Notice that $h_{f(n)} = \frac{f(n)}{n}$. Thus the smallest that h_x can get is $\frac{f(n)}{n-1}$. This limit still approaches c .

Notice,

$$\lim_{s \rightarrow 1^+} (s-1) \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \lim_{s \rightarrow 1^+} (s-1) \sum_{n=1}^{\infty} \frac{h_n^s}{n^s}.$$

The righthand side can be easily evaluated. For any $\varepsilon > 0$ we can choose N large enough such that for all $n \geq N$, $c - \varepsilon < h_n < c + \varepsilon$. With this choice, splitting the sum up into terms less than and greater than N ,

$$\lim_{s \rightarrow 1^+} (s-1)(c - \varepsilon)^s \zeta(s) \leq \lim_{s \rightarrow 1^+} (s-1) \sum_{n=1}^{\infty} \frac{h_n^s}{n^s} \leq \lim_{s \rightarrow 1^+} (s-1)(c + \varepsilon)^s \zeta(s).$$

Thus the limit is sandwiched between $c - \varepsilon$ and $c + \varepsilon$ and so goes to c . \square

Proposition 5.4. *One can find Q in a given equivalence class such that a is relatively prime to a given number m .*

Proof. This is equivalent to saying that we can choose x and y so that $Q(x, y)$ is relatively prime m . Choose any prime $p|m$. If $p|a$ and $p|c$, then $p \nmid b$, so if we choose x and y both prime to p Q will also be prime to p . If $p \nmid a$ (resp. c) then we can choose x prime to p and y divisible by p (resp. x divisible by p and y prime to p). By the Chinese remainder theorem we can choose x and y subject to the above conditions for every prime $p|m$. \square

Theorem 5.5. *For any fixed Q , (taking the sum over $Q(x, y)$ relatively prime to D as usual)*

$$\lim_{s \rightarrow 1^+} s \sum_{x, y} Q(x, y)^{-s} = \frac{\varphi(|D|)}{|D|} \frac{2\pi}{\sqrt{|D|}}.$$

Proof. By our first lemma it is enough to compute the ordinary density $\lim_{n \rightarrow \infty} \frac{f(n)}{n}$ where $f(n)$ is the number of values $Q(x, y) \leq n$ relatively prime to D .

First we deal with the issue of finding which pairs make $Q(x, y)$ relatively prime to D . Notice that this is just a question of what the values of Q are on $\mathbb{Z}/D\mathbb{Z}$. By our second lemma we can choose our representative Q such that each one has a relatively prime to D .

Suppose D is odd and thus b is odd. Thus $ax^2 + bxy + cy^2$ is relatively prime to D exactly when $2a(ax^2 + bxy + cy^2) = (2ax + by)^2 - Dy^2$ is. Now, no matter what we choose for y we only need to have $(2ax + by)$ relatively prime to D . As x varies this runs through a complete residue system, thus the total number of solutions is $D\varphi(D)$.

Suppose D is even and thus b is even. Thus $ax^2 + bxy + cy^2$ is relatively prime to D exactly when $a(ax^2 + bxy + cy^2) = (ax + \frac{b}{2}y)^2 - \frac{D}{4}y^2$ is. If y is even then it is sufficient to choose $ax + \frac{b}{2}y$ relatively prime to D . This runs through a complete system of residues as x runs through one, thus with y even there are $\frac{D}{2}\varphi(D)$ solutions. If y is odd, and $\frac{D}{4}$ is even, then we are in exactly the same situation and there are $\frac{D}{2}\varphi(D)$ more solutions. If y is odd and $\frac{D}{4}$ is odd then we need to choose $ax + \frac{b}{2}y$ even and relatively prime to $\frac{D}{4}$. Since this expression still runs through a complete residue system modulo D there are $\frac{D}{2}2\varphi(\frac{D}{4}) = \frac{D}{2}\varphi(D)$. For both of these cases the total number of pairs which give $Q(x, y)$ relatively prime to D is $D\varphi(D)$.

Thus if we let $f_{x_0, y_0}(n)$ denote the number of values $Q(x, y) \leq n$ in some particular equivalence class $(x, y) \equiv (x_0, y_0) \pmod{D}$, it is sufficient to prove

$$\lim_{n \rightarrow \infty} \frac{f(n)}{n} = \frac{1}{|D|^2} \frac{2\pi}{\sqrt{|D|}}.$$

The condition $Q(x, y) \leq n$ says that (x, y) should lie in an ellipse which expands uniformly as n increases. We would thus expect the number of points in some particular equivalence class to be $\frac{1}{|D|^2} \text{Area}$. The area of the ellipse is $\frac{2\pi}{\sqrt{|D|}}n$. Thus we would expect $\frac{f(n)}{n} \approx \frac{1}{|D|^2} \frac{2\pi}{\sqrt{|D|}}$.

To make this argument rigorous, divide the plane into squares of side $|D|$. For every square in the interior of the ellipse $Q(x, y) \leq n$ we should count it once. For squares on the boundary we may or may not count the square depending on whether the lattice point in our equivalence class lies there. Scaling the whole picture by $\frac{1}{n}$ we are looking at the plane divided into squares of side $\frac{|D|}{n}$ and we want to find the number of squares contained in (and possibly on the boundary) of the ellipse $Q(x, y) \leq 1$. By integral calculus, this limit is the area of the ellipse $Q(x, y) \leq 1$ regardless of whether we count boundary points. Therefore $\lim_{n \rightarrow \infty} \frac{f(n)}{n} = \frac{1}{|D|^2} \frac{2\pi}{\sqrt{|D|}}$.

Thus we've proved our result. \square

Theorem 5.6.

$$L(1, \chi) = h(D) \frac{2\pi}{w\sqrt{|D|}} \neq 0$$

and

$$h(D) = \frac{w\sqrt{|D|}}{2\pi} L(1, \chi).$$

Proof. We have shown that (letting Q run over representatives of each class and x and y range over pairs with $Q(x, y)$ prime to D)

$$\sum_Q \sum_{x, y} Q(x, y)^{-s} = wL(s, \chi_0)L(s, \chi).$$

Multiply both sides by $(s - 1)$ and send $s \rightarrow 1^+$. We have already evaluated these limits, thus

$$h(D) \frac{\varphi|D|}{|D|} \frac{2\pi}{\sqrt{|D|}} = \frac{w\varphi(|D|)}{|D|} L(1, \chi).$$

Rearranging gives our two formulas. \square

Notice, by the methods of homework 2 we can write $L(1, \chi)$ as a finite sum:

$$L(1, \chi) = -\frac{\pi}{\sqrt{|D|}} \sum_{m=1}^{|D|} m\chi(m) = -\frac{\pi}{\sqrt{|D|}} \frac{D}{2 - \chi(2)} \sum_{m=1}^{\frac{|D|}{2}} \chi(m).$$

Therefore,

$$h(D) = \frac{1}{2 - \chi(2)} \sum_{m=1}^{\frac{|D|}{2}} \chi(D).$$

Notice that since $h(D)$ is positive, most of the squares modulo D lie between 0 and $\frac{|D|}{2}$. Interestingly enough there is no known non-analytic proof of this fact.

This also gives a very quick way of finding a give class number. Unfortunately, the method of simply finding all reduced forms actually works more quickly. Using the functional equation of the L -series, however gives a much more efficient way of computing this value.

Finally we would like to notice that if D is squarefree (except for possibly 4) every form is primary and we could have found a formula for the number of representations of n even when n was not relatively prime to D . In this case D is a square modulo p in one way but not a square p^2 for every prime dividing n and D (unless that prime is 2 in which case it takes a tad more work). Thus we get representations when the number is also a product of primes dividing D each taken to the first power. Plugging this into our equations gives the nicer formula (where we now only sum over x and y not both zero)

$$\sum_{x,y} Q(x,y)^{-s} = \zeta(s)L(s,\chi).$$