The Mass Formula for Binary Quadratic Forms

by John Paul Cook

A well-documented question from classical number theory pertains to the different representations of an integer k by a binary quadratic form. The question we will address here is the *number* of representations of k by a binary quadratic form, i.e.

$$\#\{(x,y) \in \mathbb{Z}^2 | f(x,y) = k\}.$$

It turns out that there is only an exact result for the form in question for positive definite forms whose discriminants have class number 1. Instead, we will work towards counting the number of representations of an integer by *all* forms of a given discriminant (which, of course, for class number 1, is the exact result just mentioned), while developing the basic theory of binary quadratic forms along the way.

1. Binary Quadratic Forms

Definition 1.1. Let $a, b, c \in \mathbb{Z}$. A function

$$f(x,y) = ax^2 + bxy + cy^2$$

is called an *integral binary quadratic form* (which we shall often refer to as a "form" or "quadratic form"). The *discriminant* of f is given by $d = b^2 - 4ac$.

An immediate use of the discriminant is in the determination of which binary quadratic forms are *irreducible*, i.e. those forms which do not decompose into a product of (integral) linear factors: it is easily verified that a form can be written as a product of linear factors if and only if its discriminant is a square. Since we only wish to study irreducible forms, we will limit ourselves to nonsquare discriminants. It is worth noting that for any form, $d \equiv 0, 1 \mod 4$. In fact, for every such d, there is a form with discriminant d: If $d \equiv 0 \mod 4$, then $x^2 - \frac{d}{4}y^2$ has discriminant d; if $d \equiv 1 \mod 4$, then $x^2 - \frac{d-1}{4}y^2$ has discriminant d.

Since it is our goal to count the number of representations of an integer by a quadratic form, we distinguish between two different kinds of representations:

Definition 1.2. A representation (x, y) of k by a form f is called *proper* if $\gcd(x, y) = 1$, and is called *improper* otherwise.

Note that if $f(x, y) = k$ and $\gcd(x, y) = g$, then g^2 divides k, and we have that $\gcd\left(\frac{x}{g}, \frac{y}{g}\right) = 1$ and $f\left(\frac{x}{g}, \frac{y}{g}\right) = \frac{k}{g^2}$. We also have a similar notion for the coefficients of f:

Definition 1.3. $f(x,y) = ax^2 + bxy + cy^2$ is called a *primitive* form if $\gcd(a, b, c)$=1, otherwise it is called *imprimitive*.

The notion of a primitive form is closely related to the notion of a fundamental discriminant, i.e. a discriminant d in which all forms with discriminant d are primitive forms. Keeping in mind that the discriminant of any form is congruent to 0 or 1 mod 4, we offer the following characterization of fundamental discriminants (verification of these facts is left as an exercise):

- If $d \equiv 1 \bmod 4$, then d is a fundamental discriminant if and only if d is squarefree.
- If $d \equiv 0 \bmod 4$, then $\frac{d}{4}$ is squarefree, and $\frac{d}{4} \equiv 2$ or $3 \bmod 4$.

As we shall see later on, it suffices only to study primitive forms. For example, let $f(x,y) = ax^2 + bxy + cy^2$ be an imprimitive form such that $\gcd(a,b,c) = g$. Then clearly we have that $g^2|d$, and $f(x,y) = \frac{a}{g}x^2 + \frac{b}{g}xy + \frac{c}{g}y^2$ is a primitive form of discriminant $\frac{d}{g^2}$. We will discuss representations by primitive forms and their relevance later.

Definition 1.4. f is called *indefinite* if it takes both positive and negative values, positive (or negative) semidefinite if either $f(x,y) \geq 0$ (or $f(x,y) \leq 0$, resp.) for all $(x,y) \in \mathbb{Z}^2$. Additionally, a semidefinite binary quadratic form f is called definite if $f(x,y) = 0 \Leftrightarrow x = 0, y = 0$.

The discriminant offers an equivalent characterization of definiteness of a form, which is much more convenient for our purposes:

Proposition 1.5. Let $f(x,y) = ax^2 + bxy + cy^2$ be an integral form with discriminant d. Then if:

$d > 0$, f is indefinite
$d = 0$, f is semidefinite but not definite
$d < 0$, a and c have the same sign, and f is positive (negative) definite if $a > 0$ ($a < 0$)

Proof. We will make use of the following relation:

$$4af(x,y) = (2ax + by)^2 - dy^2 \ (*)$$

First, suppose that $d > 0$. Notice that $f(1,0) = a$ and $f(b,-2a) = -ad$, which have opposite sign unless $a = 0$. Similarly, notice that $f(0,1) = c$ and $f(-2c,b) = -cd$, which have opposite sign unless $c = 0$. So we consider what happens when $a = c = 0$: we have $f(1,1) = b$ and $f(1,-1) = -b$, which certainly have the same sign. Thus f takes both positive and negative values, so it is indefinite.

Suppose $d = 0$. If $a \neq 0$, then $(*)$ gives that the values of f have the same sign as a, so f is semidefinite. Additionally, $f(b,-2a) = -ad = 0$, so that f is not definite. Now suppose $a = 0 \Rightarrow d = b^2 \Rightarrow b = 0$ since $d = 0$. So $f(x,y) = cy^2 \Rightarrow f$ has the same sign as c, so f is semidefinite. However, $f(1,0) = 0$, so f is not definite.

Suppose $d < 0$. By $(*)$ we have f is positive for all $(x,y) \in \mathbb{Z}^2$ except $(0,0)$, so f is definite. Using the discriminant formula we have $4ac = b^2 - d \geq -d > 0 \Rightarrow ac > 0$, so a and c have the same sign (positive means f is positive definite, negative means f is negative definite. $\square$

We will concern ourselves only with definite forms (most notably positive definite forms, for if f is negative definite we need only examine $-f$, which is positive definite and behaves like f). From this point on, all forms will be assumed to have negative discriminant and $a > 0$, unless stated otherwise. Next, we proceed to the notion of equivalence classes of quadratic forms.

2. Equivalent Forms

Consider the forms

$$f(x,y) = x^2 + y^2 \qquad g(x,y) = x^2 + 2xy + 2y^2.$$

A simple calculation shows that $f(x,y) = g(x-y,y)$ and $f(x+y,y) = g(x,y)$, hence f and g represent exactly the same integers. An example of the utility of this fact lies in the following example: perhaps we would like to know if 169 is representable by g. This is certainly not readily seen. However, 169 has a well-known decomposition into a sum of two squares: $169 = 5^2 + 12^2 = f(5,12)$. By the relation $f(x,y) = g(x-y,y)$ it is easily see that $g(5-12,12) = 169$. This next section is devoted to establishing this "equivalence" of forms.

Definition 2.1. Two binary quadratic forms $f(x,y)$ and $g(x,y)$ are called *equivalent* if there is some $A \in \mathrm{SL}_2(\mathbb{Z})$ such that $f\big((x,y)\cdot A\big) = g(x,y)$ (where the right action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{Z}^2$ is given in the usual way by matrix multiplication). In other words, if $A = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$, then $f\Big((x,y)\cdot\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\Big) = f(\alpha x + \gamma y, \beta x + \delta y) = g(x,y)$. If f and g are equivalent, we write $f \sim g$.

Example 2.2. (a) Let f and g be as in the example at the start of the section. The transformation that takes f to g is $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$: $f\big((x,y)\cdot\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\big) = f(x+y,y) = g(x,y)$.

Theorem 2.3. Let f and g be binary quadratic forms. Then

1. $f \sim f$
2. If $f \sim g$, then $g \sim f$
3. If $f \sim g$ and $g \sim h$, then $f \sim h$

Proof. (1.) The identity matrix $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ clearly takes f to f, so $f \sim f$.

(2.) Suppose $f \sim g$. Then there is some $A = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ takes f into g, i.e. $f\big((x,y)\cdot A\big) = f(\alpha x + \gamma y, \beta x + \delta y) = g(x,y)$. Then $A^{-1} = \begin{pmatrix}\delta & -\beta\\ -\gamma & \alpha\end{pmatrix}$ (which exists since $\det(A) \neq 0$), and takes g into f, i.e. $g\big((x,y)\cdot A^{-1}\big) = g(\delta x - \gamma y, -\beta x + \alpha y) = f(x,y)$. So $g \sim f$.

(3.) Suppose $f \sim g$ and $g \sim h$. Let f go to g under $A = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$, and let g go to f under $B = \begin{pmatrix}\alpha' & \beta'\\ \gamma' & \delta'\end{pmatrix}$. Then f goes to h under $BA = \begin{pmatrix}\alpha\alpha' + \gamma\beta' & \beta\alpha' + \delta\beta'\\ \alpha\gamma' + \gamma\delta' & \beta\gamma' + \delta\delta'\end{pmatrix}$:

$$\begin{aligned} f\big((x,y)\cdot BA\big) &= f(\alpha\alpha' x + \gamma\beta' x + \alpha\gamma' y + \gamma\delta' y, \beta\alpha' x + \delta\beta' x + \beta\gamma' y + \delta\delta' y)\\ &= f\big((\alpha' x + \gamma' y, \beta' x + \delta' y)\cdot A\big) = g(\alpha' x + \gamma' y, \beta' x + \delta' y)\\ &= g\big((x,y)\cdot B\big) = h(x,y). \end{aligned}$$

So $f \sim h$.

□

Thus $\sim$ is an equivalence relation, and as a result it partitions the set of binary quadratic forms into equivalence classes of forms. With this next theorem we can form a better idea of how the equivalence classes are determined:

Theorem 2.4. Let f and g be binary quadratic forms, and suppose $f \sim g$. Then f and g represent exactly the same integers, and disc(f) =disc(g).

Proof. Suppose $f \sim g$ and $f(x, y) = n$. Let A take f to g. Then $g\big((x, y) \cdot A^{-1}\big) = f(x, y) = n$. Thus g represents the same integers as f. Transitivity of equivalence similarly gives that f also represents the same integers as g. Verifying that f and g have equal discriminants is easily verified by a direct calculation, and a little brute force (see, for example, [Landau] pg. 173). □

Since equivalent forms have the same discriminant, we know that $\sim$ not only partitions the entire set of binary quadratic forms, but even more specifically it partitions the set of all forms with a given discriminant. Our next task is to find an appropriate representative for each equivalence class, which will in turn help us to prove the finiteness of the class number (in the positive definite case).

3. Finiteness of the Class Number

Definition 3.1. Let $d \in \mathbb{Z}$ be nonsquare. Then the number of equivalence classes of binary quadratic forms with discriminant d is call the *class number* of d, written $h(d)$.

Proposition 3.2. Let $d \in \mathbb{Z}$ be nonsquare. Then each equivalence class contains a form such that

$$|b| \leq |a| \leq |c|$$

.

Proof. Let $f(x, y) = a_0x^2 + b_0xy + c_0y^2$ be a fixed form in an arbitrary equivalence class, and let a be the integer represented by f with smallest absolute value (aside from 0). Then $a = f(r, t)$ for suitable $r, t \in \mathbb{Z}$. Then $\gcd(r, t) = 1$, otherwise $\frac{k}{\gcd(r,t)}$ would be the integer of smallest absolute value represented by f. Thus there exist $s, u \in \mathbb{Z}$ such that $ru - st = 1$. So $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Notice that $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ takes f into $g(x, y) = ax^2 + b'xy + c'y^2$, for some $b', c' \in \mathbb{Z}$. Now the transformation $\begin{pmatrix} 1 & \epsilon \\ 0 & 1 \end{pmatrix}$ takes g to $h(x, y) = ax^2 + (2k\epsilon + b')xy + cy^2$, for some $c \in \mathbb{Z}$ (ϵ is currently an arbitrary integer). Put $b = 2k\epsilon + b'$. Then for a suitable ϵ we can get that $|b| \leq |a|$. Since c is nonzero and is representable by h, f also represents c (equivalent forms represent the same numbers). Since we chose a so that $|a|$ is minimal, $|a| \leq |c|$. Thus h is of the desire form, and is equivalent to f. □

The idea of forms such that $|b| \leq |a| \leq |c|$ is more general and very similar to the notion of reduced forms, which we will define soon. This condition, however, is all that is needed to prove the finiteness of the class number (and makes the proof easier), so it's all we need for now.

Theorem 3.3. Let $d \in \mathbb{Z}$ be nonsquare. Then $h(d)$ is finite.

Proof. We will show the class number is finite by bounding the coefficients of forms such that $|b| \leq |a| \leq |c|$ for a given discriminant. This will show that there are a finite number of these forms for a given discriminant, and thus finitely many equivalence classes.

Suppose $d > 0$: Suppose $f(x, y) = ax^2 + bxy + cy^2$ be a form of discriminant d such that $|b| \leq |a| \leq |c|$. Then $|a||c| \geq b^2 = d + 4ac > 4ac \Rightarrow |ac| \geq 4ac \Rightarrow ac < 0$. So $4a^2 \leq 4|ac| = -4ac = d - b^2 \leq d \Rightarrow |b| \leq |a| \leq \frac{\sqrt{d}}{2}$. Thus there are only finitely many possibilities for a, $b \Rightarrow c$ has a finite number of possibilities (since $b^2 - 4ac$).

Suppose $d > 0$. Then $b^2 - 4ac < 0 \Rightarrow a$ and c have the same sign. So it suffices to treat the two cases $a, c > 0$ (i.e. positive definite) and $a, c < 0$ (i.e. negative definite). Since $a, c > 0$ then be have $|b| \leq a \leq c \Rightarrow 4a^2 \leq 4ac = b^2 - d \leq a^2 + |d| \Rightarrow 3a^2 \leq |d| \Rightarrow |b| \leq a \leq \sqrt{\frac{|d|}{3}}$. Thus, there are a finite number of choices for a, b, so again there are finitely many choices for c. □

For our purposes, it is enough to stop here and move on to the next section. However, the notion of reduced forms is important in the theory of binary quadratic forms, so we examine some of the basic theory involved. Since this is not directly related to our primary topic of study, several of the proofs have been omitted (references have been listed).

Definition 3.4. Let f be a binary quadratic form. f is called *reduced* if

$$-|a| < b \leq |a| < |c|$$

or

$$0 \leq b \leq |a| = |c|.$$

Example 3.5. Notice that the form $x^2 + ny^2$ is always reduced form for any $n \in \mathbb{Z}$. In practice, this helps to find a reduced form of a given discriminant d, where $d \equiv 0 \bmod 4$ (we will see why this condition is necessary, as d needs to be divisible by 4). For example, for $d = -12$, all we need to do is find the corresponding form $x^2 + ny^2$, i.e. we have $d = b^2 - 4ac \Rightarrow -12 = -4n \Rightarrow n = 3$. So $x^2 + 3y^2$ is a reduced form of discriminant -12 since $h(-12) = 1$.

Theorem 3.6. Every equivalence class contains a reduced form.

Proof. We already know that each class contains a form for which

$$-a \leq b \leq a \leq c.$$

Some of these such forms already satisfy the conditions to be a reduced form. However, there are some forms for which it is not immediately clear. These forms are precisely those for which

(1) $b = -a$ and $a < c$, and
(2) $-a \leq b < 0$

We will show that forms of types (1) and (2) are equivalent to reduced forms:

(1) Suppose $b = -a$ and $a < c$, i.e. if f is a form satisfying these conditions, then $f(x, y) = ax^2 - axy + cy^2$ where $a < c$. Then f goes to $g(x, y) = ax^2 + axy + cy^2$, $a < c$, under $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and g is a reduced form.

(2) Suppose $-a \leq b < 0$ and $a = c$, i.e. if f is a form satisfying these conditions, then $f(x, y) = ax^2 - bxy + ay^2$ where $-a \leq b < 0$. f goes to $g(x, y) = ax^2 + bxy + ay^2$ under $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and g is a reduced form.

Thus, every equivalence class contains a reduced form. □

Theorem 3.7. Let $d < 0$. Then each equivalence class contains a unique reduced form.

Proof. See [Niven] pg. 172, or [Landau] pg. 177. □

Example 3.8. This fact can often be helpful in determining the class number for a given discriminant. For example, two reduced forms of discriminant -40 are $x^2 + 10y^2$ and $2x^2 + 5y^2$. Since $d < 0$, we know that reduced means unique, and thus each must come from a different equivalence class, so $h(d) \geq 2$. Since there are a finite number of possibilities for reduced definite forms, we can exhaust all possible cases to show that, in fact, $h(-40) = 2$. The following theorem, which follows immediately from the previous two, generalizes this method:

Theorem 3.9. The number of classes of positive definite forms is the number of solutions of $d = b^2 - 4ac$, where a, b, c satisfy the reduced conditions $-a < b \leq a < c$, or $0 \leq b \leq a = c$.

Example 3.10. Here is a class number table for some small, negative values of $d \equiv 0$ mod4, along with some of the corresponding reduced forms:

d	$h(d)$	Reduced forms of discriminant d
-4	1	$x^2 + y^2$
-8	1	$x^2 + 2y^2$
-12	1	$x^2 + 3y^3$
-20	2	$x^2 + 5y^2, 2x^2 + 2xy + 3y^2$
-28	1	$x^2 + 7y^2$
-40	2	$x^2 + 10y^2,\ 2x^2 + 5y^2$
-56	4	$x^2 + 14y^2, 2x^2 + 7y^2, 3x^2 \pm 2xy + 5y^2$
-108	3	$x^2 + 27y^2, 4x^2 \pm 2xy + 7y^2$
-256	4	$x^2 + 64y^2, 4x^2 + 4xy + 17y^2, 5x^2 \pm 2xy + 13y^2$

4. Automorphs

Consider the form $f(x, y) = x^2 + y^2$ as before. One of the solutions of $f(x, y) = 169$ is $(x, y) = (5, 12)$. Notice, however, that $(-5, 12)$, $(-5, -12)$, and $(5, -12)$ are solutions as well. In other words, $(5, 12)$ yields 4 different, though very similar, solutions. Since our goal is to find the the *number* of solutions to equations like $f(x, y) = 169$, we must have develop a way to account for these "repeat" solutions. Conveniently, the method in which we developed the theory of equivalences of forms makes it easy to account for these "repeats" by a special kind of transformation, called an automorph.

Definition 4.1. An *automorph* is a transformation which takes f to itself. In other words, $A \in \mathrm{SL}_2(\mathbb{Z})$ is an automorph if $f((x, y) \cdot A) = f(x, y)$.

Theorem 4.2. Let $f(x, y) = ax^2 + bxy + cy^2$ be primitive. Then $A \in \mathrm{SL}_2(\mathbb{Z})$ is an automorph of f if and only if

$$A = \begin{pmatrix} \dfrac{t - bu}{2} & -cu \\ au & \dfrac{t + bu}{2} \end{pmatrix}$$

for some (t, u) that satisfies the Pell equation

$$t^2 - du^2 = 4.$$

Proof. It is easy to check that that $\dfrac{t - bu}{2}$, $\dfrac{t + bu}{2} \in \mathbb{Z}$, and that $\det(A)$=1.

($\Rightarrow$) Suppose that $A = \begin{pmatrix} r & s \\ m & n \end{pmatrix}$ is an automorph of f. Then by direction computation, we have

$$\begin{aligned} a =& ar^2 + brm + cm^2 \\ b =& 2rs + b(1 + 2sm) + 2cmn, \end{aligned}$$

the latter of which gives us $0 = ars + bsm + cmn$. Combining the two to eliminate b gives:

$$as = csm^2 - crmn = cm(sm - rn) = -cm \qquad (1)$$

Similarly, combining the two to eliminate c gives:

$$an = ar^2n + brmn - arsm - bsm^2 = ar + bm \Rightarrow a(n - r) = bm \qquad (2)$$

Thus $a|cm$ and $a|bm$. Since f is primitive, $\gcd(a, b, c) = 1$, which implies that $a|m$, i.e. $m = au$ for some $u \in \mathbb{Z}$. Going back to (1) and (2) give that $s = -cu$ and $n - r = bu$.

Thus we have:

$$\begin{aligned}(n+r)^2 &= (n-r)^2 + 4nr \\ &= b^2u^2 + 4(1+sm) \\ &= b^2u^2 + 4(1-acu^2) \\ &= du^2 + 4\end{aligned}$$

Put $t = n + r$, with $r = \frac{t-bu}{2}$ and $n = \frac{t+bu}{2}$. Thus we have $t^2 = du^2$ and we are done.

($\Leftarrow$) Suppose that A is a matrix of the given form. We will show that the coefficients a and b of f are left unchanged by this transformation (and thus it will follow for c). So suppose A takes f to g, where g is given by $g(x, y) = a_1x^2 + b_1xy + c1y^2$. Then, by direct computation, we have that

$$\begin{aligned}a_1 &= a\Big(\frac{t-bu}{2}\Big)^2 + b\Big(\frac{t-bu}{2}\Big)(au) + ca^2u^2 \\ &= \frac{a}{4}(t^2 - (b^2 - 4ac)u^2) \\ &= \frac{a}{4}(t^2 - du^2) \\ &= a\end{aligned}$$

Similarly for b:

$$\begin{aligned}b_1 &= -2a\Big(\frac{t-bu}{2}\Big) + b(1 - 2acu^2) + 2cau\Big(\frac{t+bu}{2}\Big) \\ &= -actu + abcu^2 + b - 2abcu^2 + actu + abcu^2 \\ &= b.\end{aligned}$$

Thus $f = g$, so A is an automorph of f. □

One of the reasons that we are only concerning ourselves with forms of negative discriminant here is that otherwise the number of automorphs is not guaranteed to be finite (and generally is not). For example: the form $f(x, y) = x^2 - 5y^2$ has discriminant 20. For this case, the Pell equation above becomes $t^2 - 20u^2 = 4$, which has infinitely many solutions (and thus f has infinitely many automorphs). When $d < 0$, however, the number of automorphs is finite, and we know exactly how many exist:

Theorem 4.3. Let $d < 0$. Then the number of automorphs of a form of discriminant d, denoted $w(d)$, is given by:

$$w(d) = \begin{cases} 2 & \text{for } d < -4 \\ 4 & \text{for } d = -4 \\ 6 & \text{for } d = -3 \end{cases}$$

Proof. For each case, $w(d)$ is simply the number of integer solutions to $t^2 - du^2 = 4$. □

Theorem 4.4. Let $k \in \mathbb{Z}_{>0}$, f be a primitive positive definite form of discriminant $d < 0$, and fix a proper representation (x, y) of k. Then the integers r, s, and l may be chosen in a unique way such that $\begin{pmatrix} x & r \\ y & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ takes f to $g(x, y) = kx^2 + lxy + my^2$, where $m \in \mathbb{Z}$ is chosen uniquely such that $d = l^2 - 4km$, and where $l \equiv d \bmod 4k$ for $0 \leq l < 2k$.

Remark 4.5. Essentially, the theorem states that for each proper representation (x, y) of k there is a unique l such that $0 \leq l < 2k$. The significance of this fact will be revealed in the next theorem.

Proof. If we are given any solution $(r, s) = (r_0, s_0)$ of $xs - ry = 1$, then all solutions can be generated by the formulas

$$r = r_0 + \epsilon x \qquad s = s_0 + \epsilon y,$$

where $\epsilon \in \mathbb{Z}$ is arbitrary (the proof of this fact is not difficult, but fairly irrelevant in regards to our goals; see [Landau] pg. 46). Then for an arbitrary solution (r, s), the above matrix takes f into g, and direct calculation gives

$$\begin{aligned} l &= 2axr + b(xs + yr) + 2cys \\ &= 2axr_0 + b(xs_0 + yr_0) + 2cys_0 + 2\epsilon(ax^2 + bxy + cy^2) \\ &= 2axr_0 + b(xs_0 + yr_0) + 2cys_0 + 2\epsilon k \quad (\text{Put } l_0 = 2axr_0 + b(xs_0 + yr_0) + 2cys_0) \\ &= l_0 + 2\epsilon k \end{aligned}$$

Since we want $0 \leq l_0 + 2\epsilon k < 2k$, i.e. $0 \leq \frac{l_0}{2k} + \epsilon < 1$, there is exactly one $\epsilon \in \mathbb{Z}$ for which this is possible. Since there is only one such ϵ, then there is in turn one such r, s, and l (respectively). Thus, for *exactly* one ϵ, there is *exactly* one solution (r, s) and *exactly* one l such that $0 \leq l < 2k$. Furthermore, since $d = l^2 - 4km$ we have that $l^2 \equiv d \bmod 4k$. □

The next theorem is where automorphs come into play: we start with a proper representation, and then count the number of "repeat" representations caused by automorphs of f. Since we have found a one-to-one correspondence between proper representations of k, and l such that $l^2 \equiv d \bmod 4k$ with $0 \leq l < 2k$, all we have to do is work in the automorphs of f.

Theorem 4.6. Let $f(x, y) = ax^2 + bxy + cy^2$ be a primitive positive definite form of discriminant $d < 0$, and $k \in \mathbb{Z}_{>0}$ be properly representable by f. Then for every such l as in the previous theorem, there are exactly $w(d)$ proper representations of k.

5. The Mass Formula

We can now count the number of proper representations: count the number of such l that satisfy the needed conditions, and multiply this number by the number of automorphs. In fact, we can adjust this to account for both proper and improper representations by a form. First we need a lemma:

Lemma 5.1. Let $k > 0$ and $(d, k) = 1$. Then the number of l such that $x^2 \equiv d \bmod 4k$ is

$$2\sum_{t|k}\left(\frac{d}{t}\right)$$

where t runs through the squarefree positive divisors of k.

Proof. See [Landau] pg. 71. □

We will now state and prove our main result:

Theorem 5.2. (The Mass Formula) Let d be a fundamental discriminant (i.e. all forms with discriminant d are primitive), $k > 0$, and $\gcd(k, d) = 1$. Then the number $R_d(k)$ of representations of k by positive definite forms of discriminant d is finite and given by

$$R_d(k) = w(d)\sum_{n|k}\left(\frac{d}{n}\right)$$

Proof. The number of l such that $l^2 \equiv d \bmod 4k$ is given by

$$2\sum_{t|k}\left(\frac{d}{t}\right)$$

where t runs through the square-free divisors of k. However, since $(l_0 + 2k)^2 \equiv l_0^2 \bmod 4k$, taking only those l for which $0 \leq l < 2k$ cuts the number, i.e. the number of such l becomes

$$\sum_{t|k}\left(\frac{d}{t}\right).$$

By the previous theorem, for every such l there are exactly $w(d)$ representations of k. So the number of proper representations of k is given by

$$w(d)\sum_{t|k}\left(\frac{d}{t}\right).$$

Now we need to include improper representations. Recall by the remark following definition 1.2 that if (x, y) is an improper representation of k such that $\gcd(x, y) = g$, then $\frac{k}{g^2}$ has a corresponding proper representation $\left(\frac{x}{g}, \frac{y}{g}\right)$. Thus, there are exactly as many proper and improper representations (x, y) of k as there are proper ones $\left(\frac{x}{g}, \frac{y}{g}\right)$ of $\frac{k}{g}$. Thus

the number of all representations of k is

$$\begin{aligned} R_d(k) &= w(d) \sum_{g^2|k, g>0} \sum_{t|\frac{k}{g^2}} \left(\frac{d}{t}\right) \\ &= w(d) \sum_{g^2|k, g>0} \sum_{tg^2|k} \left(\frac{d}{tg^2}\right) \\ &= w(d) \sum_{n|k} \left(\frac{d}{n}\right), \end{aligned}$$

where in the last equality we put $n = tg^2$, since any positive integer n can be written in this form. □

6. References

[Cox]Cox, David A. Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication. A Wiley-Interscience Publication. John Wiley and Sons, Inc., New York, 1989.

[Landau]Landau, Edmund. Elementary number theory. Translated by J. E. Goodman. Chelsea Publishing Co., New York, N.Y., 1958.

[Niven]Niven, Ivan, Herbert Zuckerman, and Hugh L. Montgomery. An introduction to the Theory of Numbers. John Wiley and Sons, Inc., New York, 1991.