

ADVANCED NUMBER THEORY 2008

ZEÉV RUDNICK

1. THE MASS FORMULA FOR BINARY QUADRATIC FORMS

This is a rough draft - may have various misprints!

1.1. The representation problem. Given an anisotropic¹ binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ and an integer k , the fundamental problem is the existence of an integer solution to the Diophantine equation

$$f(x, y) = k$$

One may quickly reduce to the case of *primitive forms*, that is when $\gcd(a, b, c) = 1$, and for *proper* representation, that is one with x, y coprime.

It turns out that there is usually not an exact answer for an individual form f . However if we ask for representation by *some* form with discriminant D , then the answer is simple: An integer k , coprime to D , is properly represented by some form with discriminant D if and only if D is a quadratic residue mod $4k$. Indeed, if we can solve $l^2 = D \pmod{4k}$ then for some integer m , we can write $D = l^2 - 4km$ and then the form $f(x, y) = kx^2 + lxy + my^2$ properly represents k (since $k = f(1, 0)$), has discriminant D and is primitive. Conversely, if a form f of discriminant D properly represents k then f is equivalent to a form $kx^2 + lxy + my^2$ and then $D = l^2 - 4km \equiv l^2 \pmod{4k}$.

Note that in the case that the class number $h(D)$ is one, this reduces to an answer for the individual form at hand!

We may ask for finer information: What is the “number” of representations. A fundamental difference between the cases of negative and positive discriminant is that in the latter case, if there is one solution then there will be infinitely many, due to the existence of infinitely many automorphs of the form. The well-posed question then becomes that of the number $r_f(k)$ of *equivalence classes* of (proper) representations, a notion which makes sense for any discriminant.

¹This condition is equivalent to f being irreducible or to the discriminant not being a perfect square

If we consider the sum

$$r_D(k) = \sum_{j=1}^{h(d)} r_f(k)$$

over the finitely many classes of forms of given discriminants then there is an exact result available; this is the “mass formula”:

Theorem 1.1. *Let $k \neq 0$ be coprime to D . Then*

$$r_D(k) = \sum_{\substack{m|k \\ m \text{ square-free}}} \chi_D(m)$$

where χ_D is the quadratic character given by the Kronecker symbol $\chi_D(m) = \left(\frac{D}{m}\right)$ and the sum is over all square-free divisors of D .

1.2. **Examples.** i) Let $f(x, y) = x^2 + y^2$, which has discriminant -4 and $w_{-4} = 4$ automorphs $\pm I, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. In fact it also has the improper automorph $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} : (x, y) \mapsto (y, x)$. All forms with discriminant -4 are equivalent to $x^2 + y^2$ and hence the number $r_f(k)$ of equivalence classes of representations of an odd integer as a sum of two square ($k = x^2 + y^2$) is given by

$$\sum_{\substack{m|k \\ m \text{ square-free}}} \chi_{-4}(m)$$

In particular, the number of proper equivalence classes of representing an odd prime p as a sum of two squares is

$$\chi_{-4}(1) + \chi_{-4}(p) = 1 + (-1)^{\frac{p-1}{2}} = \begin{cases} 2 & p \equiv 1 \pmod{4} \\ 0 & p \equiv 3 \pmod{4} \end{cases}$$

Taking into account the improper automorph of f , we find that for $p \equiv 1 \pmod{4}$ there is essentially a *unique* way to write $p = a^2 + b^2$, and in total 8 representations $(\pm a, \pm b)$ and $(\pm b, \pm a)$.

ii) Let $f(x, y) = x^2 + xy + y^2$, which is the unique form of discriminant -3 and has $w_{-3} = 6$ proper automorphs $\pm I, \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$, as well as the improper automorph $(x, y) \mapsto (y, x)$. Then the number of proper equivalence classes of representing a prime $p \neq 3$ as $p = x^2 + xy + y^2$ is

$$\chi_{-3}(1) + \chi_{-3}(p) = 1 + \left(\frac{-3}{p}\right)$$

By quadratic reciprocity, for $p \neq 2, 3$ this equals

$$1 + \left(\frac{p}{3}\right) = \begin{cases} 2 & p \equiv 1 \pmod{3} \\ 0 & p \equiv 2 \pmod{3} \end{cases}$$

For $p = 2$ this equals 0 since $\left(\frac{-3}{2}\right) = -1$. Taking into account the improper automorph $(x, y) \mapsto (y, x)$, we see that for $p = 1 \pmod 3$ there is essentially a unique way to write $p = a^2 + ab + b^2$, with a total of 12 representations $\pm(a, b)$, $\pm(b, a)$, $\pm(-b, a + b)$, $\pm(a + b, -b)$, $\pm(a + b, -a)$, $\pm(-a, a + b)$.

1.3. Automorphs. Let $f = [a, b, c]$ be an integral binary quadratic form, which is anisotropic (equivalently, not decomposable, equivalently whose discriminant D is not a perfect square). The group of integral automorphs is

$$\text{Aut}(f) = \{G \in \text{SL}_2(\mathbb{Z}) : f|_G = f\}$$

Note that $\text{Aut}(f)$ acts without fixed points on $\mathbb{R}^2 \setminus \{0\}$, that is if $v \neq 0$ and $I \neq S \in \text{Aut}(f)$ then $Sv \neq v$. This is because for a nondegenerate ($D \neq 0$) binary quadratic form f , the automorphs are diagonalizable over the complex numbers and have eigenvalues λ, λ^{-1} and in particular if one eigenvalue is 1 (that is there is a fixed vector) the matrix is necessarily the identity matrix.

All automorphs are of the form

$$\begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix}$$

where (t, u) is a solution of the Pell equation

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

In the case that $D < 0$, that is f is definite (positive definite if $k > 0$, negative definite if $k < 0$), $\text{Aut}(f)$ is finite, and its cardinality w_D depends only on D : $w_{-3} = 6$, $w_{-4} = 4$, $w_D = 2$ for $D < -4$. Thus each $\text{Aut}(f)$ orbit in $\mathbb{R}^2 \setminus \{0\}$ consists of exactly w_D points.

If $D > 0$ then $\text{Aut}(f)$ is *infinite*, and each $\text{Aut}(f)$ orbit in $\mathbb{R}^2 \setminus \{0\}$ is infinite.

1.4. Classes of proper representations by a form f . Let $f = [a, b, c]$ be a binary quadratic form of non-square discriminant D . We say that f *properly represents* k if there is a solution of $f(x, y) = k$ with x, y coprime. If k is square-free then every representation is proper.

Let $k \neq 0$ be an integer properly represented by f . Denote by $\mathcal{P}_{k,f}$ the set of proper representations of k by f , that is the set of primitive vectors (x, y) with $f(x, y) = k$. These are the set of primitive vectors lying on a conic - either an ellipse if $D < 0$ or a hyperbola if $D > 0$. In particular $\mathcal{P}_{k,f}$ is finite if $D < 0$. The group of automorphs $\text{Aut}(f)$ acts on the set $\mathcal{P}_{k,f}$. Since $\text{Aut}(f)$ is infinite if $D > 0$, this implies that

$\mathcal{P}_{k,f}$, if non-empty, is infinite. In any case, if $k \neq 0$ then we will show that there are only finitely many orbits. Let

$$r_f(k) = \# \text{Aut}(f) \backslash \mathcal{P}_{k,f}$$

denote the number of orbits, that is the number of equivalence classes of proper representations of k by f .

The finiteness of the number of classes of proper representations of k by f for all $k \neq 0$ easily implies that the number $r_f(k)$ of classes of *all* representations of k by f is also finite.

In the case that $D < 0$, that is f is definite (positive definite if $k > 0$, negative definite if $k < 0$), $\# \text{Aut}(f)$ is finite, and its cardinality w_D depends only on D . Thus each $\text{Aut}(f)$ orbit in $\mathbb{R}^2 \setminus \{0\}$ consists of exactly w_D points. In particular the number $n_f(k)$ of proper representations of k by f is

$$n_f(k) = w_D r_f(k)$$

and the number $N_f(k)$ of all representations of k by f is

$$N_f(k) = w_D r_f(k)$$

1.5. All classes of representations by a form. Let $R_f(k)$ be the number of equivalence classes of *all* representations of k by f . It is a simple matter to compute this in terms of primitive representations:

Proposition 1.2.

$$R_f(k) = \sum_{\delta^2 | k} r_f\left(\frac{k}{\delta^2}\right)$$

Indeed, if $f(x, y) = k$ then we can uniquely write $(x, y) = \delta(x_0, y_0)$ where $\delta = \gcd(x, y) \geq 1$ and (x_0, y_0) is a primitive vector, and then

$$f(x_0, y_0) = \frac{k}{\delta^2}$$

gives a primitive representation of k/δ^2 , and conversely any primitive representation of k/δ^2 by f gives a representation of k in this manner.

1.6. Classes of proper representations by all forms with discriminant D . For an integer $k \neq 0$ let

$$r_D(k) = \sum_{\{f\}} r_f(k)$$

be the number of equivalence classes of *proper* representations of k by equivalence classes of primitive forms f of discriminant D , where for $D < 0$ and $k > 0$ we restrict to positive-definite forms, and for $D < 0$ and $k < 0$ we restrict to negative-definite forms.

Likewise let

$$R_D(k) = \sum_{\{f\}} r_f(k)$$

be the number of equivalence classes of all representations of k by equivalence classes of primitive forms f of discriminant D (with the same restrictions as above for negative discriminants).

Theorem 1.3. *If $\gcd(k, D) = 1$ then the number of equivalence classes of proper representations is*

$$(1.1) \quad r_D(k) = \sum_{\substack{m|k \\ m \text{ squarefree}}} \left(\frac{D}{m} \right)$$

1.7. The correspondence. Let $k \neq 0$ and

$$\mathcal{L}_{D,k} := \{0 \leq l < 2|k| : l^2 \equiv D \pmod{4k}\}$$

Given an equivalence class of proper representations of k by f , we construct a unique integer $l \in \mathcal{L}_{D,k}$, and corresponding to it a form $[k, l, m]$ (where m solves $l^2 - 4km = D$) equivalent to f .

Claim: *The map $v \mapsto l_v$ is an injection*

$$\text{Aut}(f) \backslash \mathcal{P}_{k,f} \rightarrow \mathcal{L}_{D,k}$$

In particular there are only finitely many $\text{Aut}(f)$ -orbits in $\mathcal{P}_{k,f}$.

Given a primitive (column) vector $v = \begin{pmatrix} r \\ t \end{pmatrix} \in \mathcal{P}_{k,f}$, there is a primitive vector $v' = \begin{pmatrix} s \\ u \end{pmatrix}$ so that

$$G = [v|v'] = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$$

that is (s, u) solves the linear Diophantine equation $ru - ts = 1$. The vector v' is unique up to addition of an integer multiple of v : $v' \mapsto v' + hv$. This corresponds to changing $G \mapsto G \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$.

Transforming the form f by G gives a form

$$f|_G = [k, l, *], \quad k = f(r, t)$$

and changing G to $G \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ will change $l \mapsto l + 2kh$:

$$f|_{G \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}} = (f|_G) \left| \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right. = [k, l + 2kh, **]$$

There is a unique choice of $h \in \mathbb{Z}$ so that $0 \leq l_v := l + 2kh < 2|k|$; thus we have found some $G = [v|v'] \in \mathrm{SL}_2(\mathbb{Z})$ and $0 \leq l_v < 2|k|$ so that

$$f|_G = [k, l_v, m]$$

where m is determined from the discriminant condition

$$D = \mathrm{disc}(f) = \mathrm{disc}(f|_G) = l_v^2 - 4mk$$

In particular, $l_v^2 \equiv D \pmod{4k}$.

Changing v to another vector on the $\mathrm{Aut}(f)$ -orbit $v \mapsto Sv$, $S \in \mathrm{Aut}(f)$, will result in changing $G \mapsto SG = [Sv, Sv']$ and keep $[k, l_v, m]$ unchanged since $f|_{SG} = (f_S)|_G = f|_G = [k, l_v, m]$ using $f|_S = f$.

1.8. Summing over all forms.

Theorem 1.4. *Let $k \neq 0$ be coprime to D . Then*

$$r_D(k) = \#\mathcal{L}_{D,k}$$

Proof. Given $l \in \mathcal{L}_{D,k}$, we get the binary form $f_l := [k, l, m]$, where m is defined uniquely by $l^2 - 4km = D$. The form f_l is *primitive* since we assume $\mathrm{gcd}(k, D) = 1$ (if $\delta \mid k, l, m$ then $\delta^2 \mid D$ so $\delta \mid \mathrm{gcd}(k, D) = 1$). Moreover $f_l(1, 0) = k$ so f_l properly represents k .

By the construction above, any form of discriminant D which properly represents k is equivalent to one (possibly several) of these. Any of these forms $[k, l, m]$ which are equivalent to f gives a proper representation of k by f , since an equivalence $f|_G = [k, l, m]$, $G = [v|v']$ in particular gives a proper representation $f(v) = k$. Thus we get a *bijection* between the set \mathcal{L}_D and the classes of proper representations of k by primitive forms of discriminant D . \square

1.9. Computing $\mathcal{L}_{D,k}$.

Proposition 1.5. *If $\mathrm{gcd}(D, k) = 1$ then*

$$\#\mathcal{L}_{D,k} = \sum_{\substack{m|k \\ m \text{ squarefree}}} \left(\frac{D}{m} \right)$$

the sum over all square-free divisors of D .

We set

$$S(D, M) := \#\{x \pmod{M} : x^2 = D \pmod{M}\}$$

so that

$$2\#\mathcal{L}_{D,k} = S(D, 4k)$$

Thus it suffices to show

Lemma 1.6. *If $D \equiv 0, 1 \pmod{4}$ and $\gcd(k, D) = 1$ then*

$$S(D, 4k) = 2 \sum_{\substack{m|k \\ m \text{ squarefree}}} \left(\frac{D}{m}\right)$$

Proof. By the Chinese Remainder Theorem, $S(D, M)$ is multiplicative. Moreover,

$$\sum_{\substack{m|k \\ m \text{ squarefree}}} \left(\frac{D}{m}\right) = \prod_{\substack{p|k \\ p \text{ prime}}} \left(1 + \left(\frac{D}{p}\right)\right)$$

The matter reduces than to Hensel's lemma. Precisely, it suffices to show that if $k = 2^a \prod_{p \neq 2} p^{\alpha_p}$ then

i) If $p \neq 2$ is an odd prime, $\alpha > 0$ and $p \nmid D$ then

$$S(D, p^\alpha) = 1 + \left(\frac{D}{p}\right)$$

ii) For $p = 2$ and $a \geq 0$,

$$S(D, 2^{a+2}) = \begin{cases} 2, & a = 0 \text{ (here the parity of } D \text{ is irrelevant!)} \\ 0, & a > 0, \quad D \equiv 5 \pmod{8} \\ 4, & a > 0, \quad D \equiv 1 \pmod{8} \end{cases}$$

(The only interesting case for $p = 2$ is when $a > 0$ and $D \equiv 1 \pmod{8}$). Note that by the definition of the Kronecker symbol, the RHS above is $2(1 + (\frac{D}{2}))$. \square

Combining Theorem 1.4 with Proposition 1.5 proves Theorem 1.1.

1.10. Improper representations.

Theorem 1.7. *Let $k \neq 0$ be coprime to D . Then the number of classes of all representations of k by the classes of forms of discriminant D is*

$$R_D(k) = \sum_{m|k} \left(\frac{D}{m}\right)$$

Proof. To prove this, we use Proposition 1.2, that is

$$R_f(k) = \sum_{\delta^2|k} r_f\left(\frac{k}{\delta^2}\right)$$

Summing over all classes of forms of discriminant D gives

$$R_D(k) = \sum_{\delta^2|k} r_D\left(\frac{k}{\delta^2}\right)$$

Inserting the formula (1.1) for $r_D(k)$ gives

$$R_D(k) = \sum_{\delta^2 | k} \sum_{\substack{m | \frac{k}{\delta^2} \\ m \text{ square-free}}} \left(\frac{D}{m} \right)$$

Now since k is coprime to D , so is δ and hence $\left(\frac{D}{\delta^2} \right) = 1$. Thus

$$\left(\frac{D}{m} \right) = \left(\frac{D}{m} \right) \left(\frac{D}{\delta^2} \right) = \left(\frac{D}{m\delta^2} \right)$$

As we range over all δ with $\delta^2 | k$ and all square free $m | \frac{k}{\delta^2}$ we get all divisors of k exactly once. Hence

$$R_D(k) = \sum_{n|k} \left(\frac{D}{n} \right)$$

as claimed. □

In particular, for the case of negative discriminant, where each equivalence class of representations contains exactly w_D vectors, we have

Corollary 1.8. *Let $D < 0$, $k > 0$ coprime to D . Then the total number $N_D(k)$ of representations of k by primitive positive definite forms of discriminant D is*

$$N_D(k) = w_D \sum_{m|D} \left(\frac{D}{m} \right)$$