ANALYTIC NUMBER THEORY, SPRING 2022
BINARY QUADRATIC FORMS

ZEÉV RUDNICK

Contents

1. Binary quadratic forms

1.1. **Basics.** An binary quadratic form is a function of the form $f(x, y) = ax^2 + bxy + cy^2$. We also denote $f = [a, b, c]$. The associated symmetric matrix M_f so that

$$f(x, y) = (x, y) \cdot M_f \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

is

$$M_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

The *discriminant* of f is defined as

$$D = \operatorname{disc} f = b^2 - 4ac = -4 \det \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

For instance

$$\operatorname{disc}(x^2 + y^2) = -4, \qquad \operatorname{disc}(x^2 + xy + y^2) = -3.$$

Completing the square gives

$$\boxed{4af(x,y) = (2ax+by)^2 - Dy^2.}$$

Hence f is *definite* if and only if $D = \operatorname{disc} f < 0$, and in addition is positive (resp. negative) definite iff $a > 0$ (resp., $a < 0$).

Definition. *We say that* $f = [a,b,c]$ *is* integral *if* $a,b,c \in \mathbb{Z}$. *An integral binary quadratic form is* primitive *if* $\gcd(a,b,c) = 1$.

Note that for integral forms, the discriminant is an integer and satisfies $D = b^2 - 4ac \equiv b^2 \bmod 4 = 0,1 \bmod 4$.

An integer $D = 0,1 \bmod 4$ is called a discriminant. For a discriminant D we denote by $h(D)$ the number of proper equivalence classes of primitive (integer binary quadratic) forms of discriminant D (positive definite if $D < 0$). We call $h(D)$ the "class number".

Note that there is always a form of discriminant D, in the "principal class", so that $h(D) \geq 1$:

- If $D = 0 \bmod 4$, take $x^2 - \frac{D}{4}y^2$.
- If $D = 1 \bmod 4$, take $x^2 + xy + \frac{1-D}{4}y^2$.

1.2. **Equivalence and proper equivalence.** An invertible linear integer change of variables leads to the notion of equivalent forms: Given $A = \begin{pmatrix} m & r \\ n & s \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z})$, we set $f \circ A$ to be the form

$$(f \circ A)(x,y) = f(A\begin{pmatrix} x \\ y \end{pmatrix}) = f(mx+ny, rx+sy).$$

We say that f is equivalent to g if $g = f \circ A$. This is clearly an equivalence relation. Recall that for $A \in \mathrm{GL}(2,\mathbb{Z})$, we have $\det A = \pm 1$. We say that f and g are properly equivalent if $g = f \circ A$ with $\det A = +1$, i.e. if $A \in \mathrm{SL}(2,\mathbb{Z})$.

Exercise 1. *Show that the matrix of* f *transforms under* A *as*

$$M_{f\circ A} = A^T \cdot M_f \cdot A.$$

This gives

$$\operatorname{disc}(f \circ A) = (\det A)^2 \operatorname{disc} f.$$

Hence equivalent forms have the same discriminant.

Exercise 2. *Show that* f *is primitive if and only if* $f \circ A$ *is primitive.*

For further reference, we record the action of the matrix $A = \begin{pmatrix} m & r \\ n & s \end{pmatrix}$ on the coefficients of $f = [a, b, c]$: $f \circ A = [a', b', c']$ with

$$\begin{aligned} a' &= f(m,n) = am^2 + bmn + cn^2, \\ b' &= 2amn + bnr + bms + 2crs, \\ c' &= f(r,s) = ar^2 + brs + cs^2. \end{aligned} \tag{1}$$

In particular, the matrices $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (which turn out to generate $\mathrm{SL}(2, \mathbb{Z})$) transform $f = [a, b, c]$ by

$$S : [a, b, c] \mapsto [c, -b, a] \tag{2}$$

and

$$T^n : [a, b, c] \mapsto [a, b + 2a \cdot n,\ c'], \tag{3}$$

with $c' = f(n, 1) = an^2 + bn + c$.

1.3. **Representation by f.**

Definition. *We say that an integral form represents an integer m if there are integers $r, s \in \mathbb{Z}$ such that $f(r, s) = m$. It properly represents m if we can take r, s coprime.*

Exercise 3. *A prime that is represented, is necessarily properly represented.*

Note that equivalent integral forms represent the same integers: If $f(x, y) = m$ then $(f \circ A)(A^{-1} \begin{pmatrix} x \\ y \end{pmatrix}) = m$.

Lemma 1.1. *An integral form f properly represents an integer k if and only if f is properly equivalent to $[k, *, *]$.*

Proof. If $f = [k, *, *]$ then $f(1, 0) = k$ so that f properly represents k, as does any form equivalent to f.

Conversely, if $f(m, n) = k$ with m, n coprime, find r, s with $ms - nr = 1$ and then take $A = \begin{pmatrix} m & r \\ n & s \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$ and $g = f \circ A$, so $g(x, y) = f(mx + ry, nx + sy)$. Then by (1)

$$g(x, y) = f(m, n)x^2 + b'xy + c'y^2 = kx^2 + b'xy + c'y^2$$

so that f is properly equivalent to $g = [k, *, *]$. $\square$

1.4. **Questions.** Given an integral form f, we want to understand which integers are represented by f. For instance, one asks which primes are represented. As an example, Fermat showed that a prime is represented by the form $x^2 + y^2$ if and only if $p = 2$ or $p = 1 \bmod 4$.

A much easier question is if we ask for representation by some form with discriminant D, then the answer is simple:

Proposition 1.2. *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 $4k$.*

Proof. Indeed, if we can solve $\ell^2 = D \bmod 4k$ then for some integer m, we can write $D = \ell^2 - 4km$ and then the form $f(x; y) = kx^2 + \ell xy + my^2$ 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 by Lemma 1.1, f is equivalent to a form $kx^2 + \ell xy + my^2$ and then $D = \operatorname{disc}(f) = \ell^2 - 4km = \ell^2 \bmod 4k$. □

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

Another question that we want to understand is: Given two (primitive) integral binary quadratic forms, when are they equivalent? A necessary condition is that they have the same discriminant. But that need not be sufficient. For instance, take $1 < m < n$, $\gcd(m, n) = 1$ and

$$f(x, y) = x^2 + mny^2 = [1, 0, mn], \quad g(x, y) = mx^2 + ny^2 = [m, 0, n]$$

Both forms have discriminant $-4mn$. Note that g is primitive because we assume that m, n are coprime. The first one is the principal form, and represents 1: $f(1, 0) = 1$. We will show that g is not equivalent to f by showing that g does not represent 1. Indeed, $g(0, 0) = 0$,

$$g(0, y) = ny^2 \geq n \cdot 1^2 > 1$$

and if $x \neq 0$ then

$$g(x, y) = mx^2 + ny^2 \geq mx^2 \geq m \cdot 1^2 > 1.$$

As a consequence, we have shown here that for discriminants of the form $D = -4mn$ with m, n coprime, $1 < m < n$, we have $h(D) > 1$.

With a little more work, coupled with the reduction theory developed in § 2, we can recover the following Theorem of E. Landau (1902):

Theorem 1.3. *The only even negative discriminants with $h(D) = 1$ are $D = -4, -8, -12, -16, -28$.*

Exercise 4. *Show that if $D = 1 - 4q$, $q > 1$, and $h(D) = 1$ then q is prime.*

2. Reduction theory of positive definite forms

From now on we only deal with positive definite forms. The theory for indefinite forms ($D > 0$), though well established, is more complicated. We discuss "reduction theory", which allows us to

- see that $h(D)$ is finite,
- effectively enumerate all equivalence classes, and
- decide when two forms are (properly) equivalent.

2.1. Reduction theory.

Definition. *A (real) positive definite form $f = [a, b, c]$ is* reduced *if*

$$\boxed{-a < b \leq a < c \quad \text{or} \quad 0 \leq b \leq a = c.}$$

For instance, the principal form $[1, 0, -\frac{D}{4}]$ or $[1, 1, \frac{1-D}{4}]$ is reduced.

Exercise 5. *A reduced form $[a, b, c]$ with $a = 1$ must be the principal form.*

Proposition 2.1. *Every integer positive definite form is properly equivalent to a reduced form.*

Note: The claim is also valid for arbitrary real positive definite forms.

Proof. We give the proof in algorithmic form: Recall that the generators $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ transform a form $f = [a, b, c]$ by

$$S : [a, b, c] \mapsto [c, -b, a]$$
$$T^n : [a, b, c] \mapsto [a, b + 2a \cdot n, c'],$$

with $c' = f(n, 1) = an^2 + bn + c$.

We transform any form $f = [a, b, c]$ to a reduced form by the sequence of the following operations:

1. If $a > c$, then apply S to replace f by $f' = Sf = [c, -b, a] = [a', b', c']$; If $-a' = -c < b' = -b \leq a' = c$ (i.e. $-c \leq b < c$) then f' is reduced - stop. Otherwise move to step 2.
2. If $a \leq c$ then apply T^{-n} with the unique n for which $b' = b - 2a \cdot n \in (-a, a]$, to replace f by $f' = [a, b', c']$ where $b' = b - 2a \cdot n \in (-a, a]$ and $c' = f(-n, 1)$ is determined by $b'^2 - 4ac' = D$. If $c' > a$ then f' is reduced - stop. If $c' < a$ move to step 1. Otherwise, i.e. if $c' = a$, move to step 3.

(3) If $a = c$ and $-a < b < 0$, apply S to replace $f = [a, b, a]$ by $f' = [a, -b, a]$. Now f is reduced - stop.

Example 2.2. *Take* $f = [6, 7, 6]$, *which has discriminant* $D = -95$ *(note that* $h(-95) = 8$*).*

Apply step 2 (with $n = 1$) to replace f by $[6, 7-2\cdot 6\cdot 1, c'] = [6, -5, 5]$. Apply step 1 to replace by $\boxed{[5, 5, 6]}$, which is reduced.

Example 2.3. *Take* $f = [6, -27, 31]$ *which has discriminant* $D = -15$ *(note* $h(-15) = 2$*).*

Apply the steps:

$$[6, -27, 31] \quad \xrightarrow{T^2} \quad [6, -3, 1] \quad \xrightarrow{S} \quad [1, 3, 6] \quad \xrightarrow{T^{-1}} \quad [1, 1, 4]$$

which give the principal form (always reduced).

To see that the algorithm terminates, we note that at each step, we either reduce the integer a (but keep it positive) or if not, we either reduce the integer $|b|$ or at the last step change the sign of b. So the algorithm terminates. $\square$

We also have uniqueness (we shall skip the proof):

Theorem 2.4. *Each primitive integral positive definite form is equivalent to a* <u>*unique*</u> *reduced form.*

Exercise 6. *Decide which of the following forms are equivalent:*

$$[10, -16, 7], \quad [11, -14, 5], \quad [21, -30, 11].$$

Corollary 2.5. *Let* $D < 0$, $D = 0, 1 \bmod 4$. *The class number* $h(D)$ *equals the number of (primitive) reduced forms of discriminant* D.

2.2. **Finiteness of the class number.**

Corollary 2.6. $h(D)$ *is finite, in fact we have*

$$h(D) \ll |D|.$$

Proof. We first note that for a reduced form of discriminant $D < 0$, we have

$$1 \le a \le \sqrt{\frac{|D|}{3}} \tag{4}$$

Indeed, we have

$$4ac = b^2 - D = b^2 + |D| \le a^2 + |D|$$

since $|b| \le a$. Also, $c \ge a > 0$ so that $4ac \ge 4a^2$. Thus

$$4a^2 \le 4ac \le a^2 + |D|$$

which gives (4).

Next observe that $|b| \le a \le \sqrt{\frac{|D|}{3}}$, and c is determined by a and b, so that we find that $h(D) \le 2|D|/3 < \infty$. $\square$

Remark: The proof gives $h(D) \ll |D|$. One can get a better bound of order $O(\sqrt{|D|}\log|D|)$.

Example 2.7. *Determine all reduced forms of discriminant $D = -4$:*

We need to solve $b^2 - 4ac = -4$, with $[a, b, c]$ reduced, $a > 0$. Condition (4) gives $1 \le a \le 2/\sqrt{3} < 2$, hence $\boxed{a = 1}$. Also we need $|b| \le a = 1$ so that $\boxed{b = 0, \pm 1}$. For $b = 0$ we get $-4 = \cdot 1 \cdot c - 0^2 = -4$ or $c = 1$, which gives the principal form $x^2 + y^2$.

For $|b| = 1 = 1$, we must have $b \ge 0$, so that $b = 1$, and so $-4 = 1^2 - 4 \cdot 1 \cdot c$ which has no solution. Hence $\boxed{h(-4) = 1}$.

Example 2.8. *Determine all reduced forms of discriminant $D = -15$:*

We know that $1 \le a \le \sqrt{|D|/3} = \sqrt{5} = 2.2\ldots$ so that $a = 1, 2$.

The choice $a = 1$ gives the principal form $[1, 1, 4]$.

Choosing $a = 2$, we have $-2 < b \le +2$ so that $b = -1, 0, 1, 2$. Since $b^2 = D + 4ac \equiv D \bmod 2$ and $D = -15$ is odd, we can only have $b = \pm 1$, and then c is determined by $(\pm 1)^2 - 4 \cdot 2 \cdot c = -15$ to equal $c = 2$. Now the form $[2, -1, 2]$ is not reduced, while $[2, 1, 2]$ is reduced, giving $h(-15) = 2$, with reduced forms $[1, 1, 4]$ and $[2, 1, 2]$.

Exercise 7. *Find the class number $h(D)$ and all reduced forms of discriminant D for all discriminants $-12 \le D < -4$.*

Exercise 8. *Find the class number $h(D)$ and all reduced forms of discriminant D for $D = -4(2^s - 1)$, $s = 1, 2, 3, 4, 5$.*

Exercise 9. *Find the class number $h(D)$ and all reduced forms of discriminant D for $D = -4 \cdot 2^4$, $r = 0, 1, 2, 3$.*

Moral: The class number is effectively computable.

2.3. **Representation by forms with class number one.** Having class number one is useful for determining representability. If a form $f = [a, b, c]$ has discriminant D with only one class $h(D) = 1$, then by Proposition 1.2, an integer k coprime to D is properly representable by f if and only if $D = \ell^2 \bmod 4k$.

d	$h_f(d)$	d	$h_f(d)$	d	$h_f(d)$	d	$h_f(d)$	d	$h_f(d)$
−3	1	−39	4	−75	2	−111	8	−147	2
−4	1	−40	2	−76	3	−112	2	−148	2
−7	1	−43	1	−79	5	−115	2	−151	7
−8	1	−44	3	−80	4	−116	6	−152	6
−11	1	−47	5	−83	3	−119	10	−155	4
−12	1	−48	2	−84	4	−120	4	−156	4
−15	2	−51	2	−87	6	−123	2	−159	10
−16	1	−52	2	−88	2	−124	3	−160	4
−19	1	−55	4	−91	2	−127	5	−163	1
−20	2	−56	4	−92	3	−128	4	−164	8
−23	3	−59	3	−95	8	−131	5	−167	11
−24	2	−60	2	−96	4	−132	4	−168	4
−27	1	−63	4	−99	2	−135	6	−171	4
−28	1	−64	2	−100	2	−136	4	−172	3
−31	3	−67	1	−103	5	−139	3	−175	6
−32	2	−68	4	−104	6	−140	6	−176	6
−35	2	−71	7	−107	3	−143	10	−179	5
−36	2	−72	2	−108	3	−144	4	−180	4

FIGURE 1. A table of class numbers $h(d)$ for discriminants $1 \le -d \le 180$. Circled are all examples with class number one.

Example 2.9. *Find all primes of the form $x^2 + 2y^2$.*

Answer: $p = x^2 + 2y^2$ if and only if $p = 1, 3 \bmod 8$ or $p = 2$.

The form $x^2 + 2y^2$ has discriminant -8. We compute $h(-8) = 1$ because for a reduced form $[a, b, c]$, we need $1 \le a \le \sqrt{|-8|/3} < 2$ so that $a = 1$, which forced $[a, b, c]$ to be the principal form $[1, 0, 2]$.

We determine all odd primes of the form $x^2 + 2y^2$, which for $p \ne 2$ is equivalent (since $h(-8) = 1$) to $-8 = \ell^2 \bmod 4p$, which by the Chinese Remainder theorem is equivalent to $-8 = \ell^2 \bmod p$ (since $p \ne 2$), equivalently the Legendre symbol $\left(\frac{-8}{p}\right) = +1$.

Using the law of quadratic reciprocity we find

$$\begin{aligned}\left(\frac{-8}{p}\right) = \left(\frac{-2}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\\ &= \left\{\begin{cases}1, & p = 1 \bmod 4\\ -1, & p = 3 \bmod 4\end{cases}\right\} \cdot \left\{\begin{cases}1, & p = 1,7 \bmod 8\\ -1, & p = 3,5 \bmod 8\end{cases}\right\}\\ &= \left\{\begin{cases}1, & p = 1,5 \bmod 8\\ -1, & p = 3,7 \bmod 8\end{cases}\right\} \cdot \left\{\begin{cases}1, & p = 1,7 \bmod 8\\ -1, & p = 3,5 \bmod 8\end{cases}\right\}\end{aligned}$$

and we find $\left(\frac{-8}{p}\right) = +1$ if and only if $p = 1,3 \bmod 8$. Thus $p = x^2+2y^2$ if and only if $p = 1,3 \bmod 8$ (or $p = 2$).

2.4. **A geometric interpretation.** To a positive definite real form $f = [a,b,c]$ with discriminant $D = b^2 - 4ac$, we associate a unique point $\tau_f \in \mathbb{H}$ by requiring τ_f to be the unique solution in the upper half-plane (there are exactly two solutions in $\mathbb{C}$) of

$$f(\tau, 1) = 0.$$

We call such $\tau_f \in \mathbb{H}$ a "Heegner point".

Solving the resulting quadratic equation gives

$$\tau_f = \frac{-b + i\sqrt{|D|}}{2a}.$$

Note that for a properly equivalent form $g = f \circ A$, $A = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$, we have

$$\tau_f = \frac{\alpha\tau_g + \beta}{\gamma\tau_g + \delta} = A(\tau_g) \quad \Leftrightarrow \quad A(\tau_g) = \tau_{g\circ A^{-1}}$$

where we now think of A as a Möbius transformation. Indeed, we have

$$f \circ A(z,1) = f(\alpha z + \beta, \gamma z + \delta) = (\gamma z + \delta)^2 f(\frac{\alpha z + \beta}{\gamma z + \delta}, 1).$$

For $z \in \mathbb{H}$, we have $\gamma z + \delta \neq 0$ if $\gamma, \delta \in \mathbb{R}$ so that $(f \circ A)(z,1) = 0$ iff $f(\frac{\alpha z+\beta}{\gamma z+\delta}, 1) = 0$. Uniqueness of the solution in the upper half-plane gives $\tau_f = \frac{\alpha\tau_g+\beta}{\gamma\tau_g+\delta}$.

Lemma 2.10. *Let $f = [a,b,c]$, $g = [a',b,c']$ be two (positive definite, integral binary quadratic) forms of the* same *discriminant D. Then $f = g$ if and only if $\tau_f = \tau_g$.*

Proof. Since $\operatorname{disc} f = \operatorname{disc} g = D$, we have

$$\tau_f = \frac{-b + i\sqrt{|D|}}{2a}, \qquad \tau_g = \frac{-b' + i\sqrt{|D|}}{2a'}$$

Comparing imaginary parts gives

$$\frac{\sqrt{|D|}}{2a'} = \frac{\sqrt{|D|}}{2a}$$

which gives $a' = a$, and then comparing real parts gives

$$-\frac{b}{2a} = -\frac{b'}{2a'} = -\frac{b'}{2a}$$

so that $b' = b$. Finally, $c' = c$ is determined from

$$b^2 - 4ac = D = b'^2 - 4a'c' = b^2 - 4ac'.$$

□

Corollary 2.11. *Two primitive forms f, g of the same discriminant $D < 0$ are properly equivalent if and only if the corresponding Heegner points $\tau_f, \tau_g \in \mathbb{H}$ are equivalent under* $\mathrm{SL}(2, \mathbb{Z})$.

It is easily checked that a form f is reduced if and only if the corresponding Heegner point τ_f lies in the region (see Figure 2)

$$\mathcal{F} = \left\{ \tau \in \mathbb{H} : \mathrm{Re}(\tau) \in [-\frac{1}{2}, \frac{1}{2}), \quad |\tau| > 1 \text{ or } |\tau| = 1 \text{ and } \operatorname{Re}\tau \le 0 \right\}$$

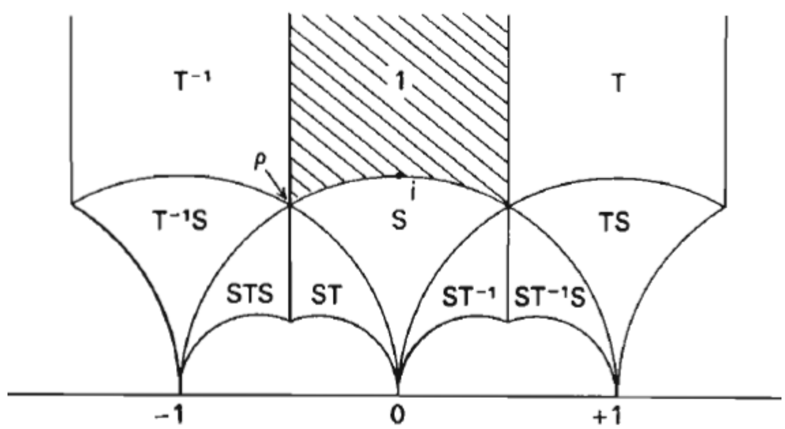

FIGURE 2. The fundamental domain $\mathcal{F}$ (shaded) and it's translates.