MODULAR FORMS 2019: BINARY QUADRATIC FORMS WEEKS OF MARCH 10 & 17, 2019

ZEÉV RUDNICK

1. Binary quadratic forms

An integral binary quadratic form is $f(x,y) = ax^2 + bxy + cy^2$ with $a, b, c \in \mathbb{Z}$. 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

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

We say that f is primitive if $\gcd(a,b,c) = 1$.

Such a 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 1. *A prime that is represented, is necessarily properly represented.*

For instance, one asks which primes are represented by a given form f. Fermat showed that a prime is represented by the form $x^2 + y^2$ if and only if $p = 2$ or $p = 1 \bmod 4$.

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

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

Note that

$$4af(x,y) = (2ax + by)^2 - Dy^2$$

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., $a < 0$).

Date: March 25, 2019.

Note that $D = b^2 - 4ac \equiv b^2 \bmod 4$ so that b is even if and only if $D = 0 \bmod 4$. This was an earlier notion of binary quadratic forms, in which b was only allowed to be even (so that the matrix M_f had integer entries), and it was Gauss whose definitions we use.

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

$$(f \circ A)(x,y) = f(A \begin{pmatrix} x \\ y \end{pmatrix}) = f(\alpha x + \beta y, \gamma x + \delta y)$$

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 <u>properly</u> equivalent if $g = f \circ A$ with $\det A = +1$, i.e. if $A \in \mathrm{SL}(2,\mathbb{Z})$.

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

Exercise 2. *Show that the matrix of f transforms under A as*

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

Exercise 3. *Show that*

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

Hence equivalent forms have the same discriminant.

Exercise 4. *Show that f is primitive if and only if $f \circ A$ is primitive.*

From now on we only deal with positive definite forms.

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

First of all, 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 $x^2 + xy + \frac{1-D}{4} y^2$.

We shall soon see that $h(D)$ is finite, and how to effectively enumerate all equivalence classes.

1.2. **Reduction theory and finiteness of class numbers.** To a (positive definite integral binary quadratic) 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 $\tau_f = \frac{\alpha\tau_g+\beta}{\gamma\tau_g+\delta}$.

Note that the imprimitive form $ef(x, y)$ $(e > 1)$ has the same root $\tau_{ef} = \tau_f$

Lemma 1.1. *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 1.2. *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 $\mathrm{SL}(2, \mathbb{Z})$.*

Definition. *(Lagrange): A primitive (positive definite integral binary quadratic) form $f = [a, b, c]$ is reduced if the corresponding Heegner point τ_f lies in the fundamental domain $\mathcal{F}$. Equivalently, if we have*

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

As a consequence of our result on the fundamental domain, we obtain

Corollary 1.3. *Any primitive form is properly equivalent to a unique reduced form.*

Corollary 1.4. *Let $D < 0$, $D = 0, 1 \bmod 4$. The class number $h(D)$ equals the number of (primitive) reduced forms of discriminant D.*

A moral: The imaginary part $\mathrm{Im}\,\tau = \sqrt{|D|}/2a$ of a reduced Heegner point is at least $\sqrt{3}/2$ (the lowest point in the fundamental domain), so that we obtain that

$$1 \leq a \leq \sqrt{\frac{|D|}{3}}$$

Moreover, $|b| \leq a \leq \sqrt{\frac{|D|}{3}}$, and c is determined by a and b, so that we find that

Corollary 1.5. *$h(D)$ is finite!*

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

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

We need to solve $b^2 - 4ac = -4$, and that $\frac{-b+i2}{2a} \in \mathcal{F}$. So in particular the imaginary part is at least $\sqrt{3}/2$, or

$$\frac{1}{a} \geq \frac{\sqrt{3}}{2}$$

which gives $1 \leq a \leq 2/\sqrt{3} < 2$, hence $\boxed{a = 1}$. Also we need $|b| \leq a = 1$ 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 $b \geq 0$, so that $b = 1$, and so $-4 = 1^2 - 4 \cdot 1 \cdot c$ which has no solution. Hence $\boxed{h(-4) = 1}$.

Exercise 5. *Find the class number $h(D)$ and all reduced forms of discriminant D for all discriminants $-12 \leq D < -4$.*

Moral: The class number is effectively computable.

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 $1 \leq -d \leq 180$. Circled are all examples with class number one (taken from Corentin Perret-Gentil's MSc thesis).

Exercise 6. *Show that if $D = 1 - 4q$, $q > 1$, and $h(D) = 1$ then q is prime.*

1.3. **A reduction algorithm.** Recall that a form $f = [a, b, c]$ is *reduced* if it satisfies

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

This corresponds to the corresponding Heegner point $\tau_f = (-b + \sqrt{D})/2a$ lying the fundamental domain $\mathcal{F}$ (Figure 2), with the condition $0 \leq b \leq a = c$ corresponding to points on the boundary arc $|\tau|^2 = c/a = 1$ and $\mathrm{Re}(\tau) = -b/(2a) \leq 0$. 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

$$S : [a, b, c] \mapsto [c, -b, a]$$

$$T^n : [a, b, c] \mapsto [a, b + 2a \cdot n, c'], \quad c' = f(n, 1) = an^2 + bn + c$$

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

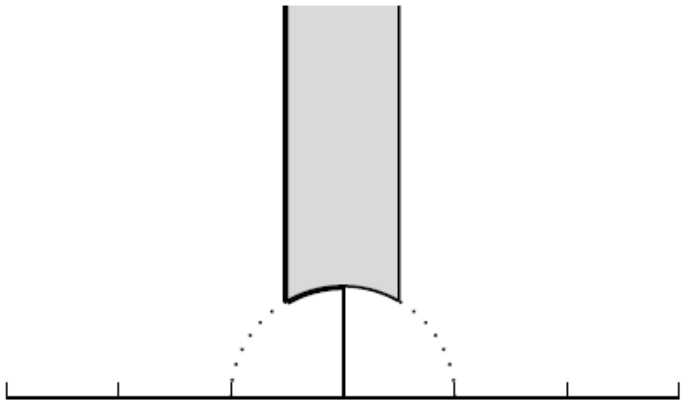

FIGURE 2. The fundamental domain $\mathcal{F}$ for $\mathrm{SL}(2,\mathbb{Z})$.

(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: 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: Take $f = [16, 23, 9]$ which has discriminant $D = -47$ (note that $h(-47) = 5$).

$$[16, 23, 9] \xrightarrow{\text{step 1}} [9, -23, 16] \xrightarrow[n=-1]{\text{step 2}} [9, -23 + 2 \cdot 9 \cdot 1, c'] = [9, -5, 2]$$
$$\xrightarrow{\text{step 1}} [2, 5, 9] \xrightarrow[n=1]{\text{step 2}} [2, 5 - 2 \cdot 2 \cdot 1, c'] = \boxed{[2,1,6]}$$

which is reduced.

Note: At each step, we either reduce a (but keep it positive) or if not, we either reduce $|b|$ or at the last step change the sign of b. So the algorithm terminates.

Exercise 7. *Decide which of the following forms are equivalent:*

$$[6, 12, 7], \quad [3, 6, 5], \quad [5, 14, 11].$$

1.4. **Ideal theory in imaginary quadratic fields.** The theory of binary quadratic forms runs parallel to ideal theory in quadratic fields. We focus on the positive definite case, corresponding to *imaginary* quadratic fields.

Let $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}1 + \mathbb{Q}\sqrt{d}$, where $d < 0$ is squarefree, be an imaginary quadratic field. This is a 2-dimensional field extension of $\mathbb{Q}$.

The ring of integers O_K is defined as the set of all elements of K which are roots of monic integer polynomials. It is a computation that

$$O_K = \mathbb{Z}[w_K] = \mathbb{Z}1 + \mathbb{Z}w_K$$

where

$$w_K = \begin{cases} \sqrt{d}, & d \neq 1 \bmod 4 \\ \frac{1+\sqrt{d}}{2}, & d = 1 \bmod 4 \end{cases}$$

The *discriminant* of K is defined as

$$D_K = \begin{cases} 4d, & d \neq 1 \bmod 4 \\ d, & d = 1 \bmod 4 \end{cases}$$

so that $D_K = 0, 1 \bmod 4$.

So for instance the discriminant of $Q(\sqrt{-1})$ is -4, and of $\mathbb{Q}(\sqrt{-3})$ is -3.

An intrinsic definition of the discriminant is as the discriminant of the "trace form" of O_K, which is the quadratic form $Q : O_K \times O_K \to \mathbb{Z}$ given by $Q(x, y) = \mathrm{tr}_{K/\mathbb{Q}}(xy)$.

The discriminants of quadratic fields are called "fundamental discriminants", and are characterized as integers $D = 0, 1 \bmod 4$ of the form either $D = 1 \bmod 4$ and squarefree, or $D = 4m$ where $m = 2, 3 \bmod 4$ is squarefree.

A nonzero ideal $I \subset O_K$ has a norm, defined as

$$N(I) = \#O_K/I < \infty$$

For instance, for a principal ideal $I = (\alpha)$, with $0 \neq \alpha \in O_K$, we have $N((\alpha)) = N_{K/\mathbb{Q}}(\alpha) = \alpha \cdot \bar{\alpha}$.

Any ideal $I \subset O_K$ is itself a rank-2 lattice, so has an integral basis $I = \mathbb{Z}\alpha + \mathbb{Z}\beta$. The choice of bases gives a quadratic form $N(x\alpha + y\beta) = ax^2 + bxy + cy^2$, whose coefficients are all divisible by the norm $N(I)$ of the ideal, and the integral quadratic form

$$Q_{\alpha,\beta}(x, y) := \frac{N_{K/\mathbb{Q}}(x\alpha + y\beta)}{N(I)}$$

is a *primitive* integral quadratic form, whose discriminant is $D_K = d$ or $4d$, the discriminant of the field $K = \mathbb{Q}(\sqrt{d})$. For instance, for the unit ideal $I = O_K$, where $N(O_K) = 1$, taking the basis $O_K = \langle 1, w_K \rangle$ gives the principal form

$$Q(x,y) = N(x + yw_K) = x^2 + (w + \bar{w})xy + N_{K/\mathbb{Q}}(w)y^2$$
$$= \begin{cases} x^2 - dy^2 = x^2 - \frac{D_K}{4}y^2, & D_K = 0 \bmod 4 \\ x^2 + xy + \frac{1-D_K}{4}y^2, & D_K = d = 1 \bmod 4 \end{cases}$$

We say that an ordered basis $I = [\alpha, \beta]$ is *positive* if

$$\frac{\alpha\bar{\beta} - \bar{\alpha}\beta}{\sqrt{D}} > 0$$

It turns out that different (positive) bases give rise to (properly) equivalent quadratic forms, so that an ideal I gives us a well-defined (proper) equivalence class $[Q_I]$ of binary quadratic forms, and that two ideals which are in the same ideal class (that is $(\alpha) \cdot I = (\beta) \cdot J$ for $\alpha, \beta \in O_K$) give the same class; and inequivalent ideals give inequivalent forms.

Conversely, to a positive definite primitive form $ax^2 + bxy + cy^2$ with fundamental discriminant D_K, we associate the ideal (with positive basis)

$$I = [a, \frac{b - \sqrt{D_K}}{2}] \subseteq O_K$$

Exercise 8. *check that $I = \mathbb{Z}a + \mathbb{Z}\frac{b-\sqrt{D_K}}{2}$ as above is an ideal of O_K, with a positive ordered basis.*

In this way we get a bijection

$$\boxed{\text{ideal classes in } O_K} \leftrightarrow \text{ (proper) equivalence classes of positive definite forms of discriminant } D_K$$

Consequently we find that O_K has unique factorization into irreducibles (is a Principal Ideal Domain) if and only if $h(D_K) = 1$.

1.5. **An example of a non PID.** As an example, consider the field $Q(\sqrt{-6})$, which has discriminant $D = -4 \cdot 6 = -24$. The ring of integers is $O_K = \mathbb{Z}[\sqrt{-6}]$, and the units are $O_K^\times = \{\pm 1\}$. We check that there is no unique factorization by observing that

$$6 = 2 \cdot 3 = -(\sqrt{-6})^2$$

We claim that $2, 3, \sqrt{-6}$ are irreducible and are clearly non-associate (as the units are ± 1) so we get a non-unique factorization into irreducibles. To see that for instance 2 is irreducible, suppose we have a factorization $2 = \alpha\beta$ with $\alpha, \beta \neq \pm 1$. Then taking norms gives

$$4 = N(2) = N(\alpha\beta) = N(\alpha)N(\beta)$$

and since $N(\alpha) \neq 1$ as α is not a unit, we must have $N(\alpha) = N(\beta) = 2$. But if $\alpha = x + y\sqrt{-6}$, with $x, y \in \mathbb{Z}$ then

$$2 = N(\alpha) = x^2 + 6y^2$$

which by inspection has no integer solutions. Hence $\mathbb{Z}[\sqrt{-6}]$ is not a PID.

A computation by reduction theory shows that the class number is $h(-24) = 2$. The reduce forms are the principal form $[1, 0, 6]$ (corresponding to to the principal ideal class), and $[2, 0, 3]$.

1.6. **The class number one problem.** Using the correspondence and reduction theory, we can quickly check several discriminants and obtain 9 imaginary quadratic fields $Q(\sqrt{d})$ with unique factorization (class number one), namely those with

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

of these, it can be shown that only the first five are Euclidean: $d = -1, -2, -3, -7, -11$ (and in fact are Euclidean w.r.t. the norm).

Gauss' class number one problem was to show that these 9 fields are the only imaginary quadratic fields with class number one.

Assuming GRH there is an effective $c > 0$ so that $h(D) > c\sqrt{|D|}/\log|D|$ (Hecke/Landau 1918), so that on GRH Gauss' problem is easy.

Heilbronn (1934) showed that $h(D) \to \infty$ as $D \to -\infty$, so that there are only finitely many imaginary quadratic fields of class number one. This was done by combining work of Deuring, Mordell and Heilbronn to obtain the the falsity of GRH implies $h(D) \to \infty$ as $D \to -\infty$, with the effective lower bound obtained from GRH.

Heilbronn and Linfoot (1934) showed that there are at most 10 imaginary quadratic fields of class number one (9 were known to Gauss).

Siegel (1935) showed unconditionally that $h(D) \gg_\epsilon |D|^{1/2-\epsilon}$ for all $\epsilon > 0$, but his constant was not effective so cannot be used to check that we have obtained all fields with class number one.

The class number one problem was finally settled by Stark (1967) and Baker (1966) (Kurt Heegner seemed to have the correct proof in 1952 but was not believed at the time).