Proof of Thm 7.2 Let $Q = [a, b, c] \in \mathcal{Q}_D$ be given.

Let $a' = \min\{|Q(x,y)| \mid x, y \in \mathbb{Z}^2 \setminus \{0,0\}\}$

Tie choose a' as the smallest in abs value of the values taken by Q.

Note this set is non-empty since $a = Q(1,0) \neq 0$ $(D \neq \square)$

Hence $\exists\ \alpha, \gamma$ such that

$$|Q(\alpha,\gamma)| = a' = |a\alpha^2 + b\alpha\gamma + c\gamma^2| \neq 0$$

Moreover $\gcd(\alpha,\gamma) = 1$. Since if not $\gcd(\alpha,\gamma) = r \neq 1$ then

$$\frac{a'}{r^2} = \left|a\left(\frac{\alpha}{r}\right)^2 + b\frac{\alpha}{r}\frac{\gamma}{r} + c\left(\frac{\gamma}{r}\right)^2\right| = |Q(\alpha/r, \gamma/r)|$$

is represented by Q and $\left(\frac{a'}{r^2}\right) < |a'|$ ↯

Hence we can find integers β, δ s.t

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$$

$$Q \sim \tilde{Q} = Q((x,y)M^t) = [\overset{=Q(\alpha,\gamma)}{a'}, \tilde{b}, \tilde{c}]$$

and a' is in abs value the smallest integer represented by Q.

Now choose $n \in \mathbb{Z}$ so that

$b' := \tilde{b}' - 2a'n$ has abs. value less than or equal to $|a'|$. Let $\tilde{M} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$

Then $\tilde{Q}\left((x \; y)\begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}\right) =: Q' = \tilde{M} \cdot \tilde{Q}$

$$= \tilde{a}'(x-ny)^2 + \tilde{b}'(x-ny)y + \tilde{c}'y^2$$

$$= a'x^2 + (\tilde{b}' - 2a'n)xy + (a'n^2 - \tilde{b}n + \tilde{c})y^2$$

$$= a'x^2 + b'xy + c'y^2$$

is equivalent to $\tilde{Q}$, hence also to Q and $Q' = [a', b', c']$ satisfy

$|b'| \leq |a'|$. By the choice of a', $|a'| \leq |c'| = Q'(0,1)$

Hence $Q' = [a', b', c']$ satisfy (*). and $Q \sim Q'$ ∎.

Remark This proof is not really constructive since given $Q = [a\ b, c]$, How do we find a' ie min of $|Q|$?

Instead we can use the following effective algorithm.

(I) Given $[a,b,c]$, choose $n \in \mathbb{Z}$ s.t. $|b-2na| < |a|$

replace $[a,b,c]$ with $[a, b-2na, c-nb+n^2a]$

This step replaces b with a new b w/ $|b| < |a|$

Note $[a, b-2na, c-nb+n^2a]$

$= Q((x,y)\begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix})$ as above

Hence $[a, b-2na, c-nb+n^2a] \sim [a,b,c]$

(II) Is $|c| \geq |a|$?

Yes: stop. Since then $[a,b,c]$ satisfies (*)

NO: Replace $[a,b,c]$ with $[c,-b,a]$ and go back to (I)

Note $[a,b,c] \sim [c,-b,a]$ via $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Note this alg. stops since in each loop $|a|$ goes down at least by 1

Ex = Thm 7.2 gives a bound on the size of $|\Gamma \backslash \mathcal{D}|$

Let $D = -35$ then the conditions (*) imply $\sqrt{\frac{|D|}{3}} = 3.4156\ldots$

so $|a| \leq \sqrt{\frac{D}{3}} = 3.4\ldots$ and

$|b| \leq |a| \leq 3$ Hence

$1 \leq |a| \leq 3$, and $|b| \leq 3$, $a \in \{\pm 1, \pm 2, \pm 3\}$

But $b^2 - 4ac = -35 \Rightarrow b$ is odd

$\Rightarrow b \in \{\pm 1, \pm 3\}$

If $b = \pm 1$, then $b^2 - D = 4ac = 36$

and $c = \frac{b^2 - D}{4a} = \frac{9}{a}$ must be an integer

Hence $a \neq \pm 2$.

In fact if we restrict to positive definite forms then $a, c > 0$ and we can have $a=1$, $b=\pm 1$ then $c=9 \rightsquigarrow [1, \pm 1, 9]$

$a=3$ $b=\pm 1$ then $c=3$ $[3, \pm 1, 3]$

If $b = \pm 3$ then $|a| \geq |b| \Rightarrow a = 3$

but then $c = \frac{b^2 - D}{4a} = \frac{44}{4a} \notin \mathbb{Z}$.

Hence this cannot happen.

$$\Rightarrow \left| \Gamma \backslash Q_{-35} \right| \leq 4.$$

In the case of positive definite forms w/ $D < 0$, i.e. $Q_D = \{[a,b,c] \mid D < 0, a > 0\}$ we have

Thm 7.3 Every form $Q = [a,b,c] \in Q_D$ $D<0$, is equivalent to exactly one form which satisfies

$$(**) \quad \begin{cases} |b| \leq a \leq c \text{ and} \\ b \geq 0 \text{ if either } |b| = a \text{ or } a = c \end{cases}$$

Proof: Exercise. A form satisfying (**) is called reduced

Example (1) $D = -4$, the principal form $Q_1 = [1,0,1] = x^2 + y^2$. If $[A,B,C] \in Q_{-4}$ then we have seen $|B| \leq \sqrt{4/3} \Rightarrow |B| = 1$ or 0

If $|B| = 1$ then $B^2 - 4AC = -4$ gives $B^2 \equiv 0 \bmod 4$ hence cannot happen. So $|B| = 0$.

Then $B^2 - 4AC = -4AC = -4 \Rightarrow AC = 1 \Rightarrow A = C = 1$

Hence there is only one form $[1,0,1] \in \Gamma \backslash Q_{-4}$.

Ex 2. $D = -3$

then $[1, 1, 1] \in \mathcal{Q}_D$

If $Q = [A, B, C]$ is reduced then

$|B| \leq \sqrt{|D|/3} = 1$ Hence $|B| = 1$ or 0.

But $B^2 \equiv -3 \equiv 1 \ (4) \Rightarrow B \neq 0$ Hence

and $B = \pm 1$. Now $B^2 - 4AC = -3$

$\Rightarrow AC = 1 \Rightarrow AC = 1$ and $A = C = 1$

Since $A = C$, $B > 0$ by the conditions in thm 7.3

Hence $Q = [1, 1, 1]$ and $\left(\frac{Q_{-3}}{p}\right) = 1$ ✓

Ex 3 $D = -15 \equiv 1 \ (4)$

$|B| \leq \sqrt{|D|/3} \Rightarrow |B| \leq \sqrt{5} = 2 \ldots$

$\Rightarrow |B| = 0, 1, 2$

Since $B^2 \equiv D \equiv -15 \equiv 1 \ (4)$ $|B| \neq 0, 2$

Hence $|B| = 1$. $B^2 - 4AC = -15 \Rightarrow AC = 4$

$\Rightarrow$ either $A = 1$, $C = 4$ or

$A = 2$, $C = 2$

In the first case $A = |B|$ hence B must be positive hence $B = 1$

In the second case $A = C$, and again $B > 0$ hence $B = 1$

so we see 2 classes

$[1, 1, 4]$ and $[2, 1, 2]$

The equivalence and reduction of positive definite forms has the following geometric interpretation.

Let $F = \{ z \in \mathbb{H} : |z| \geq 1, -1/2 \leq \mathrm{Re}\, z \leq 1/2 \}$ be the standard fund. domain for $\Gamma \backslash \mathbb{H}$.

Given a form $Q = [A, B, C]$ of disc $D < 0$ we define the principal root of Q to be $\tau_Q = \dfrac{-B + \sqrt{D}}{2A} \in \mathbb{H}$.

Note τ_Q is one of the roots of $Ax^2 + Bx + C = 0$

Then we have

Prop 7.3 A form Q is reduced iff $\tau_Q \in F$.

Proof: The condition $|B| \leq A$ is equivalent to the condition that $-\frac{1}{2} \leq \mathrm{Re}\, \tau_Q \leq \frac{1}{2}$

The condition $A \leq C$ is equivalent to

$$1 \leq \frac{C}{A} = \frac{4AC}{4A^2} = \frac{B^2 - D}{4A^2} = \frac{(-B + \sqrt{D})(-B - \sqrt{D})}{2A \cdot 2A}$$

$$= \tau_Q \cdot \overline{\tau_Q} = |\tau_Q|^2$$

For a reduced form $Q = [A, B, C] \in \mathcal{Q}_D$ ($D < 0$) we have the following

Lemma 7.4 Suppose $Q = [A, B, C]$ satisfies $|B| \leq A \leq C$.

Then $A = \min \{ Q(x, y) \mid (x, y) \in \mathbb{Z}^2 \setminus \{(0,0)\} \}$

i.e. $\forall (x, y) \neq (0, 0)$, $Q(x, y) \geq A$.

Proof - Note $Q(1, 0) = A$

$Q(0, 1) = C$

If $x \neq 0$ then $Q(x, 0) = Ax^2 \geq A$

Similarly if $y \neq 0$ $Q(0, y) = Cy^2 \geq C \geq A$.

In the general case when neither x nor $y \in \mathbb{Z}$ is zero $Q(x, y) = Ax^2 + Bxy + Cy^2$

$$\geq Ax^2 - |B||x||y| + Cy^2$$

$$\geq Ax^2 - |B||x||y| + Cy^2 - A(x-y)^2$$

$$\geq (2A - |B|)|x||y| + (C - A)y^2$$

$$\geq (2A - |B|) + (C - A) = A + C - |B|$$

$$\geq 0$$

$$\geq A$$

□

We next want to define the class number h_D of discriminant D.

For this we note that there is another invariant of quadratic forms under the action of Γ. Namely $\gcd(a,b,c)$

To see this: Suppose that $r = \gcd(a,b,c)$

Recall if $[a',b',c'] \sim [a,b,c]$ with

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \text{then}$$

$$a' = a\alpha^2 + b\alpha\gamma + c\gamma^2$$

$$b' = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta$$

$$c' = a\beta^2 + b\beta\delta + c\delta^2$$

Hence $r \mid a', b', c'$ hence $\gcd(a,b,c) \mid \gcd(a',b',c')$

Due to symmetry ($Q \sim Q' \Leftrightarrow Q' \sim Q$) we also have $\gcd(a',b',c') \mid \gcd(a,b,c)$

Hence indeed $\gcd(a,b,c)$ is invariant under equivalence.

Def A form $[a,b,c]$ is called <u>primitive</u> if $\gcd(a,b,c) = 1$.

We can restrict ourselves to primitive forms

Since a form $Q=[a,b,c]$ of disc D with $\gcd(a,b,c)=r$ is simply $Q = r[a',b',c']$ with $\gcd(a',b',c')=1$ and $\operatorname{disc}[a',b',c'] = D/r^2$.

I.e. it is r times a primitive form of disc D/r^2

Defn The class number of D, denoted by $h(D)$ or h_D is

the { number of equivalence classes of primitive forms of disc D if $D>0$

number of equiv. classes of primitive positive defn forms of disc D if $D<0$

$h_D < \infty$ Because of Thm 7-1 and $h_D \geq 1$ since there is at least the class of the principal form $\mathcal{D}_1$

The next natural question for quadratic forms is

① Which integers $n \in \mathbb{Z}$ are represented by a given form $Q \in \mathcal{D}_D$

and ② How often? I.e. how many such repn exist?