Recall: $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1, \ a, b, c, d \in \mathbb{Z} \right\}$

Two quadratic forms $Q_1 = \begin{pmatrix} a_1 & \frac{b_1}{2} \\ \frac{b_1}{2} & c_1 \end{pmatrix}$ and $Q_2 = \begin{pmatrix} a_2 & b_2/2 \\ b_2/2 & c_2 \end{pmatrix}$ are <u>equivalent</u> if $Q_1 = {}^t g \, Q_2 \, g$ for some $g \in SL_2(\mathbb{Z})$.

Let $Q(x,y) = ax^2 + bxy + cy^2$ be a qudratic form.

let $n \geq 1$ be an integer. Set

$$R_Q(n) := \# \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : Q(x,y) = n \right\}$$

$$R_Q^*(n) := \# \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : Q(x,y) = n, \ (x,y) = 1 \right\}$$

Definition: Let $n \geq 1$, We say that $n$ is <u>representable</u> by $Q$ if $R_Q(n) > 0$.

Observation: Let $Q_1$ and $Q_2$ be two equivalent qudratic forms. Then $R_{Q_1}(n) = R_{Q_2}(n)$.

Proof: $Q_1 \sim Q_2 \Rightarrow Q_1 = \begin{pmatrix} a_1 & b_1/2 \\ b_1/2 & c_1 \end{pmatrix} = {}^t g \begin{pmatrix} a_2 & b_2/2 \\ b_2/2 & c_2 \end{pmatrix} g = {}^t g \, Q_2 \, g$

We also have: $Q_1(x,y) = (x,y) \begin{pmatrix} a_1 & b_1/2 \\ b_1/2 & c_1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$

$$Q_2(x,y) = (x,y) \begin{pmatrix} a_2 & b_2/2 \\ b_2/2 & c_2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Then for $n \geq 1$, we have a bijection:

$$\left\{ \begin{pmatrix} x \\ y \end{pmatrix} : R_{Q_1}(x,y) = n \right\} \longrightarrow \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : R_{Q_2}(x,y) = n \right\}$$

$$(*) \quad \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto g \begin{pmatrix} x \\ y \end{pmatrix}$$

with inverse map: $$g^{-1}\begin{pmatrix} x \\ y \end{pmatrix} \longleftarrow \begin{pmatrix} x \\ y \end{pmatrix}$$

We only check $(*)$: if $\begin{pmatrix} x \\ y \end{pmatrix} \in \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : Q_1(x,y) = n \right\}$

then $$(x,y)\, Q_1 \begin{pmatrix} x \\ y \end{pmatrix} = n$$

We have $Q_1 = {}^t g\, Q_2\, g \Rightarrow {}^t\!\left(g\begin{pmatrix} x \\ y \end{pmatrix}\right) Q_2\; g\begin{pmatrix} x \\ y \end{pmatrix} = n$

$$\Rightarrow \quad g\begin{pmatrix} x \\ y \end{pmatrix} \in \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : Q_2(x,y) = n \right\} \qquad \square.$$

Remark: If $Q_1 \sim Q_2$, then $R^*_{Q_1}(n) = R^*_{Q_2}(n)$.

Lemma: Every quadratic form is equivalent to some quadratic form $[a,b,c]$ with $|b| \leq |a| \leq |c|$.

Proof: We start with $Q_0 = [a_0, b_0, c_0]$

Set $R(Q) = \{ n : n \text{ is representable by } Q \}$

and take $a = \min\{|n| : n \neq 0,\ n \in R(Q)\}$

Then we can find $\alpha, \beta \in \mathbb{Z}$ s.t.

$$a = Q_0(\alpha, \gamma) = a_0\alpha^2 + b_0\alpha\gamma + c_0\gamma^2$$

We can assume $(\alpha, \ ) = 1$. Otherwise, $\frac{a}{(\alpha,\gamma)^2}$ is also representable by $Q_0$ and $\frac{a}{(\alpha,\gamma)^2} < a$.

$(\alpha, \gamma) = 1$, then we can find $\beta, \delta \in \mathbb{Z}$ s.t. $\alpha\delta - \beta\gamma = 1$

In other words $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$.

Then we consider

$$Q_0 \sim Q' = {}^t\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} Q_0 \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a' & b'/2 \\ b'/2 & c' \end{pmatrix}$$

check: $a' = (\alpha\ \gamma) Q_0 \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} = a$

$\Rightarrow Q' = [a, b', c']$

Next, we consider $g = \begin{pmatrix} 1 & h \\ & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$.

$$Q = {}^tg \begin{pmatrix} a & b'/2 \\ b'/2 & c' \end{pmatrix} g = \begin{pmatrix} 1 & \\ h & 1 \end{pmatrix} \begin{pmatrix} a & b'/2 \\ b'/2 & c' \end{pmatrix} \begin{pmatrix} 1 & h \\ & 1 \end{pmatrix}$$

$$\begin{array}{ll} \wr & \\ Q' & = \begin{pmatrix} a & b'/2 + ah \\ b'/2 + ah & ah^2 + hb' + c' \end{pmatrix} \\ \wr & \\ Q_0 & = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \end{array}$$

Then $b = b' + 2ah$.

By choosing $h$ properly, we can make $|b| \leq |a|$

Taking $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\quad (1\ 0)\, Q \begin{pmatrix} 1 \\ 0 \end{pmatrix} = c$

$\Rightarrow$ $c$ is representable by $Q$ $\qquad Q \sim Q' \sim Q_0$

$\Rightarrow$ $c$ is representable by $Q_0$

By the choice of $a$, $\quad |a| \leqslant |c|$

This proves $|b| \leqslant |a| \leqslant |c|$

$\square$

Corollary: Let $d$ be a fundamental discriminant. Then there are only finitely many inequivalent quadratic forms of discriminant $d$.

Proof: By the lemma, the number of such quadratic forms

$$\leqslant \# \underbrace{\{ [a,b,c] : b^2 - 4ac = d,\ |b| \leqslant |a| \leqslant |c| \}}_{Q(d)}$$

Take $[a,b,c] \in Q(d)$, then: $\quad 4ac = b^2 - d$

$$4a^2 \leqslant 4|a| \cdot |c| \leqslant |b|^2 + |d| \leqslant |a|^2 + |d|$$

$$\Rightarrow |a| \leqslant \sqrt{\frac{|d|}{3}} \quad \Rightarrow |b| \leqslant \sqrt{\frac{|d|}{3}}$$

$$\Rightarrow |c| = \left| \frac{b^2-d}{4a} \right| \leq \frac{\frac{d^2}{3}+d}{4}$$

$\Rightarrow$ There are only finitely many choices for $a, b, c$

$\Rightarrow \# (Q|d) < \infty$.

Definition: A quadratic form $Q=[a,b,c]$ is <u>primitive</u> if $(a,b,c)=1$.

An equivalent class of qudratic forms is <u>primitive</u> if the class contains one primitive quadratic form.

Fact: If an equivalent class is primitive, then all quadratic forms in the class are primitive.

Definition: Let $d$ be a fundamental discriminant. Then

$$h(d) := \# \{ \text{inequivalent primitive classes of quadratic forms} \}.$$

Observation: $h(d) \geq 1$ as we have:

- $[1, 1, -\frac{1}{4}(d-1)]$ $\quad d \equiv 1 \pmod 4$
- $[1, 0, -\frac{1}{4}d]$ $\quad$ otherwise.

This is called the principal form of discriminat $d$.

Class number formula.

Let $d$ be a fundamental discriminant. Thee there is a unique primitive non principal Dirichlet character $\chi_d \pmod{|d|}$

$$\chi_d(n) = \left(\frac{d}{n}\right) \rightarrow \text{Kronecker symbol.}$$

Then we have the Dirichlet L-function $L(s, \chi_d)$, $s>1$

$$L(s, \chi_d) = \sum_{n\geq 1} \frac{\chi_d(n)}{n^s} = \sum_{n\geq 1} \frac{\left(\frac{d}{n}\right)}{n^s}$$

In Part II, we showed, $L(s, \chi_d)$ is continously diffeentiable in $(0, \infty)$. Therefore $L(1, \chi_d)$ is well defined.

Theorem (Class number formula)

- If $d<0$, $\quad L(1, \chi_d) = \frac{2\pi}{w\sqrt{|d|}} h(d)$

- If $d>0$, $\quad L(1, \chi_d) = \frac{\log \varepsilon_d}{\sqrt{d}} h(d)$

Here $\quad w = \begin{cases} 2 & \text{if } d<-4 \\ 4 & \text{if } d=-4 \\ 6 & \text{if } d=-3 \end{cases}$

and

$$\varepsilon_d = \frac{1}{2}(x_0 + y_0\sqrt{d}) \neq 1 \quad \text{with } (x_0, y_0) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$$

is the minimal solution for $x^2 - dy^2 = 4$.

Remark: We showed: $h(d) \geq 1$. This implies:

$L(1, \chi_d) \neq 0$ for any real primitive characters

This proves Dirichlet's Theorem.

For simplicity, we will focus on the case $\underline{d < 0}$.

Recall: let $F$ be a number field and $H(F)$ its class group.

Let $F$ be a quadratic field. Then we can find a fundamental discriminant $d$ s.t. $F = \mathbb{Q}(\sqrt{d})$

Then set: $h_d = \# H(\mathbb{Q}(\sqrt{d}))$

Theorem: There is a bijection:

$$\left\{ \begin{array}{l} \text{inequivalent primitive} \\ \text{classes of quadratic forms} \\ \text{of discriminant } d \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{fractional ideals} \\ \text{(mod principal fractional ideals)} \\ \text{in } \mathbb{Q}(\sqrt{d}) \end{array} \right\}$$

This implies: $h(d) = h_d$.

Combine two theorems, and we obtain:

Theorem (Class number formula)

- If $d<0$, $L(1, \chi_d) = \frac{2\pi}{w\sqrt{|d|}} h_d$
- If $d>0$, $L(1, \chi_d) = \frac{\log \varepsilon_d}{\sqrt{d}} h_d$

(1) $h_d \geq 1 \Rightarrow L(1, \chi_d) \neq 0$

(2) $L(s, \chi_d)$ is continuous at $s=1 \Rightarrow L(1, \chi_d)$ is bounded

$\Rightarrow h_d$ is finite.

This proves that $H(\mathbb{Q}(\sqrt{d}))$ is a finite group.