Definition: An <u>integral binary quadratic form</u> is a 2-variable function:

$$Q(x,y) = ax^2 + bxy + cy^2$$

where $a, b, c \in \mathbb{Z}$.

The <u>discriminant</u> of Q is $\operatorname{dis}(Q) = b^2 - 4ac$

Some notations for a quadratic form:

$$Q(x,y) = ax^2 + bxy + cy^2$$

$$Q = [a, b, c]$$

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

The last one is due to the fact:

$$(x \ y)\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = ax^2 + bxy + cy^2.$$

In this case: $d = -4 \cdot \det\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$.

In the following, we always that d is a fundamental discriminant, that is:

either $d \equiv 1 \pmod 4$ and d square free

, or $d = 4d_0$, $d_0 \equiv 2, 3 \pmod 4$ with d_0 squarefree.

Let $Q = [a, b, c]$ a quadratic form with $\mathrm{dis}(Q) = d$.

d is a fundamental discriminant $\Rightarrow$ $ac \neq 0$.

Then $Q(x, y) = ax^2 + bxy + cy^2$

$$= \frac{1}{4a}\left((2ax + by)^2 - dy^2 \right).$$

Therefore:

(1) if $d < 0$, then $Q(x, y) \geq 0$ if $a > 0$.

$Q(x, y) \leq 0$ if $a \leq 0$

(2) if $d > 0$, then $Q(x, y)$ has positive value and negative value.

Definition: Let $Q(x, y)$ be a quadratic form.

Q is <u>positive definite</u>

if $Q(x, y) > 0$ for any $(x, y) \in \mathbb{R}^2 - \{(0, 0)\}$

is <u>negative definite</u> if $Q(x, y) \leq 0$ for any $(x, y) \in \mathbb{R}^2$.

if $Q(x, y) < 0$ for any $(x, y) \in \mathbb{R}^2 - \{(0, 0)\}$

is <u>indefinite</u> if $Q(x_0, y_0) > 0$ and $Q(x_1, y_1) < 0$ for some $(x_0, y_0) \in \mathbb{R}^2$, $(x_1, y_1) \in \mathbb{R}^2$

This implies:

(1) when $d < 0$ and $a > 0$, Q is positive definite.

(2) when $d < 0$ and $a < 0$, Q is negative definite.

(3) when $d > 0$, Q is indefinite.

Definition: The modular group, $SL_2(\mathbb{Z})$, is defined to be:

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

This is a group with matrix multiplication.

Note: $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $g^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Set ${}^t g = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, the transpose of g.

Definition: Two quadratic forms $Q_1 = \begin{pmatrix} a_1 & b_1/2 \\ b_1/2 & c_1 \end{pmatrix}$ and $Q_2 = \begin{pmatrix} a_2 & b_2/2 \\ b_2/2 & c_2 \end{pmatrix}$ are <u>equivalent</u> if we can find $g \in SL_2(\mathbb{Z})$ s.t.

$$\begin{pmatrix} a_1 & b_1/2 \\ b_1/2 & c_1 \end{pmatrix} = {}^t g \begin{pmatrix} a_2 & b_2/2 \\ b_2/2 & c_2 \end{pmatrix} g$$

We use the notation "$\sim$" for the equivalence.

Note: if $Q_1 \sim Q_2$, then $\operatorname{dis}(Q_1) = \operatorname{dis}(Q_2)$

Lemma: Every quadratic form is equivalent to some quadratic form $[a, b, c]$ satisfying:

$$|b| \leq |a| \leq |c|.$$