CONNECTIONS BETWEEN $SL_2(\mathbb{Z})$ MATRICES, QUADRATIC FORMS, AND ORDERS OF QUADRATIC FIELDS

Abstract

We investigate $SL_2(\mathbb{Z})$ matrices and look for a criterion when such matrix is conjugate to its inverse.
A correspondence is set-up between $SL_2(\mathbb{Z})$ matrices with trace t and quadratic forms with discriminant $D = t^2 - 4$. We describe an effective algorithm to find all classes of quadratic forms with a given discriminant, hence all conjugacy classes of matrices in $SL_2(\mathbb{Z})$ with the corresponding positive trace t. Moreover, the algorithm can determine if a form q is equivalent to its inverse, hence determines whether the corresponding matrix is conjugate to its inverse.
A correspondence is also set-up between $SL_2(\mathbb{Z})$ matrices with trace t, $|t| > 2$, and ideals of orders of quadratic fields, such that conjugate matrices correspond to strictly equivalent ideals. We investigate the connections between the ideal I_g corresponding to a matrix g, its conjugate I'_g, and the ideal $I_{g^{-1}}$ corresponding to g^{-1}. For matrices with trace t such that $|t| > 3$, g is conjugate to g^{-1} if and only if $I_g \sim I'_g$, and when I_g is an invertible ideal, then $I_g \not\approx I'_g$.

Contents

1. Introduction

The study of matrices, their conjugates and their inverses, goes back a long way. In this thesis we will examine the following question: When is a matrix in the modular group $SL_2(\mathbb{Z})$ conjugate to its inverse?
This question may be considered as purely arithmetical problem, interesting in its own right in the context of algebraic number theory, but has also had some recent impact on questions arising in the theory of dynamical systems. In a recent paper [PR], Polterovich and Rudnick studied "kicked systems" arising from perturbing the action of a hyperbolic element $g \in SL_2(\mathbb{Z})$ on the torus $\mathbb{R}^2/\mathbb{Z}^2$ by the action ("kicks") of elements of $SL_2(\mathbb{Z})$ having bounded trace. They showed that the resulting dynamics is "stably mixing" if and only if the matrix g is conjugate to its inverse in $SL_2(\mathbb{Z})$.
In [BR], Baake and Roberts provide classification of the symmetry and reverse symmetry group (elements by which a matrix is conjugate to itself or to its inverse, respectively) by trace values for $GL_2(\mathbb{Z})$ and $PGL_2(\mathbb{Z})$ matrices. Another recent paper by Long, describes a reduction of the conjugacy determination to the problem of solving a corresponding Pell equation (see [Long]).

The discussion in this paper is two-fold: on one hand, it formulates relations between binary integral quadratic forms and $SL_2(\mathbb{Z})$ matrices, while on the other hand it investigates the relationship between $SL_2(\mathbb{Z})$ matrices and ideals of orders in real quadratic extensions of $\mathbb{Q}$. The correspondence to quadratic forms reveals an algorithmic method by which we can effectively find out which matrices with a given trace belong to the same $SL_2(\mathbb{Z})$ conjugacy class as their inverse. This provides a deterministic tool by which specific questions about conjugacy classes of matrices, or equivalence classes of quadratic forms, can be answered.
The correspondence to ideals of orders of quadratic fields shows that for $SL_2(\mathbb{Z})$ matrices with trace t such that $|t| > 3$, a matrix that is conjugate to its inverse and corresponds to an invertible ideal, then that ideal is weakly but not strictly equivalent to its conjugate. More explicitly, a matrix $g \in SL_2(\mathbb{Z})$ with trace t such that $|t| > 2$, is conjugate to its inverse g^{-1} exactly when the corresponding ideals I_g and $I_{g^{-1}}$ are strictly equivalent, denoted $I_g \approx I_{g^{-1}}$. For a matrix g with trace t where $|t| > 3$ which is conjugate to its inverse, then we also have $I_g \sim I'_g$, and when I_g is an invertible ideal then $I_g \not\approx I'_g$.

1.1. **Quadratic Forms.** The classical theory of quadratic forms was developed by Lagrange and Gauss (see [ScOp]). A quadratic form is a function

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

where a, b and c are integers. The discriminant of a quadratic form is $D = b^2 - 4ac$. Two binary quadratic forms are called (strictly) equivalent, denoted $p \approx q$, if there exists an integral transformation $h = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ such that

$$(q \circ h)(x,y) := q((x,y)h^t) = q(\alpha x + \beta y, \gamma x + \delta y) = p(x,y)$$

When $\det h = -1$ the forms are called weakly equivalent, denoted $p \sim q$. Equivalent forms have the same discriminant. The totality of forms with discriminant D therefore falls into classes of strictly equivalent forms, and the number of classes is denoted by $H_+(D)$.

The correspondence between $SL_2(\mathbb{Z})$ matrices with trace t such that $|t| \neq 2$, to quadratic forms with discriminant D where $D = t^2 - 4$, is defined in Section 2.8 as follows:

$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \longrightarrow Q_g(x,y) = \gamma x^2 + (\delta - \alpha)xy - \beta y^2$$

$$Q(x,y) = ax^2 + bxy + cy^2 \longrightarrow g(Q) = \begin{pmatrix} \frac{-b+t}{2} & -c \\ a & \frac{b+t}{2} \end{pmatrix}$$

This correspondence guarantees that conjugate matrices correspond to equivalent forms. Simple calculation shows that for a matrix g that corresponds to form Q, the inverse matrix g^{-1} corresponds to $-Q$.

Forms can be roughly divided into **definite** forms with discriminant $D < 0$, and **indefinite** forms with $D > 0$. Matrices with trace t such that $|t| > 2$ imply that $D > 0$, i.e. correspond to indefinite forms.

The notion of **definite reduced** form can be defined for definite forms such that a single reduced form exists in each class. For definite forms, it is always true that $Q \not\approx -Q$. Section 2.3.2 uses this fact in order to find all reduced forms with a given discriminant $D < 0$, hence calculate the number of equivalence classes of such forms.

Indefinite reduced forms can also be defined, so that each indefinite form is equivalent to a reduced form.

Theorem 1. *There is an effective algorithm to reduce an indefinite form. The complexity of reducing an indefinite form $[a,b,c]$ with discriminant $D = b^2 - 4ac$ is $O(\max(1, \log(\frac{a^2}{D})))$. When $|a| < \sqrt{\frac{D}{3}}$ then the complexity is $O(1)$.*

For indefinite forms, multiple reduced forms may exist in each class. These equivalent reduced forms are related to each other in so-called chains, and each class contains a single chain. For indefinite forms it is possible that $Q \approx -Q$, implying that the corresponding matrices, which would be some matrix g and its inverse g^{-1}, are conjugates in $SL_2(\mathbb{Z})$.
For an indefinite form $Q = [a, b, c]$ with discriminant D, the complexity of determining whether $Q \approx -Q$ is bounded by $O(\log(\frac{a^2}{D}) \cdot D)$ from above.

Section 2 uses reduced forms and chain calculations, to gain the following result:

Theorem 2. *Given a trace t, $|t| \neq 2$:*

(1) *There is an effective algorithm to determine whether a given $SL_2(\mathbb{Z})$ matrix is conjugate to its inverse. Given a form Q, it can be effectively found whether $Q \approx -Q$.*
(2) *There is an effective algorithm to find representatives for $SL_2(\mathbb{Z})$ matrices with trace t. There is an effective algorithm to find all non-equivalent reduced forms with discriminant $D = t^2 - 4$. This allows to find the class number, $H_+(D)$.*
(3) *The number of classes of $SL_2(\mathbb{Z})$ matrices with trace t in which matrices are conjugate to their inverse can be effectively calculated. This is also the number of classes of forms with discriminant $D = t^2 - 4$ in which forms are equivalent to their inverse. The complexity of this algorithm is $O(D \log D)$.*

1.2. **Ideal Theory in Quadratic Fields.** The classical ideal theory was developed by Gauss and then by Dedekind.
Let K be a quadratic extension of $\mathbb{Q}$, $K = \mathbb{Q}(\sqrt{d_0})$, $d_0 \neq 0 \in \mathbb{Z}$, d_0 is square free. $\mathfrak{O}_K$ denotes the ring of integers of K, which is a Dedekind Ring. By $\mathfrak{O}_n$ we denote orders of $\mathfrak{O}_K$, where n is the index of $\mathfrak{O}_n$ in $\mathfrak{O}_K$.
As we shall see, the units of $\mathfrak{O}_K$ and $\mathfrak{O}_n$ are of special importance and in particular, the sign of the norm of the fundamental units η_1 of $\mathfrak{O}_K$ and η_n of $\mathfrak{O}_n$.
For quadratic extensions of $\mathbb{Q}$ it is not always true that unique factorization to integers exists, however there is always unique factorization to ideals. Furthermore, an equivalence relation can be defined between ideals, and it is well known that the classes of ideals of $\mathfrak{O}_K$ under this equivalence form a group. When this group has a single element,

meaning there is a single class of ideals of $\mathfrak{O}_K$, then $\mathfrak{O}_K$ has unique factorization of integers. Hence the class group can be used to "measure" the failure of unique factorization to integers.

The unit element in the class group of $\mathfrak{O}_K$ is the class of all principal ideals, meaning the ideals that are created via a single element. Each ideal I of $\mathfrak{O}_K$ belongs to a class C_I in the class group of $\mathfrak{O}_K$, and has an inverse ideal I^{-1}, which resides in the inverse class $C_I^{-1} = C_{I^{-1}}$, so that $I \cdot I^{-1}$ is a principal ideal.

When turning to $\mathfrak{O}_n$ the situation is somewhat more complicated. Not all ideals of $\mathfrak{O}_n$ are invertible, but only those which contain an element α such that $(N(\alpha), n) = 1$. This creates a more complex situation, where classes of ideals do not necessarily form a group anymore.

Usually weak equivalence between ideals is used. In order to use strict equivalence a new concept is needed - an ordered ideal. An ideal $I = [\alpha, \beta]$ is called ordered when $\Delta_{K/\mathbb{Q}}(\alpha, \beta) = \alpha\beta' - \beta\alpha' > 0$ holds. This also effects the definition of ideal equivalence: for ideals I, J of an integral domain $\mathfrak{O}$, $I \sim J$ meant that there exist $\zeta_1, \zeta_2 \in \mathfrak{O}$ such that $\zeta_1 I = \zeta_2 J$. Now for strict equivalence $I \approx J$ it is also required that $N(\zeta_1\zeta_2) > 0$.

A correspondence can be set-up between $SL_2(\mathbb{Z})$ matrices with trace t and ordered ideals of an integral domain $\mathfrak{O}$ of a quadratic field, such that an eigenvalue λ of the matrix generates $\mathfrak{O}$ over $\mathbb{Z}$, meaning $\mathfrak{O} = \mathbb{Z}[\lambda]$. An alternative way to obtain $\mathfrak{O}$ is by looking at $D = t^2 - 4 = n^2 \cdot d$, where d is a field discriminant of the field $K = \mathbb{Q}(d_0)$ ($d_0 = d$ when $d \equiv 1 \pmod 4$, $d_0 = d/4$ when $d \equiv 0 \pmod 4$), then we have $\mathfrak{O} = \mathfrak{O}_n \subseteq \mathfrak{O}_K$.

The exact correspondence is as follows: Let $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$. The corresponding ideal is

$$I_g = [v_1, v_2] = \begin{cases} [\gamma, \frac{(\delta-\alpha)-n\sqrt{d}}{2}] & \text{when } \gamma > 0 \\ [\gamma\sqrt{d}, \frac{(\delta-\alpha)-n\sqrt{d}}{2}\sqrt{d}] & \text{when } \gamma < 0 \end{cases} \tag{1}$$

This is an $\mathfrak{O}_n$ ideal with an ordered basis. For a conjugate matrix hgh^{-1}, $h \in SL_2(\mathbb{Z})$, the corresponding ideal is received by $(v_1, v_2)h^{-1}$, which is also an $\mathfrak{O}_n$ ordered ideal.

Conversely, for an ordered ideal $I = [v_1, v_2]$ there is a corresponding matrix $g(I) \in SL_2(\mathbb{Z})$ such that for $J = [w_1, w_2]$, where $(w_1, w_2) = (v_1, v_2) \circ h$, $h \in SL_2(\mathbb{Z})$ the corresponding matrix is $h^{-1}gh$.

The main result of Section 4 is as follows:

Theorem 3. *Let $g \in SL_2(\mathbb{Z})$ with trace t such that $|t| > 2$, and an eigenvalue λ. Denote $D = t^2 - 4 = n^2 d > 0$, where d is a field discriminant. Let K denote the quadratic field with discriminant d. Then:*

- *The following are equivalent:*
  1. *g is conjugate to its inverse g^{-1} (there exists a matrix $h \in SL_2(\mathbb{Z})$ such that $g^{-1} = hgh^{-1}$).*
  2. *The corresponding forms Q_g and $Q_{g^{-1}} = -Q_g$ (with discriminant D) are strictly equivalent: $Q_g \approx -Q_g$.*
  3. *The ideal $J(g)$ in the order $\mathbb{Z}[\lambda] = \mathfrak{O}_n$ of $\mathfrak{O}_K$, is strictly equivalent to $J(g^{-1})$: $J(g) \approx J(g^{-1})$.*
  4. *The ideal $J(g)$ in the order $\mathbb{Z}[\lambda] = \mathfrak{O}_n$ of $\mathfrak{O}_K$, is weakly equivalent to $J(g)'$: $J(g) \sim J(g)'$.*

     Let η be the fundamental unit of the order $\mathbb{Z}[\lambda]$. Then we have

$$\begin{cases} J(g) \approx J(g)' & \text{if } N(\eta) < 0 \\ J(g) \not\approx J(g)' & \text{if } N(\eta) > 0, J(g) \text{ is invertible} \end{cases}$$

- *The norm of the fundamental unit of the order $\mathbb{Z}[\lambda]$ is negative for $|t| = 3$, and is always positive for $|t| > 3$. This implies that for a matrix g with $|\operatorname{tr}(g)| > 3$ for which g is conjugate to g^{-1} in $SL_2(\mathbb{Z})$ then always $J(g) \sim J(g)'$. When $J(g)$ is an invertible ideal of $\mathbb{Z}[\lambda]$, then $J(g) \not\approx J(g)'$.*

2. Integral Binary Quadratic Forms

This section provides an exposition of the classical theory of quadratic forms. We freely quote from [Di] and [Lan].

Definition 1. *Let a, b, c be constant integers, x, y are independent variables. The function $q(x,y) = ax^2 + bxy + cy^2$ is called a* **binary quadratic form,** or, in brevity, a form, and is also written: $q = [a, b, c]$. The **discriminant** of the form is the number $D = b^2 - 4ac$.

It is always true that $D \equiv 0$ or 1 (mod 4).

Lemma 1. *There exists an integral factorization for q exactly when D is a perfect square.*

Proof. Let $R = \sqrt{D} = \sqrt{b^2 - 4ac}$.

$$\begin{aligned} q(x,y) &= ax^2 + bxy + cy^2 \\ 4aq(x,y) &= 4a^2x^2 + 4abxy + 4acy^2 = \\ &= (2ax + by)^2 + y^2(-(b^2 - 4ac)) = \\ &= (2ax + by)^2 - y^2R^2 = \qquad (2) \\ &= (2ax + (b+R)y)(2ax + (b-R)y) \end{aligned}$$

We need to show this is an integral factorization when D is a perfect square, meaning $R \in \mathbb{Z}$. b and D are of the same parity, therefore also b and R are of the same parity, and $\frac{b+R}{2}, \frac{b-R}{2} \in \mathbb{Z}$. We have:
$4ac = b^2 - D = b^2 - R^2 = (b+R)(b-R)$
$ac = \frac{b+R}{2} * \frac{b-R}{2}$
Let $a = a_1a_2$, such that $a_1 | \frac{b+R}{2}$ and $a_2 | \frac{b-R}{2}$, and so:

$$q(x,y) = (\frac{2a}{2a_1}x + \frac{b+R}{2a_1}y)(\frac{2a}{2a_2}x + \frac{b-R}{2a_2}y)$$

is an integral factorization of q.
In the other direction, if we have $q(x,y) = ax^2 + bxy + cy^2 = (rx + sy)(tx + uy)$ where r,s,t,u are integers, then $D = b^2 - 4ac = (ru + st)^2 - 4(rt)(su) = (ru - st)^2$. □

From now on, let D be non square, and $\equiv 0$ or 1 (mod 4). Consequently, for each form having discriminant D we certainly have $a \neq 0$ and $c \neq 0$.

2.1. **Classes of Forms.** Binary quadratic forms are called **properly equivalent** (or strictly equivalent) and denoted $p \approx q$ if there exists an integral transformation $h = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ with $\det h = 1$ such that

$$(q \circ h)(x,y) := q((x,y)h^t) = q((x,y)\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}) = q(\alpha x + \beta y, \gamma x + \delta y) = p(x,y)$$

We say: q goes into p by the matrix h.
When $\det h = -1$ the forms are called **weakly equivalent,** denoted $p \sim q$.

Lemma 2. *Reflexivity, symmetry and transitivity of strict and weak form equivalence.*

Proof. (1) Reflexivity: $q \approx q$; for q goes into q by the unit matrix, which has determinant 1.

(2) Symmetry: When $q(x,y) = p(\alpha x + \beta y, \gamma x + \delta y)$ then we also have $p(x,y) = q(\delta x - \beta y, -\gamma x + \alpha y)$, and the corresponding matrices have the same determinant.

(3) Transitivity: When q goes into p by $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ and p goes into r by $\begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix}$ then q goes into r by the product matrix

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix} = \begin{pmatrix} \alpha\alpha_1 + \beta\gamma_1 & \alpha\beta_1 + \beta\delta_1 \\ \gamma\alpha_1 + \delta\gamma_1 & \gamma\beta_1 + \delta\delta_1 \end{pmatrix}$$

With the appropriate determinant (+1 if both original matrices have determinant +1, ±1 if the original matrices have determinant ±1).

□

Lemma 3. *Properly or weakly equivalent forms always have the same discriminant.*

Proof. Let $q(x,y) = ax^2 + bxy + cy^2$, $Q(x,y) = Ax^2 + Bxy + Cy^2$, and $q(\alpha x + \beta y, \gamma x + \delta y) = Q(x,y)$.
By evaluating $q(\alpha x + \beta y, \gamma x + \delta y) = Ax^2 + Bxy + Cy^2$ we have the **Coefficient Transformation Formula:**

$$\begin{cases} A = a\alpha^2 + b\alpha\gamma + c\gamma^2, \\ B = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, \\ C = a\beta^2 + b\beta\delta + c\delta^2 \end{cases} \tag{3}$$

The discriminant of Q is then $B^2 - 4AC = (b^2 - 4ac)(\alpha\delta - \beta\gamma)^2$. As q is properly or weakly equivalent to Q, then $(\alpha\delta - \beta\gamma)^2 = 1$, therefore the discriminant of q equals the discriminant of Q. □

The totality of forms with discriminant D therefore fall into classes of properly equivalent forms, the class number is denoted $H_+(D)$.
A form q is said to **represent** an integer A if there exist integers x and y such that $q(x,y)$ =A. Equivalent forms represent the same integers, as $q(x,y) = Q(\alpha x + \beta y, \gamma x + \delta y)$ and $Q(x,y) = q(\delta x - \beta y, -\gamma x + \alpha y)$.

2.2. **Definite and Indefinite Forms.** We saw earlier in (2) that for $q = [a,b,c]$:

$$4aq(x,y) = (2ax+by)^2 + y^2(-(b^2-4ac)) = (2ax+by)^2 + y^2(-D)$$

For $D < 0$, $4aq(x,y)$ is always positive, and therefore the sign of $q(x,y)$ is dependent only on the sign of a, and not on the values of x and y.

- A form with $D < 0$ and $a > 0$, takes positive values for all x and y not both zero, and is called a **positive form.**
- A form with $D < 0$ and $a < 0$, takes negative values for all x and y not both zero, and is called a **negative form.**
- A form with $D < 0$ is called a **definite form** and is always either negative or positive.
- A form with $D > 0$ takes both positive and negative values and is called an **indefinite form.**

A Positive form can be equivalent only to positive forms, a negative form can be equivalent only to negative forms. This implies that for $q = [a,b,c]$ with $D < 0$, all equivalent forms $Q = [A,B,C]$ must have sign(A)=sign(a).

2.3. **Definite Forms.** A definite form is a form $[a,b,c]$ with discriminant $D = b^2 - 4ac < 0$, and is either a positive form with $a > 0$ or a negative form with $a < 0$. It suffices to explore the properties of positive forms, as the properties of negative forms follow immediately.

2.3.1. *Positive Reduced Forms.*

Definition 2. *A positive definite form is called* **reduced** if $-a < b \leq a$, $c \geq a$ and $b \geq 0$ if $c = a$.

Theorem 4. (1) *Every positive form is equivalent to a reduced form.*
(2) *No two positive reduced forms are equivalent.*

Proof. (1) Fix a form $q = [a,b,c]$. Let A be the smallest positive number, which is representable by q. Then we have

$$A = q(\alpha, \gamma) = a\alpha^2 + b\alpha\gamma + c\gamma^2$$

for suitable α and γ. We certainly have $(\alpha,\gamma) = 1$, for otherwise $\frac{A}{(\alpha,\gamma)^2}$ would be representable and smaller than A. We can therefore find numbers β and δ such that $\alpha\delta - \beta\gamma = 1$. By the

Coefficient Transformation Formula (in (3) above) the transformation $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ takes $[a, b, c]$ to $[A, b', c']$. The transformation $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ with determinant 1, takes $[A, b', c']$ to $Q = [A, B, C]$ where $B = 2Ah + b'$. We can choose an integer h so that $-A \leq B \leq A$. Since C is the value for Q when $x = 0$, $y = 1$, it is representable by the equivalent form q, hence C is not less than the minimum A of q. In case C=A, if $B < 0$ we can use the transformation $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ with determinant 1 to replace Q with $[A, -B, A]$.

(2) Let $q = [a, b, c]$ be equivalent to $Q = [A, B, C]$, both reduced. We need to show $q = Q$. We have

$$\begin{array}{llll} -a < b \leq a, & c \geq a & and & b \geq 0 \quad if \quad c = a \\ -A < B \leq A, & C \geq A & and & B \geq 0 \quad if \quad C = A \end{array}$$

We may take $a \geq A$. $q \approx Q$ so there is an integral transformation of determinant unity such that

$$Q(x, y) = q(\alpha x + \beta y, \gamma x + \delta y)$$

and the Coefficient Transformation Formula (in (3) above) holds. Since $(\alpha \pm \gamma)^2 \geq 0$, then $\alpha^2 + \gamma^2 \geq 2|\alpha\gamma|$. Hence

$$A = a\alpha^2 + b\alpha\gamma + c\gamma^2 \geq a\alpha^2 - a|\alpha\gamma| + a\gamma^2 \geq a|\alpha\gamma|$$

$$1 \geq \frac{A}{a} \geq |\alpha\gamma|$$

But α and γ are integers, so either $\alpha = 0$ or $\gamma = 0$.

$$a \geq A = a\alpha^2 + b\alpha\gamma + c\gamma^2 = a\alpha^2 + c\gamma^2 \geq a\alpha^2 + a\gamma^2 \geq a$$

So it must be that $A = a$. Now we have 2 cases: either one of $c > a$ or $C > A$ holds, or $c = a$ and $C = A$. First let one of $c > a$ or $C > A$ hold. By interchanging q and Q if necessary, we may take $c > a$ without disturbing $a = A$.

If $\gamma \neq 0$ then $c\gamma^2 > a\gamma^2$. Similarly to above:

$$A = a\alpha^2 + b\alpha\gamma + c\gamma^2 > a\alpha^2 - a|\alpha\gamma| + a\gamma^2 \geq a|\alpha\gamma|$$

$$1 = \frac{A}{a} > |\alpha\gamma|$$

Thus $|\alpha\gamma| = 0$, $\alpha = 0$, $a = A = c\gamma^2 \geq c$. This is a contradiction, hence $\gamma = 0$. By $\alpha\delta - \beta\gamma = 1$ we have $\alpha\delta = 1$, $\alpha = \delta = \pm 1$. By the Coefficient Transformation Formula (in (3) above):

$$B = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta = 2a\alpha\beta + b(1 + 0) + 0$$

$$B - b = 2a\alpha\beta$$

We know that $-a < b \leq a$, $-A < B \leq A$, $a \geq A$, so $|B - b| \leq 2a$, $|\beta| \leq 1$. If $|\beta| = 1$ then $|B - b| = 2a$, and so one of b and B is a and the other is $-a$. But as both forms are reduced we cannot have $b = -a$ nor $B = -A$, so $\beta = 0$, $b = B$, therefore also $c = C$ and then $q = Q$.
Second, let $c = a$, $C = A$. Then $b = \pm\sqrt{D + 4ac} = \pm\sqrt{D + 4AC}$, but only positive values are possible for b (B) in a reduced form with $a = c$ ($A = C$), therefore $q = Q$.

□

All positive reduced forms must have $a \leq c$ and $b \leq a$, therefore they also satisfy:

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

$$3a^2 \leq -D$$

Positive forms always have $D < 0$ and $a > 0$, and so we conclude:

$$a \leq \sqrt{\frac{-D}{3}}$$

There is a finite number of possible combinations where $|b| \leq a \leq \sqrt{\frac{-D}{3}}$ (and c can be calculated given a, b and D), and so this shows that there is a finite number of positive reduced forms for a fixed discriminant D. We conclude that the class number for positive forms is finite, and there is a single reduced form in each class. Finding all positive reduced forms presents a way to calculate the number of classes of positive forms with a given negative discriminant D. The correspondence between positive and negative forms allows us to calculate the class number $H_+(D)$ for all definite forms, positive and negative.

2.3.2. *An Algorithm to Find All Positive Reduced Forms.* Let L be the largest integer $\leq \sqrt{\frac{-D}{3}}$. $-D \equiv 0$ or $3 \pmod 4$, and from this we can conclude the parity of b (b is even if $-D \equiv 0 \pmod 4$, odd otherwise). $|b|$ is between 0 to L. For each such integer b, $ac = \frac{b^2+D}{4}$ is an integer. Consider every a such that $|b| \leq a \leq L$, check if $4a$ divides $b^2 + D$. For such a, we then have $c = \frac{b^2+D}{4a}$, make sure $c \geq a \geq |b|$. When b is negative, omit cases where $c = a$ or $a = -b$.
Clearly, the number of required steps is $< 2D$.

Proposition 1. *The complexity of this algorithm is $O(D)$.*

In order to calculate $H_+(D)$ for $D < 0$, the algorithm can be used to find the number of reduced positive forms, and then multiply it by 2, as for each positive reduced [a,b,c], [-a,b,-c] is a representative of a different class of negative forms.

Remark: The above use of the reduction theory gives a bound of $H_+(D) = O(D)$. However, Dirichlet's Class Number formula gives $H_+(D) = O(\sqrt{D} \cdot logD)$, which one assumes to be the correct exponent of D.

2.4. **Indefinite Forms.** An indefinite reduced form is a form $q = [a, b, c]$ with discriminant $D = b^2 - 4ac > 0$. Let R denote the positive square root of D. Now, $x - \omega y$ is a factor of q if and only if

$$a\omega^2 + b\omega + c = 0$$

Its first and second roots are respectively

$$f = \frac{R - b}{2a}, \quad s = \frac{-R - b}{2a} \tag{4}$$

2.4.1. *Indefinite Reduced Forms.*

Definition 3. *An indefinite form is called* **reduced** when

$$0 < R - b < 2|a| < R + b$$

or, equivalently, when $|f| = |\frac{R-b}{2a}| < 1$, $|s| = |\frac{-R-b}{2a}| > 1$, and $fs = (\frac{R-b}{2a})(\frac{-R-b}{2a}) < 0$.

Note that f has the same sign as a, and c the opposite sign, since for a reduced form $4ac = b^2 - R^2 = -(R - b)(R + b) < 0$. For an indefinite reduced form it holds that $0 < b < R$.

Lemma 4. *If one of* $[a, b, c]$ *and* $[c, b, a]$ *is reduced, the other is reduced.*

Proof. In view of $(R - b)(R + b) = 4|ac|$, a can be replaced in $0 < R - b < 2|a| < R + b$ so we have $0 < R - b < 2|c| < R + b$. □

Lemma 5. *Every indefinite form is equivalent to a form* $[a, b, c]$ *in which* $|b| \leq |a| \leq \sqrt{\frac{D}{3}}$.

Proof. We first show how to secure the second inequality. If $|a| > \sqrt{\frac{D}{3}}$ in a given [a,b,c], we apply the transformation $\begin{pmatrix} h & 1 \\ -1 & 0 \end{pmatrix}$ with determinant unity and obtain $[a_1, b_1, a]$, where by the Coefficient Transformation Formula (in (3) above)) $b_1 = 2ah + b(-1) + 0 = 2ah - b$. We choose an integer h such that $|b_1| \leq |a|$. Then

$$4a_1a = b_1^2 - D < b_1^2 \leq a^2$$

$$-4a_1a = D - b_1^2 \leq D < 3a^2$$

(by our assumption $\sqrt{\frac{D}{3}} < |a|$). Hence $4|a_1a| < 3a^2$, $|a_1| < \frac{3}{4}|a|$.

If $|a_1| > \sqrt{\frac{D}{3}}$, we repeat the process and obtain an equivalent form $[a_2, b_2, a_1]$, having $|a_2| < \frac{3}{4}|a_1| < (\frac{3}{4})^2|a|$. Since $(\frac{3}{4})^n$ may be made as small as we please by taking n sufficiently large, we ultimately obtain an equivalent form $[a', b', c']$ in which $|a'| \leq \sqrt{\frac{D}{3}}$, sufficing the second inequality. Now we still need to secure the first inequality. Replacing x by $x + ky$, using the matrix $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, we obtain $[a', B, C]$ where $B = b' + 2ka'$ (by the Coefficient Transformation Formula). We can choose an integer k such that $|B| \leq |a'|$. □

Theorem 5. *Every indefinite form is equivalent to a reduced form.*

Proof. By the above lemma we may assume that $b^2 \leq \frac{D}{3}$, but we make use only of $b^2 \leq D$. Then $4|ac| = D - b^2 \leq D$, whence not both $2|a|$ and $2|c|$ are $> R$, when R denotes the positive square root of D. If necessary we use the transformation $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and we have $2|c| \leq R$. Also, $c \neq 0$ as D is not a perfect square. In $[a, b, c]$ replace y by $y - kx$, where $k \in \mathbb{Z}$. We get $[a', b', c]$, where $b - b' = 2kc$, where k is an integer. We can choose k so that $R - 2|c| \leq b' \leq R$. Therefore we have $0 \leq R - b' \leq 2|c| \leq R + b'$. None of the signs can be =, as D is not a perfect square. We have $0 < R - b' < 2|c| < R + b'$ and so $[c, b', a']$ is reduced. By a previous theorem $[a', b', c]$ is also reduced. □

Proposition 2. *The complexity of reducing an indefinite form $[a, b, c]$ with $D = b^2 - 4ac$ is $O(\max(1, \log(\frac{a^2}{D})))$. When $|a| < \sqrt{\frac{D}{3}}$ then the complexity is $O(1)$.*

Proof. Given a definite form $[a, b, c]$, then by Lemma 5 and Theorem 5 above the steps for its reduction are:

(1) Find $h \in \mathbb{Z}$ such that $|2ah - b| \leq |a|$. Using h we find an equivalent form $[a_1, b_1, c_1]$. Complexity is $O(1)$.

(2) If $|a_1| > \sqrt{\frac{D}{3}}$, we repeat the process till $|a_n| \leq \sqrt{\frac{D}{3}}$. By Lemma 5, the number of steps n should satisfy:

$$|a_n| < (\frac{3}{4})^n|a| \leq \sqrt{\frac{D}{3}}$$

$$n \leq log_{\frac{3}{4}}\sqrt{\frac{D}{3a^2}}$$

The complexity of this step is $O(log\frac{a^2}{D})$. At the end of this process we have an equivalent form $[a', b', c']$ where $|a'| \leq \sqrt{\frac{D}{3}}$.

(3) Find $k \in \mathbb{Z}$ such that $|b' - 2ka'| \leq |a'|$, the complexity is $O(1)$. Using k we find an equivalent form $[a'', b'', c'']$.

(4) By Theorem 5, we find $l \in \mathbb{Z}$ such that $\sqrt{D} - 2|c''| \leq b'' - 2lc'' \leq \sqrt{D}$. The complexity of this step is $O(1)$.

Hence, the overall complexity of reducing an indefinite form $[a, b, c]$ is $O(\max(1, log\frac{a^2}{D}))$.

□

2.4.2. *Chains of Equivalent Indefinite Reduced Forms.* It is possible that different indefinite reduced forms would be equivalent, and then they form a chain of such forms. Every element in a chain has a left neighbor and a right neighbor within the chain. The right neighbor of $[a, b, a_1]$ is $[a_1, b_1, a_2]$, where

$$b_1 = -b - 2\delta a_1 \tag{5}$$

and is received using the transformation

$$\begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix} \tag{6}$$

where δ is chosen so that $[a_1, b_1, a_2]$ is reduced.

For example, take the form [-2,1,2] with discriminant 17. Its right neighbor is $[2, b_1, a_2] = [2, -1 - 2\delta \cdot 2, a_2]$. δ should be selected to satisfy definition 3:

$$0 < R - b < 2|a| < R + b$$

$$0 < \sqrt{1}7 - (-1 - 4\delta) < 4 < \sqrt{1}7 + (-1 - 4\delta)$$

Therefore $\delta = -1$, $b_1 = 3$, and we find a_2 by discriminant calculation: $3^2 - 4 \cdot 2 \cdot a_2 = 17$, $a_2 = -1$, and so the right neighbor of [-2,1,2] is [2, 3, -1].

Lemma 6. *Each indefinite reduced form $q = [a, b, a_1]$ has exactly one reduced, right neighbor.*

Proof. Let $f = \frac{R-b}{2a}$, let $|\delta|$ denote the largest integer $< \frac{1}{|f|}$, and δ has the same sign as f and a, hence opposite sign to a_1. The form is reduced so we have $0 < R - b < 2|a| < R + b$, so $|f| < 1$, and $|\delta| > 0$. The right neighbor of $[a, b, a_1]$ is $q_1 = [a_1, b_1, a_2]$ where $b_1 = -b - 2\delta a_1$ and by the discriminant we can find that $a_2 = D^2 a_1 + b\delta + a$. We need to show this form is reduced, we will use the second definition and show:

$$|f_1| = |\frac{R-b_1}{2a_1}| < 1,\ |s_1| = |\frac{-R-b_1}{2a_1}| > 1,\ f_1 s_1 = (\frac{R-b_1}{2a_1})(\frac{-R-b_1}{2a_1}) < 0$$

The first root f_1 of the form q_1 is:

$f_1 = \frac{R-b_1}{2a_1} = \frac{R-(-b-2\delta a_1)}{2a_1} = (\frac{R+b}{2a_1})(\frac{R-b}{R-b})+\delta = \frac{R^2-b^2}{2a_1(R-b)}+\delta = \frac{D-b^2}{2a_1(R-b)}+\delta = \frac{-4aa_1}{2a_1(R-b)} + \delta = \frac{-2a}{R-b} + \delta = -\frac{1}{f} + \delta$

Hence f_1 is numerically < 1, and has the opposite sign to δ and f. The second root s_1 of q_1 is:

$s_1 = \frac{-R-b_1}{2a_1} = \frac{-R-(-b-2\delta a_1)}{2a_1} = (\frac{-R+b}{2a_1})(\frac{b+R}{b+R}) + \delta = \frac{-D+b^2}{2a_1(b+R)} + \delta = \frac{4aa_1}{2a_1(b+R)} + \delta = \frac{2a}{b+R} + \delta = -\frac{1}{s} + \delta$

Since the sign of s is opposite to that of f and δ, s_1 has the same sign as δ (assuring $f_1 s_1 < 0$) and is numerically > 1. Hence q_1 is a reduced form.
Moreover, q_1 is reduced only when δ is chosen as indicated. For, if q and q_1 are reduced, f_1 has the same sign as a_1, and f has a sign opposite to a_1. Thus $|f| < 1$, $|f_1| < 1$, and $F = -\frac{1}{f} + \delta$ requires that δ be of same sign as f and that $|\delta|$ be the largest integer $< \frac{1}{|f|}$. □

Lemma 7. *Each indefinite reduced form $q = [a, b, a_1]$ has exactly one reduced, left neighbor.*

Proof. If $[a, b, a_1]$ is reduced, then $[a_1, b, a]$ is also reduced. It has a unique reduced, right neighboring form $[a, l, m]$, with $l = -b + 2\delta a$. Hence the reduced form $[m, l, a]$ has $[a, b, a_1]$ as a right neighboring form, with $b = -l + 2\delta a$. □

Let Φ_0 be any reduced form. Let Φ_1 and Φ_{-1} be its unique reduced left and right neighboring forms. In this manner we obtain a chain of equivalent, reduced forms:

$$...,\Phi_{-2},\Phi_{-1},\Phi_0,\Phi_1,\Phi_2,... \tag{7}$$

An example of a chain of reduced forms: for discriminant 221 the following chain can be found: $\Phi_0 = [7, 9, -5]$, $\Phi_1 = [-5, 11, 5]$, $\Phi_2 = [5, 9, -7]$, $\Phi_3 = [-7, 5, 7]$, with $\delta_0 = 2$ to find Φ_1 from Φ_0, $\delta_1 = -2$, $\delta_2 = 1$, and $\delta_3 = -1$ to find the right neighbor of Φ_3 which is is again Φ_0.

2.4.3. *An Algorithm to Find All Indefinite Reduced Forms.* $D \equiv 0$ or 1 (mod 4), and from this we can conclude the parity of b (b is even when D ≡0 (mod 4), odd otherwise). $0 < b < R = \sqrt{D}$. For each such integer b, $|ac| = \frac{D-b^2}{4}$ is an integer. For each a such that $\frac{R-b}{2} \leq a \leq \frac{R+b}{2}$, check if $c = \frac{D-b^2}{4a}$ is an integer. This ensures that also $\frac{R-b}{2} \leq c \leq \frac{R+b}{2}$. Prefix opposite signs to the factors a and c that were found. This leads to a finite number of reduced forms. Consider only a single form of every chain. There is a finite number of elements in each chain, as the total number of reduced forms is finite.

Proposition 3. *The complexity of this algorithm is $O(D \cdot logD)$.*

Proof. In order to find all reduced forms $O(D)$ operations are needed. For each $0 < b < \sqrt{D}$, $O(b)$ forms may be found. As $b \sim \sqrt{D}$, the total number of forms found for a given discriminant D is $O(\sqrt{D}) \cdot O(\sqrt{D}) = O(D)$. In order to ignore reduced forms which are in the same chain $O(D^2)$ operations are needed, as for each reduced form its right neighbor is calculated and must be searched among all other reduced forms. This complexity can be improved to $O(D \cdot logD)$ by using a data structure in which the forms are kept sorted. Thus searching for a right neighbor of a form among all other reduced forms requires $O(logD)$ operations, yielding total of $O(DlogD)$ operations when searching for all $O(D)$ forms. □

Remark: Dirichlet's class number formula gives a bound of $h(D) = O(\sqrt{D})$. It is a conjecture of Gauss that $h(D) = 1$ infinitely often for $D > 0$.

Corollary 1. *Given an indefinite form $Q = [a, b, c]$ with discriminant $D = b^2 - 4ac > 0$, the complexity of determining whether $Q \approx -Q$ is bounded by $O(\log(\frac{a^2}{D}) \cdot D)$ from above.*

Proof. In order to determine whether $Q \approx -Q$, Q is reduced to q, $-Q$ is reduced to q', then we check if q and q' are in the same chain of reduced forms.
By Proposition 2, the complexity of reducing Q (or $-Q$) is $O(\log(\frac{a^2}{D}))$. Finding the right neighbor of a form q has complexity $O(1)$ (see (5)). By proposition 3 the total number of reduced forms for a given discriminant D is $O(D)$. Hence the complexity of checking whether the reduced forms q and q' are in the same chain is at most $O(D)$, and we conclude the total complexity is bounded from above by $O(\log(\frac{a^2}{D}) \cdot D)$. □

2.5. **Indefinite Reduced Forms and Continued Fractions.** Purely periodic continued fractions are precisely the real (irrational) roots w

of a quadratic equation that satisfies

$$w > 1, -1 < w' < 0$$

Recall that for a quadratic form $Q = [a, b, c]$ with $D = b^2 - 4ac > 0$, we have defined (in (4)): $f = \frac{-b+R}{2a}$, $s = \frac{-b-R}{2a}$, where R denotes the positive square root of D. By Definition 3, a form Q is reduced when $|f| < 1$, $|s| > 1$ and $fs < 0$, or, more explicitly, when:

$$0 < f < 1,\ s < -1 \quad \text{or} \quad 0 > f > -1,\ s > 1$$

Following (7), it is convenient to write

$$\Phi_i = [(-1)^i A_i, B_i, (-1)^{i+1} A_{i+1}] \tag{8}$$

Let transformation (6) with $\delta = \delta_i$ replace Φ_i by Φ_{i+1}, then by (5) we have

$$B_i + B_{i+1} = 2g_i A_{i+1},\ g_i = (-1)^i \delta_i \tag{9}$$

Since the chain (7) is determined by any one of its members, we may choose Φ_0 so that A_0 is positive. Then A_i, B_i, g_i are positive for every i. Let f_i and s_i denote f and s for Φ_i.

In general, for a form $q_{i+1} = [a_{i+1}, b_{i+1}, c_{i+1}]$ related to $q_i = [a_i, b_i, c_i]$ by the transformation

$$x_{i+1} = \alpha x_i + \beta y_i,\ \ y_{i+1} = \gamma x_i + \delta y_i,\ \ \alpha\delta - \beta\gamma = 1$$

the first roots f_i of q_i and f_{i+1} of q_{i+1} and the second roots s_i and s_{i+1} are related by

$$f_{i+1} = \frac{\alpha f_i + \beta}{\gamma f_i + \delta},\ \ s_{i+1} = \frac{\alpha s_i + \beta}{\gamma s_i + \delta} \tag{10}$$

For a complete proof see [Di]. In the case of neighboring forms, the transformation is

$$x_{i+1} = y_i,\ \ y_{i+1} = -x_i + \delta y_i$$

hence we have

$$f_{i+1} = \delta - \frac{1}{f_i},\ \ s_{i+1} = \delta - \frac{1}{s_i} \tag{11}$$

Denote:

$$F_i = \frac{(-1)^i}{f_i},\ \ S_i = \frac{(-1)^{i+1}}{s_i} \tag{12}$$

Using (11) we have:

$$F_i = \frac{R + B_i}{2A_{i+1}},\ \ S_i = \frac{R - B_i}{2A_{i+1}} \tag{13}$$

Note that using F_i and S_i instead of f and s, we can guarantee that $F_i > 1,\ \ 0 < S_i < 1$.
By multiplying (11) by $(-1)^i$ we have

$$F_i = g_i + \frac{1}{F_{i+1}}, \quad \frac{1}{S_i} = g_{i-1} + S_{i-1}$$

after the subscripts of the second are reduced by one.
For example, for $D = 221$ as in the example in section 2.4.2, $g_0 = 2$, $g_1 = 2$,$g_2 = 1$, $g_3 = 1$, $\Phi_4 = \Phi_0$, whence

$$F_0 = 2 + \frac{1}{F_1}, \ \ F_1 = 2 + \frac{1}{F_2}, \ \ F_2 = 1 + \frac{1}{F_3}, \ \ F_3 = 1 + \frac{1}{F_1}$$

or, $F_0 = [\overline{2, 2, 1, 1}]$, the first root of $\Phi_0 = [7, 9, -5]$ is $f_0 = \frac{1}{F_0} = [0, \overline{2, 2, 1, 1}]$. We easily see that, for example, $F_1 = [\overline{2, 1, 1, 2}] = \frac{-1}{f_1}$, where f_1 is the first root of $\Phi_1 = [-5, 11, 5]$. Similarly, $F_2 = [\overline{1, 1, 2, 2}] = \frac{1}{f_2}$, and $F_3 = [\overline{1, 2, 2, 1}] = \frac{-1}{f_3}$.

In general, recalling that the F_i come from a cycle of period n we obtain the continued fraction expansion

$$F_i = [\overline{g_i, ..., g_n, g_1, ..., g_{i-1}}]$$

Corollary 2. *A quadratic form $q = [a, b, c]$ with a first root $f = \frac{\sqrt{D}-b}{2a}$ is a reduced form if and only if $F = (sign(a))\frac{1}{f}$ is a purely periodic continued fraction.*

Corollary 3. (1) *Let Φ_0, Φ_1, ... be a chain of n indefinite reduced forms, with δ_i used in transformation (6) to replace Φ_i by Φ_{i+1}, and such that the first coefficient of Φ_0, $A_0 > 0$. Then the periodic continued fractions of F_i are consecutive "shifts" of the same digits cycle, so that for $F_i = [\overline{x_1, ...x_n}]$ then $F_{i+1} = [\overline{x_2, ...x_n, x_1}]$.*
(2) *The opposite is also true, for a reduced indefinite quadratic form $q = [a, b, c]$, if $F_q = [\overline{x_1, ...x_n}] = (\mathrm{sign}(a))\frac{1}{f}$, then Q, the right neighbor of q, has $F_Q = [\overline{x_2, ...x_n, x_1}]$, and there are exactly n reduced forms in the chain of q.*

2.6. **Primitive Forms and Inverse Forms.**

2.6.1. *Primitive Forms and $h_+(D)$.* Recall that Class Number of properly equivalent binary quadratic forms with discriminant D is denoted $H_+(D)$.

Definition 4. *A form [a,b,c] is called* **primitive** if gcd(a,b,c)=1, otherwise it is called **imprimitive.**

When $gcd(a,b,c) = g > 1$ then $g^2 \mid D$ and the form $[\frac{a}{g}, \frac{b}{g}, \frac{c}{g}]$ is a primitive integral form with discriminant $\frac{D}{g^2}$.
Denote the class number of properly equivalent primitive binary forms with discriminant D by $h_+(D)$. Then $H_+(D) = \sum_{g^2|D,\, g>0} h_+(\frac{D}{g^2})$.
Note that when $D = 4d_0$ such that $d_0 \equiv 2$ or 3 (mod 4) and is square free, then d_0 is not a discriminant, therefore $h_+(d_0) = 0$ and $H_+(D) = h_+(D)$.

2.6.2. *Inverse Forms and $I(D)$.* For a form Q=[a,b,c], we introduce its **inverse** -Q=[-a,-b,-c]. (The reason for this arises from the correspondence to matrices, described in section 2.8.2). When $q \approx Q$, then by the Coefficient Transformation Formula (in (3)) also $-q \approx -Q$. Therefore, if a form q is equivalent to its inverse $-q$, then for any other form Q which is in the same class as q, we have $Q \approx q \approx -q \approx -Q$. Denote the number of classes in which reduced forms are equivalent to their inverse by $I(D)$.
When $D < 0$, for a positive form [a,b,c], [-a,-b,-c] is a negative form, therefore a definite form can never be equivalent to its inverse. Therefore for $D < 0$ we always have $I(D) = 0$.
When $D > 0$, in order to find if a form Q is equivalent to its inverse, one should reduce -Q and see if the result is in the same chain with Q. if Q=[a,b,c] is reduced, then -Q=[-a,-b,-c] is equivalent to the reduced form [-c,b,a], and all left is to see whether [a,b,c] and [-c,b,a] are in the same chain.

2.7. **An Algorithm to calculate $H_+(D)$ and $I(D)$.**

```
Make sure $D$ is a legal discriminant (not a perfect square, $D \equiv 0$ or 1 (mod4))
if $D < 0$:
  Find positive reduced forms (use algorithm described in Section 2.3.2)
  Multiply number of reduced forms by 2 to find $H_+(D)$
  $I(D) = 0$, as $D < 0$
if $D > 0$:
  Find indefinite reduced forms, consider a single form in every chain (use
  algorithm described in Section 2.4.3)
  For each reduced form Q: reduce -Q and check if in the same chain with Q
  Calculate $I(D)$
```

The complexity of this algorithm is $O(DlogD)$.

2.8. $SL_2(\mathbb{Z})$ Matrices and Quadratic Forms.

2.8.1. *$SL_2(\mathbb{Z})$ Matrices.* $SL_2(\mathbb{Z})$ denotes the group of matrices $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ with integral coefficients, such that the determinant $\alpha\delta - \beta\gamma = 1$. Consider the following action $SL_2(\mathbb{Z})$ defines on $\mathbb{R}$:

$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z}),\ \tau \in \mathbb{R}, \text{ then } g(\tau) = \tfrac{\alpha\tau+\beta}{\gamma\tau+\delta}.$$

We are interested in $\tau \in \mathbb{R}$ which is fixed under the operation of g, i.e. $g(\tau) = \frac{\alpha\tau+\beta}{\gamma\tau+\delta} = \tau$, which results in

$$\tau_\pm = \frac{\alpha - \delta \pm \sqrt{\operatorname{tr}(g)^2 - 4\det(g)}}{2\gamma} = \frac{\alpha - \delta \pm \sqrt{\operatorname{tr}(g)^2 - 4}}{2\gamma}$$

2.8.2. *Correspondence to Quadratic Forms.* We define a corresponding quadratic form $Q_g(x, y)$ to the matrix $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ as follows:

$$\begin{aligned} Q_g(x, y) &= \gamma(x - \tau_+ y)(x - \tau_- y) = \gamma(x^2 - (\tau_+ + \tau_-)xy + \tau_+\tau_- y^2) = \\ &= \gamma x^2 + (\delta - \alpha)xy - \beta y^2 \end{aligned}$$

Note that for $g^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$, the corresponding form is

$$Q_{g^{-1}}(x, y) = -\gamma x^2 + (\alpha - \delta)xy + \beta y^2 = -Q_g(x, y)$$

The discriminant D for Q_g is

$$D = (\delta - \alpha)^2 - 4\gamma(-\beta) = (\delta + \alpha)^2 - 4(\alpha\delta - \beta\gamma) = \operatorname{tr}(g)^2 - 4$$

Conjugate matrices in $SL_2(\mathbb{Z})$ have the same trace, and therefore correspond to forms with the same discriminant.

The discriminant satisfies $D = \operatorname{tr}(g)^2 - 4 \equiv 0$ or $1 \pmod 4$. Also, for $|\operatorname{tr}(g)| \neq 2$, D is not a perfect square. This can be easily checked for $|\operatorname{tr}(g)| = 0,\ 1$. For $|\operatorname{tr}(g)| > 2$, suppose $D = k^2$. It is enough to consider positive $\operatorname{tr}(g)$ and k. We have

$$4 = \operatorname{tr}(g)^2 - k^2 = (\operatorname{tr}(g) + k)(\operatorname{tr}(g) - k)$$

As $(\operatorname{tr}(g) + k)$ and $(\operatorname{tr}(g) - k)$ are of the same parity, the only way to factor 4 is $2 \cdot 2$, implying $\operatorname{tr}(g) = 2$, $k = 0$, but $|\operatorname{tr}(g)| > 2$.

Recall that for $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$:

$$(Q \circ h)(x, y) := Q((x, y)h^t) = Q(ax + by, cx + dy)$$

For $h \in SL_2(\mathbb{Z})$ we say that Q is strictly equivalent to $Q \circ h$, for $h \in GL_2(\mathbb{Z})$ we say that Q and $Q \circ h$ are weakly equivalent.

Theorem 6. *Let $h \in SL_2(\mathbb{Z})$, then $Q_{h^{-1}gh} = Q_g \circ h$. This means that conjugate matrices correspond to equivalent forms, and vice versa.*

Proof. Let $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ with $\alpha\delta - \beta\gamma = 1$, and $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc = 1$. Then $h^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, and

$$h^{-1}gh = \begin{pmatrix} A{=}\alpha ad{+}\beta cd{-}\gamma ab{-}\delta bc & B{=}\alpha bd{+}\beta d^2{-}\gamma b^2{-}\delta bd \\ C{=}{-}\alpha ac{-}\beta c^2{+}\gamma a^2{+}\delta ac & D{=}{-}\alpha bc{-}\beta cd{+}\gamma ab{+}\delta ad \end{pmatrix}$$

$$\begin{aligned} Q_{h^{-1}gh}(x,y) &= Cx^2 + (D-A)xy - By^2 = \\ &= [(\delta-\alpha)ac - \beta c^2 + \gamma a^2]x^2 \\ &\quad +[(\delta-\alpha)(ad+bc) - 2\beta cd + 2\gamma ab]xy \\ &\quad +[(\delta-\alpha)bd - \beta d^2 + \gamma b^2]y^2 \end{aligned}$$

On the other hand, $Q_g(x,y) = \gamma x^2 + (\delta - \alpha)xy - \beta y^2$,

$$\begin{aligned} (Q_g \circ h)(x,y) &= Q_g((x,y)h^t) = Q_g((x,y)\begin{pmatrix} a & c \\ b & d \end{pmatrix}) = \\ &= Q_g(ax+by, cx+dy) = \\ &= \gamma(ax+by)^2 + (\delta-\alpha)(ax+by)(cx+dy) - \beta(cx+dy)^2 \end{aligned}$$

which is exactly the same as $Q_{h^{-1}gh}(x,y)$ above. □

The correspondence also allows us to find the matrix to which a given form corresponds, as long as the trace t is also provided: let $Q(x,y) = Ax^2 + Bxy + Cy^2$, with discriminant $D = B^2 - 4AC$ such that $t = \sqrt{D+4} \in \mathbb{Z}$, or $t = -\sqrt{D+4} \in \mathbb{Z}$. Then, the corresponding matrix is $g(Q) = \begin{pmatrix} \alpha & -C \\ A & \delta \end{pmatrix}$, where $\delta - \alpha = B$, $\det(g(Q)) = \alpha\delta + AC = 1$ and $\alpha + \delta = t = \pm\sqrt{D+4} = \pm\sqrt{(B^2 - 4AC) + 4}$. The only solution for these equations is $\delta = \frac{B+t}{2}$, $\alpha = \frac{-B+t}{2}$.

To summarize, we have the following bidirectional correspondence between matrices with trace t, $|t| \neq 2$, and forms discriminant D where $D = t^2 - 4$:

$$\begin{gathered} g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \rightarrow Q_g(x,y) = \gamma x^2 + (\delta - \alpha)xy - \beta y^2 \\ Q(x,y) = Ax^2 + Bxy + Cy^2 \rightarrow g(Q) = \begin{pmatrix} \frac{-B+t}{2} & -C \\ A & \frac{B+t}{2} \end{pmatrix} \end{gathered} \tag{14}$$

With this correspondence, and by the Theorem 6, the number of conjugate classes for matrices in $SL_2(\mathbb{Z})$ with trace t is equal to $H_+(D)$, the number of equivalence classes of forms with discriminant $D = t^2 - 4$.

2.8.3. *Characteristic Polynomial and Eigenvalues for an $SL_2(\mathbb{Z})$ Matrix.* The characteristic polynomial of $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is:

$$|\begin{pmatrix} x-\alpha & \beta \\ \gamma & x-\delta \end{pmatrix}| = x^2 - \mathrm{tr}(g)x + \det(g) = x^2 - \mathrm{tr}(g)x + 1$$

The eigenvalues of g, which are the roots of the characteristic polynomial, are:

$$\lambda = \frac{\mathrm{tr}(g) \pm \sqrt{\mathrm{tr}(g)^2 - 4}}{2}$$

2.9. **Examples.** Table 1 lists, for different trace values, the respective discriminant $D = trace^2 - 4$, $H_+(D)$ (the number of strict equivalence classes), and $I(D)$ (the number of classes in which reduced forms are equivalent to their inverse).

Table 2 shows, for different trace values, an example of a matrix which is conjugate to its inverse, and an example of a matrix which is not, when available. For each matrix g, the corresponding form is also listed.

TABLE 1. $H_+(D)$ and $I(D)$ for trace values

|trace|	D	$H_+(D)$	$I(D)$
3	5	1	1
4	12	2	0
5	21	2	0
6	32	3	1
7	45	3	1
8	60	4	0
9	77	2	0
10	96	6	0
11	117	3	1
12	140	4	0
13	165	4	0
14	192	8	0
15	221	4	2
16	252	6	0
17	285	4	0
18	320	8	2

Table 2. Matrices and forms for trace values

trace	$g \approx g^{-1}$	$g \not\approx g^{-1}$
3	$\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \approx \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ $Q_g = [-1, 1, 1]$	None
4	None	$\begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix} \not\approx \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$ $Q_g = [-1, 2, 2]$
5	None	$\begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix} \not\approx \begin{pmatrix} 4 & -3 \\ -1 & 1 \end{pmatrix}$ $Q_g = [1, 3, -3]$
6	$\begin{pmatrix} 1 & -2 \\ -2 & 5 \end{pmatrix} \approx \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$ $Q_g = [-2, 4, 2]$	$\begin{pmatrix} 1 & 4 \\ 1 & 5 \end{pmatrix} \not\approx \begin{pmatrix} 5 & -4 \\ -1 & 1 \end{pmatrix}$ $Q_g = [1, 4, -4]$
7	$\begin{pmatrix} 2 & -3 \\ -3 & 5 \end{pmatrix} \approx \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$ $Q_g = [-3, 3, 3]$	$\begin{pmatrix} 1 & 5 \\ 1 & 6 \end{pmatrix} \not\approx \begin{pmatrix} 6 & -5 \\ -1 & 1 \end{pmatrix}$ $Q_g = [1, 5, -5]$
15	$\begin{pmatrix} 3 & 5 \\ 7 & 12 \end{pmatrix} \approx \begin{pmatrix} 12 & -5 \\ -7 & 3 \end{pmatrix}$ $Q_g = [7, 9, -5]$	$\begin{pmatrix} 1 & 13 \\ 1 & 14 \end{pmatrix} \not\approx \begin{pmatrix} 14 & -13 \\ -1 & 1 \end{pmatrix}$ $Q_g = [1, 13, -13]$
-3	$\begin{pmatrix} -2 & -1 \\ -1 & -1 \end{pmatrix} \approx \begin{pmatrix} -1 & 1 \\ 1 & -2 \end{pmatrix}$ $Q_g = [-1, 1, 1]$	None
-4	None	$\begin{pmatrix} -3 & -2 \\ -1 & -1 \end{pmatrix} \not\approx \begin{pmatrix} -1 & 2 \\ 1 & -3 \end{pmatrix}$ $Q_g = [-1, 2, 2]$

3. Ideal Theory in Quadratic Fields

3.1. **Survey.**

3.1.1. *Quadratic Fields.* Let K be a quadratic extension of $\mathbb{Q}$, $K = \mathbb{Q}(\sqrt{d_0})$, $d_0 \in \mathbb{Z}$. Note that when $d = n^2 \cdot d_0$, then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d_0})$. $\mathfrak{O}_K$ denotes the ring of all quadratic integers of K, which is a Dedekind Ring.

3.1.2. *Discriminant of Quadratic Fields.* For $\alpha = a + b\sqrt{m} \in K$, $a, b \in \mathbb{Q}$, denote $\alpha' = a - b\sqrt{m}$, the conjugate of α. For $\alpha, \beta \in K$, let $\Delta_{K/\mathbb{Q}}(\alpha, \beta) := \alpha\beta' - \beta\alpha'$. $D_{K/\mathbb{Q}}(\alpha, \beta) := \Delta_{K/\mathbb{Q}}(\alpha, \beta)^2$, is called the discriminant of α, β in K over $\mathbb{Q}$. $D_{K/\mathbb{Q}}(\alpha, \beta) = 0$ if and only if α, β are linearly dependent over $\mathbb{Q}$. It appears that $D_{K/\mathbb{Q}}$ is invariant to different bases $[\alpha, \beta]$ of $\mathfrak{O}_K$ as a module over $\mathbb{Z}$. Let $d = d(\mathfrak{O}_K) = d(K)$ denote the **discriminant of the field,** it is the discriminant of any basis of $\mathfrak{O}_K$ (over $\mathbb{Z}$). For $d_0 \in \mathbb{Z}$ square free we have:

$$(15)\qquad \begin{array}{lll} d_0 \equiv 2\ ,3 \pmod 4 & \text{then}\ \ \mathfrak{O}_K = \mathbb{Z}[\sqrt{d_0}], & d = d(K) = 4d_0 \\ d_0 \equiv 1 \pmod 4 & \text{then}\ \ \mathfrak{O}_K = \mathbb{Z}[\frac{1+\sqrt{d_0}}{2}], & d = d(K) = d_0 \end{array}$$

For $n \in \mathbb{N}$ we define the following integral domain (contained in $\mathfrak{O}_K$):

$$(16)\qquad \mathfrak{O}_n = \begin{cases} \mathbb{Z}[n\frac{1+\sqrt{d_0}}{2}] = \mathbb{Z}[\frac{n}{2}\sqrt{d_0}] & \text{if } d_0 \equiv 1 (\text{mod } 4), n \text{ even} \\ \mathbb{Z}[n\frac{1+\sqrt{d_0}}{2}] = \mathbb{Z}[\frac{1+n\sqrt{d_0}}{2}] & \text{if } d_0 \equiv 1 (\text{mod } 4), n \text{ odd} \\ \mathbb{Z}[n\sqrt{d_0}] & \text{if } d_0 \not\equiv 1 (\text{mod } 4) \end{cases}$$

Such integral domain is called an **order** of $\mathfrak{O}_K$. Note that $\mathfrak{O}_1 = \mathfrak{O}_K$. $\mathfrak{O}_n$ for $n \neq 1$ is not a Dedeking ring, as it is not integrally closed in K. The discriminant of $\mathfrak{O}_n$ is $d(\mathfrak{O}_n) = n^2 d(\mathfrak{O}_K)$.

3.1.3. *Elements of $\mathfrak{O}_n$.* For $\alpha = a + b\sqrt{d_0} \in \mathfrak{O}_n$, $a, b \in \mathbb{Q}$, denote $N(\alpha) = \alpha\alpha'$ the norm of α. The norm of elements of $\mathfrak{O}_n$ is multiplicative, as $(\alpha\beta)' = \alpha'\beta'$. We say that $\alpha \in \mathfrak{O}_n$ divides an element π in $\mathfrak{O}_n$, if there exists $\beta \in \mathfrak{O}_n$ such that $\pi = \alpha\beta$. A **unit** in $\mathfrak{O}_n$ is an element which divides 1 in $\mathfrak{O}_n$, and $N(\pi) = \pm 1$ if and only if π is a unit in $\mathfrak{O}_n$. We define a prime in $\mathfrak{O}_n$ as a nonunit element $\pi \in \mathfrak{O}_n$ with the property that if π divides the product of two elements α and β in $\mathfrak{O}_n$, then π divides α or β in $\mathfrak{O}_n$. It is not always true that every element of $\mathfrak{O}_n$ has a unique factorization into primes.

3.1.4. *Fundamental Units of $\mathfrak{O}_K$ and $\mathfrak{O}_n$.* There exists a special unit $\eta_1 > 1$ in $\mathfrak{O}_K$ such that all units ρ in $\mathfrak{O}_K$ are given by $\rho = \pm\eta_1^j$, $j = 0, \pm 1, \pm 2 \ldots$

This unit η_1 is called the **fundamental unit** of $\mathfrak{O}_K$. The answer to the

question whether $N(\eta_1) = +1$ or $N(\eta_1) = -1$ in an arbitrary $\mathfrak{O}_K$ is not known completely.
Note that when $N(\eta_1) = +1$ then for any unit ρ, $N(\rho) = +1$.
Similarly, $\eta_n > 1$ denotes the fundamental unit for the order $\mathfrak{O}_n$. Clearly $\eta_n = \eta_1^u$ for some u, where η_1 is the fundamental unit of $\mathfrak{O}_K$, since η_n is also a unit of $\mathfrak{O}_K$.

3.1.5. *Ideals of* $\mathfrak{O}_n$. An ideal of a ring is a module over the ring which is contained in the ring and is closed under multiplication with elements of the ring. An ideal J of $\mathfrak{O}_n$ is a module over $\mathbb{Z}$, meaning there is a basis $[w_1, w_2]$ for J over $\mathbb{Z}$. If another such basis $[v_1, v_2]$ exists then there is a transformation matrix A between the bases, such that $\det A \in \mathbb{Z}^* = \{\pm 1\}$, meaning $A \in GL_2(\mathbb{Z})$.
An ideal J is called a prime ideal if whenever $\alpha\beta \in J$ $(\alpha, \beta \in \mathfrak{O}_n)$ then either $\alpha \in J$ or $\beta \in J$. For ideals $I \neq 0$, J of $\mathfrak{O}_n$, we say that I divides J and write $I|J$ if there exists an ideal H of $\mathfrak{O}_n$ such that $J = IH = \{ih \mid i \in I, h \in H\}$. We denote $(1) = \mathfrak{O}_n$, which divides (and contains) any other ideal of $\mathfrak{O}_n$. Ideals I,J of $\mathfrak{O}_n$ are said to be relatively prime when $I + J = \{\sum ai + bj \mid a, b \in \mathfrak{O}_n, i \in I, j \in J\} = \mathfrak{O}_n$.
A norm of an ideal I of $\mathfrak{O}_K$, denoted $N(I)$, is its index in $\mathfrak{O}_K$, $[\mathfrak{O}_K : I]$, the ideal norm is multiplicative. Let J be an ideal of $\mathfrak{O}_K$, with a basis $[\alpha, \beta]$ as a module over $\mathbb{Z}$. Then:

$$(17)\ \ |\Delta_{K/\mathbb{Q}}(\alpha, \beta)| = |\alpha\beta' - \beta\alpha'| = [\mathfrak{O}_K : J] \cdot \sqrt{d(\mathfrak{O}_K)} = N(J) \cdot \sqrt{d(K)}$$

For an ideal I of $\mathfrak{O}_n$ we similarly denote $N(I) = [\mathfrak{O}_n : I]$. Let I be an ideal of $\mathfrak{O}_n$, with a basis $[\alpha, \beta]$ as a module over $\mathbb{Z}$. Then we have the following generalization of (17):

$$(18)\ \ |\Delta_{K/\mathbb{Q}}(\alpha, \beta)| = |\alpha\beta' - \beta\alpha'| = [\mathfrak{O}_n : J] \cdot \sqrt{d(\mathfrak{O}_n)} = N(J) \cdot n\sqrt{d(K)}$$

For ideals $I, J \in \mathfrak{O}_n$, if $I|J$, meaning there exists ideal $L \in \mathfrak{O}_n$ such that $J = IL$, then $I \supseteq J$. Conversely, for ideals $I \neq 0$, J of $\mathfrak{O}_n$, with $\alpha \in I$ such that $(N(\alpha), n) = 1$, $I \supseteq J$ then $I|J$.
Some attributes are unique to ideals of $\mathfrak{O}_K$: For ideals $I \neq 0$, J of $\mathfrak{O}_K$, $I|J$ if and only if $I \supseteq J$ ("to divide is to contain"). Any non-zero ideal J of $\mathfrak{O}_K$ can be expressed uniquely as a finite product of prime ideals: $J = \prod_{i=1}^{k} P_i^{e_i}$ where P_i prime ideals of $\mathfrak{O}_K$, $e_i \in \mathbb{N}$. $\mathfrak{O}_K$ has unique factorization if and only if all ideals of $\mathfrak{O}_K$ are principal.

3.1.6. *The Class Group for* $\mathfrak{O}_K$. We say that two ideals, I,J of $\mathfrak{O}_K$ fall into the same class, written $I \sim J$, if $I(\beta) = J(\alpha)$, for $\alpha, \beta \in \mathfrak{O}_K$ not both zero. The classes of ideals of $\mathfrak{O}_K$ form a finite (multiplicative, commutative) group, called the Class Group. The number of elements in the class group is denoted $h(d(K))$. The unit of this group, is the

class of the principal ideals (α), $\alpha \in \mathfrak{O}_K$. If there are h elements in the class group, then for any ideal I is is true that I^h is a principal ideal, and I^{h-1} is the inverse of I. For any ideal I of $\mathfrak{O}_K$, we can find ideal I^* and a non-zero element $\alpha \in \mathfrak{O}_K$ such that $II^* = (\alpha)$.
Elements of $\mathfrak{O}_K$ have unique factorization if and only if the class group is 1, meaning all ideals of $\mathfrak{O}_K$ are principal.

3.1.7. *Class Number for $\mathfrak{O}_n$.* A unique factorization theorem for $\mathfrak{O}_n$ could be developed, by considering only ideals I for which exists $\alpha \in I$ such that $N(\alpha)$ is prime to n.
Another possible approach for unique factorization in $\mathfrak{O}_n$ is to restrict the ideal theory to $\mathfrak{O}_1 = \mathfrak{O}_K$ and find the ideals of $\mathfrak{O}_n$ by a "projection" procedure afterwards.
Ideals of $\mathfrak{O}_n$ do not necessarily have an inverse ideal. For example, consider $K = \mathbb{Q}(\sqrt{-35})$, $\mathfrak{O}_2 = \mathbb{Z}[\sqrt{-35}]$, the ideal $[2, 1 + \sqrt{-35}]$ is equivalent to its square, implying it has no inverse [Tau2].

Corollary 4. *If $n > 1$ then the classes of ideals of $\mathfrak{O}_n$ do not necessarily form a group.*

For an ideal I of $\mathfrak{O}_n$ for which there exists $\alpha \in I$ such that $N(\alpha)$ is prime to n, we can find ideal I^* and a non-zero element $\beta \in \mathfrak{O}_n$ such that $II^* = (\beta)$. Such ideals are called invertible ideals of $\mathfrak{O}_n$, where all ideals of $\mathfrak{O}_K$ are invertible.

3.1.8. *Factorization of Rational Primes in $\mathbb{Q}(\sqrt{d_0})$.* Each prime ideal $\wp$ of $\mathfrak{O}_K$ can arise only from a rational prime p, determined uniquely by $\wp|(p)$. Also, the prime ideals completely determine the class structure in that every equivalence class, say that of $J = \prod_{i=1}^{k} \wp_i^{e_i}$ is determined by the equivalence classes of the $\wp_i$. We need to know how to construct the $\wp_i$ from the rational primes.
The Legendre Symbol is defined for $d \equiv 0$ or $1 \pmod 4$, d is not a perfect square, and p prime where $(p, d) = 1$ as follows:

$$(\tfrac{d}{p}) = \begin{cases} 1 & \text{if d is a quadratic residue (mod } p), \\ -1 & \text{if d is not a quadratic residue (mod } p), \end{cases}$$

The Kronecker symbol is defined for $d \equiv 0$ or $1 (\bmod 4)$, d is not a perfect square, $d_0 > 0$ as follows:

$$\begin{array}{lll} (\tfrac{d}{p}) = & 0 & \text{if } p|d \\ (\tfrac{d}{2}) = & \begin{cases} 1 & \text{if } d \equiv 1 \pmod 8 \\ -1 & \text{if } d \equiv 5 \pmod 8 \end{cases} & \\ (\tfrac{d}{p}) = & \text{Legendre Symbol} & \text{if } p > 2 \\ (\tfrac{d}{m}) = & \prod_{i=1}^{k} (\tfrac{d}{p_i}) & m = \prod_{i=1}^{k} p_i \end{array}$$

A rational prime $p \in \mathbb{Z}$ factors in the quadratic field $K = \mathbb{Q}(\sqrt{d_0})$ (with $d_0 \in \mathbb{Z}$ square free) according to the following rules, based on the discriminant of the field, $d(K)$ and $(\frac{d(K)}{p})$, the Kronecker symbol:

$$\begin{cases} (p) = (p), \text{ or } p \text{ does not factor if and only if } (\frac{d(K)}{p}) = -1 \\ (p) = \wp\wp', \text{ or } p \text{ splits into two different factors if and only if } (\frac{d(K)}{p}) = +1 \\ (p) = \wp^2 \text{ (and } \wp = \wp'\text{),or } p \text{ ramifies if and only if } (\frac{d(K)}{p}) = 0 \end{cases}$$

Corollary 5. *For every non-zero ideal J in $\mathfrak{O}_K$, it is true that JJ' is a principal ideal. This means that ideal classes $C(J)$ of J and $C(J')$ of J' are inverses of each other: $C(J)^{-1} = C(J')$.*

3.2. **Strict Equivalence of Ordered Ideals.** This section follows closely [Cohn], Chapter XII.

We have defined weak equivalence between ideals of $\mathfrak{O}_n$: $I \sim J$ when $\alpha I = \beta J$ for $\alpha, \beta \in \mathfrak{O}_n$. We would like to set up a strict equivalence relation between bases of ideals of $\mathfrak{O}_n$.
First we define an **ordered ideal basis:** for an ideal basis $[\alpha, \beta]$ of $\mathfrak{O}_n$ to be considered ordered, the ratio $\frac{\Delta_{K/\mathbb{Q}}(\alpha,\beta)}{\sqrt{(d(\mathfrak{O}_n))}}$ must be positive:

$$\frac{\Delta_{K/\mathbb{Q}}(\alpha, \beta)}{\sqrt{(d(\mathfrak{O}_n))}} = \frac{\alpha\beta' - \beta\alpha'}{n\sqrt{(d(K))}} = N([\alpha, \beta]) > 0 \tag{19}$$

(By (17) and (18) above). If this ratio is negative, then the ideal basis should be reordered to $[\beta, \alpha]$ to be an ordered ideal basis.
Consider a change of basis, for ordered bases of ideals, $[\alpha, \beta] = [\gamma, \delta]$ holds if and only if:

$$\begin{cases} \alpha = P\gamma + Q\delta, \quad PS - QR = +1 \\ \beta = R\gamma + S\delta, \end{cases} \tag{20}$$

In other words - two ordered bases of an ideal are equivalent under a strictly unimodular transformation, and conversely.
The conjugate relationship for an ordered ideal can be formed as:

$$\text{for } J = [\alpha, \beta], \text{ its conjugate is } J' = [\beta', \alpha'] \tag{21}$$

3.2.1. *Strictly Equivalent ideals.* Once introducing the notion of an ordered ideal basis, we must revise our notion of equivalence of ideals. For ideals I, J of $\mathfrak{O}_n$:
(22)

$$I \approx J \text{ if } \alpha I = \beta J \text{ for } \alpha, \beta \in \mathfrak{O}_n \text{ not both zero and } N(\alpha\beta) > 0$$

When $I \approx J$ we say the two ideals are **strictly equivalent.** Also,

$$\begin{cases} \rho J = \rho[\alpha, \beta] = & [\rho\alpha, \rho\beta] \text{ if } N(\rho) > 0 \\ & [\rho\beta, \rho\alpha] \text{ if } N(\rho) < 0 \end{cases} \tag{23}$$

Theorem 7. *Two ideals in an integral ring $\mathfrak{O}_n$ of $K = \mathbb{Q}(\sqrt{d_0})$ are strictly equivalent if they are equivalent in the ordinary sense, when:*

1. *$d_0 < 0$ or*
2. *$d_0 > 0$ while the fundamental unit of $\mathfrak{O}_n$ has negative norm.*

In the remaining case, in which $d_0 > 0$ while the fundamental unit of $\mathfrak{O}_n$ has positive norm:

- *If $I \sim J$, then either $I \approx J$ or $I \approx n\sqrt{d_0}J$.*
- *When J is an invertible ideal of $\mathfrak{O}_n$, then only one of these equivalence relations holds, but not both.*

Proof. Let I, J be ideals of $\mathfrak{O}_n$ such that $I \sim J$.

1. $d_0 < 0$. This case is obvious, since norms in a field with $d_0 < 0$ are always positive: $N(\alpha + \beta n\sqrt{d_0}) = \alpha^2 - \beta^2 n^2 d_0 > 0$.
2. $d_0 > 0$, let η_n be the fundamental unit of $\mathfrak{O}_n$, $N(\eta_n) = -1$. It is easy to guarantee $I \approx J$ from $\alpha I = \beta J$ when $N(\alpha\beta) < 0$, by using $\eta_n \alpha I = \beta J$ instead, with $N(\eta_n \alpha\beta) > 0$.

For the remaining case, let $d_0 > 0$, η_n is the fundamental unit of $\mathfrak{O}_n$, $N(\eta_n) = +1$.

- When $I \sim J$ whereas $I \not\approx J$, it must follow that

  $$\alpha I = \beta J, \; N(\alpha\beta) < 0$$

  We set $n\sqrt{d_0}J = J^*$, and it follows that $n\sqrt{d_0} \cdot \alpha I = \beta J^*$, where

  $$N(\alpha\beta \cdot n\sqrt{d_0}) = N(\alpha\beta)N(n\sqrt{d_0}) = N(\alpha\beta)(-n^2 d_0) > 0$$

  Thus, if $I \sim J$ and $I \not\approx J$ then $I \approx n\sqrt{d_0}J$.
  This proves that at least one of $I \approx J$ or $I \approx n\sqrt{d_0}J$ holds.

- Show that $(1) \not\approx (n\sqrt{d_0})$. For, if $(1) \approx (n\sqrt{d_0})$, then $\alpha(1) = \beta(n\sqrt{d_0})$, whereas $N(\alpha\beta) > 0$, meaning $N(\alpha)$ and $N(\beta)$ have the same sign. For some unit η^*, $\alpha\eta^* = \beta n\sqrt{d_0}$, but $N(\alpha)N(\eta^*) = N(\alpha\eta^*) = N(\beta n\sqrt{d_0}) = N(\beta)(-n^2 d_0)$. Hence, $N(\eta^*) < 0$ if $(1) \approx (n\sqrt{d_0})$.
  Now show that $(1) \not\approx (n\sqrt{d_0})$ means for an invertible J that $J \not\approx n\sqrt{d_0}J$, meaning that the equivalences cannot both hold. Assume J is invertible and $J \approx n\sqrt{d_0}J$. When J is an invertible

ideal of $\mathfrak{O}_n$, then there exists J^* of $\mathfrak{O}_n$ and $0 \neq \alpha \in \mathfrak{O}_n$ such that $JJ^* = (\alpha)$ (by Section 3.1.7). Then

$$\alpha(1) = (\alpha) = JJ^* \approx n\sqrt{d}_0 JJ^* = n\sqrt{d}_0(\alpha) = \alpha(n\sqrt{d}_0)$$

As $N(\alpha\alpha) = N(\alpha)^2 > 0$ we have $(1) \approx (n\sqrt{d}_0)$, which is a contradiction. Hence, under such conditions, only one of the above equivalences holds.

□

Note: It is always true that $(n\sqrt{d}_0) \approx (n\sqrt{d})$, as either $d = d_0$, and then $(n\sqrt{d}_0) = (n\sqrt{d})$, or $d = 4d_0$, and then

$$(n\sqrt{d}_0) \approx 2(n\sqrt{d}_0) = (n\sqrt{4d_0}) = (n\sqrt{d})$$

Therefore the last part of the previous theorem can be rephrased: When $d_0 > 0$ while the fundamental unit of $\mathfrak{O}_n$ has positive norm, if $I \sim J$, either $I \approx J$ or $I \approx n\sqrt{d}J$, and when J is an invertible ideal then only one of these holds.

For example, consider $I = [3, \frac{9-3\sqrt{13}}{2}]$, $J = I' = [\frac{9+3\sqrt{13}}{2}, 3]$. I and J are ideals of $\mathfrak{O}_3$ in $K = \mathbb{Q}(\sqrt{13})$. I is non-invertible in $\mathfrak{O}_3$, as a general element of I has the form $3a + \frac{9-3\sqrt{13}}{2}b = \frac{(6a+9b)-3b\sqrt{13}}{2} = 3\frac{(2a+3b)-b\sqrt{13}}{2}$, hence its norm is not relatively prime to 3. Similarly, J is non-invertible in $\mathfrak{O}_3$. We have

$$I\begin{pmatrix} 3 & 1 \\ -1 & 0 \end{pmatrix} = J$$

Where the matrix has determinant +1. This shows that $I = J$, hence $I \sim J$ and $I \approx J$. On the other hand:

$$I\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot (-3\frac{13+3\sqrt{13}}{2}) = J \cdot 3\sqrt{13}$$

The transformation matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ has determinant +1, and $N(-3\frac{13+3\sqrt{13}}{2}) = 117 > 0$, hence $I \approx J \cdot 3\sqrt{13}$.
Therefore we have $I \sim J$, and $J \approx I \approx J \cdot 3\sqrt{13}$.

Recall that all $\mathfrak{O}_K$ ideals are invertible, hence the following Corollary:

Corollary 6. *Let $h_+(d(K))$ denote the number of strict equivalence classes of ideals in $\mathfrak{O}_K$, with discriminant $d(K)$. Then we have:*

$$\begin{cases} h_+(d(K)) = h(d), \text{ if } d_0 < 0, \text{ or if } d_0 > 0 \text{ and } N(\eta_1) < 0, \\ h_+(d(K)) = 2h(d), \text{ if } d_0 > 0 \text{ and } N(\eta_1) > 0 \end{cases} \tag{24}$$

3.3. **A Correspondence Between Matrices and Ideals.** We now set up a precise correspondence between matrices in $SL_2(\mathbb{Z})$ and ideals of orders of $\mathfrak{O}_K$.
Let $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$, with $|\operatorname{tr}(g)| > 2$. Denote

$$D = \operatorname{tr}(g)^2 - 4 = n^2 d$$

where d is a field discriminant, meaning that either $d \equiv 0 \pmod 4$ and then $d = 4d_0$, d_0 square free, or $d \not\equiv 0 \pmod 4$, and then $d = d_0$ square free. As $D \equiv 0$ or $1 \pmod 4$, and d is a field discriminant, then such factorization exists, and is unique.
The characteristic polynomial of g is

$$x^2 - \operatorname{tr}(g)x + \det(g) = x^2 - \operatorname{tr}(g) + 1$$

Its roots, the eigenvalues of g, are $\lambda = \frac{\operatorname{tr}(g) \pm \sqrt{\operatorname{tr}(g)^2 - 4}}{2}$, which generate a field extension

$$K = \mathbb{Q}(\lambda) = \mathbb{Q}(\sqrt{\operatorname{tr}(g)^2 - 4}) = \mathbb{Q}(\sqrt{d_0})$$

This is a real quadratic field as $\operatorname{tr}(g)^2 > 4$. The eigenvalues λ, $\lambda^{-1} (= \lambda')$ of g are units in $\mathfrak{O}_K$. Adjoining λ to $\mathbb{Z}$ gives an order $\mathfrak{O} = \mathbb{Z}[\lambda] \subseteq \mathfrak{O}_K$ in K. Note that $\mathfrak{O} = \mathbb{Z}[\lambda] = \mathfrak{O}_n$, and $\mathfrak{O} = \mathfrak{O}_K$ exactly when D is a field discriminant (meaning $n = 1$ and $D = d$).

Theorem 8. *Let $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$, $|\operatorname{tr}(g)| > 2$. The corresponding ideal is:*

$$I_g = [v_1, v_2] = \begin{cases} [\gamma, \frac{(\delta-\alpha) - n\sqrt{d}}{2}] & \textit{when } \gamma > 0 \\ [\gamma n\sqrt{d}, \frac{(\delta-\alpha) - n\sqrt{d}}{2} n\sqrt{d}] & \textit{when } \gamma < 0 \end{cases} \tag{25}$$

*This is an $\mathfrak{O}_n$ ideal with an ordered basis. For a conjugate matrix hgh^{-1}, $h \in SL_2(\mathbb{Z})$, the corresponding ideal is received by $[v_1, v_2]h^{-1}$, which is also an $\mathfrak{O}_n$ ordered ideal, and is strictly equivalent to $[v_1, v_2]$. Conversely, given an eigenvalue λ of an $SL_2(\mathbb{Z})$ matrix, an ordered ideal $I = [v_1, v_2]$ has a corresponding matrix $g(I) \in SL_2(\mathbb{Z})$ such that λ is an eigenvalue of g and for $J = [w_1, w_2] \approx I$, where $[w_1, w_2] = [v_1, v_2] \circ h$, $h \in SL_2(\mathbb{Z})$, the corresponding matrix is $h^{-1}gh$.
This establishes a 1-1 correspondence between $SL_2(\mathbb{Z})$ matrix classes with the same characteristic polynomial (meaning - with the same trace, see Section 2.8.3) to ideal classes in the order $\mathbb{Z}[\lambda]$.*

Proof. Let λ be an eigenvalue of g, then the (unique) characteristic vector of a matrix g corresponding to λ can be chosen to lie in $\mathbb{Z}[\lambda]$:

$$(v_1, v_2)g = \lambda(v_1, v_2), \quad v_1, v_2 \in \mathbb{Z}[\lambda] = \mathfrak{O}_n$$

This implies that a $\mathbb{Z}$-combination of v_i is equal to λv_i for $i = 1, 2$. Similarly, $p(\lambda)v_i$, $i = 1, 2$, is a $\mathbb{Z}$-combination of v_i for any integral polynomial $p(x)$ via $p(g)$:

$$(v_1, v_2)p(g) = p(\lambda)(v_1, v_2)$$

This shows that v_1, v_2 form a $\mathbb{Z}$-basis for an ideal in $\mathbb{Z}[\lambda] = \mathfrak{O}_n$. Let $I_g = [v_1, v_2]$, an ideal of $\mathfrak{O}_n$.

Explicitly, $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$, with characteristic polynomial $x^2 - (\alpha+\delta)x + 1$, and eigenvalues λ, λ^{-1}. Let λ be the eigenvalue with the $-$ sign, $\lambda = \frac{(\alpha+\delta)-\sqrt{(\alpha+\delta)^2-4}}{2} = \frac{(\alpha+\delta)-n\sqrt{d}}{2}$. Now solve

$$(v_1, v_2)\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \lambda(v_1, v_2) \tag{26}$$

$$v_2 = \frac{(\delta-\alpha)-n\sqrt{d}}{2\gamma}v_1 \tag{27}$$

We have the following ordered ideal I_g of $\mathfrak{O}_n$:

$$\begin{cases} [\gamma, \frac{(\delta-\alpha)-n\sqrt{d}}{2}] & \text{when } \gamma > 0, (v_1 = \gamma) \\ [\gamma n\sqrt{d}, \frac{(\delta-\alpha)-n\sqrt{d}}{2}n\sqrt{d}] & \text{when } \gamma < 0, (v_1 = \gamma n\sqrt{d}) \end{cases} \tag{28}$$

Recall (16), and notice that the basis elements of I_g are indeed in $\mathfrak{O}_n$:

- If $d_0 \equiv 1 \pmod 4$ and n is even, then $d = d_0$, $\delta - \alpha$ is even, $\frac{n\sqrt{d_0}}{2} \in \mathfrak{O}_n$ and so $\frac{(\delta-\alpha)-n\sqrt{d_0}}{2} = \frac{\delta-\alpha}{2} - \frac{n}{2}\sqrt{d_0} \in \mathfrak{O}_n$.
- If $d_0 \equiv 1 \pmod 4$ and n is odd, then $d = d_0$, $\delta - \alpha$ is odd, $\frac{1+n\sqrt{d_0}}{2} \in \mathfrak{O}_n$, and so $\frac{(\delta-\alpha)-n\sqrt{d_0}}{2} \in \mathfrak{O}_n$,
- If $d_0 \not\equiv 1 \pmod 4$, then $d = 4d_0$, $D = n^2d = n^2 4d_0 \equiv 0 \pmod 4$, then $\delta - \alpha$ must be even, $\frac{(\delta-\alpha)-n\sqrt{d}}{2} = \frac{(\delta-\alpha)-n\sqrt{4d_0}}{2} = \frac{\delta-\alpha}{2} - n\sqrt{d_0} \in \mathfrak{O}_n$.

For $\gamma < 0$ the ideal is the same as for $\gamma > 0$, multiplied by $n\sqrt{d} \in \mathfrak{O}_n$. Next, show this is an ordered ideal:

$$\Delta_{K/\mathbb{Q}}(v_1, v_2) = \begin{cases} \gamma \cdot \frac{(\delta-\alpha)+n\sqrt{d}}{2} - \frac{(\delta-\alpha)-n\sqrt{d}}{2} \cdot \gamma' = \gamma n\sqrt{d} \\ (\gamma n\sqrt{d}) \cdot n\frac{-nd-(\delta-\alpha)\sqrt{d}}{2} - n\frac{-nd+(\delta-\alpha)\sqrt{d}}{2} \cdot (-\gamma n\sqrt{d}) = \gamma n\sqrt{d}(-n^2d) \end{cases}$$

(remember that $\gamma = \gamma' \in \mathbb{Z}$), and so by (19) we calculate:

$$N(I_g) = \frac{\Delta_{K/\mathbb{Q}}(v_1,v_2)}{\sqrt{D}} = \frac{\Delta_{K/\mathbb{Q}}(v_1,v_2)}{n\sqrt{d}} = \begin{cases} \gamma > 0 & \gamma > 0 \\ -\gamma n^2 d > 0 & \gamma < 0 \end{cases}$$

Hence the basis is ordered.
The ideal is unique apart from possible common factor of v_1, v_2. Hence, only the ideal class of this ideal corresponds to g. If instead of g a conjugate matrix is considered, hgh^{-1} where $h \in SL_2(\mathbb{Z})$, this matrix has the same characteristic polynomial, as hgh^{-1} has the same trace and determinant as g, then $(v_1, v_2)h^{-1}$ would turn up as characteristic vector corresponding to λ:

$$((v_1, v_2)h^{-1})(hgh^{-1}) = \lambda((v_1, v_2)h^{-1})$$

Since $h \in SL_2(\mathbb{Z})$, this gives the same ideal referred to a different basis (see (20)).
Conversely, let $[v_1, v_2]$ be an ordered basis over $\mathbb{Z}$ for an ideal of $\mathfrak{O}_n$ in $\mathbb{Q}(\sqrt{d_0})$, d_0 square free. Then there exist $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that

$$\begin{cases} \lambda v_1 = \alpha v_1 + \gamma v_2 \\ \lambda v_2 = \beta v_1 + \delta v_2 \end{cases}$$

Then $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ has the property that (v_1, v_2) is a characteristic vector with respect to the characteristic root λ. $g \in SL_2(\mathbb{Z})$ and has the required trace, by the selection of λ to be its eigenvalue, as λ dictates the characteristic polynomial, which fixes the trace and determinant of g. If instead of $[v_1, v_2]$ another basis $[v_1, v_2]h$ with $h \in SL_2(\mathbb{Z})$, had been considered, then g would be replaced by $h^{-1}gh$: $((v_1, v_2)h)(h^{-1}gh) = ((v_1, v_2)h)$. □

Recall that in $\mathfrak{O}_n$ not all ideals are invertible (Section 3.1.7). Hence, it may occur that the ideal corresponding to a matrix is not invertible. A non-invertible ideal may correspond to a matrix which is or is not conjugate to its inverse. For example, consider the following matrices, both with trace 6:

- $g = \begin{pmatrix} 1 & 1 \\ 4 & 5 \end{pmatrix}$, $\det(g) = 1$, $\mathrm{tr}(g)^2 - 4 = 32 = 2^2 \cdot 8$, $n = 2$, $d = 8$, $d_0 = 2$. This matrix is not conjugate to its inverse. The corresponding ideal is: $I_g = [\gamma, \frac{(\delta-\alpha)-n\sqrt{d}}{2}] = [4, 2 - 2\sqrt{2}]$, which is a non-invertible ideal of $\mathfrak{O}_2$.

- $g = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$, $\det(g) = 1$, $\mathrm{tr}(g)^2 - 4 = 32 = 2^2 \cdot 8$, $n = 2$, $d = 8$, $d_0 = 2$. It is easy to see that this matrix conjugate to its inverse, as it is symmetric. Taking $h = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, we have $hgh^{-1} = g^{-1}$. The corresponding ideal is: $I_g = [\gamma, \frac{(\delta-\alpha)-n\sqrt{d}}{2}] = [2, 2\sqrt{2}]$, which is not invertible in $\mathfrak{O}_2$. Here we can also calculate directly $I_g^2 = 2I_g \approx I_g$, implying I_g has no inverse.

3.4. **A Correspondence Between Quadratic Forms and Ideals.**

Another approach is to set up a correspondence between quadratic forms and ideals of integral rings of quadratic fields. However, this approach is limited to ideals of $\mathfrak{O}_K$, rather then ideals of any order, hence we must have $D = d$ field discriminant, $n = 1$. This also implies that only primitive quadratic forms are used, rather then all quadratic forms with a given discriminant.

Recall that a quadratic form Q is called **primitive** when its coefficients are not all divisible by any rational integer except ±1. The form discriminant D always satisfies $D \equiv 0$ or $1 \pmod 4$. When $D = d$ is also a discriminant of a quadratic field, then either D is square free, or $\frac{D}{4}$ is square free and then $\frac{D}{4} \equiv 2$ or $3 \pmod 4$ (by (15)).

- When $D \equiv 1 \pmod 4$ square free, the form is primitive.
- When $D \equiv 0 \pmod 4$, then $\frac{D}{4}$ is square free, we must have $\frac{D}{4} \equiv 2$ or $3 \pmod 4$.
  - If $gcd(a, b, c) = 1$, b even, so the form is primitive.
  - If $gcd(a, b, c) = 2$, then $[\frac{a}{2}, \frac{b}{2}, \frac{c}{2}]$ is a primitive form, with discriminant $\frac{D}{4} \equiv 0$ or $1 \pmod 4$, which contradicts $D = d$ is a field discriminant.

We conclude that if a form Q has discriminant $D = d$ which is a field discriminant, then Q must be a primitive form.

As is shown below, the same ideal corresponds to a matrix (using correspondence between matrices and ideals) and to the form that corresponds to that matrix, meaning the two methods coincide.

The correspondence between quadratic forms and ideals of $\mathfrak{O}_K$ is described in detail in [Cohn].

Theorem 9. *$K = \mathbb{Q}(\sqrt{d_0})$, d_0 square free, is a quadratic field with discriminant d (either $d \equiv 0 \pmod 4$ and then $d = 4d_0$, or $d \not\equiv 0 \pmod 4$, and then $d = d_0$).*

The following defines a correspondence between primitive quadratic forms with discriminant d and ordered ideals of $\mathfrak{O}_K$:

(1) *If $J = [\alpha, \beta]$ is an (ordered) ideal of $\mathfrak{O}_K$, then the corresponding form is:*

$$Q(J) = Q(x, y) = N(\alpha x + \beta y)/N(J) = ax^2 + bxy + cy^2$$

This form has integral coefficients and is a primitive form of discriminant d.

If $J_1 \approx J_2$ are ideals of $\mathfrak{O}_K$, then the corresponding forms $Q(J_1)$ and $Q(J_2)$ satisfy $Q(J_1) \approx Q(J_2)$.

(2) *Given a quadratic form, not necessarily primitive, which we write as:*

$$Q(x,y) = Ax^2 + Bxy + Cy^2 = t(ax^2 + bxy + cy^2)$$

where $\pm t$ is the greatest common divisor of A, B and C. We let $t > 0$ if $B^2 - 4AC > 0$, but if $B^2 - 4AC < 0$, we choose t so that $a > 0$. Denote $d = b^2 - 4ac$. Then the corresponding ideal is:

$$J(Q) = [\alpha, \beta] = \begin{cases} [a, \frac{b-\sqrt{d}}{2}], & a > 0, \textit{ any } d, \\ [\frac{b-\sqrt{d}}{2}, a]\sqrt{d} = [a\sqrt{d}, \frac{-d+b\sqrt{d}}{2}] & a < 0,\ d > 0 \end{cases}$$

This is an ordered ideal of $\mathfrak{O}_K$; $J(Q)$ is primitive when $a > 0$, whereas $J(Q)/\sqrt{d}$ is primitive when $a < 0$.

If two forms Q_1 and Q_2 with discriminant d satisfy $Q_1 \approx Q_2$, then $J(Q_1) \approx J(Q_2)$ in $\mathfrak{O}_K$.

3.4.1. *The Approaches Coincide.* For a matrix $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ we have defined a corresponding quadratic form:

$$Q_g(x,y) = \gamma x^2 + (\delta - \alpha)xy - \beta y^2$$

The discriminant D for Q_g is $\operatorname{tr}^2(g) - 4$. We assume that $D > 0$, meaning that $|\operatorname{tr}(g)| > 2$. Here we also assume the $D = d$ is a field discriminant, such that $d = d_0$ when $d \equiv 1 \pmod 4$, or $d_0 = d/4$ when $d \equiv 0 \pmod 4$, and d_0 is square free. This implies that Q_g is a primitive form. To this form we have defined the following corresponding ideal of $\mathfrak{O}_K$, $K = \mathbb{Q}(\sqrt{d_0})$ $(d > 0)$:

$$J(Q_g) = \begin{cases} [\gamma, \frac{(\delta-\alpha)-\sqrt{d}}{2}], & \gamma > 0 \\ [\frac{(\delta-\alpha)-\sqrt{d}}{2}, \gamma]\sqrt{d}, & \gamma < 0 \end{cases}$$

On the other hand, in Theorem 8 we have defined a correspondence between matrices and ideals of $\mathfrak{O}_n \subseteq \mathfrak{O}_K$ where $K = \mathbb{Q}(\sqrt{d_0})$ ($D = n^2 d$, d is a field discriminant, and d_0 as above). In this case $n = 1$, hence $D = d$ and $\mathfrak{O}_n = \mathfrak{O}_K$. For the matrix g as above corresponds the $\mathfrak{O}_K$ ideal:

$$J(g) = \begin{cases} [\gamma, \frac{(\delta-\alpha)-\sqrt{d}}{2}], & \gamma > 0 \\ [\frac{(\delta-\alpha)-\sqrt{d}}{2}, \gamma]\sqrt{d}, & \gamma < 0 \end{cases}$$

It can be easily verified that $J(Q_g) = J(g)$ for any value of γ.

3.5. **Norm of The Fundamental Unit of $\mathbb{Z}[\lambda]$.** There is no complete answer for the sign of the norm of the fundamental unit in the general case. However, when the discussion is limited to orders $\mathfrak{O} = \mathbb{Z}[\lambda]$ where λ is an eigenvalue of an $SL_2(\mathbb{Z})$ matrix, the answer is definite.
For a matrix with trace $= \pm 3$, then $D = 5$, $K = \mathbb{Q}(\sqrt{5})$, and $\mathbb{Z}[\lambda] = \mathbb{Z}[\sqrt{5}] = \mathfrak{O}_K$. The fundamental unit is $\frac{1+\sqrt{5}}{2}$, and its norm is -1. We now show that this is the only case for which the corresponding order has a unit with a negative norm.

Theorem 10. *Let $g \in SL_2(\mathbb{Z})$ with trace t such that $|t| > 3$, and eigenvalue $\lambda = \frac{t+\sqrt{t^2-4}}{2}$. Then the sign of the norm of the fundamental unit of $\mathbb{Z}[\lambda]$ is positive. In other words, any unit in $\mathbb{Z}[\lambda]$ has a positive norm.*

Proof. We can take $t > 0$, as $\lambda = \frac{t+\sqrt{t^2-4}}{2}$, $\mathbb{Z}[\lambda]$ is not effected by the sign of t. There are 2 cases, t is either odd or even.

(1) t is odd. In this case $t^2 - 4 \equiv 1 \pmod 4$, this means that none of the factors of $D = t^2 - 4$ is even. $D = t^2 - 4 = n^2 d$ where d is a field discriminant, in this case it must be that $d \equiv 1 \pmod 4$, hence $d = d_0$, n is odd, and we have $\mathbb{Z}[\lambda] = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. A general unit of $\mathbb{Z}[\lambda]$ is then $\frac{x+y\sqrt{D}}{2}$ such that $N(\frac{x+y\sqrt{D}}{2}) = \frac{x+y\sqrt{D}}{2} \cdot \frac{x-y\sqrt{D}}{2} = \frac{x^2-y^2D}{4} = \pm 1$, implying $x^2 - y^2 D = \pm 4$. We can always take $x = t$, $y = 1$ to receive a unit $\rho = \frac{t+\sqrt{D}}{2}$ with norm of $+1$: $N(\rho) = N(\frac{t+\sqrt{t^2-4}}{2}) = \frac{t^2-(t^2-4)}{4} = 1$. It may still happen that the fundamental unit of the relevant order has a negative norm, so that ρ is a power of that fundamental unit. By Section 3.1.4, the fundamental unit η satisfies $1 < \eta < \rho$. Let $\eta = \frac{a+b\sqrt{D}}{2}$, such that $a^2 - b^2 D = -4$, $a, b > 0$. We have $\eta < \rho = \frac{t+\sqrt{D}}{2}$, and as $b \geq 1$, we have $a \leq t$. Take $a = t - k$, $b = 1 + l$, $k, l \in \mathbb{N}$. $t > 3$ and odd, meaning $t \geq 5$ and $D = t^2 - 4 \geq 21$. We have
$$\begin{aligned} -4 &= a^2 - b^2 D = (t-k)^2 - (1+l)^2 D = \\ &= t^2 - D - k(2t-k) - D(2l + l^2) = \\ &= 4 - k(2t-k) - D(2l+l^2) \\ 8 &= k(2t-k) + D(2l+l^2) \geq k(10-k) + 21(l+l^2) \end{aligned}$$
with no integral solutions, except $k = l = 0$, but then $\rho = \eta$, with norm $+1$. Therefore, for any odd t, the fundamental unit of $\mathbb{Z}[\lambda]$ must have a positive norm.

(2) t is even. Then $\lambda = \frac{t+\sqrt{t^2-4}}{2} = \frac{t}{2} + \frac{\sqrt{D}}{2}$, and $\mathfrak{O} = \mathbb{Z}[\frac{\sqrt{D}}{2}]$. This can be solved as above, noting that $\rho = \frac{t}{2} + \frac{\sqrt{D}}{2}$ is always a unit

with a positive norm. If a fundamental unit $\eta = a + b\frac{\sqrt{D}}{2}$ with a negative norm exists, then $1 < \eta < \rho$, and $0 < a \leq \frac{t}{2}$, $b \geq 1$. Let $a = \frac{t}{2} - k$, $b = 1 + l$, $k, l \in \mathbb{Z}$. We have, with $t > 3$:

$$\begin{array}{rcl} -1 & = & (\frac{t}{2} - k)^2 - (1+l)^2\frac{D}{4} \\ 2 & = & k(t-k) + l\frac{D}{4}(2+l) > k \cdot \frac{t}{2} + l\frac{D}{4}2 \end{array}$$

Which has no integral solutions, except $k = l = 0$, but then $\rho = \eta$, with norm $+1$.

Another approach uses a Pell equation: a general element in $\mathbb{Z}[\lambda]$ is $a + b\frac{\sqrt{D}}{2} = \frac{2a+b\sqrt{D}}{2}$. There are always elements with norm of $+1$, we look for an element with norm -1:

$$(2a)^2 - b^2D = -4$$

t is even, hence $s = \frac{t}{2} \in \mathbb{Z}$, $\frac{D}{4} = \frac{t^2-4}{4} = (\frac{t}{2})^2 - 1 = s^2 - 1 \in \mathbb{Z}$. We can divide the equation by 4 and we have

$$a^2 - b^2(s^2 - 1) = -1$$

We need to determine if this Pell equation is solvable. To do so, we find the representation of $\sqrt{s^2-1}$ by continued fractions:

$$\sqrt{s^2-1} = [s-1, \overline{1, 2(s-1)}]$$

The cycle length is even, indicating that the Pell equation is unsolvable. This means that for any odd t there is no unit with a negative norm.

□

4. Summary and Examples

For a matrix $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ we have defined a corresponding quadratic form $Q_g(x,y) = \gamma x^2 + (\delta - \alpha)xy - \beta y^2$. For $g^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$, the corresponding form is $Q_{g^{-1}}(x,y) = -\gamma x^2 + (\alpha - \delta)xy + \beta y^2 = -Q_g(x,y)$. The discriminant D for Q_g is $\mathrm{tr}^2(g) - 4$. We assume that $D > 0$, meaning that $|\,\mathrm{tr}(g)| > 2$.

Also, we have defined a correspondence between matrices and ideals of $\mathfrak{O}_n \subseteq \mathfrak{O}_K$ where $K = \mathbb{Q}(\sqrt{d_0})$ ($D = n^2d$, $d_0 = d$ when $d \equiv 1 \pmod 4$, $d_0 = d/4$ when $d \equiv 0 \pmod 4$). To the matrix g above corresponds the ideal:

$$J(g) = \begin{cases} [\gamma, \frac{(\delta-\alpha)-n\sqrt{d}}{2}], & \gamma > 0 \\ [\frac{(\delta-\alpha)-n\sqrt{d}}{2}, \gamma]n\sqrt{d}, & \gamma < 0 \end{cases}$$

And for the inverse matrix g^{-1}, corresponds the ideal:

$$J(g^{-1}) = \begin{cases} [\frac{(\alpha-\delta)-n\sqrt{d}}{2}, -\gamma]n\sqrt{d} = [\frac{(\delta-\alpha)+n\sqrt{d}}{2}, \gamma](-n\sqrt{d}), & -\gamma < 0 \\ [-\gamma, \frac{(\alpha-\delta)-n\sqrt{d}}{2}] = [\gamma, \frac{(\delta-\alpha)+n\sqrt{d}}{2}](-1), & -\gamma > 0 \end{cases}$$

in the same integral ring $\mathfrak{O}_n$ of K.

Let us take a look at the equivalence relations between $J(g^{-1})$ and $J(g)'$, the conjugate of $J(g)$, which, for the case $\mathfrak{O}_K = \mathfrak{O}_n$, or $n = 1$, is also the inverse of $J(g)$, by Corollary 5. It is enough to look at the case $\gamma > 0$, as if $\gamma < 0$ we can replace g with g^{-1}. For $\gamma > 0$, by the correspondence formulas we have:

$$\begin{cases} J(g) & = [\gamma, \frac{(\delta-\alpha)-n\sqrt{d}}{2}] \\ J(g^{-1}) & = [\frac{(\delta-\alpha)+n\sqrt{d}}{2}, \gamma](-n\sqrt{d}) \end{cases}$$

By (21) above:

$$J(g)' = [\frac{(\delta-\alpha)+n\sqrt{d}}{2}, \gamma]$$

and so we have $J(g)'(-n\sqrt{d}) = J(g^{-1})$, which means $J(g)' \sim J(g^{-1})$. For strict equivalence, we use Theorem 7:

(1) For $d_0 < 0$, $J(g)' \sim J(g^{-1})$ implies $J(g)' \approx J(g^{-1})$. However, we have $D = n^2 d > 0$, as $d_0 > 0$, so this case is irrelevant.
(2) When $d_0 > 0$ and the fundamental unit of $\mathfrak{O}_n$ has a negative norm, then $J(g)' \sim J(g^{-1})$ implies $J(g)' \approx J(g^{-1})$.
(3) When $d_0 > 0$ and the fundamental unit of $\mathfrak{O}_n$ has positive norm, then for two (weakly) equivalent ideals $I \sim J$, one of $I \approx J$ and $I \approx (n\sqrt{d})J$ must hold. For J invertible we also know that only one of these holds, but not both.
    We use this to show that for an invertible $J(g)'$, $J(g)' \not\approx J(g^{-1})$. Obviously, when $I = J = J(g)'$ the case is $J(g)' \approx J(g)'$ and $J(g)' \not\approx (n\sqrt{d})J(g)'$. We can always multiply by (-1), as $N(-1) = (-1)(-1) = 1 > 0$, without losing strict equivalence (by (22)), so $(n\sqrt{d})J(g)' \approx (-n\sqrt{d})J(g)'$ and so we conclude $J(g)' \not\approx (-n\sqrt{d})J(g)' = J(g^{-1})$.
    When $J(g)'$ is non-invertible, it may happen that $J(g)' \approx (-n\sqrt{d})J(g)' = J(g^{-1})$. Note that $J(g)$ and $J(g)'$ are either both invertible or both non-invertible, as the elements in them have the same norms.

An example for $J(g)' \approx (-n\sqrt{d})J(g)' = J(g^{-1})$ where $J(g)'$ is non-invertible:

Let $g = \begin{pmatrix} 1 & 3 \\ 3 & 10 \end{pmatrix}$, then $I(g) = [3, \frac{9-3\sqrt{13}}{2}]$, $I(g^{-1}) = [\frac{9+3\sqrt{13}}{2}, 3](-3\sqrt{13})$.

Denote $I(g)' = J$, then $I(g^{-1}) = J(-3\sqrt{13})$.

By the example that follows Theorem 7, $I(g)$ and $I(g)'$ are non invertible ideals of $\mathfrak{O}_3$ in $K = \mathbb{Q}(\sqrt{13})$, $I(g) = I(g)'$, and $I(g)' = J \approx I(g) \approx J \cdot 3\sqrt{13} = J \cdot (-3\sqrt{13}) = I(g^{-1})$.

Corollary 7. *For any $SL_2(\mathbb{Z})$ matrix g with trace t such that $|t| > 2$, implying that $d_0 > 0$, $J(g)' \sim J(g^{-1})$ and*

$$\begin{cases} J(g)' \approx J(g^{-1}) & \textit{if } N(\eta) < 0 \\ J(g)' \not\approx J(g^{-1}) & \textit{if } N(\eta) > 0, J(g) \textit{ is invertible} \end{cases}$$

In the remaining case where $N(\eta) > 0$ and $J(g)$ is a non-invertible ideal, then the strict equivalence relation between $J(g)'$ and $J(g^{-1})$ is not determined.

By what we had shown till now, it is easy to verify the next theorem.

Theorem 11. *Let $g \in SL_2(\mathbb{Z})$ with trace t such that $|t| > 2$, and an eigenvalue λ. Denote $D = t^2 - 4 = n^2 d > 0$, where d is a field discriminant, and let K denote the quadratic field with discriminant d. The following are equivalent:*

1. *g is conjugate to its inverse g^{-1} (there exists a matrix $h \in SL_2(\mathbb{Z})$ such that $g^{-1} = hgh^{-1}$).*
2. *The corresponding forms Q_g and $Q_{g^{-1}} = -Q_g$ (with discriminant D) are strictly equivalent: $Q_g \approx -Q_g$.*
3. *The ideal $J(g)$ in the order $\mathbb{Z}[\lambda] = \mathfrak{O}_n$ of $\mathfrak{O}_K$, is strictly equivalent to $J(g^{-1})$: $J(g) \approx J(g^{-1})$.*
4. *The ideal $J(g)$ in the order $\mathbb{Z}[\lambda] = \mathfrak{O}_n$ of $\mathfrak{O}_K$, is weakly equivalent to $J(g)'$: $J(g) \sim J(g)'$.*
   Let η be the fundamental unit of the order $\mathbb{Z}[\lambda]$. Then we have

$$\begin{cases} J(g) \approx J(g)' & \textit{if } N(\eta) < 0 \\ J(g) \not\approx J(g)' & \textit{if } N(\eta) > 0, J(g) \textit{ is invertible} \end{cases}$$

Proof. The equivalence of (1), (2) and (3) was shown above.

- (3) ⇒ (4): By Corollary 7 we always have $J(g^{-1}) \sim J(g)'$. By (3) in this theorem we have $J(g) \sim J(g^{-1})$, therefore all three ideals $J(g)$, $J(g^{-1})$ and $J(g)'$ are weakly equivalent to each other, and in particular we have $J(g) \sim J(g)'$.
  When $N(\eta) < 0$ then weak equivalence implies strong equivalence, hence $J(g) \approx J(g)'$. When $N(\eta) > 0$, each weak equivalence class is composed of exactly two strict equivalence classes. In this case, $J(g) \approx J(g^{-1})$, and and for $J(g)$ invertible, from Corollary 7, $J(g^{-1}) \not\approx J(g)'$, hence it must be that $J(g) \not\approx J(g)'$.

- (4) ⇒ (3): When $N(\eta) < 0$ then $J(g) \approx J(g)'$, and from Corollary 7: $J(g)' \approx J(g^{-1})$, hence $J(g) \approx J(g^{-1})$.
  When $N(\eta) > 0$, each weak equivalence class is composed of exactly two strict equivalence classes. When $J(g)$ is invertible then $J(g) \not\approx J(g)'$, and by Corollary 7 $J(g^{-1}) \not\approx J(g)'$, hence it must be that $J(g) \approx J(g^{-1})$.

□

Corollary 8. *Under the above conditions, when $Z[\lambda] = \mathfrak{O}_K$, then $J(g)^2 \sim (1)$ and*

$$\begin{cases} J(g)^2 \approx (1) & \text{if } N(\eta) < 0 \\ J(g)^2 \not\approx (1) & \text{if } N(\eta) > 0 \end{cases}$$

Proof. This results from (4) of Theorem 11 above:

$$J(g) \sim J(g)' \Leftrightarrow J(g)J(g) \sim J(g)'J(g) \Leftrightarrow J(g)^2 \sim (1)$$

The last step is due to Corollary 5, by which we have $JJ' \sim (1)$ in $\mathfrak{O}_K$. For strict equivalence we use the same steps, remembering that all ideals in $\mathfrak{O}_K$ are invertible. □

Corollary 9. *Let $g \in SL_2(\mathbb{Z})$ a matrix with trace t satisfying $|t| > 3$, such that g is conjugate to g^{-1} in $SL_2(\mathbb{Z})$. Then when $J(g)$ is an invertible ideal, then $J(g) \sim J(g)'$ but $J(g) \not\approx J(g)'$.*

Proof. Follows immediately from theorems 10 and 11. □

Note: Considering ideals of $\mathfrak{O}_K$, and by Corollary 8, we can use the following theorem of Gauss to determine the number of ideal classes of $\mathfrak{O}_K$ with order of 2 (for a proof see, for example, [Moll]).

Theorem 12. (Gauss) Let K be a quadratic number field, with discriminant d. Suppose that d has N distinct prime factors. Let $\mathfrak{C}_{K,2}$ denote the maximum elementary abelian 2-subgroup of the ideal class group of $\mathfrak{O}_K$, meaning the maximal subgroup in which any element is of order 2. Then $\mathfrak{C}_{K,2}$ has order 2^{t_K}, where:

$$t_K = \begin{cases} N-2 & \text{if } d > 0 \text{ and } p \mid d \text{ for some prime } p \equiv 3 (\text{mod } 4) \\ N-1 & \textit{otherwise} \end{cases}$$

We can conclude that in most cases there is at least one ideal class with order of 2, and by the proof of [Moll], each such class has at least one ideal with order of 2.

If an ideal J of $\mathfrak{O}_K$ of order 2 corresponds to a matrix $g(J)$ with trace $t = \pm 3$ then the matrix is conjugate to its inverse, if the trace of the $g(J)$ satisfies $|t| > 3$ then such matrix is not conjugate to its inverse.

4.1. **Examples.**

(1) Find representatives for quadratic forms and for matrices with a positive trace, which correspond to the trivial ideal (1) of $\mathfrak{O}_n$.

$$(1) = \mathfrak{O}_n = \begin{cases} [1, -\frac{n}{2}\sqrt{d_0}] & \text{if } d_0 \equiv 1(\text{mod } 4), \text{ n even, } d_0 = d \\ [1, -\frac{1+n\sqrt{d_0}}{2}] & \text{if } d_0 \equiv 1(\text{mod } 4), \text{ n odd, } d_0 = d \\ [1, -n\sqrt{d_0}] & \text{if } d \not\equiv 1(\text{mod } 4), \ d_0 = \frac{d}{4} \end{cases}$$

By the correspondence between matrices and ideals (Theorem 8 in Section 3.3), we look for matrices with trace $t = \sqrt{D+4}$, $D = n^2 d$, where d is the field discriminant. We calculate:

$$\begin{cases} \lambda v_1 = \alpha v_1 + \gamma v_2 \\ \lambda v_2 = \beta v_1 + \delta v_2 \end{cases}$$

where $\lambda = \frac{t - n\sqrt{d}}{2}$, $v_1 = 1$ and v_2 as in the relevant ideal as detailed above. We find:

$$g(\mathfrak{O}_n) = \begin{cases} \begin{pmatrix} \frac{t}{2} & \frac{n^2 d_0}{4} \\ 1 & \frac{t}{2} \end{pmatrix} & \text{if } d \equiv 1(\text{mod } 4), \text{ n even} \\ \begin{pmatrix} \frac{t+1}{2} & \frac{n^2 d_0 - 1}{4} \\ 1 & \frac{t-1}{2} \end{pmatrix} & \text{if } d \equiv 1(\text{mod } 4), \text{ n odd} \\ \begin{pmatrix} \frac{t}{2} & n^2 d_0 \\ 1 & \frac{t}{2} \end{pmatrix} & \text{if } d \not\equiv 1(\text{mod } 4) \end{cases}$$

We can easily verify that these matrices are indeed integral:

- $d \equiv 1(\text{mod } 4)$, n even, then $d = d_0$, $4 | n^2 d_0 = \text{tr}(g)^2 - 4$, hence we also have $\frac{t}{2} \in \mathbb{Z}$.
- $d \equiv 1(\text{mod } 4)$, n odd, then $d = d_0$. $n^2 d_0 = \text{tr}(g)^2 - 4 \equiv 1(\text{mod } 4)$ hence $\frac{n^2 d_0 - 1}{4} \in \mathbb{Z}$. This also implies that t is odd, and so $\frac{t+1}{2}, \frac{t-1}{2} \in \mathbb{Z}$.
- $d \not\equiv 1(\text{mod } 4)$, then $d \equiv 0(\text{mod } 4)$, $d = 4d_0$. $n^2 d = \text{tr}(g)^2 - 4 \equiv 0 \ (\text{mod } 4)$, hence $\frac{t}{2} \in \mathbb{Z}$.

It is also easy to verify the discriminants of the above matrices are indeed 1, and so these matrices belong to $SL_2(\mathbb{Z})$.

By correspondence between matrices and forms (Section 2.8.2), for a matrix $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ the corresponding form is $\gamma x^2 + (\delta - \alpha)xy - \beta y^2$. The corresponding forms in this case are:

$$Q(x,y) = \begin{cases} x^2 - \frac{n^2 d_0}{4} y^2 & \text{if } d \equiv 1 (\text{mod } 4), \text{ n even} \\ x^2 - xy - \frac{n^2 d_0 - 1}{4} y^2 & \text{if } d \equiv 1 (\text{mod } 4), \text{ n odd} \\ x^2 - n^2 d_0 y^2 & \text{if } d \not\equiv 1 (\text{mod } 4) \end{cases}$$

Alternatively, the forms can be calculated directly from the ideals, using Theorem 9:

$$Q(x,y) = \begin{cases} (N(x - \frac{n}{2}\sqrt{d_0} y)/N(1) = x^2 - \frac{n^2 d_0}{4} y^2 & d \equiv 1 (\text{mod } 4), \text{ n even} \\ (N(x + \frac{-1 - n\sqrt{d_0}}{2} y)/N(1) = x^2 - xy - \frac{n^2 d_0 - 1}{4} y^2 & d \equiv 1 (\text{mod } 4), \text{ n odd} \\ (N(x - n\sqrt{d_0} y)/N(1) = x^2 - n^2 d_0 y^2 & d \not\equiv 1 (\text{mod } 4) \end{cases}$$

Which provides exactly the same result.
Note that any matrix with trace t for which $|t| > 3$ that corresponds to an order, cannot be conjugate to its inverse: by Theorem 11 and Corollary 9, for a matrix conjugate to its inverse with trace t, $|t| > 3$, the ideal $J(g)$ corresponding to g satisfies $J(g) \not\approx J(g)'$. But for $\mathfrak{O}$ it is always true that $\mathfrak{O} \approx \mathfrak{O}'$ ($\mathfrak{O}$ is always invertible as it must contain an element relatively prime to its index).
Examples:

- $d \equiv 1(\text{mod } 4)$, $n = 1$: $d = d_0 = 5$, $t = 3$. The matrix $g = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, corresponds to $\mathfrak{O}_K$. This is a symmetric matrix, for $h = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ we have $hgh^{-1} = g^{-1}$.
- $d \equiv 1(\text{mod } 4)$, n even: $D = 320 = (2^3)^2 \cdot 5$, $d = d_0 = 5$, $n = 2^3$, $t = 18$. The matrix $g = \begin{pmatrix} 9 & 80 \\ 1 & 9 \end{pmatrix}$ corresponds to $\mathfrak{O}_8$ in $K = \mathbb{Q}(\sqrt{5})$. The corresponding form is $x^2 - 80y^2$, which is equivalent to the reduced form $Q(x,y) = -16x^2 + 16xy + y^2$ which is not equivalent to $-Q$. Hence this matrix is not conjugate to its inverse matrix.
- $d \equiv 0(\text{mod } 4)$: $d = 8$, $d_0 = 2$, $n = 2$, D=32, $t = 6$. The matrix $g = \begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix}$ corresponds to $\mathfrak{O}_2$ in $K = \mathbb{Q}(\sqrt{2})$. The corresponding form is $x^2 - 8y^2$, which is equivalent to the reduced form $Q(x,y) = -4x^2 + 4xy + y^2$, which is not equivalent to $-Q$, hence g is not conjugate to its inverse.

(2) Matrices with trace= 3. $D = 3^2 - 4 = 5 = d = d_0$, by the algorithm described in Section 2.7 we find that there is a single class of quadratic forms with discriminant 5: $Q(x, y) = -x^2+xy+y^2$. Complete chain is [-1,1,1], [1,1,-1]. By the correspondence between forms and matrices ((14) in Section 2.8.2), we see that this form corresponds to the matrix $g = g(Q) = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$. g is a symmetric matrix and is conjugate to its inverse, for $h = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ we have $g = hg^{-1}h^{-1}$. The corresponding ideal is:

$$I(g) = [\frac{(\delta - \alpha) - \sqrt{d}}{2}, \gamma]\sqrt{d} = [\frac{1 - \sqrt{5}}{2}, -1]\sqrt{5} = \mathfrak{O}_K\sqrt{5}$$

By the general theory $N(\eta_1) < 0$ and $h(5) = 1$ and so by (24) we have $h_+(5) = h(5) = 1$, meaning that I_g is equivalent to its inverse.

(3) Matrices with trace= 5. $D = 5^2 - 4 = 21 = d = d_0$, by the algorithm described in Section 2.7 we find that there are two classes of quadratic forms with discriminant 21, and both are not reversible (not equivalent to the "inverse" form, meaning the form that corresponds to the inverse matrix):

(a) $Q_1(x, y) = -x^2 + 3xy + 3y^2$, complete chain is [-1,3,3], [3,3,-1].

(b) $Q_2(x, y) = x^2+3xy-3y^2$, complete chain is [1,3,-3], [-3,3,1].

By the correspondence between forms and matrices ((14) in Section 2.8.2), we see that these forms correspond to the matrices

(a) $g_1 = g(Q_1) = \begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix}$,

(b) $g_2 = g(Q_2) = \begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix}$

Which are not conjugate to their inverse.

The corresponding ideals are ideals of $\mathfrak{O}_K$ and therefore invertble:

(a) $I(g_1) = [-\sqrt{21}, \frac{3-\sqrt{21}}{2}\sqrt{21}] = [\frac{3-\sqrt{21}}{2}, -1]\sqrt{21} = \mathfrak{O}_K\sqrt{21}$

(b) $I(g_2) = [1, \frac{3-\sqrt{21}}{2}] = \mathfrak{O}_K$

It is easy to see that $I(g_1) = I(g_1)'$, and $I(g_2) = I(g_2)'$. By the general theory $N(\eta_1) > 0$. We can again conclude that neither g_1 nor g_2 is conjugate to its inverse.

(4) Matrices with trace= 6. $D = 6^2 - 4 = 32$. In this case the discriminant is not square free, $32 = 2 \cdot 4^2$, $d = 8$, $d_0 = 2$, $n = 2$. By the algorithm described in Section 2.7 we find the following classes of quadratic forms with discriminant 32:
(a) $Q_1(x, y) = -x^2 + 4xy + 4y^2$ not reversible
(b) $Q_2(x, y) = x^2 + 4xy - 4y^2$ not reversible
(c) $Q_3(x, y) = -2x^2 + 4xy + 2y^2$ reversible
By the correspondence between forms and matrices ((14) in Section 2.8.2), we see that these forms correspond to the matrices
(a) $g_1 = g(Q_1) = \begin{pmatrix} 1 & -4 \\ -1 & 5 \end{pmatrix}$,
(b) $g_2 = g(Q_2) = \begin{pmatrix} 1 & 4 \\ 1 & 5 \end{pmatrix}$
(c) $g_3 = g(Q_3) = \begin{pmatrix} 1 & -2 \\ -2 & 5 \end{pmatrix}$
From the information about the forms we know that g_1 and g_2 are not conjugate to their inverse, but g_3 is, and indeed for $h = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ we have $g_3 = hg_3^{-1}h^{-1}$.
The corresponding ideals are:
(a) $I(g_1) = [\frac{(\delta-\alpha)-n\sqrt{d}}{2}, \gamma]n\sqrt{d} = [\frac{4-2\sqrt{8}}{2}, -1]2\sqrt{8} = \mathfrak{O}_2 4\sqrt{2}$
(b) $I(g_2) = [\gamma, \frac{(\delta-\alpha)-n\sqrt{d}}{2}] = [1, \frac{4-2\sqrt{8}}{2}] = \mathbb{Z}[2\sqrt{2}] = \mathfrak{O}_2$
(c) $I(g_3) = [\frac{(\delta-\alpha)-n\sqrt{d}}{2}, \gamma]n\sqrt{d} = [\frac{4-2\sqrt{8}}{2}, -2]2\sqrt{8} = [2\sqrt{2}, 2](-4\sqrt{2})$
We already know that the sign of the fundamental unit is positive. We can calculate it directly: $\eta_1 = 1+\sqrt{2}$ is the fundamental unit of $\mathbb{Q}(\sqrt{2})$ and has negative norm, and $\eta_1^2 = 3 + 2\sqrt{2}$ is the fundamental unit of $\mathfrak{O}_2$, with a positive norm.
$I(g_2) = \mathfrak{O}_2 = I(g_2)'$, we conclude that g_2 is not conjugate to its inverse.
$I(g_1)$ and $I(g_3)$ are non-invertible ideals of $\mathfrak{O}_2$. We cannot conclude from this whether g_1 or g_3 are conjugate to their inverses. From the information about the forms we know that g_1 is conjugate to its inverse, and g_3 is not. We can calculate and find that both $I(g_1)$ and $I(g_3)$ are equal to their conjugates:
$I(g_1) = \mathfrak{O}_2 4\sqrt{2} = (\mathfrak{O}_2 4\sqrt{2})' = I(g_1)'$.
$I(g_3) = [-8\sqrt{2}, -16]$, $I(g_3)' = [-16, 8\sqrt{2}]$ and they are equal by the $SL_2(\mathbb{Z})$ transformation:

$$[-8\sqrt{2}, -16]\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = [-16, 8\sqrt{2}]$$

Hence $I(g_3) = I(g_3)'$.

(5) Matrices with trace= 7. $D = 7^2 - 4 = 45 = 3^2 \cdot 5$, here $n = 3$, $d = d_0 = 5$. By the algorithm described in Section 2.7 we find the following classes of quadratic forms with discriminant 45:

(a) $Q_1(x, y) = -3x^2 + 3xy + 3y^2$ reversible
(b) $Q_2(x, y) = -x^2 + 5xy - 5y^2$ not reversible
(c) $Q_3(x, y) = x^2 + 5xy - 5y^2$ not reversible

By the correspondence between forms and matrices ((14) in Section 2.8.2), we see that these forms correspond to the matrices:

(a) $g_1 = g(Q_1) = \begin{pmatrix} 2 & -3 \\ -3 & 5 \end{pmatrix}$,
(b) $g_2 = g(Q_2) = \begin{pmatrix} 1 & -5 \\ -1 & 6 \end{pmatrix}$
(c) $g_3 = g(Q_3) = \begin{pmatrix} 1 & 5 \\ 1 & 6 \end{pmatrix}$

By the conclusion about the forms we know that g_1 is conjugate to to its inverse, but g_2 and g_3 are not. Indeed, for $h = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ we have $g_1 = hg_1^{-1}h^{-1}$.

The corresponding ideals are:

(a) $I(g_1) = [\frac{(\delta-\alpha)-n\sqrt{d}}{2}, \gamma]n\sqrt{d} = [\frac{3-3\sqrt{5}}{2}, -3]3\sqrt{5}$
(b) $I(g_2) = [\frac{(\delta-\alpha)-n\sqrt{d}}{2}, \gamma]n\sqrt{d} = [\frac{5-3\sqrt{5}}{2}, -1]3\sqrt{5} = \mathfrak{O}_3 3\sqrt{5}$
(c) $I(g_3) = [\gamma, \frac{(\delta-\alpha)-n\sqrt{d}}{2}] = [1, \frac{5-3\sqrt{5}}{2}] = \mathfrak{O}_3$

We already know that the sign of the fundamental unit is positive. We can calculate it directly: $\eta_1 = \frac{1+\sqrt{5}}{2}$ is the fundamental unit of $\mathbb{Q}(\sqrt{5})$, and $\eta_1^4 = \frac{7+3\sqrt{5}}{2}$ is the fundamental unit of $\mathfrak{O}_3$, and indeed $N(\eta_1^4) = 1$.

$I(g_3) = \mathfrak{O}_3$ is an invertible ideal, and is strictly equivalent to its conjugate. We conclude that g_3 is not conjugate to its inverse. $I(g_1)$ and $I(g_2)$ are non-invertible ideals of $\mathfrak{O}_3$. We cannot conclude from this whether g_1 or g_2 are conjugate to their inverse or not. By conclusion from forms we know that g_1 is conjugate to its inverse, but g_2 is not. We find that both these ideals are equal to their conjugates:

$I(g_2) = \mathfrak{O}_3 3\sqrt{5} = (\mathfrak{O}_3 3\sqrt{5})' = I(g_2)'$.

Also, $I(g_1) = [-9\sqrt{5}, \frac{9\sqrt{5}-45}{2}]$, and by the following $SL_2(\mathbb{Z})$ transformation:

$$[-9\sqrt{5}, \frac{-45+9\sqrt{5}}{2}] \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} = [\frac{-45-9\sqrt{5}}{2}, 9\sqrt{5}]$$

we have $I(g_1) = I(g_1)'$.

(6) Matrices with trace= 15. $D = 15^2 - 4 = 221$, $d = d_0 = 221$, $n = 1$. By the algorithm described in Section 2.7 we find the following classes of quadratic forms with discriminant 221:
   (a) $Q_1(x, y) = 7x^2 + 9xy - 5y^2$ reversible, complete chain is [-7,5,7], [7,9,-5], [-5,11,5], [5,9,-7].
   (b) $Q_2(x, y) = 7x^2 + 5xy - 7y^2$ reversible, complete chain is [7,5,-7], [-7,9,5], [5,11,-5], [-5,9,7].
   (c) $Q_3(x, y) = -x^2+13xy+13y^2$ not reversible, complete chain is [-1,13,13], [13,13,-1].
   (d) $Q_4(x, y) = x^2 + 13xy - 13y^2$ not reversible, complete chain is [1,13,-13], [-13,13,1].

By the correspondence between forms and matrices in (14), we see that these forms correspond to the matrices:
   (a) $g_1 = g(Q_1) = \begin{pmatrix} 3 & 5 \\ 7 & 12 \end{pmatrix}$
   (b) $g_2 = g(Q_2) = \begin{pmatrix} 5 & 7 \\ 7 & 10 \end{pmatrix}$
   (c) $g_3 = g(Q_3) = \begin{pmatrix} 1 & -13 \\ -1 & 14 \end{pmatrix}$
   (d) $g_4 = g(Q_4) = \begin{pmatrix} 1 & 13 \\ 1 & 14 \end{pmatrix}$

From the information about the forms we know that g_1 and g_2 are conjugate to their inverse, but g_3 and g_4 are not. It is easy to verify that g_2 is conjugate to its inverse, as it is is symmetric. g_1 is conjugate to its inverse with $h = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}$, as $g_1 = hg_1^{-1}h^{-1}$.

The corresponding ideals are:
   (a) $I(g_1) = [\gamma, \frac{(\delta-\alpha)-n\sqrt{d}}{2}] = [7, \frac{9-\sqrt{221}}{2}]$
   (b) $I(g_2) = [\gamma, \frac{(\delta-\alpha)-n\sqrt{d}}{2}] = [7, \frac{5-\sqrt{221}}{2}]$
   (c) $I(g_3) = [\frac{(\delta-\alpha)-n\sqrt{d}}{2}, \gamma]n\sqrt{d} = [\frac{13-\sqrt{221}}{2}, -1]\sqrt{221} = \mathfrak{O}_K\sqrt{221}$
   (d) $I(g_4) = [\gamma, \frac{(\delta-\alpha)-n\sqrt{d}}{2}] = [1, \frac{13-\sqrt{221}}{2}] = \mathfrak{O}_K$

We know that the sign of the fundamental unit is positive, we can also calculate it directly: $\eta_1 = \frac{15+\sqrt{221}}{2}$, with norm of +1. As easy to see: $I(g_3) = \mathfrak{O}_K\sqrt{221} = I(g_3)'$, and $I(g_4) = \mathfrak{O}_K = I(g_4)'$, and we conclude again that neither g_3 nor g_4 is conjugate to its inverse. $I(g_1)$ and $I(g_2)$ are (invertible) ideals of $\mathfrak{O}_K$. From the information about forms we can conclude that these ideals are weakly but not strictly equivalent to their conjugates, respectively.

Appendix A: Discriminant, order and fundamental unit by trace

|trace|	D	d	d_0	n	$N(\eta)$
3	5	5	5	-	-1
4	12	12	3	-	+1
5	21	21	21	-	+1
6	32	8	2	2	+1
7	45	5	5	3	+1
8	60	60	15	-	+1
9	77	77	-	-	+1
10	96	24	6	2	+1
11	117	13	13	3	+1
12	140	140	35	-	+1
13	165	165	165	-	+1
14	192	12	3	2^2	+1
15	221	221	221	-	+1
16	252	28	7	3	+1
17	285	285	285	-	+1
18	320	5	5	2^3	+1
19	357	357	357	-	+1
20	396	44	11	3	+1
21	437	437	437	-	+1
22	480	120	30	2	+1
23	525	21	21	5	+1
24	572	572	143	-	+1
25	621	69	69	3	+1
26	672	168	42	2	+1
27	725	29	29	5	+1
28	780	780	195	-	+1
29	837	93	93	3	+1
30	896	56	14	2^2	+1
31	957	957	957	-	+1
32	1020	1020	255	-	+1
33	1085	1085	1085	-	+1
34	1152	8	2	$2^2 \cdot 3$	+1
35	1221	1221	1221	-	+1
36	1292	1292	323	-	+1
37	1365	1365	1365	-	+1
38	1440	40	10	$2 \cdot 3$	+1
39	1517	1517	1517	-	+1
40	1596	1596	399	-	+1

|trace|	D	d	d_0	n	$N(\eta)$
41	1677	1677	1677	-	+1
42	1760	440	110	2	+1
43	1845	205	205	3	+1
44	1932	1932	483	-	+1
45	2021	2021	2021	-	+1
46	2112	132	33	2^2	+1
47	2205	5	5	$3 \cdot 7$	+1
48	2300	92	23	5	+1
49	2397	2397	2397	-	+1
50	2496	156	39	2^2	+1
51	2597	53	53	7	+1
52	2700	12	3	$3 \cdot 5$	+1
53	2805	2805	2805	-	+1
54	2912	728	182	2	+1
55	3021	3021	3021	-	+1
56	3132	348	87	3	+1
57	3245	3245	3245	-	+1
58	3360	840	210	2	+1
59	3477	3477	3477	-	+1
60	3596	3596	899	-	+1
61	3717	413	413	3	+1
62	3840	60	15	2^3	+1
63	3965	3965	3965	-	+1
64	4092	4092	1023	-	+1
65	4221	469	469	3	+1
66	4352	17	17	2^4	+1
67	4485	4485	4485	-	+1
68	4620	4620	1155	-	+1
69	4757	4757	4757	-	+1
70	4896	136	34	$2 \cdot 3$	+1
71	5037	5037	5037	-	+1
72	5180	5180	1295	-	+1
73	5325	213	213	5	+1
74	5472	152	38	$2 \cdot 3$	+1
75	5621	5621	5621	-	+1
76	5772	5772	1443	-	+1
77	5925	237	237	5	+1
78	6080	380	95	2^2	+1
79	6237	77	77	3^2	+1
80	6396	6396	1599	-	+1

References

[BR] M.Baake and J.Roberts, *Reversing Symmetry Group of $GL(2,\mathbb{Z})$ and $PGL(2,\mathbb{Z})$ matrices with connections to cat maps and trace maps*, J. Phys. A: Math Gen. 30 (1997) 1549-1573.

[Cohn] H.Cohn, *Advanced Number Theory*, Dover Publications Inc, New York, 1962.

[Di] L.E.Dickson, *Introduction to the Theory of Numbers*, University of Chicago Press, Chicago, 1929.

[Lan] E. Landau, *Elementary Number Theory*, Chelesea Publishing Company, New York, 1958.

[Long] Y.Long, *Criterion for $SL(2,\mathbb{Z})$-matrix to be conjugate to its inverse*, Preprint (2001).

[Moll] R.A. Mollin, *Algebraic Number Theory*, Chapman & HALL/CRC, Boca Raton, London, New York, Washington DC, 1999.

[PR] L.Polterovich and Z.Rudnick, *Stable mixing for cats maps and quasi-morphisms of the modular group*, Preprint (2000).

[ScOp] W.Scharlau and H. Opolka, *From Fermat to Minkowsky, Lectures on the Theory of Numbers and its Historical Developement*, Springer, New York, 1985.

[Tau] O.Tausky, "Connections Between Algebraic Number Theory and Integral Matrices", appendix to *A Classical Invitation to Algebraic Numbers and Class Fields*, By H. Cohn, Universitext, Springer, New York, 1978.

[Tau2] O.Tausky, *Matrices of Rational Integers*, Bulletin American Mathematical Society 66 (1960), 327-345.