BULLETIN OF THE
INSTITUTE OF MATHEMATICS
ACADEMIA SINICA
Volume 11, Number 1, March 1983

A NOTE ON TERNARY QUADRATIC FORMS

BY

CHAO-LIANG SHEN (沈昭亮)

Abstract. Let F be the adjoint form of a ternary quadratic form f, and D be a square free integer which is represented by F. In this note we introduce an equivalence relation on the set of integral solutions of the equation $F(\mathbf{x})=D$. Let $\tilde{S}(F;\ D)$ be the set of equivalence classes. Then we prove that the number of orbits in $\tilde{S}(F;\ D)$ under the action of the group of automorphisms of F is less than or equal to h_D, the class number of proper equivalence classes of binary forms with discriminant D. In particular, if $h_D=1$, the action of the group of automorphisms of F on $\tilde{S}(F;\ D)$ is transitive.

Introduction. Compare to $SL(2, \mathbf{Z})$, people know very little about $SL(3, \mathbf{Z})$. Among subgroups of $SL(3, \mathbf{Z})$, the groups of automorphisms of ternary quadratic forms (see §1 for definitions) are of particular importance since, as pointed out by Gauss, that ternary quadratic forms are important for studying binary quadratic forms (Art. 266–284, [G]). The purpose of this series of papers is to study the arithmetic and the geometric properties of certain subgroups of $SL(3, \mathbf{Z})$ as such, and their applications to problems concerning binary forms.

In this note we introduce a notion of equivalence, which we call $\Gamma_D(F)$-equivalence, on the set $S(F;\ D)$ of integral solutions of the equation $F(\mathbf{x})=D$, where F is a ternary form, and D is a square free integer. If we denote $\tilde{S}(F;\ D)$ the set of $\Gamma_D(F)$-equivalence classes in $S(F;\ D)$, we prove that the number of orbits in $\tilde{S}(F;\ D)$ under the action of the group of automorphisms of F is not larger than the class number of properly equivalent binary

Received by the editors May 21, 1982.
This research is partially supported by a grant from NSC of R.O.C.

forms with discriminant D. Certain relevant analytic invariants shall be observed in the subsequent papers.

1. Preliminaries on ternary quadratic forms. In this section we summarize some basic facts about ternary quadratic forms which shall be used later.

By a *ternary quadratic form* we mean a homogeneous polynomial of degree two of the form

$$f(\underline{x}) = ax_1^2 + a' x_2^2 + a'' x_3^2 + 2bx_2 x_3 + 2b' x_1 x_3 + 2b'' x_1 x_2,$$

where $\underline{x}$ denotes column vector with component x_1, x_2, x_3 in order, and a, a', a'', b, b', b'' are integer. Equivalently, if we denote

$$M_f = \begin{Bmatrix} a & b'' & b' \\ b'' & a' & b \\ b' & b & a'' \end{Bmatrix},$$

then $f(\underline{x}) = \langle M_f \underline{x} | \underline{x} \rangle$, here we use the notation $\langle \underline{x} | \underline{y} \rangle$ to denote the inner product of vectors. We call M_f the associate (symmetric) matrix of f, and the quadratic form f the associate quadratic form of the symmetric matrix M_f. We denote $|M_f|$ the ***determinant*** of M_f, $D_f = -|M_f|$ the ***discriminant*** of the quadratic form f. If $D_f \neq 0$ we say that f is ***non-degenerated.*** In this note we only consider non-degenerated ternary (quadratic) forms. Following Gauss we define the ***adjoint form*** of a quadratic form f the quadratic form F such that its associate matrix is the negative of the adjoint of M_f, i. e., $M_F = -\operatorname{adj} M_f$, where the adjoint of a matrix $A = (\underline{u}, \underline{v}, \underline{w})$ is defined to be $\operatorname{adj} A = (\underline{v} \times \underline{w}, \underline{w} \times \underline{u}, \underline{u} \times \underline{v})$. Recall that $A^{-1} = (|A|)^{-1}. (\operatorname{adj} A)'$. We denote F by adj f if it is the adjoint form of f. Thus $D_{\operatorname{adj} f} = (D_f)^2$. The following is a basic property of adjoint forms.

LEMMA 1.1. $\operatorname{adj}(\operatorname{adj} f) = D_f \cdot f$.

Proof. Put $F = \operatorname{adj} f$. It follows from definition that $(1/D_f)\, M_F \cdot M_f = E$, the identity matrix, $M_F = D_f \cdot M_f^{-1}$. This implies

$$\frac{1}{|M_f/D_f|} \cdot \operatorname{adj}\left(\frac{M_f}{D_f}\right) = M_f,$$

$$\text{i. e.,}\quad -\frac{\operatorname{adj} M_F}{D_f} = M_f, \qquad \text{since}\quad |M_F| = -D_f^2.$$

Hence adj $F = D_f \cdot f$. ♯

We say two ternary forms f and g are ***equivalent*** if there exists $X \in \mathrm{SL}(3, Z)$ such that $X' M_f X = M_g$, where X' denotes the transpose of the matrix X. Let $\tilde{f}$ and $\tilde{g}$ be two binary forms. We say that $\tilde{f}$ and $\tilde{g}$ are ***properly equivalent*** if there exists $Y \in \mathrm{SL}(2, Z)$ such that $Y' M_{\tilde{f}} Y = M_{\tilde{g}}$. We use the notation $X: f \to g$ for $M_g = X' M_f X$ and the notation $X: f \simeq g$ for $X \in \mathrm{SL}(3, Z)$ such that $X' M_f X = M_g$.

PROPOSITION 1.2. *f is equivalent to g if and only if* adj f *is equivalent to* adj g. *In notation*: $X : f \simeq g$ *if and only if* adj X : adj $f \simeq$ adj g.

Proof. Say that $X : f \simeq g$. By using the fact $\operatorname{adj}(XY) = (\operatorname{adj} X)(\operatorname{adj} Y)$ we have

$$\begin{aligned} M_{\operatorname{adj} g} &= -\operatorname{adj} M_g \\ &= -\operatorname{adj}\,(X' M_f X) \\ &= (\operatorname{adj} X)'\,(-\operatorname{adj} M_f)\,(\operatorname{adj} X) \\ &= (\operatorname{adj} X)'\, M_{\operatorname{adj} f}\,(\operatorname{adj} X). \end{aligned}$$

Hence adj $X : M_{\operatorname{adj} f} \simeq M_{\operatorname{adj} g}$.

By using the same method and Lemma 1.1 we see that adj $f \sim$ adj g implies $f \sim g$. ♯

PROPOSITION 1.2. has a useful consequence which shall be used later.

COROLLARY 1.3. *Let $E(f) = \{X \in \mathrm{SL}(3, Z) : X : M_f \simeq M_f\}$ be the group of automorphisms of f. Then $E(\operatorname{adj} f) = \{\operatorname{adj} X : X \in E(f)\}$.*

We say a binary (quadratic) form $\tilde{f}(t, u)$ is ***represented*** by a ternary form $f(\underline{x})$ if there exists a transformation

$$\begin{aligned} x_1 &= m_1 t + n_1 u \\ x_2 &= m_2 t + n_2 u, \quad \text{or in notation } \underline{x} = (\underline{m}, \underline{n}) \begin{pmatrix} t \\ u \end{pmatrix}, \\ x_3 &= m_3 t + n_3 u \end{aligned}$$

such that $f(\underline{x}) = \tilde{f}(t, u)$, or in notation $(\underline{m}, \underline{n})' M_f(\underline{m}, \underline{n}) = M_{\tilde{f}}$. Concerning this notion Gause proved the following basic result which is the foundation of our observation.

THEOREM 1.4 (Art. 280, [G]). *If the binary form $\tilde{f}$ is represented by the ternary form $f(\underline{x})$, then the discriminant $D_{\tilde{f}}$ of $\tilde{f}$ is represented by the adjointed form of f. [Following Gauss, we call $D_{\tilde{f}} = b^2 - ac$ the discriminant of the binary form $\tilde{f}(t, u) = at^2 + 2btu + cu^2$.]*

Proof. We may think $\tilde{f}(t, u)$ as a degenerated ternary form $\tilde{f}(t, u, w)$ where the coefficients of the terms involving w are zero. Then $(\underline{m}, \underline{n}, \underline{0}) : f \to \tilde{f}$, where $\underline{0}$ is the column vector with components 0. By an argument similar to that in the proof of Proposition 1.2 we see that adj $(\underline{m}, \underline{n}, \underline{0})$: adj $f \to$ adj $\tilde{f}$. Since

$$M_{\tilde{f}} = \begin{pmatrix} a & b & 0 \\ b & c & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \text{adj } M_{\tilde{f}} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & ac - b^2 \end{pmatrix},$$

$$\text{adj } (\underline{m}, \underline{n}, \underline{0}) = \begin{pmatrix} 0 & 0 & m_2 n_3 - m_3 n_2 \\ 0 & 0 & m_3 n_1 - m_1 n_3 \\ 0 & 0 & m_1 n_2 - m_2 n_1 \end{pmatrix},$$

we see that

$$(b^2 - ac)\, x_3^2 = \text{adj } f((m_2 n_3 - m_3 n_2)\, x_3, \\ (m_3 n_1 - m_1 n_3)\, x_3, (m_1 n_2 - m_2 n_1)\, x_3)\,.$$

Substitute $x_3 = 1$, we obtain

$$\text{adj } f(m_2 n_3 - m_3 n_2, m_3 n_1 - m_1 n_3, m_1 n_2 - m_2 n_1) = b^2 - ac. \quad \#$$

REMARK 1.5. Theorem 1.4 tells us that if $\tilde{f}$ is respresented by f via the substitution $(\underline{m}, \underline{n})$, then adj $f(\underline{m} \times \underline{n}) = D_{\tilde{f}}$, where $\underline{m} \times \underline{n}$ expresses the cross product of the vectors $\underline{m}$ and $\underline{n}$. The cross product is called, according to Gauss, the *adjoint* of the representation $(\underline{m}, \underline{n})$ of $\tilde{f}$ by f.

2. **On the solution set of a Diophantine equation.** Theorem 1.4 is quite an interesting phenomenon since it tells us that integral points on the surface adj $f(\underline{x}) = D$ have certain arithmetic meaning.

To be more precise, suppose $\underline{l}$ is an integral point such that $\text{adj } f(\underline{l}) = D$ then, by Art. 279 [G], we can find two integral vectors $\underline{m}$, $\underline{n}$ such $\underline{l} = \underline{m} \times \underline{n}$, then $\tilde{f} = f\left((\underline{m}, \underline{n})\binom{t}{u}\right)$ is a binary form with discriminant D, i.e., $\underline{l}$ is the adjoint of a representation of the binary form $\tilde{f}$ by f. The purpose of this section is to study, by using the result mentioned above as tool, the action of $E(\text{adj } f)$ on the set of integral solutions of the equation $\text{adj } f(\underline{x}) = D$.

We need some lemmas.

LEMMA 2.1. *If $\underline{l}$ has a cross product decomposition $\underline{m} \times \underline{n}$, then for any three by three matrix T we have $(T\underline{m}) \times (T\underline{n}) = (\text{adj } T)\, \underline{l}$.*

Proof. Say that $T = (a_{ij})$,

$$T\underline{m} = (a_{11} m_1 + a_{12} m_2 + a_{13} m_3,\quad a_{21} m_1 + a_{22} m_2 + a_{23} m_3,\ a_{31} m_1 + a_{32} m_2 + a_{33} m_3)',$$

$$T\underline{n} = (a_{11} n_1 + a_{12} n_2 + a_{13} n_3,\quad a_{21} n_1 + a_{22} n_2 + a_{23} n_3,\ a_{31} n_1 + a_{32} n_2 + a_{33} n_3)'.$$

Then

$$\left(\sum_{i=1}^{3} a_{2i}\, m_i\right)\left(\sum_{j=1}^{3} a_{3j}\, n_j\right) - \left(\sum_{i=1}^{3} a_{3i}\, m_i\right)\left(\sum_{j=1}^{3} a_{2j}\, n_j\right)$$
$$= (a_{22} a_{33} - a_{23} a_{32})\, l_1 + (a_{23} a_{31} - a_{21} a_{33})\, l_2 + (a_{21} a_{32} - a_{31} a_{22}) l_3,$$

$$\left(\sum_{i=1}^{3} a_{3i}\, m_i\right)\left(\sum_{j=1}^{3} a_{1j}\, n_j\right) - \left(\sum_{i=1}^{3} a_{1i}\, m_i\right)\left(\sum_{j=1}^{3} a_{3j}\, n_j\right)$$
$$= (a_{13} a_{32} - a_{12} a_{33})\, l_1 + (a_{11} a_{33} - a_{13} a_{31}) l_2 + (a_{12} a_{31} - a_{11} a_{32})\, l_3,$$

$$\left(\sum_{i=1}^{3} a_{1i}\, m_i\right)\left(\sum_{j=1}^{3} a_{2j}\, n_j\right) - \left(\sum_{i=1}^{3} a_{2i}\, m_i\right)\left(\sum_{j=1}^{3} a_{1j}\, n_j\right)$$
$$= (a_{12} a_{23} - a_{13} a_{22})\, l_1 + (a_{13} a_{21} - a_{11} a_{23})\, l_2 + (a_{11} a_{22} - a_{12} a_{21})\, l_3\,.$$

The coefficients of these three identities are the three rows of the adjoint of T. Thus we obtain the result $(T\underline{m}) \times (T\underline{n}) = (\text{adj } T)\underline{l}$. #

LEMMA 2.2. *If $\underline{g} \times \underline{h} = \underline{m} \times \underline{n}$, then we have the identity $\langle \underline{h} | \underline{x} \times \underline{m} \rangle \underline{g} - \langle \underline{g} | \underline{x} \times \underline{m} \rangle \underline{h} = \langle \underline{m} \times \underline{n} | \underline{x} \rangle \underline{m}$ for all vector $\underline{x}$.*

Proof. By the formula on page 64 of [*W*] $(\underline{r} \times \underline{s}) \times \underline{t} = \langle \underline{r} | \underline{t} \rangle \underline{s} - \langle \underline{s} | \underline{t} \rangle \underline{r}$ we have

$$\begin{aligned}
\langle \underline{h} | \underline{x} \times \underline{m} \rangle \underline{g} - \langle \underline{g} | \underline{x} \times \underline{m} \rangle \underline{h} &= (\underline{h} \times \underline{g}) \times (\underline{x} \times \underline{m}) \\
&= (\underline{g} \times \underline{h}) \times (\underline{m} \times \underline{x}) \\
&= -(\underline{m} \times \underline{x}) \times (\underline{g} \times \underline{h}) \\
&= -(\underline{m} \times \underline{x}) \times (\underline{m} \times \underline{n}) \\
&= -\langle \underline{m} | \underline{m} \times \underline{n} \rangle \underline{x} + \langle \underline{x} | \underline{m} \times \underline{n} \rangle \underline{m} \\
&= \underline{0} + \langle \underline{m} \times \underline{n} | \underline{x} \rangle \underline{m} \\
&= \langle \underline{m} \times \underline{n} | \underline{x} \rangle \underline{m}. \quad \#
\end{aligned}$$

LEMMA 2.3. *If* $\underline{m} \times \underline{n} = \underline{g} \times \underline{h}$, $\langle \underline{m} \times \underline{n} | \underline{x} \rangle = 1$, *then we have the following identities*

$$\begin{aligned}
\underline{g} &= \langle \underline{g} | \underline{n} \times \underline{x} \rangle \underline{m} + \langle \underline{g} | \underline{x} \times \underline{m} \rangle \underline{n}, \\
\underline{h} &= \langle \underline{h} | \underline{n} \times \underline{x} \rangle \underline{m} + \langle \underline{h} | \underline{x} \times \underline{m} \rangle \underline{n}.
\end{aligned}$$

Proof. By hypothesis and [Widder, p. 64]

$$\begin{aligned}
\underline{g} &= \langle \underline{m} \times \underline{n} | \underline{x} \rangle \underline{g} \\
&= \langle \underline{m} | \underline{n} \times \underline{x} \rangle \underline{g} \\
&= (\underline{m} \times \underline{g}) \times (\underline{n} \times \underline{x}) + \langle \underline{g} | \underline{n} \times \underline{x} \rangle \underline{m}.
\end{aligned}$$

Since $\underline{r} \times (\underline{s} \times \underline{t}) = \langle \underline{r} | \underline{t} \rangle \underline{s} - \langle \underline{r} | \underline{s} \rangle \underline{t}$,

$$\begin{aligned}
(\underline{m} \times \underline{g}) \times (\underline{n} \times \underline{x}) &= \langle \underline{m} \times \underline{g} | \underline{x} \rangle \underline{n} - \langle \underline{m} \times \underline{g} | \underline{n} \rangle \underline{x} \\
&= \langle \underline{g} | \underline{x} \times \underline{m} \rangle \underline{n} \\
&= \langle \underline{g} | \underline{x} \times \underline{m} \rangle \underline{n} + \langle \underline{g} | \underline{g} \times \underline{h} \rangle \underline{x} \\
&= \langle \underline{g} | \underline{x} \times \underline{m} \rangle \underline{n}.
\end{aligned}$$

Hence $\underline{g} = \langle \underline{g} | \underline{n} \times \underline{x} \rangle \underline{m} + \langle \underline{g} | \underline{x} \times \underline{m} \rangle \underline{n}$.

By similar argument we can also obtain the identity $\underline{h} = \langle \underline{h} | \underline{n} \times \underline{x} \rangle \underline{m} + \langle \underline{h} | \underline{x} \times \underline{m} \rangle \underline{n}$. #

Let $S(F;\, D) = \{\underline{x} \in Z^3 : F(\underline{x}) = D\} / \pm I$ be the set of integral solutions of the equations $F(\underline{x}) = D$, where F is a ternary form, and we identify the solutions $\underline{x}$ and $-\underline{x}$. Then it is clear that $T\underline{x} \in S(F;\, D)$ for $T \in E(F)$ and $\underline{x} \in S(F;\, D)$. For our purpose we need to study the action of $E(F)$ on $S(F;\, D)$. Suppose F is the adjoint form of the ternary form f and $\underline{l} \in S(F;\, D)$ with a cross product decomposition $\underline{l} = \underline{m} \times \underline{n}$. Then $f\left((\underline{m}, \underline{n}) \begin{pmatrix} t \\ u \end{pmatrix}\right)$ is a binary form with disciminant D. It is natural to ask that if

$T \in E(f)$, $\underline{\mu} = (\text{adj } T)\, \underline{l}$ such that $\underline{l} = \underline{m} \times \underline{n}$, $\underline{\mu} = \underline{\xi} \times \underline{\eta}$, then is there any relation between the binary forms $f\left((\underline{m}, \underline{n}) \binom{t}{u}\right)$ and $f\left((\underline{\xi}, \underline{\eta}) \binom{t}{u}\right)$? The answer is as follows.

THEOREM 2.4. *Say that D is square free integer, i.e., without square divisor. For $\underline{l} \in S$ (adj f; D) such that it is the adjoint of a representation of the binary form ϕ by f. Then for any $T \in E(f)$, if ψ is a binary form with discriminant D which is represented by f with the adjoint* (adj T) $\underline{l}$, *ψ must be properly equivalent to ϕ.*

Proof. Put $\underline{l} = \underline{m} \times \underline{n}$ s.t. ϕ is represented by f via $(\underline{m}, \underline{n})$. Then, by lemma 2.1, we have $(\text{adj } T)\underline{l} = (T\underline{m}) \times (T\underline{n})$, write $\underline{\mu} = (\text{adj } T)\, \underline{l}$, $\underline{\mu} = \underline{\xi} \times \underline{\eta}$ such that Ψ is represented by f via $(\underline{\xi}, \underline{\eta})$.

We notice that there exists $\underline{x} \in Z^3$ such that $\langle \underline{\mu} | \underline{x} \rangle = 1$ since D is square free and hence the components of $\underline{\mu}$ must be coprime. Since $T\underline{m} \times T\underline{n} = \underline{\xi} \times \underline{\eta}$, by Lemma 2.3, we have

$$\langle \underline{\xi} | T\underline{n} \times \underline{x} \rangle T\underline{m} + \langle \underline{\xi} | \underline{x} \times T\underline{m} \rangle T\underline{n} = \underline{\xi}$$
$$\langle \underline{\eta} | T\underline{n} \times \underline{x} \rangle T\underline{m} + \langle \underline{\eta} | \underline{x} \times T\underline{m} \rangle T\underline{n} = \underline{\eta},$$

That is

$$(T\underline{m},\ T\underline{n}) \begin{bmatrix} \langle \underline{\xi} | T\underline{n} \times \underline{x} \rangle & \langle \underline{\eta} | T\underline{n} \times \underline{x} \rangle \\ \langle \underline{\xi} | \underline{x} \times T\underline{m} \rangle & \langle \underline{\eta} | \underline{x} \times T\underline{m} \rangle \end{bmatrix} = (\xi, \eta).$$

Denote the square matrix by $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$.

The last identity implies

$$\left\langle M_f T(\underline{m}, \underline{n}) \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} t \\ u \end{bmatrix} \middle|\, T(\underline{m}, \underline{n}) \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} t \\ u \end{bmatrix} \right\rangle$$
$$= \left\langle M_f (\underline{\xi}, \underline{\eta}) \begin{bmatrix} t \\ u \end{bmatrix} \middle|\, (\underline{\xi}, \underline{\eta}) \begin{bmatrix} t \\ u \end{bmatrix} \right\rangle$$
$$= \psi(t, u)\,.$$

On the other hand, as $T \in E(f)$, $T' M_f T = M_f$, so that

$$\left\langle M_f T(\underline{m}, \underline{n}) \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} t \\ u \end{bmatrix} \middle|\, T(\underline{m}, \underline{n}) \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} t \\ u \end{bmatrix} \right\rangle$$
$$= \left\langle M_f (\underline{m}, \underline{n}) \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} t \\ u \end{bmatrix} \middle|\, (\underline{m}, \underline{n}) \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} t \\ u \end{bmatrix} \right\rangle$$
$$= \phi\left(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} t \\ u \end{bmatrix} \right).$$

Since

$$\begin{aligned}\alpha\beta-\beta\gamma &= \langle\underline{\xi}\,|\,T\underline{n}\times\underline{x}\rangle\langle\underline{\eta}\,|\,\underline{x}\times T\underline{m}\rangle\\ &\quad-\langle\underline{\eta}\,|\,T\underline{n}\times\underline{x}\rangle\langle\underline{\xi}\,|\,\underline{x}\times T\underline{m}\rangle\\ &= \langle\langle\underline{\eta}\,|\,\underline{x}\times T\underline{m}\rangle\underline{\xi}\,|\,T\underline{n}\times\underline{x}\rangle\\ &\quad-\langle\langle\underline{\xi}\,|\,\underline{x}\times T\underline{m}\rangle\underline{\eta}\,|\,T\underline{n}\times\underline{x}\rangle\\ &= \langle\langle\underline{\eta}\,|\,\underline{x}\times T\underline{m}\rangle\underline{\xi}\times T\underline{n}\,|\,\underline{x}\rangle\\ &\quad-\langle\langle\underline{\xi}\,|\,\underline{x}\times T\underline{m}\rangle\underline{\eta}\times T\underline{n}\,|\,\underline{x}\rangle\\ &= \langle[\langle\underline{\eta}\,|\,\underline{x}\times T\underline{m}\rangle\underline{\xi}-\langle\underline{\xi}\,|\,\underline{x}\times T\underline{m}\rangle\underline{\eta}]\times T\underline{n}\,|\,\underline{x}\rangle,\end{aligned}$$

where, by Lemma 2.2,

$$\langle\underline{\eta}\,|\,\underline{x}\times T\underline{m}\rangle\underline{\xi}-\langle\underline{\xi}\,|\,\underline{x}\times T\underline{m}\rangle\underline{\eta}=\langle T\underline{m}\times T\underline{n}\,|\,\underline{x}\rangle T\underline{m}.$$

Hence

$$\begin{aligned}\alpha\delta-\beta\gamma &= \langle\langle T\underline{m}\times T\underline{n}\,|\,\underline{x}\rangle T\underline{m}\times T\underline{n}\,|\,\underline{x}\rangle\\ &= [\langle T\underline{m}\times T\underline{n}\,|\,\underline{x}\rangle]^2\\ &= [\langle\underline{\mu}\,|\,\underline{x}\rangle]^2\\ &= 1^2\\ &= 1,\end{aligned}$$

(Note that this argument also shows the transformation in Lemma 2.3 is special linear), and this proves the proper equivalence of ϕ and Ψ. #

Now let $\phi(t,u)=pt^2+2qtu+ru^2$ be a binary form with discriminant D which is represented by the ternary form f via $(\underline{m},\underline{n})$, where D is square free. Then, as the components of $\underline{m}\times\underline{n}$ are coprime, we can find an integral vector $\underline{x}$ such that $\langle\underline{m}\times\underline{n}\,|\,\underline{x}\rangle=\det(\underline{m},\underline{n},\underline{x})=1$. Furthermore, calculation shows that

$$f(\underline{m})=\langle M_f\underline{m}\,|\,\underline{m}\rangle=p,\ f(\underline{n})=\langle M_f\underline{n}\,|\,\underline{n}\rangle=r,$$
$$\langle M_f\underline{m}\,|\,\underline{n}\rangle=q,$$

and

$$(\underline{m},\underline{n},\underline{x})'M_f(\underline{m},\underline{n},\underline{x})=\begin{bmatrix}p & q & \langle M_f\underline{m}\,|\,\underline{x}\rangle\\ q & r & \langle M_f\underline{n}\,|\,\underline{x}\rangle\\ \langle M_f\underline{m}\,|\,\underline{x}\rangle & \langle M_f\underline{n}\,|\,\underline{x}\rangle & f(\underline{x})\end{bmatrix}\ldots(\mathrm{A})$$

If we take the adjoint of both sides of (A), we obtain an expression of the following shape:

$$(\underline{\alpha},\ \underline{\beta},\ \underline{l})'(-\mathrm{adj}\,M_f)(\underline{\alpha},\ \underline{\beta},\ \underline{l})=\begin{bmatrix} * & * & * \\ * & * & * \\ * & * & D \end{bmatrix},$$

i. e.,

$$(\underline{\alpha},\ \beta,\ \underline{l})'\,(M_{\mathrm{adj}\,f})(\underline{\alpha},\ \beta,\ \underline{l})=\begin{bmatrix} * & * & * \\ * & * & * \\ * & * & D \end{bmatrix},$$

where $\underline{l}=\underline{m}\times\underline{n}$, $\underline{l}'M_{\mathrm{adj}\,f}\,\underline{l}=D$. In general, as shown in Disquisitiones Arithematicae, the choice of the representation $(\underline{m},\ \underline{n})$ of the binary form ϕ by the ternary form f is not unique, and there is no clear relation between two such representations. In order to study the action of $E(\mathrm{adj}\ f)$ on $S(\mathrm{adj}\ f;\ D)$, we introduce a notion of equivalence.

We shall use the notation ${}_f\Sigma_D\left(\begin{bmatrix} p & q \\ q & r \end{bmatrix}\right)$ to denote the set of the associate matrices of those ternary forms which are equivalent to f and are of the form

$$\begin{bmatrix} p & q & * \\ q & r & * \\ * & * & * \end{bmatrix},$$

where $q^2-pr=D$.

Let F be the adjoint form of the ternary form f, which represents a square free integer D. We say two integral vectors $\underline{l}$ and $\underline{\mu}$ in $S(F;\ D)$ are "$\Gamma_D(F)$-*equivalent*" if there exist integral vectors $\underline{\alpha}$, $\underline{\beta}$ such that $|(\underline{\alpha},\ \underline{\beta},\ \underline{l})|=1$, say adj $(\underline{m},\ \underline{n},\ \underline{x})=(\underline{\alpha},\ \underline{\beta},\ \underline{l})$, and $U\in SL(3,\ \boldsymbol{Z})$ such that

1°. if the symmetric matrix $(\underline{m},\ \underline{n},\ \underline{x})'M_f\,(\underline{m},\ \underline{n},\ \underline{x})$ is in ${}_f\Sigma_D\left(\begin{bmatrix} p & q \\ q & r \end{bmatrix}\right)$, then so is $(\mathrm{adj}\ U)'(\underline{m},\ \underline{n},\ \underline{x})'M_f\,(\underline{m},\ \underline{n},\ \underline{x})\ \mathrm{adj}\ U$,

2°. the third column vector of $(\underline{\alpha},\ \underline{\beta},\ \underline{l})\,U$ is $\underline{\mu}$ (If 1° and 2° hold, we denote $U\langle\underline{l}\rangle\cong\underline{\mu}$.)

If is clear that $\underline{l}$ is $\Gamma_D(F)$-equivalent to itself, and if $\underline{l}$ is $\Gamma_D(F)$-equivalent to $\underline{\mu}$, then $\underline{\mu}$ is $\Gamma_D(F)$-equivalent to $\underline{l}$. Now suppose $\underline{l}$ is $\Gamma_D(F)$-equivalent to $\underline{\mu}$, and $\underline{\mu}$ is $\Gamma_D(F)$-equivalent to $\underline{\nu}$ say, $\underline{l}=\underline{m}\times\underline{n}$, $\underline{\mu}=\underline{\xi}\times\underline{\eta}=\underline{\varepsilon}\times\underline{\delta}$ and U, V in SL(3, $\boldsymbol{Z}$) such that

$(\underline{m}, \underline{n}, \underline{x})'M_f \cdot (\underline{m}, \underline{n}, \underline{x})$ and $(\text{adj } U)'(\underline{m}, \underline{n}, \underline{x})'M_f(\underline{m}, \underline{n}, \underline{x})$ adj U are in ${}_f\Sigma_D\left(\begin{bmatrix} p_1 & q_1 \\ q_1 & r_1 \end{bmatrix}\right)$, where $(\underline{m}, \underline{n}, \underline{x})$ adj $U = (\underline{\xi}, \underline{\eta}, \underline{t})$; $(\underline{\varepsilon}, \underline{\delta}, \underline{y})'M_f(\underline{\varepsilon}, \underline{\delta}, \underline{y})$ and $(\text{adj } V)'(\underline{\varepsilon}, \underline{\delta}, \underline{y})'M_f(\underline{\varepsilon}, \underline{\delta}, \underline{y})$ (adj V) are in ${}_f\Sigma_D\left(\begin{bmatrix} p_2 & q_2 \\ q_2 & r_2 \end{bmatrix}\right)$, $V\langle\underline{\mu}\rangle \cong \underline{\nu}$. Since $\underline{\mu} = \underline{\xi} \times \underline{\eta} = \underline{\varepsilon} \times \underline{\delta}$, the binary forms $\begin{bmatrix} p_1 & q_1 \\ q_1 & r_1 \end{bmatrix}$ and $\begin{bmatrix} p_2 & q_2 \\ q_2 & r_2 \end{bmatrix}$ are, according to an argument similar to that in the proof of Theorem 2.4 or see Art. 280 III. [G], properly equivalent, say $A'\begin{bmatrix} p_2 & q_2 \\ q_2 & r_2 \end{bmatrix} A = \begin{bmatrix} p_1 & q_1 \\ q_1 & r_1 \end{bmatrix}$. Let $\tilde{A} = \begin{bmatrix} A & & 0 \\ & & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Then $\tilde{A}'(\underline{\varepsilon}, \underline{\delta}, \underline{y})'M_f(\underline{\varepsilon}, \underline{\delta}, \underline{y})\tilde{A}$ and $\tilde{A}'(\text{adj } V)'(\underline{\varepsilon}, \underline{\delta}, \underline{y})'M_f(\underline{\varepsilon}, \underline{\delta}, \underline{y})$ (adj V) $\tilde{A}$ are in $\Sigma\left(\begin{bmatrix} p_1 & q_1 \\ q_1 & r_1 \end{bmatrix}\right)$. Write $(\underline{\varepsilon}, \underline{\delta}, \underline{y})\tilde{A} = (\underline{\xi}_1, \underline{\eta}_1, \underline{t}_1)$, $\tilde{A}^{-1}(\text{adj } V)\tilde{A} = \text{adj } W$. Then $\underline{\varepsilon} \times \underline{\delta} = \underline{\xi}_1 \times \underline{\eta}_1 = \underline{\mu}$ since $A \in \mathrm{SL}(2, \boldsymbol{Z})$. By Lemma 2.3 and the argument in the proof of Theorem 2.4, there exists $B \in \mathrm{SL}(2, \boldsymbol{Z})$ such that

$$(\underline{\xi}_1, \underline{\eta}_1, \underline{t}_1) = (\underline{\xi}, \underline{\eta}, \underline{t}_1)\begin{bmatrix} B & & 0 \\ & & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Now we need a lemma (this lemma is actually included implicitly in Art. 282 of [G]).

LEMMA 2.5. *Suppose* $|(\underline{\xi}, \underline{\eta}, \underline{t})| = |(\underline{\xi}, \underline{\eta}, \underline{t}_1)| = 1$. *Then*

$$(\underline{\xi}, \underline{\eta}, \underline{t}_1)\begin{bmatrix} 1 & 0 & -\langle \underline{\eta} \times \underline{t} | \underline{t}_1 \rangle \\ 0 & 1 & -\langle \underline{t} \times \underline{\xi} | \underline{t}_1 \rangle \\ 0 & 0 & 1 \end{bmatrix} = (\underline{\xi}, \underline{\eta}, \underline{t})$$

Proof.

$$\begin{aligned} & -\langle \underline{\eta} \times \underline{t} | \underline{t}_1 \rangle \underline{\xi} - \langle \underline{t} \times \underline{\xi} | \underline{t}_1 \rangle \underline{\eta} + \underline{t}_1 \\ &= -\langle \underline{\eta} | \underline{t} \times \underline{t}_1 \rangle \underline{\xi} + \langle \underline{\xi} | \underline{t} \times \underline{t}_1 \rangle \underline{\eta} + \underline{t}_1 \\ &= (\underline{\xi} \times \underline{\eta}) \times (\underline{t} \times \underline{t}_1) + \underline{t}_1 \\ &= -(\underline{t} \times \underline{t}_1) \times (\underline{\xi} \times \underline{\eta}) + \underline{t}_1 \\ &= -\langle \underline{t} | \underline{\xi} \times \underline{\eta} \rangle \underline{t}_1 + \langle \underline{t}_1 | \underline{\xi} \times \underline{\eta} \rangle \underline{t} + \underline{t}_1 \\ &= \underline{t}. \quad \# \end{aligned}$$

By this lemma, we may find $\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} = C$ such that

$$(\underline{\xi},\ \underline{\eta},\ \underline{t})\ C=(\underline{\xi},\ \underline{\eta},\ \underline{t}_1)\,.$$

Then

$$(\operatorname{adj} W)'(\underline{\xi}_1,\ \underline{\eta}_1,\ \underline{t}_1)' M_f\,(\underline{\xi}_1,\ \underline{\eta}_1,\ \underline{t}_1)\ \operatorname{adj} W$$

$$=(\operatorname{adj}\ W)'\begin{bmatrix} B & & 0 \\ & & 0 \\ 0 & 0 & 1 \end{bmatrix}'(\underline{\xi},\ \underline{\eta},\ \underline{t}_1)'$$

$$\cdot\, M_f\,(\underline{\xi},\ \underline{\eta},\ \underline{t}_1)\begin{bmatrix} B & & 0 \\ & & 0 \\ 0 & 0 & 1 \end{bmatrix}\operatorname{adj} W$$

$$=(\operatorname{adj}\ W)'\begin{bmatrix} B & & 0 \\ & & 0 \\ 0 & 0 & 1 \end{bmatrix}' C'(\underline{\xi},\ \underline{\eta},\ \underline{t})$$

$$\cdot\, M_f(\underline{\xi},\ \underline{\eta},\ \underline{t})C\begin{bmatrix} B & & 0 \\ & & 0 \\ 0 & 0 & 1 \end{bmatrix}\operatorname{adj} W$$

$$=(\operatorname{adj}\ W)'\begin{bmatrix} B & & 0 \\ & & 0 \\ 0 & 0 & 1 \end{bmatrix}' C'(\operatorname{adj} U)'\ (\underline{m},\ \underline{n},\ \underline{x})'$$

$$\cdot\, M_f\,(\underline{m},\underline{n},\underline{x})(\operatorname{adj} U)C\begin{bmatrix} B & & 0 \\ & & 0 \\ 0 & 0 & 1 \end{bmatrix}\operatorname{adj} W$$

is in ${}_f\Sigma_D\left(\begin{bmatrix} p_1 & q_1 \\ q_1 & r_1 \end{bmatrix}\right)$, and the third column vector of

$$\operatorname{adj}\ (\underline{m},\ \underline{n},\ \underline{x})\left\{U\ (\operatorname{adj}\ C)\begin{bmatrix} \operatorname{adj}\ B & 0 \\ & 0 \\ 0 \quad 0 & 1 \end{bmatrix}W\right\}$$

is $\underline{\nu}$, i.e., $\underline{l}$, is $\Gamma_D(F)$-equivalent to $\underline{\nu}$. This proves that $\Gamma_D(F)$-equivalence is indeed an equivalence relation. We denote $\tilde{S}(F;\ D)$ the set of $\Gamma_D(F)$-equivalence classes in $S(F;\ D)$.

It is easily seen from Lemma 1.1, Corollary 1.3, Lemma 2.3 and the fact that $T(\underline{\alpha},\ \underline{\beta},\ \underline{l})=(T\underline{\alpha},\ T\underline{\beta},\ T\underline{l})$ that $\underline{l}$ and $\underline{\mu}$ are $\Gamma_D(F)$-equivalent if and only if $T\underline{l}$ and $T\underline{\mu}$ are $\Gamma_D(F)$-equivalent for every T in $E(F)$. Hence $E(F)$ defines an action on $\tilde{S}(F;\ D)$. Concerning this action we have the following theorem.

THEOREM 2.6. *Let F be the adjoint form of a ternary form f, and D be a square free integer which is represented by F. Then the number of orbits in $\tilde{S}(F;\ D)$ under the action of $\boldsymbol{E}(F)$ is not larger than h_D, the class number of properly equivalence classes of binary forms with discriminant D.*

Proof. By previous argument, two $\Gamma_D(F)$-equivalence classes are in the same $\boldsymbol{E}(F)$-orbit if and only if for $\underline{l}$ in one $\Gamma_D(F)$-equivalence class, we can find $\boldsymbol{T} \in \boldsymbol{E}(F)$ such that $\boldsymbol{T}\ \underline{l}$ is is in the other $\Gamma_D(F)$-equivalence class. On the other hand, by Theorem 2.4, if $\underline{l}$ is the adjoint of a representation of binary form ϕ which is represented by f, then any binary form $\underline{\Psi}$ which is represented by f with the adjoint $\boldsymbol{T}\ \underline{l}$ must be properly equivalent to ϕ. Thus if two $\Gamma_D(F)$-equivalence classes are in the same $\boldsymbol{E}(F)$-orbit, then each of them contains an element such that these two elements are the adjoints of two properly equivalent binary froms which are represented by f. If we can show that for $\underline{l}$ and $\underline{\mu}$ in $\boldsymbol{S}(F;\ D)$ are the adjoints of two preperly equivalent binary forms which are represented by f, we can find $V \in \boldsymbol{E}(F)$ such that $\boldsymbol{V}\ \underline{l}$ and $\underline{\mu}$ are in the same $\Gamma_D(F)$-equivalence class, then we have information about the number of $\boldsymbol{E}(F)$-orbits in $\tilde{\boldsymbol{S}}(F;\ D)$.

First we assume that $\underline{l} = \underline{m} \times \underline{n}$ and $\underline{\mu} = \underline{\xi} \times \underline{\eta}$ are two points in $\boldsymbol{S}(F;\ D)$ such that $(\underline{m},\ \underline{n})'M_f(\underline{m},\ \underline{n}) = (\underline{\xi},\ \underline{\eta})'M_f(\underline{\xi},\ \underline{\eta})$, i.e., they are the adjoints of the same binary form, say

$$\langle M_f\,\underline{m}\,|\,\underline{m}\rangle = \langle M_f\,\underline{\xi}\,|\,\underline{\xi}\rangle = p,$$
$$\langle M_f\,\underline{m}\,|\,\underline{n}\rangle = \langle M_f\,\underline{\xi}\,|\,\underline{\eta}\rangle = q,$$
$$\langle M_f\,\underline{n}\,|\,\underline{n}\rangle = \langle M_f\,\underline{\eta}\,|\,\underline{\eta}\rangle = r,$$

where $\phi(t,\ u) = pt^2 + 2qtu + ru^2$ is the binary form. Since $\underline{l}$ and $\underline{\mu}$ are proper vectors (this is due to the fact that D is square free), we can find integral vectors $\underline{x}$ and $\underline{y}$ such that $\langle \underline{l}\,|\,\underline{x}\rangle = \langle \underline{\mu}\,|\,\underline{y}\rangle = 1$. Then we obtain two equivalent ternary forms with associate matrices $(\underline{m},\ \underline{n},\ \underline{x})'M_f(\underline{m},\ \underline{n},\ \underline{x})$ and $(\underline{\xi},\ \underline{\eta},\ \underline{y})'M_f(\underline{\xi},\ \underline{\eta},\ \underline{y})$. By Proposition 1.2, their adjoint forms are equivalent, they are $(\underline{n} \times \underline{x},\ \underline{x} \times \underline{m},\ \underline{l})'$ $M_{\mathrm{adj}\,f}$ $(\underline{n} \times \underline{x},\ \underline{x} \times \underline{m},\ \underline{l})$ and $(\underline{\eta} \times \underline{y},\ \underline{y} \times \underline{\xi},\ \underline{\mu})'M_{\mathrm{adj}\,f}$ $(\underline{\eta} \times \underline{y},\ \underline{y} \times \underline{\xi},\ \underline{\mu})$.

[Here we use the facts that adj $(\underline{u}, \underline{v}, \underline{w}) = (\underline{v} \times \underline{w}, \underline{w} \times \underline{u}, \underline{u} \times \underline{v})$, and $\underline{m} \times \underline{n} = \underline{l}, \underline{\xi} \times \underline{\eta} = \underline{\mu}$.] Hence we can find $U \in (3, \boldsymbol{Z})$ such that

$$U'(\underline{n} \times \underline{x}, \underline{x} \times \underline{m}, \underline{l})' M_{\mathrm{adj}\, f} (\underline{n} \times \underline{x}, \underline{x} \times \underline{m}, \underline{l}) U$$
$$= (\underline{\eta} \times \underline{y}, \underline{y} \times \underline{\xi}, \underline{\mu})' M_{\mathrm{adj}\, f} (\underline{\eta} \times \underline{y}, \underline{y} \times \underline{\xi}, \underline{\mu}),$$

and this implies that $(\underline{n} \times \underline{x}, \underline{x} \times \underline{m}, \underline{l}) U (\underline{\eta} \times \underline{y}, \underline{y} \times \underline{\xi}, \underline{\mu})^{-1} = V$ is in $\boldsymbol{E}(F)$. Since

$$V(\underline{\eta} \times \underline{y}, \underline{y} \times \underline{\xi}, \underline{\mu}) = (V(\underline{\eta} \times \underline{y}), V(\underline{y} \times \underline{\xi}), V(\underline{\mu})),$$

we have $U\langle \underline{l} \rangle \simeq V(\underline{\mu})$, i.e., $\underline{l}$ and $V(\underline{\mu})$ are in the same $\Gamma_D(F)$-equivalence class.

Now suppose $\underline{l} = \underline{\varepsilon} \times \underline{\delta}$ and $\underline{\mu} = \underline{\xi} \times \underline{\eta}$ are in $\boldsymbol{S}(F; D)$ such that the binary forms $(\underline{\varepsilon}, \underline{\delta})' M_f (\underline{\varepsilon}, \underline{\delta})$ and $(\underline{\xi}, \underline{\eta})' M_f (\underline{\xi}, \underline{\eta})$ are properly equivalent, say

$$A'(\underline{\varepsilon}, \underline{\delta})' M_f (\underline{\varepsilon}, \underline{\delta}) A = (\underline{\xi}, \underline{\eta})' M_f (\underline{\xi}, \underline{\eta}),$$

where $A \in \mathrm{SL}(2, \boldsymbol{Z})$. Write $A = \begin{bmatrix} \alpha & \beta \\ \gamma & \zeta \end{bmatrix}$ and $(\underline{m}, \underline{n}) = (\underline{\varepsilon}, \underline{\delta}) A$. Then

$$\begin{aligned} \underline{m} \times \underline{n} &= (\alpha \underline{\varepsilon} + \gamma \underline{\delta}) \times (\beta \underline{\varepsilon} + \zeta \underline{\delta}) \\ &= \alpha\beta \underline{\varepsilon} \times \underline{\varepsilon} + \alpha\zeta \underline{\varepsilon} \times \underline{\delta} - \beta\gamma \underline{\varepsilon} \times \underline{\delta} + \gamma\zeta \underline{\delta} \times \underline{\delta} \\ &= (\alpha\zeta - \beta\gamma) \underline{\varepsilon} \times \underline{\delta} \\ &= \underline{\varepsilon} \times \underline{\delta}, \end{aligned}$$

and $(\underline{m}, \underline{n})$, $(\underline{\xi}, \underline{\eta})$ represent the same binary form via f. By previous argument, there exists $V \in \boldsymbol{E}(F)$ such that $V(\underline{\mu})$ and $\underline{l}$ are in the same $\Gamma_D(F)$-equivalence class.

Thus we have shown that two $\Gamma_D(F)$-equivalence classes are in the same $\boldsymbol{E}(F)$-orbit if and only if each of them contains an element such that these two elements are the adjoints of two properly equivalent binary forms which are presented by f. Hence the number of $\boldsymbol{E}(F)$-orbits in $\tilde{\boldsymbol{S}}(F; D)$ is less than or equal to the class number of binary forms with discriminant D. [Note that it may happen that certain binary forms with discriminant D which are not represented by f, since if there is one, then those binary forms which are properly equivalent to this one are also not represented by f. Here we use the fact that if ϕ is represented by f via $(\underline{m}, \underline{n})$, and if ψ is properly equivalent to ϕ, say $A'M_\phi A = M_\psi$, then Ψ is represented by f via $(\underline{\xi}, \underline{\eta}) = (\underline{m}, \underline{n}) A$. This is why we say that the number of $E(F)$-orbits in $\tilde{S}(F; D)$ may be less than h_D.]

COROLLARY 2.7. *F, D as above. If $h_D = 1$, then there is only one $E(F)$-orbit in $\tilde{S}(F; D)$, i. e., $E(F)$ acts transitively on $\tilde{S}(F; D)$.*

Proof. Since D is represented by F, say $F(\underline{l}) = D$, $\underline{l} = \underline{m} \times \underline{n}$. Then $f\left((\underline{m}, \underline{n})\begin{pmatrix} t \\ u \end{pmatrix}\right)$ is a binary form with discriminant D. Since $h_D = 1$, all binary forms with discriminant D are represented by f. By Theorem 2.6, for any two $\underline{l}$, $\underline{\mu}$ in $S(F; D)$ we can find $V \in E(F)$, and U such that $U\langle \underline{l} \rangle \cong V\underline{\mu}$, i.e., $E(F)$ acts transitively on $\tilde{S}(F; D)$. ♯

REFERENCES

1. G. Carl F. Gauss, *Disquisitiones Arithemeticae*, 1801.
2. W. David V. Widder, *Advanced Calculus*, Prentice-Hall, Inc., 1961.

INSTITUTE OF MATHEMATICS, NATIONAL TSING HUA UNIVERSITY, HSINCHU, TAIWAN R.O.C.