TOKYO J. MATH.
VOL. 16, NO. 2, 1993

A Diophantine Algorithm and a Reduction Theory of Ternary Forms

Shunji ITO and Hiroko TACHII

Tsuda College

Introduction.

The reduction theory of binary forms with a positive discriminant and the characterization of real quadratic numbers by the periodicity of partial quotients of continued fraction expansions, that is, the reciprocal relation between binary forms and quadratic numbers was established by Lagrange and Gauss (see Zagier [1]).

The purpose of this paper is to introduce a multi-dimensional diophantine algorithm instead of the continued fraction algorithm and to discuss a relation between a kind of reduction theory of indefinite ternary forms and the periodic points of the algorithm.

In Section 1, a diophantine algorithm T on $X=[0, 1)\times[0, 1)$ is introduced by

$$T(\alpha, \beta)=(-[-1/\alpha]-1/\alpha, \beta/\alpha-[\beta/\alpha]) .$$

In Section 3, a characterization of $\beta\in\boldsymbol{Q}(\alpha)$ by the algorithm is obtained as an extension of Lagrange's theorem:

(1) the point $(\alpha, \beta)\in X$ is a periodic point of the diophantine algorithm if and only if α is quadratic and $\beta\in\boldsymbol{Q}(\alpha)$,

(2) the point $(\alpha, \beta)\in X$ is a purely periodic point of the diophantine algorithm if and only if α is quadratic, $\beta\in\boldsymbol{Q}(\alpha)$ and (α, β) is reduced (the definition of reduced is in Section 3).

In Section 4, a class of ternary forms is introduced as follows: a ternary form f_A with integral coefficients given by $f_A=(x, y, z)A\,{}^t(x, y, z)$ is said to be with discriminants Δ and D if A satisfies

(1) $(a, h, b)=1$,

(2) $D:=-\begin{vmatrix} a & h \\ h & b \end{vmatrix}>0$ and non square, and

(3) $\Delta=-\det A$,

Received February 10, 1992
Revised February 1, 1993

where A is given by $A=\begin{pmatrix} a & h & g \\ h & b & f \\ g & f & c \end{pmatrix}$. On the ternary forms f_A with given discriminants Δ and D, a reduction theory of the ternary forms is discussed in a relation to the periodic points of the algorithm T.

In Section 5, an equivalence relation among ternary forms by means of a subgroup Γ of $SL(3, \mathbf{Z})$ is introduced, and an extension of Serret's theorem on continued fraction expansions is obtained.

1. Definition of the algorithm and its fundamental properties.

Let us go back to the following diophantine algorithm [2].

Let $X := [0, 1) \times [0, 1)$, and let us define the algorithm T on X by

$$T(\alpha, \beta)=\begin{cases} (a(\alpha)-1/\alpha,\ \beta/\alpha-b(\alpha, \beta)) & \text{if } \alpha\neq 0 \\ (\alpha, \beta) & \text{if } \alpha=0 \end{cases} \tag{1.1}$$

where functions $a(\alpha)$ and $b(\alpha, \beta)$ are given by

$$a(\alpha)=-[-1/\alpha] \quad \text{and} \quad b(\alpha, \beta)=[\beta/\alpha] \tag{1.2}$$

(see Figure 1). The first coordinate of the algorithm T is given by the modified continued fraction algorithm S on $[0, 1)$ (A survey of the modified continued fraction is found in Section 6 as Appendix.):

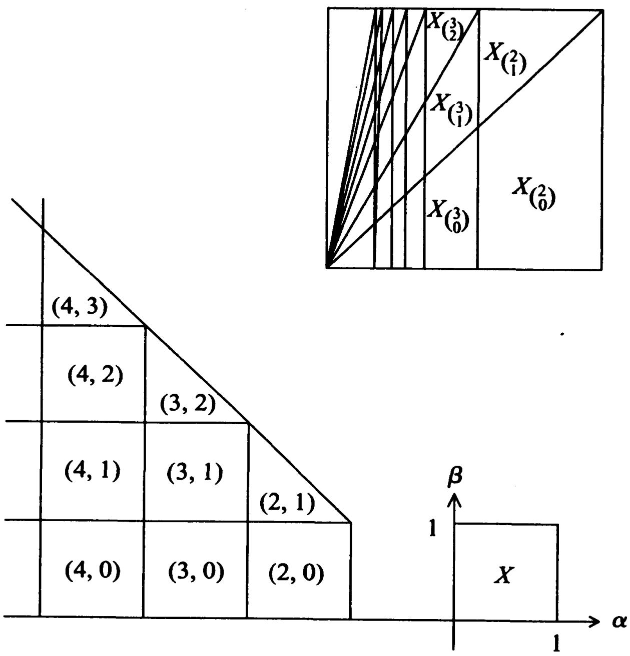


FIGURE 1

$$S(\alpha)=-[-1/\alpha]-1/\alpha .$$

REMARK 1.1. Let us observe the behavior of the algorithm T on invariant sets. Let

$$I_0:=\{0\}\times[0,1),$$
$$I:=[0,1)\times\{0\},$$
$$J:=\{(\alpha,\beta)\in X \mid \alpha+\beta=1\},$$

then we see

$$T(I_0)=I_0,$$
$$T(I)=I,$$
$$T(J)=J.$$

The restriction $T|_I$ of T on I coincides with the modified continued fraction algorithm S and the restriction $T|_J$ of T on J is also isomorphic to S by the isomorphism $\phi: (\alpha, 1-\alpha)\mapsto\alpha$, that is,

$$S\circ\phi=\phi\circ T|_J .$$

For each $(\alpha, \beta)\in X$, define a finite or infinite sequence of integral vectors $\{(a_n, b_n): n=1, 2, \cdots\}$ by

$$(a_n, b_n)=(a_n(\alpha), b_n(\alpha, \beta))=(a(\alpha_{n-1}), b(\alpha_{n-1}, \beta_{n-1})) \tag{1.3}$$

where (α_n, β_n)'s are defined by

$$(\alpha_n, \beta_n)=T^n(\alpha, \beta) . \tag{1.4}$$

We call the sequence of (a_n, b_n) *the name* of (α, β) for the algorithm (X, T). We say (α, β) has a *finite name* if there exists j such that $T^j(\alpha, \beta)\in I_0$.

REMARK 1.2. We see that $(\alpha, \beta)\in X$ has a finite name iff α is rational.

From now on, we assume that α is irrational. By the assumption, for the infinite sequence (a_n, b_n) there exist infinitely many n's such that $a_n\neq 2$.

Let us define a set of n-tuples of pairs $\begin{pmatrix} a_1, \cdots, a_n \\ b_1, \cdots, b_n \end{pmatrix}$ by

$$A(n)=\left\{\begin{pmatrix} a_1(\alpha), & a_2(\alpha), & \cdots, & a_n(\alpha) \\ b_1(\alpha, \beta), & b_2(\alpha, \beta), & \cdots, & b_n(\alpha, \beta) \end{pmatrix} \;\middle|\; (\alpha, \beta)\in X \text{ and } \alpha\notin \boldsymbol{Q}\right\},$$

then each $\begin{pmatrix} a_1, \cdots, a_n \\ b_1, \cdots, b_n \end{pmatrix}\in A(n)$ satisfies the properties called admissible sequences that

(A) $a_i\geqq 2$, $a_i>b_i\geqq 0$ $(1\leqq i\leqq n)$,

(B) if there exists a k $(1\leqq k\leqq n-1)$ such that $a_k-b_k=1$, then $a_{k+1}-b_{k+1}\geqq 2$, and moreover if there exists a j $(1\leqq j\leqq n-k-1)$ such that $a_{k+i}-b_{k+i}=2$ for $1\leqq i\leqq j$, then

$a_{k+j+1}-b_{k+j+1}\geqq 2$.

Let us define matrices associated with the name of (α, β) by

$$A(a_n, b_n)=\begin{pmatrix} a_n & -1 & 0 \\ 1 & 0 & 0 \\ b_n & 0 & 1 \end{pmatrix}$$

and

$$(1.5)\qquad \begin{pmatrix} q_n & -q_{n-1} & 0 \\ p_n & -p_{n-1} & 0 \\ r_n & -r_{n-1} & 1 \end{pmatrix}:=A(a_1, b_1)\cdots A(a_n, b_n) \qquad (n\geqq 1)$$

$$\left(\begin{pmatrix} q_0 & -q_{-1} & 0 \\ p_0 & -p_{-1} & 0 \\ r_0 & -r_{-1} & 1 \end{pmatrix}:=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right),$$

that is, q_n, p_n and r_n are given by the following recurrent formulae:

$$(1.6)\qquad \begin{aligned} q_n&=a_nq_{n-1}-q_{n-2}\,, \\ p_n&=a_np_{n-1}-p_{n-2}\,, \\ r_n&=a_nr_{n-1}-r_{n-2}+b_n\,. \end{aligned}$$

Then we see $\begin{vmatrix} q_n & -q_{n-1} \\ p_n & -p_{n-1} \end{vmatrix}=1$.

LEMMA 1.1. *The following formulae hold*:

$$(1)\qquad \begin{pmatrix} 1 \\ \alpha \\ \beta \end{pmatrix}=\alpha\alpha_1\cdots\alpha_{n-1}\begin{pmatrix} q_n & -q_{n-1} & 0 \\ p_n & -p_{n-1} & 0 \\ r_n & -r_{n-1} & 1 \end{pmatrix}\begin{pmatrix} 1 \\ \alpha_n \\ \beta_n \end{pmatrix}$$

and in particular

$$(2)\qquad \alpha=\frac{p_n-p_{n-1}\alpha_n}{q_n-q_{n-1}\alpha_n}\,, \qquad \beta=\frac{r_n-r_{n-1}\alpha_n+\beta_n}{q_n-q_{n-1}\alpha_n}\,, \quad \textit{and} \quad \alpha_n=\frac{p_n-q_n\alpha}{p_{n-1}-q_{n-1}\alpha}\,.$$

PROOF. From the definition of T, (1) is obtained by induction. (2) is deduced from (1).

Let us define $X\begin{pmatrix} a_1, \cdots, a_n \\ b_1, \cdots, b_n \end{pmatrix}$ to be

$$\left\{(\alpha, \beta)\,\middle|\, \begin{pmatrix} a_i(\alpha) \\ b_i(\alpha, \beta) \end{pmatrix}=\begin{pmatrix} a_i \\ b_i \end{pmatrix},\ 1\leqq i\leqq n\right\} \qquad \text{for} \quad \begin{pmatrix} a_1, \cdots, a_n \\ b_1, \cdots, b_n \end{pmatrix}\in A(n)\,.$$

Then $\left\{X\begin{pmatrix}a_1, \cdots, a_n \\ b_1, \cdots, b_n\end{pmatrix} \middle| \begin{pmatrix}a_1, \cdots, a_n \\ b_1, \cdots, b_n\end{pmatrix} \in A(n)\right\}$ gives a partition of X. Let $U_0 = X$ and $U_1 = \{(\alpha, \beta) \in X \mid \alpha + \beta < 1\}$, then we have the following lemma.

LEMMA 1.2. *For each $i = 0, 1$,*

(1) $$T^n X\begin{pmatrix}a_1, \cdots, a_n \\ b_1, \cdots, b_n\end{pmatrix} = U_i \quad \text{if} \quad \begin{pmatrix}a_1, \cdots, a_n \\ b_1, \cdots, b_n\end{pmatrix} \in B_i(n)$$

where $B_0(n)$ and $B_1(n)$ are given by

$$B_0(n) = \left\{\begin{pmatrix}a_1, \cdots, a_n \\ b_1, \cdots, b_n\end{pmatrix} \in A(n) \,\middle|\, \text{there exists a } k\ (1 \leqq k \leqq n) \text{ such that } a_k - b_k > 2 \text{ and } a_j - b_j = 2 \text{ for } k < j \leqq n\right\},$$

$$B_1(n) = \left\{\begin{pmatrix}a_1, \cdots, a_n \\ b_1, \cdots, b_n\end{pmatrix} \in A(n) \,\middle|\, \text{there exists a } k\ (1 \leqq k \leqq n) \text{ such that } a_k - b_k = 1 \text{ and } a_j - b_j = 2 \text{ for } k < j \leqq n\right\}.$$

(2) $$T^n : X\begin{pmatrix}a_1, \cdots, a_n \\ b_1, \cdots, b_n\end{pmatrix} \mapsto U_i \text{ is bijective}$$

and its inverse map $\varphi_{\left(\begin{smallmatrix}a_1, \cdots, a_n \\ b_1, \cdots, b_n\end{smallmatrix}\right)}$ is given by

$$\varphi_{\left(\begin{smallmatrix}a_1, \cdots, a_n \\ b_1, \cdots, b_n\end{smallmatrix}\right)}(\alpha, \beta) = \left(\frac{p_n - p_{n-1}\alpha}{q_n - q_{n-1}\alpha}, \frac{r_n - r_{n-1}\alpha + \beta}{q_n - q_{n-1}\alpha}\right).$$

The proof is seen in Lemma 5.2 [2].

2. A characterization of $\beta \in \boldsymbol{Z}\alpha + \boldsymbol{Z}$.

Let us discuss a necessary and sufficient condition of $\beta \in \boldsymbol{Z}\alpha + \boldsymbol{Z}$ where $\boldsymbol{Z}$ is the set of integers.

LEMMA 2.1. *$r_n q_{n-1} - r_{n-1} q_n \geqq 0$ and $r_n p_{n-1} - r_{n-1} p_n \geqq 0$.*

PROOF. We know by (1.6)

$$\begin{aligned} r_{n+1} q_n - r_n q_{n+1} &= (a_{n+1} r_n - r_{n-1} + b_{n+1}) q_n - r_n (a_{n+1} q_n - q_{n-1}) \\ &= (r_n q_{n-1} - r_{n-1} q_n) + b_{n+1} q_n \\ &\geqq (r_n q_{n-1} - r_{n-1} q_n) \geqq 0 . \end{aligned}$$

The other inequality is obtained similarly.

PROPOSITION 2.1. *Let us assume* $\alpha \notin \boldsymbol{Q}$ *and* $(\alpha, \beta) \in X$. *Then the following conditions are equivalent*:

(1) *there exists* k_0 *such that* $\beta_{k_0-1} \neq 0$ *and* $\beta_k = 0$ *for any* $k \geqq k_0$,

(2) *there exists* n_0 *such that* $b_{n_0} \neq 0$ *and* $b_n = 0$ *for any* $n \geqq n_0 + 1$,

(3) *there exist integers* l *and* m *such that* $\beta = l + \alpha m$, $l \leqq 0$ *and* $m \geqq 0$.

We notice that k_0 *in* (1) *is equal to* n_0 *in* (2).

PROOF. From $T(I) = I$ in Remark 1.1, we obtain (2) from (1). Conversely, let us assume (2). From that $b_n = 0$ for $n \geqq n_0 + 1$, we see

$$\beta_n = \beta_{n-1}/\alpha_{n-1} \qquad \text{for} \quad n \geqq n_0 + 1 .$$

In general, we have the following relation:

$$\beta_n = \frac{\beta_{n_0}}{\alpha_{n-1}\alpha_{n-2}\cdots\alpha_{n_0}} .$$

Suppose that $\beta_{n_0} \neq 0$, then from that $0 < \alpha_n < 1$ we see β_n is monotone increasing. Therefore, from the boundedness of β_n's we see $\prod_{k \geqq n_0}^{\infty} a_k$ converges and so $\alpha_k > 1/2$ for all large k. Thus, we have $a_k = 2$ for all large k. This contradicts $\alpha \notin \boldsymbol{Q}$. Therefore, we obtain (1). Let us assume (3). From

$$\alpha = \frac{1}{a_1 - \alpha_1} \quad \text{and} \quad \beta = \frac{b_1 + \beta_1}{a_1 - \alpha_1} ,$$

we have $\beta_1 = (la_1 + m - b_1) - l\alpha_1$. Put $l_1 := la_1 + m - b_1$ and $m_1 := -l$, then we see

$$l_1 \leqq 0 , \quad m_1 \geqq 0 \quad \text{and} \quad m \geqq m_1 .$$

Because, from $\beta = l + m\alpha$, $0 < \alpha < 1$, $m \geqq 0$ and $\beta \geqq 0$, we have

$$0 \leqq l + m\alpha \leqq l + m = -m_1 + m .$$

On the other hand, from the definition of a_1 and b_1, we know

$$a_1 - 1 < 1/\alpha < a_1 \quad \text{and} \quad b_1 \leqq l \cdot 1/\alpha + m < b_1 + 1 .$$

Therefore, from $l \leqq 0$ we have

$$1 > l \cdot 1/\alpha + m - b_1 \geqq a_1 l + m - b_1 ,$$

that is,

$$0 \geqq a_1 l + m - b_1 = l_1 .$$

Put $l_k := l_{k-1} a_k + m_{k-1} - b_k$ and $m_k := -l_{k-1}$, then we have recursively

$$\beta_k = l_k + m_k \alpha_k , \quad l_k \leqq 0 \quad \text{and} \quad m_k \geqq 0 ,$$

and

$$m \geqq m_1 \geqq m_2 \geqq \cdots \geqq m_k \geqq \cdots \geqq 0 .$$

We know that there exists k such that $m_k = m_{k+1}$. Then from $\beta_k = m_k(-1+\alpha_k)$ and $0<\alpha_k<1$, we have $m_k=0$ and so $\beta_k=0$. Let us assume (1). From the formulae (2) in Lemma 1.1 and $\beta_k=0$, we have

$$\beta=\frac{r_k-r_{k-1}\cdot(p_k-q_k\alpha)/(p_{k-1}-q_{k-1}\alpha)}{q_k-q_{k-1}\cdot(p_k-q_k\alpha)/(p_{k-1}-q_{k-1}\alpha)}$$
$$=-(r_kp_{k-1}-r_{k-1}p_k)+(q_{k-1}r_k-q_kr_{k-1})\alpha\,,$$

that is, by Lemma 2.1, β satisfies $\beta=l+\alpha m$, $l\leqq 0$ and $m\geqq 0$.

PROPOSITION 2.2. *Let us assume $\alpha\notin \boldsymbol{Q}$ and $(\alpha,\beta)\in X$. Then the following conditions are equivalent:*

(1) *there exists k_0 such that $\alpha_{k_0-1}+\beta_{k_0-1}\neq 1$ and $\alpha_k+\beta_k=1$ for any $k\geqq k_0$,*
(2) *there exists n_0 such that $a_{n_0}-b_{n_0}\neq 2$ and $a_n-b_n=2$ for any $n\geqq n_0+1$,*
(3) *there exist integers l and m such that $\beta=l+\alpha m$, $l>0$ and $m<0$.*

We notice that k_0 in (1) is equal to n_0 in (2).

PROOF. From $T(J)=J$ in Remark 1.1, we obtain (2) from (1). Conversely, let us assume (2). From $a_n-b_n=2$, $n\geqq n_0+1$, we see

$$\alpha_{n+1}+\beta_{n+1}-1=\left(a_{n+1}-\frac{1}{\alpha_n}\right)+\left(\frac{\beta_n}{\alpha_n}-b_{n+1}\right)-1=\frac{-1+\beta_n+\alpha_n}{\alpha_n}$$

for $n\geqq n_0$. In general,

$$\alpha_{n_0+n+1}+\beta_{n_0+n+1}-1=\frac{\alpha_{n_0}+\beta_{n_0}-1}{\alpha_{n_0}\alpha_{n_0+1}\cdots\alpha_{n_0+n}}\,.$$

Suppose that $\alpha_{n_0}+\beta_{n_0}-1\neq 0$, then from the boundedness of $\alpha_n+\beta_n-1$ we see $\prod_{n\geqq n_0}^{\infty}\alpha_k$ converges and so $\alpha_k>1/2$ for all large k. This leads to a contradiction as in the proof of Proposition 2.1. Let us assume (3). Put $l_1:=la_1+m-b_1$ and $m_1:=-l$, then we see

$$\beta_1=l_1+m_1\alpha_1\,,$$
$$l_1>0\,,\quad m_1<0\quad\text{and}\quad m_1\geqq m\,.$$

Because, from $\beta=l+m\alpha$, $0<\alpha<1$, $m<0$ and $1>\beta\geqq 0$, we have

$$l\geqq l+m\alpha\,(=\beta)>l+m\quad\text{and}\quad 1>l+m\,.$$

Therefore, we have $0\geqq l+m$. This means $m_1\geqq m$. From the definitions of a_1 and b_1, we know

$$a_1-1<1/\alpha<a_1\quad\text{and}\quad b_1\leqq l\cdot 1/\alpha+m<b_1+1\,.$$

Therefore, from $l>0$ we have

$$0\leqq l\cdot 1/\alpha+m-b_1<a_1l+m-b_1=l_1\,.$$

Put $l_k := l_{k-1}a_k + m_{k-1} - b_k$ and $m_k := -l_{k-1}$, then we have recursively

$$\beta_k = l_k + m_k\alpha_k\,, \quad l_k > 0 \quad \text{and} \quad m_k < 0\,,$$

$$m \leqq m_1 \leqq m_2 \leqq \cdots \leqq m_k \leqq \cdots \leqq 0\,.$$

Therefore, there exists k_0 such that

$$m_k = m_{k_0} \qquad \text{for all} \quad k \geqq k_0\,,$$

that is, $l_{k-1} = l_{k_0-1}$ for all $k \geqq k_0$. Therefore, we see

$$\beta_k = l_{k_0}(1-\alpha_k) \qquad \text{for} \quad k \geqq k_0\,.$$

Suppose $l_{k_0} \neq 1$, then from $(\alpha_k, \beta_k) \in X$, we see $\alpha_k > 1/2$ for $k \geqq k_0$. This contradicts the irrationality of α. Therefore l_{k_0} must be equal to 1. Let us assume (1) and (2). From the formula (2) in Lemma 1.1 and $\beta_k = 1 - \alpha_k$, we have

$$\beta = (p_k - p_{k-1} - r_k p_{k-1} + r_{k-1} p_k) - (q_k - q_{k-1} - q_{k-1} r_k + q_k r_{k-1})\alpha\,.$$

We notice that

$$\begin{aligned} &q_n - q_{n-1} - q_{n-1} r_n + q_n r_{n-1} \\ &\qquad = q_{n-1} - q_{n-2} - q_{n-2} r_{n-1} + q_{n-1} r_{n-2} + (a_n - b_n - 2) q_{n-1}\,. \end{aligned}$$

We see $q_n - q_{n-1} - q_{n-1} r_n + q_n r_{n-1}$ is a constant for $n \geqq n_0 + 1$ from the assumption (1) or (2). The constant is denoted by A. We also see that $p_n - p_{n-1} - p_{n-1} r_n + p_n r_{n-1}$ is a constant for $n \geqq n_0 + 1$, which is denoted by B. From that A and B are integers and that $(\alpha, \beta) \in X$, we see that $A \cdot B \geqq 0$. Let us assume $A \leqq 0$. Then we can put β in the form:

$$\beta = B - A\alpha \qquad \text{where} \quad A, B \leqq 0\,.$$

From Proposition 2.1, it is to say that $\beta_n = 0$ for large n. This contradicts the assumption.

3. A characterization of $\beta \in \boldsymbol{Q}(\alpha)$.

Let us consider a map $\bar{T}$ on $X \times \boldsymbol{R}^2$ by

$$\bar{T}(\alpha, \beta, \gamma, \delta) = \begin{cases} (a - 1/\alpha, \beta/\alpha - b, a - 1/\gamma, \delta/\gamma - b) & \text{if} \quad \alpha \neq 0 \\ (\alpha, \beta, \gamma, \delta) & \text{if} \quad \alpha = 0\,, \end{cases} \tag{3.1}$$

where $a = a(\alpha)$ and $b = b(\alpha, \beta)$. Put

$$U_1 := \{(\alpha, \beta) \in X \mid \alpha + \beta < 1\}$$

$$U_2 := \{(\alpha, \beta) \in X \mid \alpha + \beta \geqq 1\}$$

$$X_1^* := \{(\gamma, \delta) \in \boldsymbol{R}^2 \mid \gamma \geqq 1, \delta \leqq 0 \text{ and } \gamma + \delta > 0\}$$

$$X_2^* := \{(\gamma, \delta) \in \boldsymbol{R}^2 \mid \gamma \geqq 1, \delta \leqq 0 \text{ and } \gamma + \delta \geqq 1\}$$

$$\overline{X_1}=U_1\times X_1^*, \qquad \overline{X_2}=U_2\times X_2^*$$

and

(3.2) $$\bar{X}=\overline{X_1}\cup\overline{X_2},$$

then the set $\bar{X}$ is $\bar{T}$-invariant set on $X\times \boldsymbol{R}^2$, and moreover, we see that the map $\bar{T}$ is bijective on $\bar{X}$ (except on $I_0\times X_1^*$, $I\times X_1^*$ and $J\times X_2^*$). We call the restriction $\bar{T}|_{\bar{X}}$ a *natural extension* on $\bar{X}$ of the algorithm (X, T). (See figure 2.)

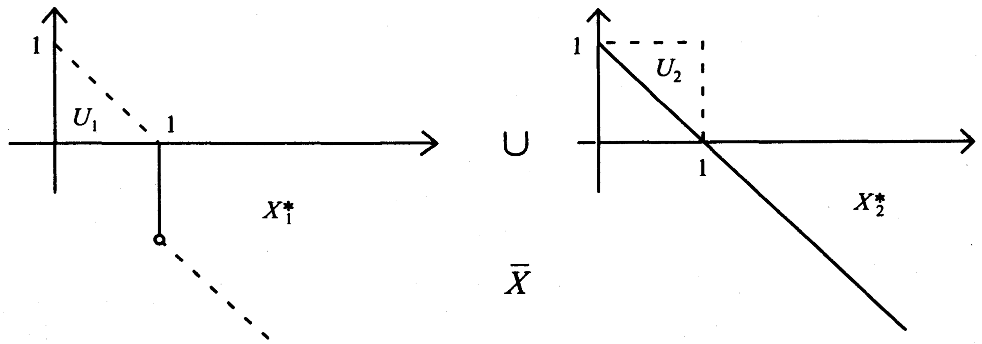


FIGURE 2

DEFINITION 3.1. We say (α, β) is reduced with respect to (X, T) if the following conditions hold:

(1) $(\alpha, \beta)\in X$,
(2) α is quadratic irrational,
(3) $\beta\in \boldsymbol{Q}(\alpha)$, where $\boldsymbol{Q}(\alpha)$ is the quadratic field generated by α, and
(4) $(\alpha, \beta, \bar{\alpha}, \bar{\beta})\in\bar{X}$, where $\bar{\alpha}$ means the algebraic conjugate of α.

LEMMA 3.1. *If (α, β) is reduced, then (α_1, β_1) is reduced.*

PROOF. From $(\alpha_1, \beta_1)=T(\alpha, \beta)$ and $(\alpha, \beta, \bar{\alpha}, \bar{\beta})\in\bar{X}$, we see

$$\begin{aligned}(\alpha_1, \beta_1, \overline{\alpha_1}, \overline{\beta_1})&=(a_1-1/\alpha, \beta/\alpha-b_1, \overline{a_1-1/\alpha}, \overline{\beta/\alpha-b_1})\\&=\bar{T}(\alpha, \beta, \bar{\alpha}, \bar{\beta})\in\bar{X}.\end{aligned}$$

Therefore, (α_1, β_1) is reduced.

We first discuss the case that $\beta\in\alpha\boldsymbol{Z}+\boldsymbol{Z}$.

PROPOSITION 3.1. (1) *(α, β) is reduced and $\beta\in\alpha\boldsymbol{Z}+\boldsymbol{Z}$ if and only if the name of (α, β) is purely periodic in the following sense: the sequence of the digits $\{a_n\}_{n=1}^{\infty}$ is purely periodic and $b_i=0$ for all i or $a_i-b_i=2$ for all i.*

(2) *If (α, β) is reduced and $\beta\in\alpha\boldsymbol{Z}+\boldsymbol{Z}$, then $(\alpha_{n_0}, \beta_{n_0})$ is reduced where n_0 is the integer given in Propositions* 2.1 *and* 2.2.

PROOF. Let us assume that (α, β) is reduced and $\beta\in\alpha\boldsymbol{Z}+\boldsymbol{Z}$. Then α is reduced with respect to ([0, 1), S). Therefore, by Theorem 6.2 in Appendix, the sequence of the digits $\{a_n\}_{n=1}^{\infty}$ is purely periodic. On the other hand, by Propositions 2.1, 2.2 and that $\beta\in\alpha\boldsymbol{Z}+\boldsymbol{Z}$ we see $b_n=0$ for $n\geqq n_0+1$ or $a_n-b_n=2$ for $n\geqq n_0+1$. Therefore, we must prove that $n_0=0$. Suppose that $b_{n_0}\neq 0$ and $b_n=0$ for any $n>n_0$, that is, $\beta_{n_0-1}\neq 0$ and $\beta_{n_0}=0$. By Lemma 3.1 we know that $(\alpha_{n_0-1}, \beta_{n_0-1})$ is reduced. On the other hand, we know

$$\alpha_{n_0}=a_{n_0}-\frac{1}{\alpha_{n_0-1}} \quad \text{and} \quad \beta_{n_0}=\frac{\beta_{n_0-1}}{\alpha_{n_0-1}}-b_{n_0}.$$

Therefore, by $b_{n_0}\neq 0$ and $\beta_{n_0}=0$ we see

$$\beta_{n_0-1}=b_{n_0}\cdot\alpha_{n_0-1}.$$

Thus, by $\overline{\beta_{n_0-1}}\notin[-\overline{\alpha_{n_0-1}}, 0]$ we see

$$(\alpha_{n_0-1}, \beta_{n_0-1}, \overline{\alpha_{n_0-1}}, \overline{\beta_{n_0-1}})\notin\bar{X}.$$

This contradicts the assumption that $(\alpha_{n_0-1}, \beta_{n_0-1})$ is reduced. Suppose that $a_{n_0}-b_{n_0}\neq 2$ for some n_0 and $a_n-b_n=2$ for any $n>n_0$, that is, $\alpha_{n_0-1}+\beta_{n_0-1}\neq 1$ and $\alpha_{n_0}+\beta_{n_0}=1$. From the assumption and

$$\alpha_{n_0}=a_{n_0}-\frac{1}{\alpha_{n_0-1}} \quad \text{and} \quad \beta_{n_0}=\frac{\beta_{n_0-1}}{\alpha_{n_0-1}}-b_{n_0},$$

we see

$$\frac{\beta_{n_0-1}-1}{\alpha_{n_0-1}}+a_{n_0}-b_{n_0}=\alpha_{n_0}+\beta_{n_0}=1.$$

Therefore

$$\beta_{n_0-1}=C\cdot\alpha_{n_0-1}+1$$

where $C=0$ or $C\leqq -2$. Thus we see

$$(\alpha_{n_0-1}, \beta_{n_0-1}, \overline{\alpha_{n_0-1}}, \overline{\beta_{n_0-1}})\notin\bar{X}.$$

This contradicts the assumption that $(\alpha_{n_0-1}, \beta_{n_0-1})$ is reduced. The converse is trivial.

Now, we must prove (2). By Proposition 2.1, 2.2 and that $\beta\in\alpha\boldsymbol{Z}+\boldsymbol{Z}$, we see $b_n=0$ for $n\geqq n_0+1$ or $a_n-b_n=2$ for $n\geqq n_0+1$. Then the name of $(\alpha_{n_0}, \beta_{n_0})$ is purely periodic. Therefore, by (1) $(\alpha_{n_0}, \beta_{n_0})$ is reduced.

COROLLARY 3.2. *(α, β) is reduced and $\beta\in\alpha\boldsymbol{Z}+\boldsymbol{Z}$ if and only if α is reduced with respect to* ([0, 1), S) *and $\beta=0$ or $\alpha+\beta=1$.*

LEMMA 3.2. *Let us assume that (α, β) is reduced and $\beta\notin\alpha\boldsymbol{Z}+\boldsymbol{Z}$ then there exists (α^*, β^*) uniquely such that (α^*, β^*) is reduced and $T(\alpha^*, \beta^*)=(\alpha, \beta)$.*

PROOF. We know that $\bar{T}$ is bijective except on $I_0\times X_1^*$, $I\times X_1^*$ or $J\times X_2^*$. By Corollary 3.2 and the assumption that $\beta\notin\alpha\boldsymbol{Z}+\boldsymbol{Z}$ we see that $(\alpha, \beta, \bar{\alpha}, \bar{\beta})$ does not belong to the above sets. Therefore, there uniquely exists $(\alpha^*, \beta^*, \gamma^*, \delta^*)$ such that

$$\bar{T}(\alpha^*, \beta^*, \gamma^*, \delta^*)=(\alpha, \beta, \bar{\alpha}, \bar{\beta}).$$

Moreover, we see

$$\gamma^*=\overline{\alpha^*} \quad\text{and}\quad \delta^*=\overline{\beta^*},$$

that is, (α^*, β^*) is reduced.

LEMMA 3.3. *If (α, β) is reduced, then the set $\{(\alpha_n, \beta_n)\mid n=0, 1, 2, \cdots\}$ is finite.*

PROOF. We know by Remark 6.1 in Appendix that the set $\{\alpha_n \mid n=0, 1, 2, \cdots\}$ is finite. Let us denote

$$\alpha_j=\frac{n_j+l_j\sqrt{D}}{m_j} \quad\text{and}\quad \beta_j=\frac{u_j+v_j\sqrt{D}}{t_j}.$$

From (2) of Lemma 1.1, we have

$$\beta_n=(q_n-q_{n-1}\alpha_n)\beta-r_n+r_{n-1}\alpha_n.$$

Therefore, t_n which is the denominator of β_n is given by $m_n\cdot t_0$, and so the set of denominators of β_n's is finite.

From Lemma 3.1, (α_n, β_n)'s are reduced for any $n\geqq 0$. Therefore, the following inequality holds:

(1) $$0\leqq\beta_n<\alpha_n \quad\text{and}\quad -\overline{\alpha_n}<\overline{\beta_n}\leqq 0, \qquad\text{or}$$

(2) $$\alpha_n\leqq\beta_n<1 \quad\text{and}\quad 1-\overline{\alpha_n}\leqq\overline{\beta_n}\leqq 0.$$

These are equivalent to

(1)′ $$0\leqq u_n+v_n\sqrt{D}<\alpha_n\cdot t_n \quad\text{and}\quad -\overline{\alpha_n}\cdot t_n<u_n-v_n\sqrt{D}\leqq 0, \qquad\text{or}$$

(2)′ $$\alpha_n\cdot t_n\leqq u_n+v_n\sqrt{D}<t_n \quad\text{and}\quad (1-\overline{\alpha_n})t_n\leqq u_n-v_n\sqrt{D}\leqq 0.$$

Therefore, from finiteness of $\{\alpha_n\}$'s and $\{t_n\}$'s we have the finiteness of $\{u_n\}$'s and $\{v_n\}$'s. This means that the set of $\{\beta_n \mid n=0, 1, 2, \cdots\}$ is finite.

PROPOSITION 3.3. *If (α, β) is reduced, then (α, β) is purely periodic with respect to T, that is, there exists k such that $T^k(\alpha, \beta)=(\alpha, \beta)$.*

PROOF. The case that $\beta\in\boldsymbol{Z}\alpha+\boldsymbol{Z}$ is discussed in Proposition 3.1. Therefore, we assume that $\beta\notin\boldsymbol{Z}\alpha+\boldsymbol{Z}$. By Lemma 3.3, there exist k and N such that $(\alpha_N, \beta_N)=(\alpha_{N+k}, \beta_{N+k})$. By Lemma 3.2, we see

$$(\alpha_{N-1}, \beta_{N-1}) = (\alpha_{N+k-1}, \beta_{N+k-1})$$

$$\cdots\cdots$$

$$(\alpha, \beta) = (\alpha_k, \beta_k)\,.$$

Let us consider the boundary of X_i^*, $i=1, 2$. We put

$$\sigma_1 = \partial X_1^* \cap \{\delta = 0\} \setminus \{(1, 0)\}$$

$$\sigma_2 = \partial X_1^* \cap \{\gamma + \delta = 0\} \setminus \{(1, -1)\}$$

$$\sigma_3 = \partial X_2^* \cap \{\delta = 0\} \setminus \{(1, 0)\}$$

$$\sigma_4 = \partial X_2^* \cap \{\gamma + \delta = 1\} \setminus \{(1, 0)\}\,.$$

Let us denote ε-neighbourhood $U(\sigma_i, \varepsilon)$ of boundaries σ_i as follows:

$$U(\sigma_1, \varepsilon) = U(\sigma_3, \varepsilon) = \{(\gamma, \delta) \mid 1 < \gamma < \infty, 0 \leqq \delta < \varepsilon\}$$

$$U(\sigma_2, \varepsilon) = \{(\gamma, \delta) \mid 1 < \gamma < \infty, -\varepsilon < \gamma + \delta \leqq 0\}$$

$$U(\sigma_4, \varepsilon) = \{(\gamma, \delta) \mid 1 < \gamma < \infty, 1 - \varepsilon < \gamma + \delta \leqq 1\}\,.$$

Then we have the following properties of the images of $U(\sigma_i, \varepsilon)$.

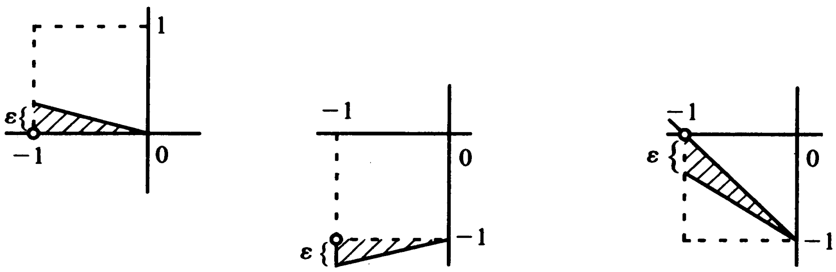
LEMMA 3.4. *For sufficiently small $\varepsilon > 0$, we have*:

(1) *For $i=1$ or 3, if $b_1 \neq 0$ then $\bar{T}((\alpha, \beta) \times U(\sigma_i, \varepsilon)) \subset (\alpha_1, \beta_1) \times (X_j^*)^\circ$ for some $j=1, 2$. If $b_1 = 0$ then $\bar{T}((\alpha, \beta) \times U(\sigma_1, \varepsilon)) \subset (\alpha_1, \beta_1) \times U(\sigma_i, \varepsilon)$ for some $i=1, 3$.*

(2) *If $a_1 - b_1 \neq 2$ then $\bar{T}((\alpha, \beta) \times U(\sigma_2, \varepsilon)) \subset (\alpha_1, \beta_1) \times (X_j^*)^\circ$ for some $j=1, 2$. If $a_1 - b_1 = 2$ then $\bar{T}((\alpha, \beta) \times U(\sigma_2, \varepsilon)) \subset (\alpha_1, \beta_1) \times (X_4^* \cup U(\sigma_4, \varepsilon))$.*

(3) *If $a_1 - b_1 \neq 1, 2$ then $\bar{T}((\alpha, \beta) \times U(\sigma_4, \varepsilon)) \subset (\alpha_1, \beta_1) \times (X_j^*)^\circ$ for some $j=1, 2$. If $a_1 - b_1 = 1$ then $\bar{T}((\alpha, \beta) \times U(\sigma_4, \varepsilon)) \subset (\alpha_1, \beta_1) \times U(\sigma_2, \varepsilon)$. If $a_1 - b_1 = 2$ then $\bar{T}((\alpha, \beta) \times U(\sigma_4, \varepsilon)) \subset (\alpha_1, \beta_1) \times U(\sigma_4, \delta)$.*

PROOF. Let us observe the picture of image of $U(\sigma_i, \varepsilon)$ by the map $(\gamma, \delta) \mapsto (-1/\gamma, \delta/\gamma)$. (See Figure 3.)



for $i=1$ or 3 for $i=2$ for $i=4$

figure of images of $U(\sigma_i, \varepsilon)$, $i=1, 2, 3, 4$, by the map $(\gamma, \delta) \mapsto (-1/\gamma, \delta/\gamma)$

FIGURE 3

Then from the observation of translations of figures by $(a_1, -b_1)$ it is easy to get the conclusion.

As the corollary of the lemma we have the following corollary.

COROLLARY. *If* $\bar{T}^n(\alpha, \beta, \gamma, \delta) \in U(\sigma_i, \varepsilon)$ *for all n, then* $b_n = 0$ *or* $a_n - b_n = 2$ *for all n.*

THEOREM 3.4. *The name of* $(\alpha, \beta) \in X$ *is eventually periodic, that is, there exist N and k such that* $(\alpha_N, \beta_N) = (\alpha_{N+k}, \beta_{N+k})$ *if and only if* α *is quadratic and* $\beta \in \boldsymbol{Q}(\alpha)$.

PROOF. From formulae (2) in Lemma 1.1, "only if" part is easy. Let us assume that α is quadratic, $\beta \in \boldsymbol{Q}(\alpha)$ and $(\alpha, \beta) \in X$. We will show that there exists N such that (α_N, β_N) is reduced. From the definition of β_n, we have

$$\beta_n = \frac{\beta_{n-1}}{\alpha_{n-1}} - b_n = \frac{1}{\alpha_{n-1}} \left\{ \frac{\beta_{n-2}}{\alpha_{n-2}} - b_{n-1} \right\} - b_n = \cdots \tag{3.3}$$

$$= -b_n - \frac{b_{n-1}}{\alpha_{n-1}} - \frac{b_{n-2}}{\alpha_{n-1}\alpha_{n-2}} - \cdots - \frac{b_1}{\alpha_{n-1} \cdots \alpha_1} + \frac{\beta_0}{\alpha_{n-1} \cdots \alpha_0}.$$

By Appendix, we may assume that $\overline{\alpha_0} > 1$. So we see that $(\alpha_0, \beta_0, \overline{\alpha_0}, 0) \in \bar{X}$.

Let us denote $(\alpha_n, \beta_n, \overline{\alpha_n}, \beta_n^*) = \bar{T}^n(\alpha_0, \beta_0, \overline{\alpha_0}, 0)$, then we know that $(\alpha_n, \beta_n, \overline{\alpha_n}, \beta_n^*) \in X$ for all n. Then by (3.1), (3.3) the distance between $(\alpha_n, \beta_n, \overline{\alpha_n}, \overline{\beta_n})$ and $(\alpha_n, \beta_n, \overline{\alpha_n}, \beta_n^*)$ on $\boldsymbol{R}^4$ is given by

$$|\overline{\beta_n} - \beta_n^*| = \left| \frac{\overline{\beta_0}}{\overline{\alpha_{n-1} \cdots \alpha_0}} \right|.$$

Therefore, from the finiteness of α_n's and the fact that $\overline{\alpha_n} > 1$ for all n, we see $|\overline{\beta_n} - \beta_n^*|$ converges to zero. If there eixsts N such that $(\alpha_N, \beta_N, \overline{\alpha_N}, \overline{\beta_N})$ is in the interior of $\bar{X}$, then the conclusion holds. Assume that $(\alpha_n, \beta_n, \overline{\alpha_n}, \overline{\beta_n}) \notin$ interior of $\bar{X}$ for all n. Then from the fact that $|\overline{\beta_n} - \beta_n^*| \to 0$ as $n \to \infty$, Lemma 3.4 and its corollary, and $\alpha_n, \overline{\alpha_n} \notin \boldsymbol{Q}$, $(\overline{\alpha_n}, \overline{\beta_n})$ must be near the boundaries σ_1 or σ_4 in $U(\sigma_i, \varepsilon)$ for all large n, that is, b_n should be equal to 0 for all large n or $a_n - b_n$ should be equal to 2 for all large n. Therefore, from Propositions 2.1 and 2.2, $\beta_n = 0$ or $\alpha_n + \beta_n = 1$ for large n. Thus from Proposition 3.1 we obtain the conclusion.

THEOREM 3.5. (α, β) *is reduced if and only if* (α, β) *is purely periodic, that is, there exists k such that* $T^k(\alpha, \beta) = (\alpha, \beta)$.

PROOF. "only if" part is proved in Proposition 3.3. Conversely, if (α, β) is purely periodic, then α and β are denoted by

$$\alpha = \frac{p_n - p_{n-1}\alpha}{q_n - q_{n-1}\alpha} \quad \text{and} \quad \beta = \frac{r_n - r_{n-1}\alpha + \beta}{q_n - q_{n-1}\alpha}.$$

Therefore, we see $q_{n-1}\alpha^2 - (q_n + p_{n-1})\alpha + p_n = 0$, that is, α is quadratic and $\beta \in \boldsymbol{Q}(\alpha)$. Thus, by the proof of Theorem 3.4 we know there exists N such that (α_N, β_N) is reduced. By Lemma 3.1 and pure periodicity, we see for some j that $(\alpha_{N+j}, \beta_{N+j})=(\alpha, \beta)$ is also reduced.

4. Reduction theory of ternary forms.

In this section, we discuss a reduction theory of ternary forms by the algorithm (X, T).

Let us denote the ternary form f_A with integer coefficients as follows:

$$f_A(x, y, z)=(x, y, z)A^t(x, y, z)$$

where A is given by

$$A=\begin{pmatrix} a & h & g \\ h & b & f \\ g & f & c \end{pmatrix}.$$

Put

$$\Delta:=-\det A\,, \qquad D:=-\det\begin{pmatrix} a & h \\ h & b \end{pmatrix}$$

and call Δ (D) the discriminant (small discriminant) of f_A.

ASSUMPTION. We assume that the small discriminant D of f_A is positive and non square. Moreover, we also assume that integers a, b and h do not have common divisor and $b>0$.

Let us denote the set of ternary forms satisfying the assumption by TF.

PROPOSITION 4.1. *For each $f_A \in TF$, $f_A(x, y, 1)$ has the following canonical representation*:

$$f_A(x, y, 1)=b(\alpha x+y+\beta)(\bar{\alpha}x+y+\bar{\beta})+k \tag{4.1}$$

where α, β and k are given by

$$\begin{aligned} &\alpha=\frac{h-\sqrt{D}}{b}, \quad \bar{\alpha}=\frac{h+\sqrt{D}}{b}, \quad x_0=\frac{bg-hf}{-D}, \quad y_0=\frac{-hg+af}{-D}, \\ &\beta=\alpha x_0+y_0\,, \quad \bar{\beta}=\bar{\alpha}x_0+y_0 \quad \textit{and} \quad k=-\Delta/D\,. \end{aligned} \tag{4.2}$$

PROOF. Let us denote

$$\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}=\begin{pmatrix} x'-x_0 \\ y'-y_0 \\ 1 \end{pmatrix}=\begin{pmatrix} 1 & 0 & -x_0 \\ 0 & 1 & -y_0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix},$$

$$H=\begin{pmatrix}1 & 0 & -x_0\\ 0 & 1 & -y_0\\ 0 & 0 & 1\end{pmatrix},$$

and consider the form:

$$f(x', y', 1)=(x', y', 1)^{t}HAH\,^{t}(x', y', 1)\,.$$

From the assumption $D>0$, the equation:

$$\begin{cases} ax+hy=g\\ hx+by=f\end{cases}$$

has the unique solution (x_0, y_0):

(4.3) $$\begin{pmatrix}x_0\\ y_0\end{pmatrix}=\frac{1}{-D}\begin{pmatrix}b & -h\\ -h & a\end{pmatrix}\begin{pmatrix}g\\ f\end{pmatrix}.$$

Therefore, we have

$$^{t}HAH={}^{t}H\begin{pmatrix}a & h & -ax_0-hy_0+g\\ h & b & -hx_0-by_0+f\\ g & f & -gx_0-fy_0+c\end{pmatrix}=\begin{pmatrix}a & h & 0\\ h & b & 0\\ 0 & 0 & -gx_0-fy_0+c\end{pmatrix},$$

that is, we have the following representation:

$$f(x', y', 1)=(x', y', 1)\begin{pmatrix}a & h & 0\\ h & b & 0\\ 0 & 0 & k\end{pmatrix}\begin{pmatrix}x'\\ y'\\ 1\end{pmatrix}$$

$$=b\left(\frac{h-\sqrt{D}}{b}x'+y'\right)\left(\frac{h+\sqrt{D}}{b}x'+y'\right)+k$$

where k is given by

$$k=-gx_0-fy_0+c\,.$$

Thus by (4.2) the form f_A has a representation:

$$f_A(x, y, 1)=b(\alpha x+y+\alpha x_0+y_0)(\bar{\alpha}x+y+\bar{\alpha}x_0+y_0)+k\,.$$

It is easy to see

$$k=-gx_0-fy_0+c=-\Delta/D\,.$$

Therefore, we have the canonical representation (4.1).

FUNDAMENTAL LEMMA 4.1. *Let us define a matrix S_1 as follows:*

$$S_1=\begin{pmatrix} m_1 & 1 & -n_1 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad m_1, n_1 \in \boldsymbol{Z}. \tag{4.4}$$

For each ternary form $f_A \in TF$, let us denote a form f_{A_1} and the canonical form of $f_{A_1}(x, y, z)$ with respect to $A_1={}^tS_1AS_1=\begin{pmatrix} a_1 & h_1 & g_1 \\ h_1 & b_1 & f_1 \\ g_1 & f_1 & c_1 \end{pmatrix}$ by $f_{A_1}(x, y, z)=(x, y, z)A_1{}^t(x, y, z)$ and $f_{A_1}(x, y, 1)=b_1(\alpha_1 x+\beta_1+y)(\overline{\alpha_1}x+\overline{\beta_1}+y)+k_1$. Then the following properties hold:

(1) $D_1\ (=-a_1b_1+h_1^2)=D$,

(2) $\Delta_1\ (=-\det A_1)=\Delta$,

(3) $k_1=k$,

(4) $\alpha_1=m_1-1/\alpha$,

(5) $\beta_1=\beta/\alpha-n_1$.

PROOF. The matrix A_1 is given as follows:

$$A_1=\begin{pmatrix} a_1 & h_1 & g_1 \\ h_1 & b_1 & f_1 \\ g_1 & f_1 & c_1 \end{pmatrix}={}^tS_1AS_1 \tag{4.5}$$

$$=\begin{pmatrix} am_1^2-2hm_1+b & am_1-h & -am_1n_1+hn_1+gm_1-f \\ am_1-h & a & -an_1+g \\ -am_1n_1+hn_1+gm_1-f & -an_1+g & an_1^2-2gn_1+c \end{pmatrix}.$$

Therefore, we know

$$D_1=-a_1b_1+h_1^2=-(am_1^2-2hm_1+b)a+(am_1-h)^2=D.$$

From $\det S_1=1$, we know

$$\Delta_1=\Delta \quad \text{and} \quad k_1=k.$$

(4) is obtained with a simple calculation:

$$\alpha_1=\frac{h_1-\sqrt{D_1}}{b_1}=\frac{am_1-h-\sqrt{D}}{a}=m_1-\frac{h+\sqrt{D}}{a}$$

$$=m_1-\frac{1}{(h-\sqrt{D})/b}=m_1-\frac{1}{\alpha}.$$

(5) is obtained as follows. We have

$$b_1g_1-h_1f_1=a(-am_1n_1+hn_1+gm_1-f)-(am_1-h)(-an_1+g)=hg-af.$$

Similarly, we have

$$\begin{aligned}-h_1g_1+a_1f_1&=-(am_1-h)(-am_1n_1+hn_1+gm_1-f)\\&\quad+(am_1^2-2hm_1+b)(-an_1+g)\\&=-m_1(hg-af)-n_1(ab-h^2)+(bg-hf)\,.\end{aligned}$$

Therefore, β_1 is written as

$$\begin{aligned}\beta_1&=\alpha_1\frac{hg-af}{ab-h^2}+\frac{-m_1(hg-af)-n_1(ab-h^2)+(bg-hf)}{ab-h^2}\\&=-(m_1-\alpha_1)\frac{hg-af}{ab-h^2}+\frac{bg-hf}{ab-h^2}-n_1\\&=\frac{1}{\alpha}\left(\frac{bg-hf}{ab-h^2}\alpha+\frac{-hg+af}{ab-h^2}\right)-n_1=\frac{\beta}{\alpha}-n_1\,.\end{aligned}$$

Let us define a map $\varphi: TF\mapsto \boldsymbol{R}^2$ by

(4.6) $$\varphi(f_A)=(\alpha,\beta)$$

where (α, β) is given by the canonical representation (4.1) of f_A.

LEMMA 4.2. *The map φ is injective on TF with the same discriminants D and Δ.*

PROOF. From the assumption of TF, i.e. $(a, b, h)=1$, the solution α of $bx^2-2hx+a=0$ is given uniquely. Let us assume that $(\alpha, \beta)=\varphi(f_{A'})$ and

$$A'=\begin{pmatrix}a' & h' & g'\\ h' & b' & f'\\ g' & f' & c'\end{pmatrix}.$$

The solution α (α') was given as the solution of $bx^2-2hx+a=0$ ($b'x^2-2h'x+a'=0$). Therefore, by the assumption $(a, b, h)=1$ and $b>0$, we see

$$a=a'\,,\quad b=b'\,,\quad h=h'\qquad\text{if}\quad \alpha=\alpha'\,.$$

On the other hand, by $\beta=\beta'$ we see

$$x_0=x'_0\quad\text{and}\quad y_0=y'_0\,.$$

Therefore, by (4.3) we know

$$g=g'\quad\text{and}\quad f=f'\,.$$

And we also know that $c=c'$ by relation between k and the pair of discriminants. This means A is equal to A'.

Let us denote by TF_1 the subset of TF in which the form satisfies the property

$$\varphi(f_A)=(\alpha,\beta)\in[0,1)\times[0,1)\,.$$

We call a ternary form $f_A \in TF_1$ *reduced* if $\varphi(f_A)$ is reduced. We denote the set of reduced ternary forms by RTF_1.

Let U be an operator on TF_1 as follows:

$$Uf_A = f_{A_1}$$

where A_1 is given by (4.5) and m_1 and n_1 are defined as follows:

$$m_1 := -[-1/\alpha] \quad \text{and} \quad n_1 := [\beta/\alpha]\,,$$

where $(\alpha, \beta) = \varphi(f_A)$. The following proposition is obtained from the Fundamental Lemma 4.1.

PROPOSITION 4.2. *The map φ given by* (4.6) *is injective and the following commutative diagram holds*:

$$\begin{array}{ccc} TF_1 & \xrightarrow{\varphi} & X \\ \big\downarrow U & & \big\downarrow T \\ TF_1 & \xrightarrow{\varphi} & X \end{array} ,$$

that is, $\varphi(Uf_A) = T(\varphi f_A)$.

THEOREM 4.3 (A reduction theory of ternary forms). *For any ternary form $f_A \in TF_1$, there exist $N \in \boldsymbol{Z}^+$ and $k \in \boldsymbol{N}$ such that*

$$U^{N+kl+j} f_A = U^{N+j} f_A \in RTF_1 \qquad (0 \leqq j < k,\ l \in \boldsymbol{N})\,.$$

This is an immediate consequence of Proposition 4.2, Theorem 3.4 and Theorem 3.5.

5. Equivalence relation on TF_1.

Let us define a subgroup Γ of $SL(3, \boldsymbol{Z})$ as follows:

$$\Gamma := \left\{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ s & t & 1 \end{pmatrix} \in SL(3, \boldsymbol{Z}) \right\}.$$

By means of Γ, we introduce an equivalence relation on X. We say (α, β) is Γ-related to (α', β') with $S \in \Gamma$ if (1) there exists $S \in \Gamma$ such that $(\alpha, \beta) = S(\alpha', \beta')$, that is, the following relation holds:

$$\alpha = \frac{c + d\alpha'}{a + b\alpha'}\,, \qquad \beta = \frac{s + t\alpha' + \beta'}{a + b\alpha'}\,,$$

and (2) $a + b\alpha' > 0$, where S is given by

$$S=\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ s & t & 1 \end{pmatrix}. \tag{5.1}$$

Let us denote $(\alpha, \beta)\sim_S(\alpha', \beta')$ if (α, β) is Γ-related to (α', β') with $S\in\Gamma$.

LEMMA 5.1. *The relation $\sim_S$ is an equivalence relation.*

PROOF. On the assumption $(\alpha, \beta)\sim_S(\alpha', \beta')$, we will see that $S^{-1}(\alpha, \beta)=(\alpha', \beta')$ and $S^{-1}\in\Gamma$. Under the notation (5.1) we have

$$S^{-1}=\begin{pmatrix} d & -b & 0 \\ * & * & 0 \\ * & * & 1 \end{pmatrix}.$$

Hence, we see that

$$d-b\alpha=d-b\frac{c+d\alpha'}{a+b\alpha'}=\frac{1}{a+b\alpha'}>0 .$$

Therefore, we have $(\alpha', \beta')\sim_{S^{-1}}(\alpha, \beta)$. Let us assume $(\alpha, \beta)\sim_{S_1}(\alpha', \beta')$ and $(\alpha', \beta')\sim_{S_2}(\alpha'', \beta'')$. Putting

$$S_1=\begin{pmatrix} a_1 & b_1 & 0 \\ c_1 & d_1 & 0 \\ s_1 & t_1 & 1 \end{pmatrix} \quad \text{and} \quad S_2=\begin{pmatrix} a_2 & b_2 & 0 \\ c_2 & d_2 & 0 \\ s_2 & t_2 & 1 \end{pmatrix},$$

$S_1\cdot S_2\in\Gamma$ is given by

$$S_1\cdot S_2=\begin{pmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 & 0 \\ * & * & 0 \\ * & * & 1 \end{pmatrix}.$$

Therefore, we see

$$(a_1a_2+b_1c_2)+(a_1b_2+b_1d_2)\alpha''=a_1(a_2+b_2\alpha'')+b_1(c_2+d_2\alpha'')$$
$$=(a_2+b_2\alpha'')\left(a_1+b_1\frac{c_2+d_2\alpha''}{a_2+b_2\alpha''}\right)=(a_2+b_2\alpha'')(a_1+b_1\alpha')>0 .$$

To discuss a decomposition of the element of Γ, we introduce the following concept. For two integer vectors (l, m, n) and (l', m', n') we say that (l, m, n) is *next* to (l', m', n'), if the following conditions hold:

(0) $l>l'\geqq 0$,

(1) $l'\cdot m-l\cdot m'=1$,

(2) $l>l'\cdot n-l\cdot n'\geqq 0$.

LEMMA 5.2. *Assume that (l, m, n) is next to (l', m', n'), and $l>m>0$, $l>n\geqq 0$. And let us denote*

$$\begin{pmatrix} l_1 & -l'_1 & 0 \\ m_1 & -m'_1 & 0 \\ n_1 & -n'_1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ -1 & a_1 & 0 \\ 0 & -b_1 & 1 \end{pmatrix} \begin{pmatrix} l & -l' & 0 \\ m & -m' & 0 \\ n & -n' & 1 \end{pmatrix}$$

where a_1 and b_1 are given by

$$a_1 = -[-l/m] \quad \text{and} \quad b_1 = [n/m]\,.$$

Then (l_1, m_1, n_1) is next to (l'_1, m'_1, n'_1), and $l_1>m_1\geqq 0$ and $l_1>n_1\geqq 0$.

PROOF. From the definitions of a_1, b_1 and

$$\begin{pmatrix} l_1 & -l'_1 & 0 \\ m_1 & -m'_1 & 0 \\ n_1 & -n'_1 & 1 \end{pmatrix} = \begin{pmatrix} m & -m' & 0 \\ -l+a_1 m & l'-a_1 m' & 0 \\ -mb_1+n & m'b_1-n' & 1 \end{pmatrix},$$

we see $l_1>m_1\geqq 0$ and $l_1>n_1\geqq 0$. From the assumptions (0), (1) and $l>m>0$, we see $m>m'\geqq 0$, that is, $l_1>l'_1\geqq 0$. From

$$\begin{vmatrix} l_1 & -l'_1 \\ m_1 & -m'_1 \end{vmatrix} = \begin{vmatrix} 0 & 1 \\ -1 & a_1 \end{vmatrix} \begin{vmatrix} l & -l' \\ m & -m' \end{vmatrix} = 1\,,$$

the condition (1) is true.

The condition (2): $l_1>l'_1 n_1-l_1 n'_1\geqq 0$ is equivalent to $m>m'n-mn'\geqq 0$. Therefore, we must show that $m>m'n-mn'\geqq 0$. By the assumptions (1), (2) and $m>0$, we have the following inequalities:

$$lm(n'+1)>n(1+lm')\geqq lmn'\,.$$

Therefore, the following inequalities hold:

$$n+l(nm'-n'm)\geqq 0 \quad \text{and} \quad n+l(nm'-n'm-m)<0\,. \tag{5.2}$$

From $l>n$ and (5.2) we have $m'n-mn'\geqq 0$. Suppose $m'n-mn'-m\geqq 0$. Then from (5.2) we have $0>n$. This contradicts $n\geqq 0$. So we have $m>m'n-mn'$. Therefore, the condition (2) is satisfied.

LEMMA 5.3. *If (l, m, n) is next to (l', m', n') and $l>m>0$, $l>n\geqq 0$ then there exists k such that*

$$\begin{pmatrix} l & -l' & 0 \\ m & -m' & 0 \\ n & -n' & 1 \end{pmatrix} = \begin{pmatrix} a_1 & -1 & 0 \\ 1 & 0 & 0 \\ b_1 & 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} a_k & -1 & 0 \\ 1 & 0 & 0 \\ b_k & 0 & 1 \end{pmatrix}$$

where $\begin{pmatrix} a_1 & \cdots & a_k \\ b_1 & \cdots & b_k \end{pmatrix}$ is given as a name of $(m/l, n/l)$ by the algorithm T.

Proof. Applying Lemma 5.2 repeatedly, we have a k such that $m_k=0$. From conditions (0) and (1) we see that $l_k=-m'_k=1$ and $l'_k=0$. And we see that $n_k=0$ from $l_k>n_k\geqq 0$, and $n'_k=0$ from condition (2). Therefore, we have

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}0&1&0\\-1&a_k&0\\0&-b_k&1\end{pmatrix}\cdots\begin{pmatrix}0&1&0\\-1&a_1&0\\0&-b_1&1\end{pmatrix}\begin{pmatrix}l&-l'&0\\m&-m'&0\\n&-n'&1\end{pmatrix}.$$

Lemma 5.4. *Assume $\beta\notin\alpha\boldsymbol{Z}+\boldsymbol{Z}$, then*

(1) $A_n=(r_nq_{n-1}-q_nr_{n-1})-(r_np_{n-1}-p_nr_{n-1})$ *is increasing for large n,*

(2) $B_n=r_nq_{n-1}-r_{n-1}q_n-q_n$ *tends to negative infinity,*

(3) $C_n=r_n(q_{n-1}-p_{n-1})-r_{n-1}(q_n-p_n)-(q_n-p_n)$ *tends to negative infinity.*

Proof. (1): By (1.6), we see

$$A_n=A_{n-1}+b_n(q_{n-1}-p_{n-1}).$$

From the assumption $\alpha\notin\boldsymbol{Q}$, $\beta\notin\alpha\boldsymbol{Z}+\boldsymbol{Z}$ and Proposition 2.1, there exists infinitely many b_n such that $b_n\neq 0$. Therefore, from $q_n-p_n>0$ we have (1).

(2): For the sequence B_n, we can show the following properties:

(B1) B_{m_k} is strictly monotone decreasing,

(B2) if $m_k+1\neq m_{k+1}$ then

$$B_{m_k+1}>B_{m_k}\quad\text{and}\quad B_{m_k+1}>B_{m_k+2}>\cdots>B_{m_{k+1}},$$

(B3)´ if $m_k+1\neq m_{k+1}$, $m_{k+j}+1=m_{k+1+j}$, $1\leqq j\leqq N-1$ and $m_{k+N}+1\neq m_{k+N+1}$ then

$$B_{m_k+1}>B_{m_{k+1}+N}.$$

Then we have the conclusion (2). From (1.6), B_{n+1} is written as

$$B_{n+1}=B_n+(-a_{n+1}+b_{n+1}+1)q_n+q_{n-1}.$$

If $-a_{n+1}+b_{n+1}+1\leqq -1$, then $B_{n+1}<B_n$. If $-a_{n+1}+b_{n+1}+1=0$, then by the property (B) of admissible sequences there exists l $(\geqq 1)$ such that

$$-a_j+b_j+2=0\qquad\text{for}\quad n+2\leqq j<n+1+l$$

and $-a_{n+1+l}+b_{n+1+l}+2<0$. Therefore, we have

$$\begin{aligned}B_{n+l}&=B_{n+l-1}+(-a_{n+l}+b_{n+l}+1)q_{n+l-1}+q_{n+l-2}\\&=B_{n+l-1}-q_{n+l-1}+q_{n+l-2},\end{aligned}$$

and similaly

$$B_{n+l-i}=B_{n+l-i-1}-q_{n+l-i-1}+q_{n+l-i-2}\qquad(1\leqq i\leqq l-2).$$

Thus, from $B_{n+1}=B_n+q_{n-1}$ we have

$$B_{n+l}=B_n-q_{n+l-1}+q_n+q_{n-1}\,.$$

By using the above equality we have

$$\begin{aligned}B_{n+l+1}&=B_{n+l}+(-a_{n+l+1}+b_{n+l+1}+1)q_{n+l}+q_{n+l-1}\\&=B_n+(-a_{n+l+1}+b_{n+l+1}+1)q_{n+l}+q_n+q_{n-1}\,.\end{aligned}$$

Now, we choose $\{m_k\}$ which is the subsequence of $\boldsymbol{N}$ as follows:

$$\begin{aligned}\{m_k \mid k=1,2,\cdots\}=\boldsymbol{N}\setminus\{n+1,\cdots,n+l \mid\ &-a_{n+1}+b_{n+1}+1=0\,,\\&-a_{n+i}+b_{n+i}+2=0\ \ (2\leqq i\leqq l)\,,\ -a_{n+l+1}+b_{n+l+1}+2<0\}\,.\end{aligned}$$

Then B_{m_k} satisfies the properties (B1) and (B2). Let us assume that $-a_{m_j+1}+b_{m_j+1}+1=0$, that is, $B_{m_j+1}=B_{m_j}+q_{m_j-1}$. Then there exists l_j such that $B_{m_j+l_j+1}=B_{m_j}+(-a_{m_j+l_j+1}+b_{m_j+l_j+1}+1)q_{m_j+l_j}+q_{m_j}+q_{m_j-1}$ and $-a_{m_j+l_j+1}+b_{m_j+l_j+1}+2<0$. Now, put $m_{j+1}=m_j+l_j+1$ then we have

$$B_{m_{j+1}}=B_{m_j}+(-a_{m_{j+1}}+b_{m_{j+1}}+1)q_{m_{j+1}-1}+q_{m_j}+q_{m_j-1}\,.$$

There exists N such that

$$-a_{m_{j+1}+i}+b_{m_{j+1}+i}+1\neq 0 \ \text{ for } \ 1\leqq i\leqq N-1 \quad \text{and} \quad -a_{m_{j+1}+N}+b_{m_{j+1}+N}+1=0\,.$$

Then $m_{j+1}+N$ is a first m_k which is larger than m_j and satisfies $m_k+1\neq m_{k+1}$. We know

$$\begin{aligned}B_{m_{j+1}+N}&=B_{m_{j+1}+N-1}+(-a_{m_{j+1}+N}+b_{m_{j+1}+N}+1)q_{m_{j+1}+N-1}+q_{m_{j+1}+N-2}\\&=B_{m_{j+1}+N-1}+q_{m_{j+1}+N-2}\\&=B_{m_{j+1}+N-2}+(-a_{m_{j+1}+N-1}+b_{m_{j+1}+N-1}+2)q_{m_{j+1}+N-2}+q_{m_{j+1}+N-3}\\&=B_{m_{j+1}}+\sum_{i=1}^{N-1}(-a_{m_{j+1}+i}+b_{m_{j+1}+i}+2)q_{m_{j+1}+i-1}+q_{m_{j+1}-1}\\&=B_{m_j}+(-a_{m_{j+1}}+b_{m_{j+1}}+2)q_{m_{j+1}-1}+q_{m_j}+q_{m_j-1}\\&\quad+\sum_{i=1}^{N-1}(-a_{m_{j+1}+i}+b_{m_{j+1}+i}+2)q_{m_{j+1}+i-1}\\&=B_{m_j+1}+\sum_{i=0}^{N-1}(-a_{m_{j+1}+i}+b_{m_{j+1}+i}+2)q_{m_{j+1}+i-1}+q_{m_j}\,.\end{aligned}$$

By the way, we know

$$-a_{m_{j+1}}+b_{m_{j+1}}+2<0$$

and

$$-a_{m_{j+1}+i}+b_{m_{j+1}+i}+2\leqq 0 \qquad (1\leqq i\leqq N-1)\,.$$

Therefore, we have

$$B_{m_{j+1}+N} < B_{m_j+1} .$$

This means that (B3) holds.

(3): Put $q_n^* := q_n - p_n$. Then there exists n_0 such that $q_n^* > q_{n-1}^* > 0$ for $n \geqq n_0$. Therefore, we can prove (3) similarly as in the proof of (2).

THEOREM 5.1. *Let us assume that*

(1) (α, β) *and* $(\alpha', \beta') \in X$,

(2) $\alpha \notin \boldsymbol{Q}$ *and* $\beta \notin \alpha\boldsymbol{Z} + \boldsymbol{Z}$,

(3) $(\alpha, \beta) \sim_S (\alpha', \beta')$ *for some* $S \in \Gamma$.

Then there exist n, m such that

$$(\alpha_n, \beta_n) = (\alpha'_m, \beta'_m) .$$

REMARK 5.1. Let us assume that

(1) (α, β) and $(\alpha', \beta') \in X$,

(2) $\alpha' \notin \boldsymbol{Q}$ and $\beta' \in \alpha'\boldsymbol{Z} + \boldsymbol{Z}$,

(3) $(\alpha, \beta) \sim_S (\alpha', \beta')$ for some $S \in \Gamma$.

Then there exist n, m such that

$$\alpha_n = \alpha'_m ,$$

$$\beta_n = 0 \text{ or } 1 - \alpha_n ,$$

$$\beta'_m = 0 \text{ or } 1 - \alpha'_m .$$

In particular, $\alpha \notin \boldsymbol{Q}$ and $\beta \in \alpha\boldsymbol{Z} + \boldsymbol{Z}$.

In fact, from (2) and (3), it is easy to see that α, β also satisfy $\alpha \notin \boldsymbol{Q}$ and $\beta \in \alpha\boldsymbol{Z} + \boldsymbol{Z}$. Therefore, by Propositions 2.1 and 2.2, $\beta_k = 0$ or $\alpha_k + \beta_k = 1$, and $\beta'_k = 0$ or $\alpha'_k + \beta'_k = 1$ for $k \geqq k_0$. From (3), we are able to assume that there exists a matrix $A \in SL(2, \boldsymbol{Z})$ such that $\alpha = A\alpha'$. Then by Serret's theorem on the modified continued fraction expansion, there exist n and m ($\geqq k_0$) such that $\alpha_n = \alpha'_m$.

PROOF OF THEOREM 5.1. Put

$$S = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ s & t & 1 \end{pmatrix},$$

$$(\alpha', \beta') = \begin{pmatrix} q'_n & -q'_{n-1} & 0 \\ p'_n & -p'_{n-1} & 0 \\ r'_n & -r'_{n-1} & 1 \end{pmatrix} (\alpha'_n, \beta'_n) .$$

Then we have

$$(\alpha, \beta)=\begin{pmatrix} aq'_n+bp'_n & -(aq'_{n-1}+bp'_{n-1}) & 0 \\ cq'_n+dp'_n & -(cq'_{n-1}+dp'_{n-1}) & 0 \\ sq'_n+tp'_n+r'_n & -(sq'_{n-1}+tp'_{n-1}+r'_{n-1}) & 1 \end{pmatrix}(\alpha'_n, \beta'_n).$$

To obtain the conclusion, we show firstly the following inequality (0) for "next" is satisfied for some n. From $\alpha' \notin \boldsymbol{Q}$, $q'_n > q'_{n-1} > 0$, we know

$$1 > q'_{n-1}/q'_n > 0$$

and from the assumption $a+b\alpha' > 0$ and $p'_n/q'_n \mapsto \alpha'$ as $n \mapsto \infty$ we see

$$a+b(p'_n/q'_n) > 0 \qquad \text{for large} \quad n.$$

The inequality (0): $aq'_n+bp'_n > aq'_{n-1}+bp'_{n-1} > 0$ is equivalent to

$$1 > \frac{q'_{n-1}}{q'_n} \frac{a+b(p'_{n-1}/q'_{n-1})}{a+b(p'_n/q'_n)} > 0.$$

Therefore, we see the inequality (0) holds for large n.

The inequality: $aq'_n+bp'_n > cq'_n+dp'_n > 0$ is equivalent to

$$1 > \frac{c+d(p'_n/q'_n)}{a+b(p'_n/q'_n)} > 0.$$

From $\alpha \in X$, $\alpha' \notin \boldsymbol{Q}$ and

$$(c+d\alpha')/(a+b\alpha') = \alpha,$$

we see that the above inequality holds for large n. Similarly, we see that the inequality: $aq'_n+bp'_n > sq'_n+tp'_n+r'_n > 0$ holds for large n.

Put

$$(\alpha'', \beta'') := (\alpha'_n, \beta'_n),$$

$$(\alpha, \beta)=\begin{pmatrix} a' & b' & 0 \\ c' & d' & 0 \\ s' & t' & 1 \end{pmatrix}(\alpha'', \beta'').$$

Then we can assume by above discussion that

$$a' > -b' > 0, \quad a' > c' > 0 \quad \text{and} \quad a' > s' > 0.$$

Putting

$$(\alpha'', \beta'')=\begin{pmatrix} q''_n & -q''_{n-1} & 0 \\ p''_n & -p''_{n-1} & 0 \\ r''_n & -r''_{n-1} & 1 \end{pmatrix}(a''_n, \beta''_n),$$

let us denote again that

$$(\alpha, \beta)=\begin{pmatrix} a'q''_n+b'p''_n & -(a'q''_{n-1}+b'p''_{n-1}) & 0 \\ c'q''_n+d'p''_n & -(c'q''_{n-1}+d'p''_{n-1}) & 0 \\ s'q''_n+t'p''_n+r''_n & -(s'q''_{n-1}+t'p''_{n-1}+r''_{n-1}) & 1 \end{pmatrix}(\alpha''_n, \beta''_n) .$$

Then we see

$$a'q''_n+b'p''_n>a't'-b's'+a'(r''_nq''_{n-1}-r''_{n-1}q''_n)+b'(r''_np''_{n-1}-r''_{n-1}p''_n)\geqq 0 ,$$

because by Lemma 5.4 (1) and $a'>-b'>0$, the inequality

$$\begin{aligned} &a't'-b's'+a'(r''_nq''_{n-1}-r''_{n-1}q''_n)+b'(r''_np''_{n-1}-r''_{n-1}p''_n) \\ &\quad >a't'-b's'+a'\{(r''_nq''_{n-1}-r''_{n-1}q''_n)-(r''_np''_{n-1}-r''_{n-1}p''_n)\}\geqq 0 \end{aligned}$$

holds for large n. On the other hand, by Lemma 5.4 (3) and $a'>-b'>0$, we see the another inequality

$$a'q''_n+b'p''_n>a't'-b's'+a'(r''_nq''_{n-1}-r''_{n-1}q''_n)+b(r''_np''_{n-1}-r''_{n-1}p''_n)$$

holds for large n. Therefore, by Lemma 5.3 there exists $N=N(n)$ for each large n such that

$$(\alpha, \beta)=\begin{pmatrix} a_1 & -1 & 0 \\ 1 & 0 & 0 \\ b_1 & 0 & 1 \end{pmatrix}\cdots\begin{pmatrix} a_N & -1 & 0 \\ 1 & 0 & 0 \\ b_N & 0 & 1 \end{pmatrix}(\alpha''_n, \beta''_n) .$$

To finish the proof of the theorem we must know finally that

$$(\alpha''_n, \beta''_n)=(\alpha_N, \beta_N) \qquad \text{for some} \quad n$$

where (α_N, β_N) is given by the relation:

$$(\alpha, \beta)=\varphi_{\binom{a_1, \cdots, a_N}{b_1, \cdots, b_N}}(\alpha_N, \beta_N) .$$

We know from the assumption $\beta'\notin\alpha'\boldsymbol{Z}+\boldsymbol{Z}$, which is equivalent to $\beta\in\alpha\boldsymbol{Z}+\boldsymbol{Z}$, that infinitely many (α''_n, β''_n) are in U_1. In fact, suppose that $(\alpha''_n, \beta''_n)\in U_2$ for all large n. This assumption is equivalent to $a'_n-b'_n=2$ for all large n. But by Proposition 2.2 this contradicts $\beta'\notin\alpha'\boldsymbol{Z}+\boldsymbol{Z}$.

Notice that U_1 is equal or subset of domain of bijective map $\varphi_{\binom{a_1, \cdots, a_N}{b_1, \cdots, b_N}}$. Then from $(\alpha''_n, \beta''_n)\in U_1$ for some n and from bijectivity of $\varphi_{\binom{a_1, \cdots, a_N}{b_1, \cdots, b_N}}$ we have

$$(\alpha_N, \beta_N)=(\alpha''_n, \beta''_n) .$$

Let us decompose RTF_1 by $\mathscr{A}$, $\mathscr{B}_1$ and $\mathscr{B}_2$ as follows:

$$\begin{aligned} &\mathscr{A}:=\{f\in RTF_1 \mid \beta\notin\alpha\boldsymbol{Z}+\boldsymbol{Z} \text{ for } (\alpha, \beta)=\varphi(f)\} \\ &\mathscr{B}_1:=\{f\in RTF_1 \mid \exists m, n: \beta=m\alpha+n, m\geqq 0, n\leqq 0 \text{ for } (\alpha, \beta)=\varphi(f)\} \\ &\mathscr{B}_2:=\{f\in RTF_1 \mid \exists m, n: \beta=m\alpha+n, m<0, n>0 \text{ for } (\alpha, \beta)=\varphi(f)\} \end{aligned}$$

and $\mathscr{B}:=\mathscr{B}_1\cup\mathscr{B}_2$.

Let us define an operator V on TF_1 by

$$Vf_A:=f_{{}^tWAW} \qquad \text{where} \quad W=\begin{pmatrix} -1 & 0 & 1 \\ 0 & -1 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then it is easy to see

$$\varphi(Vf_A)=(\alpha,\ 1-\alpha-\beta)$$

where $(\alpha, \beta)=\varphi(f_A)$. Therefore, we have

$$V(\mathscr{B}_1)=\mathscr{B}_2 \quad \text{and} \quad V(\mathscr{B}_2)=\mathscr{B}_1 .$$

Then we obtain the following theorem.

THEOREM 5.2. *For any $f, g\in RTF_1$*

(1) *if $f\sim g$ and $f, g\in\mathscr{A}$ then there exists k such that*

$$U^kf=g ,$$

(2) (A) *if $f\sim g$ and $f, g\in\mathscr{B}_i$ then there exists k such that*

$$U^kf=g ,$$

(B) *if $f\sim g$, $f\in\mathscr{B}_1$ and $g\in\mathscr{B}_2$ then there exists k such that*

$$U^kVf=g ,$$

where $f\sim g$ means $\varphi(f)\sim_S\varphi(g)$ for some $S\in\Gamma$.

The theorem is immediately obtained from Proposition 4.2, Theorem 5.1 and Remark 5.1.

6. Appendix. On modified continued fraction algorithm.

In this section, we give a rough survey without proof of the facts for the modified continued fraction expansion which are used in this paper.

The algorithm S: $[0.\ 1)\mapsto[0, 1)$ is given by

$$S\alpha=\begin{cases} -[-1/\alpha]-1/\alpha & \text{if} \quad \alpha\neq 0 \\ 0 & \text{if} \quad \alpha=0 \end{cases}$$

and

$$a_n(\alpha)\ (=a_n)=-\left[\frac{1}{S^{n-1}\alpha}\right] \qquad (n\geqq 1) ,$$

then the triple $([0, 1), S, a(\alpha))$ gives the following expansion: for irrational α,

$$\alpha=\cfrac{1}{a_1-\cdots\cfrac{1}{a_n-S^n\alpha}}\qquad(n\geqq 1)\,.$$

We call a_n ($\geqq 2$) digit of the modified continued fraction expansion which was called B-continued fraction expansion in [3].

Let us introduce 2×2 matrices as follows:

$$\begin{pmatrix} q_n & -q_{n-1} \\ p_n & -p_{n-1} \end{pmatrix}:=\begin{pmatrix} a_1 & -1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_n & -1 \\ 1 & 0 \end{pmatrix}\qquad(n\geqq 1)$$

$$\left(\begin{pmatrix} q_0 & -q_{-1} \\ p_0 & -p_{-1} \end{pmatrix}:=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right).$$

Then we know a formula:

$$\alpha=\frac{p_n-p_{n-1}\alpha_n}{q_n-q_{n-1}\alpha_n}\,.$$

THEOREM 6.1. *For each irrational* $\alpha\in[0, 1)$

(1) $0<q_{n-1}<q_n$ $(n\geqq 1)$,

(2) $\alpha-p_n/q_n>0$ $(n\geqq 1)$ *and* $p_n/q_n\uparrow\alpha$ $(n\to\infty)$.

THEOREM 6.2. (1) (Lagrange) α *is quadratic iff the sequence of digits* a_n *are eventually periodic.*

(2) (Galois) α *is quadratic and reduced iff the sequence of digits* a_n *are purely periodic, where a quadratic number* α *is reduced if* $0<\alpha<1$ *and* $\bar{\alpha}>1$, *where* $\bar{\alpha}$ *means the algebraic conjugate of* α.

REMARK 6.1. If α is reduced, then the set $\{S^n\alpha \mid n=1, 2, \cdots\}$ is finite.

For irrational α, $\alpha'\in[0, 1)$, we say that α is equivalent to α' if there exists $A\in SL(2, \mathbf{Z})$ satisfying the relation:

$$\alpha=\frac{c+d\alpha'}{a+b\alpha'}$$

where

$$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We denote it as $\alpha\sim_A\alpha'$.

Then the relation $\sim$ is an equivalence relation.

THEOREM 6.3. (Serret) *For irrational* α, $\alpha'\in[0, 1)$, *if* $\alpha\sim\alpha'$ *then there exist* m *and* n ($\geqq 1$) *such that* $S^{n-1}\alpha=S^{m-1}\alpha'$.

Now, we introduce a reduction theory of binary forms. Let us denote the binary form f_A with integer coefficients as follows:

$$f_A(x, y) := (x, y)A\,{}^t(x, y)$$

where A is given by

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

and assume that $D = -\det A > 0$, $c > 0$ and $(a, b, c) = 1$.

We denote the set of binary forms satisfying above assumption by BF. Let us define a map $\varphi : BF \mapsto R$ by $\varphi(f_A) = \alpha$ where α is the solution of $f_A(-1, x) = 0$ such that

$$\alpha := \frac{b - \sqrt{D}}{2c}.$$

And let us denote by BF_1 the subset of BF in which the form satisfies the property

$$\varphi(f_A) = \alpha \in [0, 1).$$

And, let U be an operator on BF_1 defined by $Uf_A = f_{A_1}$ where A_1 and U_{a_1} are given by

$$A_1 := {}^tU_{a_1} A U_{a_1}$$

$$U_{a_1} := \begin{pmatrix} a_1 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{where } a_1 := -[-1/\alpha].$$

Then, the following commutative diagram holds:

$$\begin{array}{ccc} BF_1 & \xrightarrow{\varphi} & [0, 1) \\ \downarrow{\scriptstyle U} & & \downarrow{\scriptstyle S} \\ BF_1 & \xrightarrow{\varphi} & [0, 1) \end{array}$$

that is, $\varphi(Uf_A) = S(\varphi f_A)$.

We call f_A reduced forms if $\varphi(f_A)$ is reduced. We denote the set of reduced forms by RBF_1. Then, we have the following theorem.

THEOREM (The Reduction Theory of Binary Forms). *For any binary form $f_A \in BF_1$, there exist $N \in Z^+$ and $k \in N$ such that*

$$U^{N+kl+j} f_A = U^{N+j} f_A \in RBF_1 \qquad (0 \leqq j < k,\ l \in N).$$

References

[1] D. B. ZAGIER, *Zeta Funktionen und Quadratische Körper*, Springer (1981).

[2] Sh. ITO and M. YURI, Number theoretical transformations with finite range structure and their ergodic

properties, Tokyo J. Math., **10** (1987), 1–32.
[3] Sh. Ito, On a diophantine approximation of real numbers from below, *Proc. Prospects of Math. Sci.*, World Scientific Publ. (1988), 41–62.

Present Address:
DEPARTMENT OF MATHEMATICS, TSUDA COLLEGE
TSUDA-MACHI, KODAIRA-SHI, TOKYO 187, JAPAN