J. Math. Tokushima Univ.
Vol. 24 (1990), 1–11

On the Structure of the Integer Solutions of $z^2 = (x^2 - 1)(y^2 - 1) + a$

By

Shin-ichi KATAYAMA and Kenji KASHIHARA

(Received September 21, 1990)

Introduction

In [3], L. J. Mordell investigated a quartic equation with integral coefficients

$$\sum_{r,s=0}^{2} a_{rs}x^r y^s = dz^2. \tag{1}$$

He noted that this quartic equation is not without interest but it seems difficult to find the integer solutions since no general criterion for solvability exists.

In this paper, we shall show that there exists a criterion for solvability when we restrict ourselves to the following special case

$$(x^2 - 1)(y^2 - 1) + a = z^2. \tag{2}$$

We denote the set of all the real solutions of (2) by F_a and the set of all the integral solutions of (2) by S_a. It is easy to show the following mappings σ, τ, ρ_i are the permutations on F_a and S_a. We denote the symmetric groups on F_a and S_a by *Sym* F_a and *Sym* S_a, respectively.

Mappings σ, τ, ρ_i are defined by putting

$$\sigma: \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & x & 1 \\ 0 & x^2 - 1 & x \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ xy + z \\ (x^2 - 1)y + xz \end{pmatrix},$$

$$\tau: \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longrightarrow \begin{pmatrix} y \\ x \\ z \end{pmatrix},$$

$$\rho_1: \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longrightarrow \begin{pmatrix} -x \\ y \\ z \end{pmatrix},$$

$$\rho_2: \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longrightarrow \begin{pmatrix} x \\ -y \\ z \end{pmatrix},$$

$$\rho_3 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longrightarrow \begin{pmatrix} x \\ y \\ -z \end{pmatrix}.$$

G denotes the permutation group generated by σ, τ, ρ_i, that is, $G = \langle \sigma, \tau, \rho_i \rangle$. Then we have $G < Sym\ F_a$ and $G < Sym\ S_a$. We call two solutions $P, Q \in F_a$ are G-equivalent when there exists an element $g \in G$ such that $g\,P = Q$. On the other hand, we call $P, Q \in F_a$ are G-independent when $g\,P \neq Q$ for any $g \in G$. We shall write $P \sim Q$ if two solutions P, Q are G-equivalent and $P \nsim Q$ if two solutions are G-independent. We denote the orbit containing P by $O(P)$. If the number of the orbits $\#[S_a/G]$ is finite, we denote this number by t_a. In the following, we shall show t_a is finite except the case $a = 0$ and shall show there exists a criterion for $S_a \neq \phi$. For a fixed integer $x = n \geqq 2$, the equation (2) is a norm equation from $\mathbf{Q}(\sqrt{n^2-1})$ to $\mathbf{Q}$. The permutation $\sigma \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y' \\ z' \end{pmatrix}$ is induced from the equation

$$z' + y'\sqrt{n^2-1} = (z + y\sqrt{n^2-1})(n + \sqrt{n^2-1}).$$

§1 The structure of the group G

With the notation as above, we have the following lemma.

Lemma 1. *$G = \langle \sigma, \tau, \rho_i \rangle < Sym\ F_a$ and $< Sym\ S_a$.*

Proof. From the equation (2), it is easy to show $\tau, \rho_i \in Sym\ F_a$ and $Sym\ S_a$. For any $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in F_a (\text{or } S_a)$, $\begin{pmatrix} x \\ y' \\ z' \end{pmatrix} = \sigma \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ satisfies the following equation.

$$(z')^2 - (x^2-1)((y')^2-1) = \{(x^2-1)y + xz\}^2 - (x^2-1)\{(xy+z)^2 - 1\}$$
$$= (x^2-1)(1-y^2-z^2) + x^2z^2 = z^2 - (x^2-1)(y^2-1) = a.$$

Since σ is bijective, $\sigma \in Sym\ F_a$ and $\sigma \in Sym\ S_a$, which completes the proof.

Lemma 2. *$\sigma, \tau, \rho_i \in G$ satisfy the following relations*

(i) $\rho_1^2 = \rho_2^2 = \rho_3^2 = \tau^2 = 1$,

$\rho_1\rho_2 = \rho_2\rho_1$, $\rho_1\rho_3 = \rho_3\rho_1$, $\rho_2\rho_3 = \rho_3\rho_2$,

$\rho_1\sigma\rho_1 = \rho_2\rho_3\sigma^{-1}$, $\rho_2\sigma\rho_2 = \sigma^{-1}$, $\rho_3\sigma\rho_3 = \sigma^{-1}$,

$\tau\rho_1\tau = \rho_2$, $\tau\rho_2\tau = \rho_1$, $\tau\rho_3\tau = \rho_3$,

$$\tau\sigma\tau=\rho_3\sigma^{-1}\tau\sigma=\sigma\tau\sigma^{-1}\rho_3.$$

(ii) *For any* $g\in G$, g *is represented in the following form*

$g=\rho_1^a\rho_2^b\rho_3^c\tau^d\sigma^{e_1}(\tau\sigma\tau)^{f_1}\sigma^{e_2}(\tau\sigma\tau)^{f_2}\cdots\sigma^{e_n}(\tau\sigma\tau)^{f_n}$, *where* $a, b, c, d=0$ *or* 1 *and all* $e_1, f_1, \ldots, e_n, f_n\geqq 0$ *or all* $e_1, f_1, \ldots, e_n, f_n\leqq 0$.

Proof of (i). $\tau\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}y\\x\\z\end{pmatrix}$ and $\sigma\tau\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}y\\xy+z\\x(y^2-1)+yz\end{pmatrix}$. Hence we have $\tau\sigma\tau\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}xy+z\\y\\x(y^2-1)+yz\end{pmatrix}$. On the other hand, we have $\sigma\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}x\\xy+z\\(x^2-1)y+xz\end{pmatrix}$ and $\tau\sigma\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}xy+z\\x\\(x^2-1)y+xz\end{pmatrix}$. Hence $\sigma^{-1}\tau\sigma\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}1&0&0\\0&xy+z&-1\\0&-(xy+z)^2+1&xy+z\end{pmatrix}\begin{pmatrix}xy+z\\x\\(x^2-1)y+xz\end{pmatrix}=\begin{pmatrix}xy+z\\y\\-x(y^2-1)-yz\end{pmatrix}$.
Therefore we have $\rho_3\sigma^{-1}\tau\sigma=\tau\sigma\tau$. In the same way as above, one can easily show the other relations.

Proof of (ii). From the relations (i), we have the following relations

$$\begin{aligned}
&\sigma\rho_1=\rho_1\rho_2\rho_3\sigma^{-1} && (\sigma^{-1}\rho_1=\rho_1\rho_2\rho_3\sigma),\\
&\sigma\rho_2=\rho_2\sigma^{-1} && (\sigma^{-1}\rho_2=\rho_2\sigma),\\
&\sigma\rho_3=\rho_3\sigma^{-1} && (\sigma^{-1}\rho_3=\rho_3\sigma),\\
&\sigma\tau=\tau(\tau\sigma\tau) && (\sigma^{-1}\tau=\tau(\tau\sigma\tau)^{-1}),\\
&(\tau\sigma\tau)\rho_1=\rho_1(\tau\sigma\tau)^{-1} && ((\tau\sigma\tau)^{-1}\rho_1=\rho_1(\tau\sigma\tau)),\\
&(\tau\sigma\tau)\rho_2=\rho_1\rho_2\rho_3(\tau\sigma\tau)^{-1} && ((\tau\sigma\tau)^{-1}\rho_2=\rho_1\rho_2\rho_3(\tau\sigma\tau)),\\
&(\tau\sigma\tau)\rho_3=\rho_3(\tau\sigma\tau)^{-1} && ((\tau\sigma\tau)^{-1}\rho_3=\rho_3(\tau\sigma\tau)),\\
&(\tau\sigma\tau)\tau=\tau\sigma && ((\tau\sigma\tau)^{-1}\tau=\tau\sigma^{-1}).
\end{aligned}$$

Moreover we have $\sigma^{-1}(\tau\sigma\tau)=\rho_3\tau\sigma$, $\sigma(\tau\sigma\tau)^{-1}=\rho_3\tau\sigma^{-1}$, $(\tau\sigma\tau)^{-1}\sigma=\rho_3\tau(\tau\sigma\tau)$, $(\tau\sigma\tau)\sigma^{-1}=\rho_3\tau(\tau\sigma\tau)^{-1}$. Combining these, one can easily show that any element $g\in G$ is represented in the following form

$\rho_1^a\rho_2^b\rho_3^c\tau^d\sigma^{e_1}(\tau\sigma\tau)^{f_1}\cdots\sigma^{e_n}(\tau\sigma\tau)^{f_n}$ for some n, where all $e_1, f_1, \ldots, f_n\geqq 0$ or $e_1, f_1, \ldots, f_n\leqq 0$.

Lemma 3. *Any element* $g\in G$ *is expressed in the following forms.*

(i) $g = \rho_1^a \rho_2^b \rho_3^c \tau^d \sigma^{e_1}(\tau\sigma\tau)^{f_1} \cdots \sigma^{e_n}(\tau\sigma\tau)^{f_n}\eta$, *for some* n,

where $a, b, c, d = 0$ or 1 *and* $e_1, f_1, \ldots, f_n \geqq 0$ *and* $\eta = 1$ *or* ρ_3.

(ii) $g = \rho_1^a \rho_2^b \rho_3^c \tau^d \sigma^{e_1}(\tau\sigma\tau)^{f_1} \cdots \sigma^{e_n}(\tau\sigma\tau)^{f_n}\xi$, *for some* n,

where $a, b, c, d = 0$ or 1 *and* $e_1, f_1, \ldots, f_n \geqq 0$ *and* $\xi = 1$ or $\rho_2\sigma^{-1}$ or $\rho_1\tau\sigma^{-1}\tau$.

Proof. First we shall show the fact (i). From Lemma 2 (i), we note here that $\rho_3\tau\rho_3 = \tau$ and $\rho_3\sigma^{-1}\rho_3 = \sigma$. Using Lemma 2 (ii), we can express any g in the form (i).
On the other hand, we have $\sigma\rho_3 = \rho_3\sigma^{-1} = \rho_2\rho_3(\rho_2\sigma^{-1})$ and $(\tau\sigma\tau)\rho_3 = (\rho_1\rho_3)(\rho_1\tau\sigma^{-1}\tau)$. Moreover we have $\sigma(\rho_2\rho_3) = (\rho_2\rho_3)\sigma$, $\sigma(\rho_1\rho_3) = (\rho_1\rho_2)\sigma$, $\sigma(\rho_1\rho_2) = (\rho_1\rho_3)\sigma$, and $\tau(\rho_2\rho_3) = (\rho_1\rho_3)\tau$, $\tau(\rho_1\rho_3) = (\rho_2\rho_3)\tau$, $\tau(\rho_1\rho_2) = (\rho_1\rho_2)\tau$. Now, from the result of (i), one can easily show the fact (ii).

For a while, we shall restrict ourselves to the case $a \geqq 1$. C_n denotes the curve which is the intersection of the surface F_a and a plane $x = n$. The curves C_n varies in the following way.

(i) In the case $n > \sqrt{a+1}$, C_n is a hyperbola

$$(y/\alpha_1)^2 - (z/\alpha_2)^2 = 1,$$

where $\alpha_1 = \sqrt{(n^2 - a - 1)/(n^2 - 1)}$ and $\alpha_2 = \sqrt{n^2 - a - 1}$.

(ii) In the case $n = \sqrt{a+1}$, C_n degenerates to two lines $z = \pm\sqrt{a}\,y$.

(iii) In the case $1 < n < \sqrt{a+1}$, C_n is a hyperbola

$$(y/\beta_1)^2 - (z/\beta_2)^2 = -1,$$

where $\beta_1 = \sqrt{(a + 1 - n^2)/(n^2 - 1)}$, $\beta_2 = \sqrt{a + 1 - n^2}$.

(iv) In the case $n = 1$, C_n degenerates to two lines $z = \pm\sqrt{a}$.

(v) In the case $0 \leqq n < 1$, C_n is an ellipse

$$(y/\gamma_1)^2 + (z/\gamma_2)^2 = 1,$$

where $\gamma_1 = \sqrt{(a + 1 - n^2)/(1 - n^2)}$, $\gamma_2 = \sqrt{a + 1 - n^2}$.

We note here the mapping $\sigma\begin{pmatrix} n \\ y \\ z \end{pmatrix} = \begin{pmatrix} n \\ y' \\ z' \end{pmatrix}$ induces a bijection of the points on C_n. In the case (i), one sees that for any $P \in C_n$, there exists only one point $P_0 = \begin{pmatrix} n \\ y_0 \\ z_0 \end{pmatrix} \in C_n$ such that $-\sqrt{(n^2 - a - 1)/2(n-1)} < y_0 \leqq \sqrt{(n^2 - a - 1)/2(n-1)}$ and $\sigma^i P_0 = P$ for some $i \in \mathbf{Z}$. In the case (ii), one sees that for any $P \in C_n$ and $\varepsilon > 0$, there exists a point $P_0 = \begin{pmatrix} n \\ y_0 \\ z_0 \end{pmatrix} \in C_n$ such that $-\varepsilon \leqq y_0 \leqq \varepsilon$ and $\sigma^i P_0 = P$ for some $i \in \mathbf{Z}$.

In the cases (iii), (iv) and (v), one sees for any $P\in C_n$, there exists only one point $P_0=\begin{pmatrix}n\\ y_0\\ z_0\end{pmatrix}\in C_n$ such that $-\sqrt{(a+1-n^2)/2(n+1)}<y_0\leqq\sqrt{(a+1-n^2)/2(n+1)}$ and $\sigma^iP_0=P$ for some $i\in\mathbf{Z}$. We note here that the action $\sigma\begin{pmatrix}n\\ y\\ z\end{pmatrix}=\begin{pmatrix}n\\ y'\\ z'\end{pmatrix}$ induces $z'\geqq z$ for any $y>0$ for the case (i). Similary, one can verify the action σ induces a permutation of the points C_n. Let H be the permutation group $\langle\sigma,\rho_1,\rho_2,\rho_3\rangle$. We denote the set $\{\begin{pmatrix}x\\ y\\ z\end{pmatrix}\in F_a|0\leqq x<\sqrt{a+1},\ 0\leqq y\leqq\sqrt{(a+1-x^2)/2(x+1)},\ 0\leqq z\}$ $\cup\{\begin{pmatrix}\sqrt{a+1}\\ y\\ z\end{pmatrix}\in F_a|0\leqq y<\varepsilon,\ 0\leqq z\}\cup\{\begin{pmatrix}x\\ y\\ z\end{pmatrix}\in F_a|\sqrt{a+1}<x,\ \sqrt{(x^2-a-1)/(x^2-1)}$ $\leqq y\leqq\sqrt{(x^2-a-1)/2(x-1)},\ 0\leqq z\}$ by $E_a(\varepsilon)$. Then, from the action of σ on C_n, one can easily show for any $P=\begin{pmatrix}x\\ y\\ z\end{pmatrix}\in F_a$ and $\varepsilon>0$, there exists a point $P_0=\begin{pmatrix}x_0\\ y_0\\ z_0\end{pmatrix}\in E_a(\varepsilon)$ such that $hP_0=P$ for some $h\in H$.

Lemma 4. *With the notation as above, we have* $HE_a(\varepsilon)=F_a$. *Here* $HE_a(\varepsilon)$ *denotes the set consisting of all the points* hP, *where* $h\in H$ *and* $P\in E_a(\varepsilon)$.

From the action of σ, $\rho_i(1\leqq i\leqq 3)$, it is easy to verify the following lemma.

Lemma 5. *Let* $P=\begin{pmatrix}x\\ y\\ z\end{pmatrix}$ $Q=\begin{pmatrix}x'\\ y'\\ z'\end{pmatrix}$ *be points of* $E_a(\varepsilon)$ *such that* $x\neq\sqrt{a+1}$, $x'\neq\sqrt{a+1}$. *If* $hP=Q$ *for some* $h\in H$, *then we have* $P=Q$.

R_a denote the set $\{\begin{pmatrix}x\\ y\\ z\end{pmatrix}\in F_a|0\leqq x\leqq y\leqq\sqrt{(a+1-x^2)/2(x+1)},\ 0\leqq z\}$. From the fact that $x\geqq\sqrt{(x^2-a-1)/2(x-1)}$ when $x\geqq\sqrt{a+1}$ and Lemma 3, we have $GR_a=F_a$. R_a^* denotes the set $R_a\cap S_a$. Then we have $GR_a^*=S_a$ in the same way. We denote the number of integer points $\#[R_a^*]$ by r_a. Then we have the following proposition.

Proposition 1. *With the notation as above, we have*

$$GR_a^*=S_a \text{ and } 0\leqq t_a=\#[S_a/G]\leqq r_a=\#[R_a^*] \text{ when } a\geqq 1.$$

In the case $a \leqq -2$, we denote the set $\{\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in F_a \mid 1 < x \leqq y, \sqrt{(x^2-a-1)/(x^2-1)} \leqq y \leqq \sqrt{(x^2-a-1)/2(x-1)}, 0 \leqq z\}$ by R_a and $R_a \cap S_a$ by R_a^*. In the same way as above, we get the following proposition.

Proposition 2. *For the case $a \leqq -1$, we have $GR_a^* = S_a$ and $0 \leqq t_a = \#[S_a/G] \leqq r_a = \#[R_a^*]$.*

Remark. In the case $a = -1$, we have $t_{-1} = r_{-1} = 1$ and $S_{-1} = \{\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}\}$.

In the case $a = 0$, we denote the set $\{\begin{pmatrix} 1 \\ n \\ 0 \end{pmatrix} \mid 0 \leqq n, n \in \mathbf{Z}\}$ by R_0^*. Then, in the same way as above, we have $R_0^* \subset S_0$ and $GR_0^* = S_0$. We shall show that any $\begin{pmatrix} 1 \\ n \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ m \\ 0 \end{pmatrix} \in R_0^*$ are G-independent when $n \neq m$. Without loss of generality, we may assume $m < n$. First we treat the case $m = 0$. If $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \sim \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, we have $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \equiv \begin{pmatrix} \pm 1 \\ 0 \\ 0 \end{pmatrix}$ or $\begin{pmatrix} 0 \\ \pm 1 \\ 0 \end{pmatrix}$ or $\begin{pmatrix} 0 \\ 0 \\ \pm 1 \end{pmatrix}$ (mod l) for any positive integer l. Hence $\begin{pmatrix} 1 \\ n \\ 0 \end{pmatrix} \sim \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ implies $\begin{pmatrix} 1 \\ n \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ (mod l) for any positive integer l, which contradicts the assumption $n > 0$. Hence $\begin{pmatrix} 1 \\ n \\ 0 \end{pmatrix} \sim \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. If $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \sim \begin{pmatrix} 1 \\ n \\ 0 \end{pmatrix}$, then we have $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \equiv \begin{pmatrix} \pm 1 \\ 0 \\ 0 \end{pmatrix}$ or $\begin{pmatrix} 0 \\ \pm 1 \\ 0 \end{pmatrix}$ or $\begin{pmatrix} 0 \\ 0 \\ \pm 1 \end{pmatrix}$ mod n. Hence $\begin{pmatrix} 1 \\ m \\ 0 \end{pmatrix} \sim \begin{pmatrix} 1 \\ n \\ 0 \end{pmatrix}$ implies $\begin{pmatrix} 1 \\ m \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ n \\ 0 \end{pmatrix}$ mod n. Hence $n \mid m$, which contradicts the assumption $0 < m < n$. Hence $\begin{pmatrix} 1 \\ n \\ 0 \end{pmatrix} \sim \begin{pmatrix} 1 \\ m \\ 0 \end{pmatrix}$.

Proposition 3. *With the notation as above, we have the following orbit decomposition*

$S_0 = \Sigma O(P)$, *where P runs all the elements of R_0^*.*

Remark 1. One can replace the set of representatives R_0^* by $\left\{\begin{pmatrix} n \\ n \\ n^2 - 1 \end{pmatrix} | 0 \leqq n,\ n \in \mathbf{Z}\right\}$.

Remark 2. The methods of the following §2 shall give another proof of Proposition 3.

§2. Proof of Main Theorem

In this section, we shall show $t_a = r_a$ for $a \geqq 1$ and $a \leqq -2$. First we shall consider the case $a \geqq 1$. We denote the set $\left\{\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in S_a | 0 \leqq x,\ 0 \leqq y,\ x^2 + y^2 \leqq a + 1\right\}$ by T_a. R_a^* denotes the set $S_a \cap R_a$. Since $\sqrt{(a + 1 - x^2)/(2x + 2)} \leqq \sqrt{a + 1 - x^2}$ for any $x \geqq 0$, we have $R_a^* \cup \tau R_a^* \subset T_a$.

Lemma 6. *Let* $P = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ *be a point of* S_a *such that* $x, y, z > 0$. *We denote the points* $\sigma P = \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$, $\tau\sigma\tau P = \begin{pmatrix} x'' \\ y'' \\ z'' \end{pmatrix}$ *by* P', P''. *Then* $P', P'' \notin R_a^* \cup \tau R_a^*$ *and* $x', y', z', x'', y'', z'' > 0$.

Proof. It is obvious that $x', y', z', x'', y'', z'' > 0$. On the other hand, we have $(x')^2 + (y')^2 = x^2 + (xy + z)^2 = x^2(y^2 + 1)(x^2 - 1)(y^2 - 1) + 2xyz + a > a + 1$. Hence $P' \notin T_a$. Similarly we have $P'' \notin T_a$. Hence $P', P'' \notin R_a^* \cup \tau R_a^*$.

Proposition 4. *Let* a *be an integer* $a \geqq 1$. *If* $P \sim Q$, *where* $P, Q \in R_a^*$, *then* $P = Q$.

Proof. From Lemma 3 (ii), there exists an element $g \in G$ such that $Q = gP$ and $g = \rho_1^a \rho_2^b \rho_3^c \tau^d \sigma^{e_1} \cdots (\tau\sigma\tau)^{f_n} \xi$. Here $a, b, c, d = 0$ or 1 and $e_1, \ldots, f_n \geqq 0$ and $\xi = 1$ or $\rho_2\sigma^{-1}$ or $\rho_1\tau\sigma^{-1}\tau$. We put $P = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$, $P' = \xi P = \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$ and $Q = \begin{pmatrix} x'' \\ y'' \\ z'' \end{pmatrix}$. First, we treat the case $x > 0$. Then the assumption $x > 0$ and $P \in R_a^*$ implies $x', y', z' > 0$ for any ξ. Therefore, from Lemma 6, we have $e_1 = \cdots = f_n = 0$. Hence $Q = \rho_1^a \rho_2^b \rho_3^c \tau^d P'$. Since $x'', y'', z'' \geqq 0$ and $x', y' z' > 0$, we have $a = b = c = 0$. If $\xi = \rho_2\sigma^{-1}$, $(\rho_2\sigma^{-1})P = \begin{pmatrix} x \\ z - xy \\ xz + (1 - x^2)y \end{pmatrix}$ and the assumption

$P \in R_a^*$ implies $z - xy > x > 0$. Hence $y' \geqq x' > 0$ for $\xi = 1$ or $\rho_2\sigma^{-1}$. Hence $d = 0$ and $\xi P = Q$. If $\xi = \rho_2\sigma^{-1}$, the relation $\xi P = Q$ contradicts.

Lemma 5. Hence $\xi \neq \rho_2\sigma^{-1}$. If $\xi = \rho_1\tau\sigma^{-1}\tau$, we can substitute x for y and σ for $\tau\sigma\tau$ and ρ_2 for ρ_1, then this case reduces to the case $\xi = \rho_2\sigma^{-1}$. Therefore $\xi = 1$ and $P = Q$.

We now consider the case $x = 0$. From the case $x > 0$, we can restrict ourselves to the case $P = \begin{pmatrix} 0 \\ y \\ z \end{pmatrix}$, $Q = \begin{pmatrix} 0 \\ y'' \\ z'' \end{pmatrix}$ and $Q = gP$. Without loss of generality, we may assume $y, z > 0$. From Lemma 3 (i), $g = \rho_1^a \rho_2^b \rho_3^c \tau^d \sigma^{e_1} \cdots (\tau\sigma\tau)^{f_n}\eta$, where $\eta = 1$ or ρ_3. First, we consider the case $\eta = 1$. Then we have

$$P_0 = P = \begin{pmatrix} 0 \\ y \\ z \end{pmatrix} \xrightarrow{\sigma} P_1 = \begin{pmatrix} 0 \\ z \\ -y \end{pmatrix} \xrightarrow{\sigma} P_2 = \begin{pmatrix} 0 \\ -y \\ -z \end{pmatrix} \xrightarrow{\sigma} P_3 = \begin{pmatrix} 0 \\ -z \\ y \end{pmatrix} \xrightarrow{\sigma} P.$$

We put $\tau\sigma\tau P_0 = \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix}$ and $\rho_1\rho_3\tau\sigma\tau P_1 = \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix}$ and $\rho_1\rho_2\tau\sigma\tau P_2 = \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix}$ and $\rho_2\rho_3\tau\sigma\tau P_3 = \begin{pmatrix} x_3 \\ y_3 \\ z_3 \end{pmatrix}$. Then it is easily verified all the integers $x_1, y_1, \ldots, y_3, z_3$ are positive. From Lemma 2 (i), we have $\sigma(\rho_2\rho_3) = (\rho_2\rho_3)\sigma$, $\sigma(\rho_1\rho_3) = (\rho_1\rho_2)\sigma$, $\sigma(\rho_1\rho_2) = (\rho_1\rho_3)\sigma$, and $\tau(\rho_2\rho_3) = (\rho_1\rho_3)\tau$, $\tau(\rho_1\rho_3) = (\rho_2\rho_3)\tau$, $\tau(\rho_1\rho_2) = (\rho_1\rho_2)\tau$. Hence, from Lemma 5, we have $f_1, \ldots, f_n = 0$. Then $Q = \rho_1^a \rho_2^b \rho_3^c \tau^d P_i (0 \leqq i \leqq 3)$. Hence we have $P = Q$.

Finally, we consider the case $\eta = \rho_3$. Then we have

$$P_0 = \rho_3 P = \begin{pmatrix} 0 \\ y \\ -z \end{pmatrix} \xrightarrow{\sigma} P_1 = \begin{pmatrix} 0 \\ -z \\ -y \end{pmatrix} \xrightarrow{\sigma} P_2 = \begin{pmatrix} 0 \\ -y \\ z \end{pmatrix} \xrightarrow{\sigma} P_3 = \begin{pmatrix} 0 \\ z \\ y \end{pmatrix} \xrightarrow{\sigma} P_0.$$

In the same way as the above case $\eta = 1$, we have $P = Q$.

Next, we shall show the case $a \leqq -2$. R_a^* denotes the set $\left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in S_a \mid 1 < x \leqq y, \sqrt{(x^2 - a - 1)/(x^2 - 1)} \leqq y \leqq \sqrt{(x^2 - a - 1)/2(x - 1)}, 0 \leqq z \right\}$. In the same way as the case $a \geqq 1$, we have the following lemma.

Lemma 7. *Let* $P = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ *be a point of* S_a *such that* $x, y, z > 0$. *We denote the points* $\sigma P = \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$, $\tau\sigma\tau P = \begin{pmatrix} x'' \\ y'' \\ z'' \end{pmatrix}$ *by* P', P''. *Then* $P', P'' \notin R_a^* \cup \tau R_a^*$ *and* $x', y', z', x'',$

$y'', z'' > 0$.

Proposition 5. *Let a be an integer $a \leqq -2$. If $P \sim Q$, where $P, Q \in R_a^*$, then we have $P = Q$.*

Proof. From Lemma 3 (i), we have $Q = gP$ and $g = \rho_1^a \rho_2^b \rho_3^c \tau^d \sigma^{e_1} \cdots (\tau\sigma\tau)^{f_n} \eta$, where $\eta = 1$ or ρ_3. If $\eta = 1$, using Lemma 7, we have $e_1 = \cdots = f_n = 0$. Hence $Q = \rho_1^a \rho_2^b \rho_3^c \tau^d P$. Hence we have $P = Q$.

If $\eta = \rho_3$, we put $P_1 = \sigma\rho_3 P = \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix}$ and $P_2 = \tau\sigma\tau\rho_3 P = \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix}$. Then we have $x_1, y_1, z_1, x_2, y_2, z_2 > 0$ and $P_1, P_2 \notin R_a^* \cup \tau R_a^*$. Therefore $e_1 = \cdots = f_n = 0$. Hence $Q = \rho_1^a \rho_2^b \rho_3^c \tau^d P$. Hence we have $P = Q$. Summarizing Proposition 2, 3, 4, 5, we have obtained the following theorem.

Theorem. *With the notation as above, we have the following orbit decomposition for any $a \in \boldsymbol{Z}$*

$R_a = \Sigma O(P)$, where P runs all the elements of R_a^*. The number of the representatives $\#[R_a^*] = \#[S_a/G] = t_a$ is finite except the case $a = 0$.

Table of G-independent solutions $-150 \leqq a \leqq 150$

a	solutions
−144	(2, 7, 0) (4, 4, 9)
−143	(2, 7, 1) (3, 5, 7)
−140	(2, 7, 2) (2, 8, 7)
−136	(3, 6, 12)
−135	(2, 7, 3) (4, 5, 15)
−128	(2, 7, 4) (3, 5, 8)
−125	(2, 8, 8) (4, 4, 10)
−120	(3, 4, 0)
−119	(2, 7, 5) (3, 4, 1)
−116	(3, 4, 2)
−111	(3, 4, 3) (3, 5, 9)
−108	(2, 7, 6)
−105	(2, 6, 0)
−104	(2, 6, 1) (3, 4, 4) (4, 4, 11)
−101	(2, 6, 2)
−96	(2, 6, 3)
−95	(2, 7, 7) (3, 4, 5)
−92	(3, 5, 10)
−89	(2, 6, 4)
−84	(3, 4, 6)
−81	(4, 4, 12)
−80	(2, 6, 5)
−72	(2, 5, 0)
−71	(2, 5, 1) (3, 4, 7)
−69	(2, 6, 6)
−68	(2, 5, 2)
−64	(3, 3, 0)
−63	(2, 5, 3) (3, 3, 1)
−60	(3, 3, 2)
−56	(2, 5, 4) (3, 4, 8)
−55	(3, 3, 3)
−48	(3, 3, 4)
−47	(2, 5, 5)
−45	(2, 4, 0)
−44	(2, 4, 1)
−41	(2, 4, 2)
−39	(3, 3, 5)
−36	(2, 4, 3)
−29	(2, 4, 4)
−28	(3, 3, 6)
−24	(2, 3, 0)
−23	(2, 3, 1)
−20	(2, 3, 2)
−15	(2, 3, 3)
−9	(2, 2, 0)
−8	(2, 2, 1)
−5	(2, 2, 2)
−1	(0, 0, 0)
0	(1, n, 0) $n \geqq 0$
1	(0, 1, 1)
3	(0, 0, 2)
4	(0, 1, 2) (1, 1, 2)
7	(0, 2, 2)
8	(0, 0, 3)
9	(0, 1, 3) (1, 1, 3)
12	(0, 2, 3)
15	(0, 0, 4)
16	(0, 1, 4) (1, 1, 4) (1, 2, 4)
17	(0, 3, 3)
19	(0, 2, 4)
24	(0, 0, 5) (0, 3, 4)
25	(0, 1, 5) (1, 1, 5) (1, 2, 5)
27	(2, 2, 6)
28	(0, 2, 5)
31	(0, 4, 4)
33	(0, 3, 5)
35	(0, 0, 6)
36	(0, 1, 6) (1, 1, 6) (1, 2, 6) (1, 3, 6)
39	(0, 2, 6)
40	(0, 4, 5) (2, 2, 7)
44	(0, 3, 6)
48	(0, 0, 7)
49	(0, 1, 7) (0, 5, 5) (1, 1, 7) (1, 2, 7) (1, 3, 7)
51	(9, 4, 6)
52	(0, 2, 7)
55	(2, 2, 8)
57	(0, 3, 7) (2, 3, 9)
60	(0, 5, 6)
63	(0, 0, 8)
64	(0, 1, 8) (0, 4, 7) (1, 1, 8) (1, 2, 8) (1, 3, 8) (1, 4, 8)
67	(0, 2, 8)
71	(0, 6, 6)
72	(0, 3, 8) (2, 2, 9)
73	(0, 5, 7)
76	(2, 3, 10)
79	(0, 4, 8)
80	(0, 0, 9) (3, 3, 12)
81	(0, 1, 9) (1, 1, 9) (1, 2, 9) (1, 3, 9) (1, 4, 9)
84	(0, 2, 9) (0, 6, 7)
88	(0, 5, 8)
89	(0, 3, 9)
91	(2, 2, 10)
96	(0, 4, 9)
97	(0, 7, 7) (2, 3, 11)
99	(0, 0, 10) (0, 6, 8) (2, 4, 12)
100	(0, 1, 10) (1, 1, 10) (1, 2, 10) (1, 3, 10) (1, 4, 10) (1, 5, 10)
103	(0, 2, 10)
105	(0, 5, 9) (3, 3, 13)
108	(0, 3, 10)
112	(0, 7, 8) (2, 2, 11)
115	(0, 4, 10)
116	(0, 6, 9)
120	(0, 0, 11) (2, 3, 12)
121	(0, 1, 11) (1, 1, 11) (1, 2, 11) (1, 3, 11) (1, 4, 11) (1, 5, 11)
124	(0, 2, 11) (0, 5, 10) (2, 4, 13)
127	(0, 8, 8)
129	(0, 3, 11) (0, 7, 9)
132	(3, 3, 14)
135	(0, 6, 10) (2, 2, 12)
136	(0, 4, 11) (3, 4, 16)
143	(0, 0, 12)
144	(0, 1, 12) (0, 8, 9) (1, 1, 12) (1, 2, 12) (1, 3, 12) (1, 4, 12) (1, 5, 12) (1, 6, 12)
145	(0, 5, 11) (2, 3, 13)
147	(0, 2, 12)
148	(0, 7, 10)

Remark. This diophantine equation for the special case $a = 1$ is first posed by Mr. T. Fushimi, who is a student of us. In [**1**], the second author considered this special case.

Department of Mathematics,
College of General Education,
Tokushima University
and
Department of Mathematics,
Anan College of Technology

References

[1] K. Kashihara, The diophantine equation $x^2 - 1 = (y^2 - 1)(z^2 - 1)$, Mem. Anan College Tech., **26** (1990), 119–130 (in Japanese).
[2] Y. Kida, UBASIC 86, Nihonhyoronsha, Tokyo, 1989.
[3] L. J. Mordell, Diophantine Equations, Academic Press, London and New York, 1969.
[4] T. Takagi, Elementary Theory of Numbers, Kyoritsu, Tokyo, 1971.