manuscripta math. 80, 373 - 392 (1993)

manuscripta mathematica
© Springer-Verlag 1993

Explicit complete solution in integers of a class of equations $(ax^2 - b)(ay^2 - b) = z^2 - c$

Kenji Kashihara

Dedicated to Dr. Taro Morishima

In this paper we will study the equation for arbitrary integers $a \neq 0$, c and $b = \pm 1$, ± 2 or ± 4. When $b = \pm 4$, we suppose c is divisible by 4. The paper will provide one with a method for finding algorithmically all integral non-trivial solutions of the title equations, where an explicit unit of $\mathbb{Q}(\sqrt{a^2n^2 - ab})$ plays an important role.

Introduction

In [2], *L.J.Mordell* commented on the quartic equation given by

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

where a's and d are integers. His comment is that when one integer solution $(x_0,\ y_0,\ z_0)$ of (1) is known, an infinity can be found under certain conditions, and that this leads to solutions $(x_0,\ y_1,\ z_1)$, $(x_1,\ y_1,\ z_2)$, $(x_1,\ y_2,\ z_3)$, $(x_2,\ y_2,\ z_4)$, etc. ..., where from a Pellian equation, $y_1,\ x_1,\ y_2,\ x_2,\ \ldots$ may each have an infinity of values.

We will further consider this fact for the following special type :

$$(ax^2 - b)(ay^2 - b) = z^2 - c, \tag{2}$$

where $a, c \in \mathbb{Z}$, $a \neq 0$, $b = \pm 1, \pm 2, \pm 4$. When $b = \pm 4$, we suppose $c \equiv 0\ (mod\ 4)$. In [3], we have investigated the equation for the case $a = 1$ and $b = 1$. In this paper, we will show that this equation can be dealt with generally in the same method.

If we fix $x = n$, equation (2) is written as

$$z^2 - (a^2n^2 - ab)y^2 = -abn^2 + b^2 + c. \tag{3}$$

We can solve equation (3) by the theory of binary quadratic forms as presented in [4] or [5]. We will show a permutation group on all integral solutions of equation (2), which will be denoted by G. And we will prove the possibility of computing algorithmically a minimal finite set of integral solutions of the title equation, such that the G-orbits of this set exhaust all integral solutions.

Here we introduce the notion of *the trivial solution.* When $(ax^2-b)(ay^2-b)(-abx^2+b^2+c)(-aby^2+b^2+c)=0$, the solution can be trivially computed. If $c=0$, then $\left(x,\ \pm x,\ \pm(ax^2-b)\right)$ are trivially integral solutions. Thus *a trivial solution* is defined as an integral solution such that

$$(ax^2-b)(ay^2-b)(-abx^2+b^2+c)(-aby^2+b^2+c)=0,$$

or (only if $c=0$) $x^2=y^2$.

The cases $b=1$, 2 or 4, will be discussed in detail and for the other cases we will state the results and give only the proofs different from the previous ones. Up to the end of section 3 we suppose $b=1$, 2, or 4. Since $(-ax^2-b)(-ay^2-b)=z^2-c$ is equivalent to $(ax^2+b)(ay^2+b)=z^2-c$, we may suppose $a>0$.

Notations.

F^b_{ac} : the set of all real solutions of equation (2).

S^b_{ac} : the set of all integral solutions of equation (2).

C_n : intersection of F^b_{ac} and the plane $x=n$.

T^b_{ac} : the set of all trivial solutions of equation (2).

C_n^{+y}, C_n^{+z} and C_n^{+} are the following branches of C_n:

$$\begin{aligned} C_n^{+y} &:= \{(x,\ y,\ z)\in C_n \mid y\ \geq\ 0\}, \\ C_n^{+z} &:= \{(x,\ y,\ z)\in C_n \mid z\ \geq\ 0\}, \\ C_n^{+} &:= \{(x,\ y,\ z)\in C_n \mid y\ \geq\ 0,\ z\ \geq\ 0\}. \end{aligned}$$

σ, τ, ρ_1, ρ_2 and ρ_3 are the following permutations on F^b_{ac} or S^b_{ac}:

$$\begin{aligned} \sigma(x,\ y,\ z) &:= \left(x,\ \frac{(2ax^2-b)y+2xz}{b},\ \frac{2x(a^2x^2-ab)y+(2ax^2-b)z}{b}\right), \\ \tau(x,\ y,\ z) &:= (y,\ x,\ z), \\ \rho_1(x,\ y,\ z) &:= (-x,\ y,\ z), \\ \rho_2(x,\ y,\ z) &:= (x,\ -y,\ z), \\ \rho_3(x,\ y,\ z) &:= (x,\ y,\ -z). \end{aligned}$$

G is the following permutation group and G_1, G_2, H and H_1 are the following subgroups of G:

$$\begin{aligned} G\ &:=<\sigma,\ \tau,\ \rho_1,\ \rho_2,\ \rho_3>, \\ G_1 &:=<\sigma,\ \rho_1,\ \rho_2,\ \rho_3>, \\ G_2 &:=<\sigma>, \\ H\ &:=<\tau,\ \rho_1,\ \rho_2,\ \rho_3>, \\ H_1 &:=<\rho_1,\ \rho_2,\ \rho_3>. \end{aligned}$$

Let P and Q be points on F^b_{ac} (or S^b_{ac}). If $Q = gP$ for some $g \in G$, then P and Q are called G-equivalent, otherwise G-independent. These relations are denoted by $P \sim Q$ and $P \not\sim Q$, respectively.

The following function is used:

$$\varphi(x, y, z) := x^2 + y^2.$$

1. The structure of G

As already noted, we assume $b = 1, 2$ or 4. If we fix $x = n (\geq 0)$, equation (2) is written as

$$z^2 - (a^2n^2 - ab)y^2 = -abn^2 + b^2 + c. \tag{3}$$

or equivalently

$$N\left(z + y\sqrt{a^2n^2 - ab}\right) = -abn^2 + b^2 + c, \tag{4}$$

where N denotes the norm from $\mathbb{Q}(\sqrt{a^2n^2 - ab})$ to $\mathbb{Q}$. Here we put

$$\varepsilon_n = \frac{2an^2 - b + 2n\sqrt{a^2n^2 - ab}}{b}.$$

Since $|b| \in \{1,\ 2,\ 4\}$, it is straightforward to check that ε_n is a unit in the ring of integers of the above quadratic field with norm equal to $+1$; moreover, it is useful to note that $\varepsilon_n^{-1} = \varepsilon_{-n}$. Let $(y_0,\ z_0)$ be one of the solutions of (4). Then

$$N\left\{\left(z_0 + y_0\sqrt{a^2n^2 - ab}\right)\varepsilon_n\right\} = -abn^2 + b^2 + c.$$

Therefore putting

$$z_1 + y_1\sqrt{a^2n^2 - ab} = \left(z_0 + y_0\sqrt{a^2n^2 - ab}\right)\varepsilon_n,$$

we have a new solution $(y_1,\ z_1)$. From this fact, if we define σ as above, σ is a permutation on C_n, and we may replace C_n with F^b_{ac} or S^b_{ac}. In the cases $b = 1$ or 2, ε_n lies in the coefficient ring of the $\mathbb{Z}$-*module* $\{1,\ \sqrt{a^2n^2 - ab}\}$. Consider the case $b = 4$. Let $(x,\ y,\ z)$ lies in S^4_{ac}, and put $(x,\ \eta,\ \zeta) = \sigma(x,\ y,\ z)$. Then from (3) and $c \equiv 0\ (mod\ 4)$,

$$(z + axy)(z - axy) = -4ay^2 - 4ax^2 + 16 + c \equiv 0 \quad (mod\ 4).$$

And so $z + axy \equiv z - axy \equiv 0\ (mod\ 2)$. Hence

$$\eta = \frac{2x(axy + z) - 4y}{4} \in \mathbb{Z}, \qquad \zeta = \frac{2ax^2(axy + z) - 8axy - 4z}{4} \in \mathbb{Z}.$$

Therefore $(x,\ \eta,\ \zeta) \in S^4_{ac}$, and so σ is a permutation on S^4_{ac}. From the symmetries of equation (2), we can obtain the other generators of G.

Lemma 1. *G is a permutation group on F^b_{ac} or S^b_{ac}.*

By easy calculation we have the following lemma.

Lemma 2. *Permutations σ, τ, ρ_1, ρ_2, ρ_3 satisfy the following relations,*

$$\begin{array}{lll} \rho_i^2 = 1, & \rho_i\rho_j = \rho_j\rho_i, & \tau^2 = 1, \\ \tau\rho_1 = \rho_2\tau, & \tau\rho_2 = \rho_1\tau, & \tau\rho_3 = \rho_3\tau, \\ \sigma\rho_i = \rho_i\sigma^{-1}, & (\tau\sigma\tau)\rho_i = \rho_i(\tau\sigma\tau)^{-1}, & \\ \sigma\tau = \tau(\tau\sigma\tau), & \sigma^{-1}\tau = \tau(\tau\sigma\tau)^{-1}, & \end{array}$$

where $i, j = 1, 2, 3$.

Corollary 1. *Let $A = \{\sigma,\ \sigma^{-1},\ \tau\sigma\tau,\ (\tau\sigma\tau)^{-1}\}$, $H =< \tau,\ \rho_1,\ \rho_2,\ \rho_3 >$, then*

$$AH = HA.$$

Corollary 2. *Any element of G has a representation in the form,*

$$\rho_1^a\rho_2^b\rho_3^c\tau^d\sigma^{e_1}(\tau\sigma\tau)^{f_1}\cdots\sigma^{e_k}(\tau\sigma\tau)^{f_k},$$

where $a, b, c, d = 0$ or 1 and $e_i, f_i \in \mathbb{Z}$.

Proof. Let g be an arbitrary element of G. Using *Corollary 1* several times, g takes the form $h\sigma^{e_1}(\tau\sigma\tau)^{f_1}\cdots\sigma^{e_k}(\tau\sigma\tau)^{f_k}$, where $h \in H$. By the relations ρ's and τ, h takes the form $\rho_1^a\rho_2^b\rho_3^c\tau^d$. □

2. The permutation σ

We continue to assume that $b = 1, 2$ or 4. In this section, we fix $x = n(\geq 0)$ and regard σ as a permutation on C_n. Sometimes, for a point $P = (n, y, z) \in C_n$, we will simply write $P = (y, z)$. The curve C_n varies as follows. In the case $an^2 - b < 0$, $-abn^2 + b^2 + c \geq 0$, C_n is an ellipse or a single point. (See *Fig. 1.*) In the case $an^2 - b = 0$, $c \geq 0$, it degenerates to one or two lines. In the case $an^2 - b > 0$, $-abn^2 + b^2 + c > 0$, it is a hyperbola with focuses on the z axis. In the case $an^2 - b > 0$, $-abn^2 + b^2 + c = 0$, it degenerates to two lines. And finally in the case $an^2 - b > 0$, $-abn^2 + b^2 + c < 0$, it is a hyperbola with focuses on the y axis. (See *Fig. 2.*) We have the following lemma.

Lemma 3. *Let $n > 0$, except for the case* (i). *For a point P_0 on C_n, put $P_1 = \sigma P_0$, and let $\overset{\frown}{P_0P_1}$ be an arc of C_n, in which P_1 is contained and P_0 is not.*

(i) *If $n = 0$ then $\sigma = \rho_2\rho_3$.*

(ii) *If $an^2 - b < 0$ and $-abn^2 + b^2 + c > 0$, let $P_0 = (-y_0,\ z_0)$ be a point on C_n such that $\sigma P_0 = \rho_2 P_0$, $y_0 \geq 0, z_0 \geq 0$. Then*

$$C_n = \bigcup_{i=0}^{r} \sigma^i \overset{\frown}{P_0P_1},$$

where $r = 2,\ 3$ *or* 5.

(iii) *If* $an^2 - b > 0,\quad -abn^2 + b^2 + c > 0$, *let* $P_0 = (-y_0,\ z_0)$ *be a point on* C_n^{+z} *such that* $\sigma P_0 = \rho_2 P_0,\ y_0 \geq 0$. *Then*

$$C_n^{+z} = \bigcup_{i \in \mathbf{Z}} \sigma^i \overset{\frown}{P_0 P_1}.$$

(iv) *If* $an^2 - b > 0$ *and* $-abn^2 + b^2 + c < 0$, *let* $P_0 = (y_0,\ -z_0)$ *be a point on* C_n^{+y} *such that* $\sigma P_0 = \rho_3 P_0,\ z_0 \geq 0$. *Then*

$$C_n^{+y} = \bigcup_{i \in \mathbf{Z}} \sigma^i \overset{\frown}{P_0 P_1}.$$

The proof of case (i) is clear from the definition of σ.

Proof of case (ii). See *Fig. 1.* From $an^2 - b < 0$ and $n > 0$, we have $(a, b, n) = (1,2,1),\ (1,4,1), (2,4,1)$ or $(3,4,1)$. σ can be expressed by the following matrix respectively:

$$A_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ A_2 = \frac{1}{2}\begin{pmatrix} -1 & 1 \\ -3 & -1 \end{pmatrix},\ A_3 = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ -4 & 0 \end{pmatrix},\ A_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ -3 & 1 \end{pmatrix}.$$

It is obvious that $A_1^4 = I,\ A_2^3 = I,\ A_3^4 = I,\ A_4^6 = I$ and that such P_0 exists. Here we put $P_i = \sigma^i P_0$ $(i = 1, 2, \cdots, 6)$. Then it holds that $P_3 = P_0,\ P_4 = P_0$ or $P_6 = P_0$. By linearity of σ, $\overset{\frown}{P_{i+1} P_{i+2}} = \sigma \overset{\frown}{P_i P_{i+1}}$. Therefore $C_n = \bigcup_{i=0}^{r} \overset{\frown}{P_i P_{i+1}} = \bigcup_{i=0}^{r} \sigma^i \overset{\frown}{P_0 P_1}$, where $r = 2,\ 3$ or 5.

Proof of case (iii). First we note that the relation $\sigma P_0 = \rho_2 P_0$ is by the definition of σ and ρ_2, equivalent to $z_0 = nay_0$ and now it is clear that such a point P_0 exists on C_n. Next let $(y,\ z) \in C_n^{+z}$ and put $(\eta,\ \zeta) = \sigma(y,\ z)$. First we show $(\eta,\ \zeta) \in C_n^{+z}$. From the definition of σ,

$$\zeta = \frac{2n(a^2n^2 - ab)y + (2an^2 - b)z}{b}. \tag{5}$$

From (3) and the assumption $-abn^2 + b^2 + c > 0$, we have

$$z^2 - (a^2n^2 - ab)y^2 > 0. \tag{6}$$

Therefore

$$\begin{aligned} (2an^2 - b)^2 z^2 &- 4n^2(a^2n^2 - ab)^2 y^2 \\ &> (a^2n^2 - ab)(2an^2 - b)^2 y^2 - 4n^2(a^2n^2 - ab)^2 y^2 \\ &= b^2(a^2n^2 - ab)y^2 \geq 0. \end{aligned}$$

Hence

$$(2an^2 - b)z > \pm 2n(a^2n^2 - ab)y. \tag{7}$$

Combining (5) with (7), we have $\zeta > 0$. And so $(\eta,\ \zeta) \in C_n^{+z}$.

Next we show $\eta > y$. From the definition of σ, we have

$$\eta = y + \frac{2}{b}\{(an^2 - b)y + nz\}. \tag{8}$$

From (6),

$$\begin{aligned} n^2z^2 - (an^2-b)^2y^2 &> n^2(a^2n^2 - ab)y^2 - (an^2-b)^2y^2 \\ &= b(an^2-b)y^2 \geq 0, \end{aligned}$$

which implies

$$nz > \pm(an^2 - b)y. \tag{9}$$

Combining (8) with (9), we have $\eta > y$. Now we put $P_{i+1} = \sigma P_i$, $P_{i-1} = \sigma^{-1}P_i$ and $P_i = (y_i, z_i)$ for all $i \in \mathbb{Z}$. Then, by (8) and (9) $y_{i+1} \geq y_i + 2/b$ for all $i \in \mathbb{Z}$. Therefore $y_i \longrightarrow \pm\infty$ as $i \longrightarrow \pm\infty$. So we have

$$C_n^{+z} = \bigcup_{i \in \mathbf{Z}} \overset{\frown}{P_iP_{i+1}}.$$

By linearity of σ, $\overset{\frown}{P_iP_{i+1}} = \sigma \overset{\frown}{P_{i-1}P_i} = \sigma^i \overset{\frown}{P_0P_1}$. The result follows.

Case (iv) is proved similarly. □

Remark 1. Sometimes we suppose an arc $\overset{\frown}{P_0P_1}$ contains both P_0 and P_1. Then *Lemma 3* still holds.

Lemma 4. *Let $n > 0$ and let $(a, b, n) \neq (1, 4, 1)$.*

I

(i) *The case* $-abn^2 + b^2 + c > 0$: *Define*

$$E_{ac}^{bn} = \left\{ (n, y, z) \in C_n^{+z} \;\middle|\; -\sqrt{\frac{b^2+c}{ab} - n^2} < y \leq \sqrt{\frac{b^2+c}{ab} - n^2} \right\}.$$

Then $C_n = G_2E_{ac}^{bn}$ *if* $an^2 - b < 0$, *and* $C_n^{+z} = G_2E_{ac}^{bn}$ *otherwise.*

(ii) *The case* $an^2 - b > 0$ *and* $-abn^2 + b^2 + c < 0$: *Define*

$$E_{ac}^{bn} = \left\{ (n, y, z) \in C_n^{+y} \;\middle|\; \sqrt{\frac{abn^2 - b^2 - c}{a^2n^2 - ab}} \leq y \leq n\sqrt{\frac{abn^2 - b^2 - c}{abn^2 - b^2}} \right\}.$$

Then $C_n^{+y} = G_2E_{ac}^{bn}$.

II *If P is any point in E_{ac}^{bn} and σP, $\sigma^{-1}P$ do not belong to H_1P, then*

$$\varphi(\sigma P) > \varphi(P), \quad \varphi(\sigma^{-1}P) > \varphi(P),$$

respectively. Moreover, if $an^2 - b > 0$ and P is any point in E_{ac}^{bn}, while $Q = (n, y, z)$ any point not belonging to E_{ac}^{bn}, then, unless $Q \in H_1P$

$$\varphi(Q) > \varphi(P).$$

Proof of case (i). From $\sigma P_0 = \rho_2 P_0$, we see that

$$y_0 = \frac{-(2an^2 - b)y_0 + 2nz_0}{b},$$

hence $z_0 = any_0$ and now, since $P_0 \in C_n$, $n^2 + y_0^2 = (b^2 + c)/ab$. Therefore, $P_0 = (n, -y_0, z_0)$, $P_1 = \sigma P_0 = (n, y_0, z_0)$, with $y_0 = \sqrt{-n^2 + (b^2 + c)/ab}$ and if we choose the arc $\overset{\frown}{P_0P_1}$ on C_n, which lies in the half plane $z \geq 0$ then, obviously, $\overset{\frown}{P_0P_1} = E_{ac}^{bn}$. Since, by the previous lemma, C_n(resp. C_n^{+z}) is a union of arcs $\sigma^i \overset{\frown}{P_0P_1}$ with $i \in \mathbb{Z}$, we may conclude that C_n(resp. C_n^{+z}) is equal to $G_2 E_{ac}^{bn}$.
Proof of case (ii). From $\sigma P_0 = \rho_3 P_0$ we see that

$$y_0 = \frac{(2an^2 - b)y_0 - 2nz_0}{b},$$

hence $nz_0 = (an^2 - b)y_0$ and now, since $P_0 \in C_n^{+y}, y_0^2 = n^2(abn^2 - b^2 - c) /(abn^2 - b^2)$. Thus, $P_0 = (n, y_0, -z_0)$, $P_1 = \sigma P_0 = (n, y_0, z_0)$, with $y_0 = n\sqrt{(abn^2 - b^2 - c)/(abn^2 - b^2)}$ and the projection of the arc $\overset{\frown}{P_0P_1}$ on the y-axis is the interval

$$\left[\sqrt{\frac{abn^2 - b^2 - c}{a^2n^2 - ab}},\; n\sqrt{\frac{abn^2 - b^2 - c}{abn^2 - b^2}}\right].$$

As y runs through the values of this interval, the point (n, y, z) runs through E_{ac}^{bn}, therefore $\overset{\frown}{P_0P_1} = E_{ac}^{bn}$. By the previous lemma, $C_n^{+y} = \bigcup_{i \in \mathbb{Z}} \sigma^i \overset{\frown}{P_0P_1} = G_2 E_{ac}^{bn}$.

Proof of part II. In the proof of part I, we saw that $E_{ac}^{bn} = \overset{\frown}{P_0P_1}$;hence $P \in E_{ac}^{bn}$ means, in case $an^2 - b > 0$, that P is a point on the arc $\overset{\frown}{P_0P_1}$ of one of the hyperbolas in *Fig.2*. Then, $\sigma P \in \overset{\frown}{P_1P_2}$ and $\sigma^{-1}P \in \overset{\frown}{P_0P_{-1}}$, from which it is clear that, unless $P = P_0$ or P_1, the y-coordinate of P is strictly less than the y coordinate of σP(resp. of $\sigma^{-1}P$). Thus in view of the definition of φ, unless $\sigma P, \sigma^{-1}P \in H_1 P$, we have $\varphi(P) < \varphi(\sigma P), \varphi(\sigma^{-1}P)$. In the case $an^2 - b < 0$ we are in one of the four cases explicitly stated at the begining of the proof of the previous lemma and we check every case separately. Consider for example, the case $(a, b, n) = (3, 4, 1)$; then, for $P = (1, y, z) \in C_1$ we have $\sigma P = (1, (y + z)/2, (-3y + z)/2)$ and the relation $\varphi(P) < \varphi(\sigma P)$ is equivalent to $y^2 < (y + z)^2/4$ and this, in turn, means $-1/3 < y/z < 1$. The last relation is seen to be true as follows. By $(1, y, z) \in E_{3c}^{41}$ it follows that $y^2 \leq (4 + c)/12$

and since $(1, y, z)$ is a solution to the title equation, $z^2 = 4 + c - 3y^2 \geq (12 + 3c)/4$, hence $(y/z)^2 \leq 1/9$; consequently $\underline{-1/3 \leq y/z} < 1$ and it is easy to see that we can have equality only if $|y| = \sqrt{(4+c)/12}$, $z = \sqrt{(12+3c)/4}$, in which case $\sigma P \in H_1 P$. We deal with the other cases analogously. The proof of the last statement is obvious from *Fig. 2.* □

In the case of $(a, b) = (1, 4)$, part II of this lemma does not hold, because the order of A_2 is equal to 3; however instead of this lemma we have the following.

Lemma 5.

I *Define*

$$E^{41}_{1c} = \left\{ (1, y, z) \in C_1^{+z} \;\middle|\; 0 \leq y \leq \sqrt{\frac{12+c}{12}} \right\}.$$

Then $C_1 = G_1 E^{41}_{1c}$.

II *If* P *is any point in* E^{41}_{1c} *and* σP *dose not coincide with* $\rho_3 P$, *then*

$$\varphi(\sigma P) > \varphi(P), \quad \varphi(\sigma^{-1} P) > \varphi(P).$$

Proof. As we saw, in this case, σ is expressed by the matrix

$$A_2 = \frac{1}{2}\begin{pmatrix} -1 & 1 \\ -3 & -1 \end{pmatrix},$$

the order of which is equal to 3. Let P_i's be the same points that are defined in the proof of the previous lemma. We consider a point $Q_0 \in C_1^{+z}$ such that $\sigma Q_0 = \rho_3 Q_0$ and put $Q_i = \sigma^i Q_0$ $(i = 1, 2)$. Next we consider a point $R_0 = (1, 0, z_r) \in C_1^{+z}$ and put $R_i = \sigma^i R_0$ $(i = 1, 2)$. (See *Fig.1.*) Then from $\sigma P_0 = \rho_2 P_0$ and $\sigma Q_0 = \rho_3 Q_0$, we have $P_1 = \left(\sqrt{\frac{12+c}{4}}, \sqrt{\frac{12+c}{4}}\right)$ and $Q_1 = \left(\sqrt{\frac{12+c}{12}}, \sqrt{\frac{36+3c}{4}}\right)$, and it is clear that $R_1 = \rho_3 P_1$, $R_2 = \rho_2 R_1$ and that both the y-coordinate of P_2 and the z-coordinate of Q_2 are equal to 0. From *Fig.1*, it is obvious that $\overset{\frown}{Q_0P_1} = \sigma^{-1}\overset{\frown}{Q_1P_2} = \sigma^{-1}\rho_3\overset{\frown}{Q_0R_0}$ and $\overset{\frown}{P_0R_0} = \rho_2\overset{\frown}{R_0P_1}$. By case (ii) of *Lemma 3*, $C_1 = \bigcup_{i=0}^{2} \sigma^i \overset{\frown}{P_0P_1}$, therefore $C_1 = G_1 \overset{\frown}{R_0Q_0} = G_1 E^{41}_{1c}$. Next we consider a point $P \in \overset{\frown}{R_0Q_0}$. From *Fig.1* we can see that $\sigma P \in \overset{\frown}{R_1Q_1}$ and $\sigma^{-1}P \in \overset{\frown}{R_2Q_2}$. This proves part II of the lemma. □

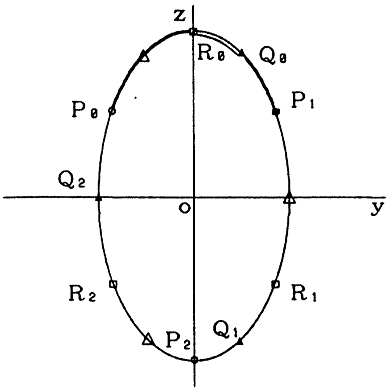

Fig. 1. C_1 & E^{41}_{1c}

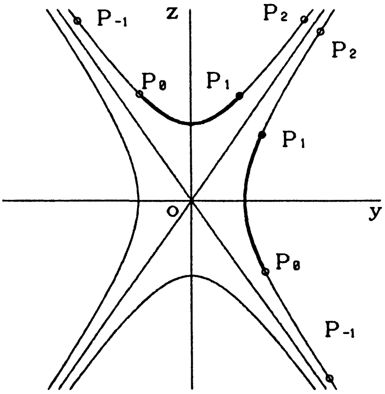

Fig. 2. C_n & E^{bn}_{ac}

3. The Main Results in the Cases $b = 1, 2, 4$

In section 2, we have investigated σ as a permutation on C_n. Now we consider the permutation group G on S^b_{ac}.

$$G = < \sigma,\ \tau,\ \rho_1,\ \rho_2,\ \rho_3 > .$$

Theorem 1. *Let $b = 1, 2, 4$, $(a, b) \neq (1, 4)$ and let T^b_{ac} be the set of integral trivial solutions of equation (2). Define*

$$R_1 = \left\{ (x, y, z) \in S^b_{ac} \;\middle|\; 0 \leq x \leq y\,,\ x^2 + y^2 \leq \frac{b^2 + c}{ab},\ z \geq 0 \right\},$$

and if $c < 0$,

$$R_2 = \left\{ (x, y, z) \in S^b_{ac} \;\middle|\; \sqrt{\frac{b}{a}} < x \leq y \leq x\sqrt{\frac{abx^2 - b^2 - c}{abx^2 - b^2}},\ z \geq 0 \right\}.$$

(i) *Put $R^b_{ac} = R_1 \cup T^b_{ac}$ if $c \geq 0$ and $R^b_{ac} = R_1 \cup R_2 \cup T^b_{ac}$ if $c < 0$. Then the set of all integral solutions of (2) coincides with GR^b_{ac}.*

(ii) *If $(x, y, z) \in R_1$ then*

$$0 \leq x \leq \sqrt{\frac{b^2 + c}{2ab}}\,,\quad x \leq y \leq \sqrt{\frac{b^2 + c}{ab}}.$$

If $(x, y, z) \in R_2 (c < 0)$ then, either $x \neq y$, in which case

$$\sqrt{\frac{b}{a}} < x < \frac{-c + \sqrt{c^2 + 16ab^3}}{4ab}\,,\quad x < y \leq x\sqrt{\frac{abx^2 - b^2 - c}{abx^2 - b^2}}\,,$$

or $x = y$ and $\sqrt{b/a} < x \leq \sqrt{(b - c)/a}$. In particular, R_1, R_2 are at most *finite and algorithmically computable.*

Proof. Let $P = (x, y, z)$ be a non-trivial solution of (2), so that $-abx^2+b^2+c \neq 0$. Since in the H_1-orbit of P there is a point with all its three coordinates non-negative, it suffices to consider only the case in which x, y and z are non-negative.

Consider a point $P_0 = (x_0, y_0, z_0)$ in the G-orbit of P, such that $\varphi(P_0)$ is minimal and x_0, y_0, z_0 are non-negative. We will show that $P \in GR^b_{ac}$. Indeed, if $P_0 \in T^b_{ac}$ then P_0 is already in R^b_{ac}, so we may suppose that P_0 is not a trivial solution. Suppose first that $-abx_0^2+b^2+c > 0$ or $-aby_0^2+b^2+c > 0$. If the first of these inequalities holds and $x_0 = 0$, then, by (3) (with $n = x_0$), P_0 is already in R_1, therefore we may suppose that $x_0 > 0$. Similarly, if the second inequality holds, then we may suppose $y_0 > 0$. By case (i) of *Lemma 4* , P_0 or τP_0, respectively, belongs to the G_2-orbit of some point $P_1 = (n, y_1, z_1) \in E^{bn}_{ac}$,(where $n = x_0$ or y_0, respectively) and $\varphi(P_1) \leq \dfrac{b^2+c}{ab}$, by the definition of E^{bn}_{ac} in this case. If $n \leq y_1$, the point P_1, is already in R_1, otherwise $\tau P_1, \rho_2 P_1$ or $\tau\rho_2 P_1$ belongs to R_1. Thus, P is in the G-orbit of $P_1 \in R_1$.

Next, let $-abx_0^2 + b^2 + c < 0$ and $-aby_0^2 + b^2 + c < 0$, so that by (3) (with $n = x_0$) $ax_0^2 - b > 0$ and $ay_0^2 - b > 0$. Suppose that $P_0 \notin E^{bx_0}_{ac}$. By case (ii) of *Lemma 4*,P_0 is in the G_2-orbit of some point $P_1 \in E^{bx_0}_{ac}$ and then, by part II of the same lemma, $\varphi(P_0) > \varphi(P_1)$. But P_1 is also in the G-orbit of P, hence, the last inequality contradicts the minimality of $\varphi(P_0)$. Thus, $P_0 \in E^{bx_0}_{ac}$. Since $\varphi(\tau P_0) = \varphi(P_0)$, we can prove, in exactly the same way, that $\tau P_0 \in E^{by_0}_{ac}$. If $c \geq 0$ we will be led to a contradiction. Indeed, by the definition of the sets $E^{bx_0}_{ac}$ and $E^{by_0}_{ac}$, we must have

$$0 < y_0 \leq x_0\sqrt{\frac{abx_0^2 - b^2 - c}{abx_0^2 - b^2}} \quad \& \quad 0 < x_0 \leq y_0\sqrt{\frac{aby_0^2 - b^2 - c}{aby_0^2 - b^2}}. \tag{10}$$

If $c = 0$, it follows that $x_0 = y_0$, which contradicts our assumption that P_0 is not trivial. Next let $c > 0$. Multiplication and squaring of the last two relations gives(as we previously saw, nominators and denominators are positive)

$$(abx_0^2 - b^2 - c)(aby_0^2 - b^2 - c) \geq (abx_0^2 - b^2)(aby_0^2 - b^2), \tag{11}$$

i.e. $c \geq ab(x_0^2 + y_0^2) - 2b^2$. However, if we add the relations $-abx_0^2 + b^2 + c < 0$ and $-aby_0^2 + b^2 + c < 0$ we get $ab(x_0^2 + y_0^2) - 2b^2 > 2c > c$, arriving at a contradiction. If $c < 0$ we put $P_1 = P_0$ if $x_0 \leq y_0$ and $P_1 = \tau P_0$ otherwise. If we put $P_1 = (x_1, y_1, z_1)$, then $0 \leq x_1 \leq y_1$, $z_1 \geq 0$ and $P_1 \in E^{bx_1}_{ac}$, hence, by the definition of this set in the case under condition$(-abx_1^2+b^2+c < 0,\ ax_1^2-b > 0)$, we see that $P_1 \in R_2$ and P is in GR_2.

Now we prove part (ii). If $(x, y, z) \in R_1$ then both x^2 and y^2 must be $\leq \dfrac{b^2+c}{ab}$ and the minimum of these two, i.e. x^2 cannot exceed $\dfrac{b^2+c}{2ab}$. If $(x, y, z) \in R_2$ and $x = y$,then $(ax^2-b)^2 = z^2-c \geq -c$ hence $(ax^2-b+z)(ax^2-b-z) = -c$ and it follows that $ax^2 - b \leq -c$, as claimed. Finally, if $(x, y, z) \in R_2$ and $x < y$, then, from the inequalities in the definition of R_2, it follows that

$$x\sqrt{\frac{abx^2-b^2-c}{abx^2-b^2}}-x \geq 1\,, \tag{12}$$

from which,

$$-cx^2 > (2x+1)(abx^2-b^2) > 2x(abx^2-b^2) \tag{13}$$

and, consequently, $2abx^2+cx-2b^2<0$, hence x is strictly less than the larger root of the left-hand side. This completes the proof. □

Remark 2. Note that the G-orbit of a trivial solution contains both trivial and non-trivial solutions. Example: $(a,b,c)=(1,1,9)$; a trivial solution is $(1,2,3)$ and $\sigma\tau\sigma(1,2,3)=(8,175,1389)$ which is not trivial.

For the case $(a,b)=(1,4)$ we have the following analogous theorem.

Theorem 2. *Let $(a,b)=(1,4)$ and let T^4_{1c} be the set of integral trivial solutions of equation (2). Define*

$$R_1' = \left\{(x,y,z)\in S^4_{1c}\;\middle|\; x\neq 1,\, y\neq 1,\, 0\leq x\leq y\,,\, x^2+y^2\leq \frac{16+c}{4}, z\geq 0\right\},$$

$$R_1'' = \left\{(1,y,z)\in S^4_{1c}\;\middle|\; y^2\leq \frac{12+c}{12},\; z\geq 0\right\},$$

and if $c<0$,

$$R_2 = \left\{(x,y,z)\in S^4_{1c}\;\middle|\; 2<x\leq y\leq x\sqrt{\frac{4x^2-16-c}{4x^2-16}}\,, z\geq 0\right\}.$$

(i) *Put $R^4_{1c}=R_1'\cup R_1''\cup T^4_{1c}$ if $c\geq 0$ and $R^4_{1c}=R_1'\cup R_1''\cup R_2\cup T^4_{1c}$ if $c<0$. Then the set of all integral solutions of (2) coincides with GR^4_{1c}.*

(ii) *If $(x,y,z)\in R_1'$ then*

$$0\leq x\leq\sqrt{\frac{16+c}{8}}\,,\; x\leq y\leq\sqrt{\frac{16+c}{4}}.$$

If $(x,y,z)\in R_2(c<0)$ then, either $x\neq y$, in which case

$$2<x<\frac{-c+\sqrt{c^2+1024}}{16}\,,\; x<y\leq x\sqrt{\frac{4x^2-16-c}{4x^2-16}}\,,$$

or $x=y$ and $2<x\leq\sqrt{4-c}$. In paticular, R_1', R_1'' and R_2 are at most finite and algorithmically computable.

Proof. Let P be a non-trivial solution of (2). Consider a point $P_0=(x_0,y_0,z_0)$ in the G-orbit of P, such that $\varphi(P_0)$ is minimal and x_0,y_0,z_0 are non-negative. If $x_0\neq 1$ and $y_0\neq 1$ then we can prove $P\in GR^4_{1c}$ in exactly the same way as in the general case. We may suppose $x_0=1$, indeed if $y_0=1$ we can replace

P_0 with τP_0. Then by *Lemma 5*, P_0 belongs to the G-orbit of some point $P_1 = (1, y_1, z_1) \in E_{1c}^{41}$ and by the definition of E_{1c}^{41}, we have $y_1 \leq (12+c)/12$, $z_1 \geq 0$, so that $P_1 \in R_1''$. Therefore P is in the G-orbit of $P_1 \in R_1''$. This proves part (i) of the theorem. Part (ii) is proved in exactly the same way as in *Theorem 1*. □

Theorem 1 and *2* give us a criterion for solvability of equation (2) with $b = 1, 2$ or 4. It is solvable if and only if R_{ac}^b is not empty. Moreover we can derive effectively all solutions by GR_{ac}^b. Next we will show that $R_{ac}^b \setminus T_{ac}^b$ is a minimal set of integral solutions of equation (2) such that the G-orbits of this set exhaust all non-trivial integral solutions except for that derived from a trivial solution.

Proposition 1. *Let $b = 1$, 2, 4. For any points A, B belonging to $R_{ac}^b \setminus T_{ac}^b$, it holds that if $A \sim B$ then $A = B$.*

Proof. Let $B = gA$, $g \in G$ then by *Corollary 2* of *Lemma 2*, we have a representation

$$g = \rho_1^a \, \rho_2^b \, \rho_3^c \, \tau^d \, \sigma^{e_1} (\tau\sigma\tau)^{f_1} \cdots \sigma^{e_k} (\tau\sigma\tau)^{f_k} \ ,$$

where k is some non-negative integer, e_i, $f_i \in \mathbb{Z}$ $(i=1,2,\ldots,k)$, a, b, c, $d = 0$ or 1. We can show $g \in H$ by reduction to absurdity. Suppose $g \notin H$ and

$$A = P_0 \xrightarrow{g_1} P_1 \xrightarrow{g_2} P_2 \longrightarrow \cdots \longrightarrow P_{n-1} \xrightarrow{g_n} P_n \xrightarrow{h} P_{n+1} = B \ ,$$

where $g_i \in \{\sigma,\ \sigma^{-1},\ \tau\sigma\tau,\ \tau\sigma^{-1}\tau\}$, $h \in H$, $n = \sum_{i=1}^{k}(e_i + f_i)$. By *Corollary 1* of *Lemma 2* we may suppose $P_j \notin HP_i$ $(i < j \leq n)$. Consider a point P_m in these P_i $(i=1,2,\ldots,n+1)$, such that $\varphi(P_m)$ is maximal.

First we show $m \neq 0$, n, $n+1$. By *Lemma 4* and *5*,

$$\varphi(\sigma P_0) > \varphi(P_0), \qquad \varphi(\sigma^{-1} P_0) > \varphi(P_0),$$

where we may replace σ with $\tau\sigma\tau$. So we have $m \neq 0$. Similarly we have also $m \neq n, n+1$. Now we may suppose

$$\varphi(P_{m-1}) < \varphi(P_m), \qquad \varphi(P_{m+1}) \leq \varphi(P_m). \tag{14}$$

Let $Q_m = (\xi,\ \eta,\ \zeta)$ be a point such that $Q_m \in HP_m$, ξ, η, $\zeta \geq 0$, $\eta \geq \xi$. By *Corollary 1* of *Lemma 2*,

$$P_{m-1},\ P_{m+1} \in H(\sigma Q_m) \cup H(\sigma^{-1} Q_m) \cup H(\tau\sigma\tau Q_m) \cup H(\tau\sigma^{-1}\tau Q_m).$$

By the definition of τ and σ,

$$\sigma Q_m = \left(\xi,\ \frac{(2a\xi^2 - b)\eta + 2\xi\zeta}{b},\ \frac{2\xi(a^2\xi^2 - ab)\eta + (2a\xi^2 - b)\zeta}{b}\right),$$

$$\sigma^{-1} Q_m = \left(\xi,\ \frac{(2a\xi^2 - b)\eta - 2\xi\zeta}{b},\ \frac{-2\xi(a^2\xi^2 - ab)\eta + (2a\xi^2 - b)\zeta}{b}\right),$$

$$\tau\sigma\tau Q_m = \left(\frac{(2a\eta^2 - b)\xi + 2\eta\zeta}{b},\ \eta,\ \frac{2\eta(a^2\eta^2 - ab)\xi + (2a\eta^2 - b)\zeta}{b}\right),$$

$$\tau\sigma^{-1}\tau Q_m = \left(\frac{(2a\eta^2 - b)\xi - 2\eta\zeta}{b},\ \eta,\ \frac{-2\eta(a^2\eta^2 - ab)\xi + (2a\eta^2 - b)\zeta}{b}\right).$$

First we consider the case:

$$\varphi(\sigma^{-1}Q_m) < \varphi(Q_m), \qquad \varphi(\tau\sigma^{-1}\tau Q_m) \leq \varphi(Q_m). \tag{15}$$

From the first inequality, we obtain $-b\eta < 2a\xi^2\eta - b\eta - 2\xi\zeta < b\eta$, hence

$$0 < \xi(a\xi\eta - \zeta) < b\eta. \tag{16}$$

Similarly from the second,

$$0 \leq \eta(a\xi\eta - \zeta) \leq b\xi. \tag{17}$$

In view of (16), $\eta > 0$, hence multiplication of (16) and (17) gives $0 < \xi\eta(a\xi\eta - \zeta)^2 < b^2\xi\eta$, from which

$$0 < (a\xi\eta - \zeta)^2 < b^2. \tag{18}$$

In the case $b = 1$, this is a contradiction. Consider the case $b = 2$. From (18) $a\xi\eta - \zeta = 1$. Here we put $S = \sigma^{-1}Q_m$, $T = \tau\sigma^{-1}\tau Q_m$. Then

$$S = (\xi,\ \xi - \eta,\ a\xi(\eta - \xi) + 1), \qquad T = (-\xi + \eta,\ \eta,\ a\eta(\xi - \eta) + 1).$$

By easy calculation, we have

$$S = \rho_1\rho_2\rho_3\tau\sigma T \qquad \textit{or equivalently} \qquad T = \rho_1\rho_2\rho_3\tau(\tau\sigma\tau)S. \tag{19}$$

It follows that $P_{m+1} = h^*g^*P_{m-1}$ with some $h^* \in H$, $g^* \in \{\sigma, \sigma^{-1}, \tau\sigma\tau, \tau\sigma^{-1}\tau\}$. By *Corollary 1* of *Lemma 2*, we have a representation

$$h \prod_{i=m+2}^{n} g_i h^* = h' \prod_{i=m+2}^{n} g_i',$$

with some $h' \in H$, $g_i' \in \{\sigma,\ \sigma^{-1},\ \tau\sigma\tau,\ \tau\sigma^{-1}\tau\}$ $(i=m+2,\dots,n)$. So we obtain a new sequence of points from A to B, where the number of P_i's decreases by one. In the case $b = 4$, from (18) and $\zeta^2 - a^2\xi^2\eta^2 \equiv 0$ $(mod\ 4)$, we have $a\xi\eta - \zeta = 2$, hence we obtain the relation (19) and the same result.

In the case

$$\varphi(\sigma Q_m) < \varphi(Q_m), \qquad \varphi(\tau\sigma\tau Q_m) \leq \varphi(Q_m),$$

we have $\xi, \eta > 0$, $a\xi^2 - b < 0$, $a\eta^2 - b < 0$, hence $\xi = \eta = 1$. Therefore

$$\sigma Q_m = \rho_3\tau\,(\tau\sigma\tau Q_m)\,,$$

which contradicts the assumption $P_{m+1} \notin HP_{m-1}$.

Next we consider the case

$$\varphi(\sigma^{-1}Q_m) < \varphi(Q_m), \qquad \varphi(\tau\sigma\tau Q_m) \leq \varphi(Q_m). \tag{20}$$

From these inequalities we have

$$0 < \eta, \quad 0 < a\xi\eta - \zeta, \quad \xi(a\xi\eta - \zeta) < b\eta, \tag{21}$$

$$0 < \xi, \quad 0 < a\xi\eta + \zeta, \quad \eta(a\xi\eta + \zeta) \leq b\xi. \tag{22}$$

Combining these, we have

$$0 < a^2\xi^2\eta^2 - \zeta^2 < b^2.$$

In the case $b = 1$, this is a contradiction. Consider the cases $b = 2$ or 4. From (22), $\xi(a\eta^2 - b) + \eta\zeta < 0$, which implies $\eta = 1$. Therefore from (21), (22), we have

$$0 < \xi, \quad 0 < a\xi - \zeta, \quad \xi(a\xi - \zeta) < b.$$

Hence $\xi = 1$, because $a\xi - \zeta \equiv 0$ $(mod\ 2)$ in the case $b = 4$. From (20), we have $\sigma^{-1}Q_m = (1, 0, \zeta')$, $\tau\sigma\tau Q_m = (0, 1, \zeta'')$. Therefore $P_{m+1} \in HP_{m-1}$, which contradicts the assumption. Similarly

$$\varphi(\sigma Q_m) < \varphi(Q_m), \qquad \varphi(\tau\sigma^{-1}\tau Q_m) \leq \varphi(Q_m),$$

leads to a contradiction.

Finally we consider the case:

$$\varphi(\sigma Q_m) < \varphi(Q_m), \qquad \varphi(\sigma^{-1}Q_m) \leq \varphi(Q_m).$$

From this assumption we have $\xi, \eta > 0$, $a\xi^2 - b < 0$. After consideration of $P_{m+1} \notin HP_{m-1}$, P_{m-1}, $P_{m+1} \notin HP_m$, only one case remains, that is $(a, b, \xi) = (1, 4, 1)$. In this case, the order of σ as a permutation on C_1 is 3, hence $\sigma^{-1}Q_m = \sigma(\sigma Q_m)$. Therefore we come to the same result. Similarly

$$\varphi(\tau\sigma\tau Q_m) < \varphi(Q_m), \qquad \varphi(\tau\sigma^{-1}\tau Q_m) \leq \varphi(Q_m),$$

leads also to the same result.

Now the assumption leads us to a contradiction or a new sequence of points from A to B, where the number of P_i's decreases by one. And if $n = 1$, either

$$\varphi(B) > \varphi(A) \quad \text{or} \quad \varphi(A) > \varphi(B),$$

which contradicts A, $B \in R^b_{ac}$. Consequently $g \in H$, which implies $A = B$. □

Remark 3. In the case $b^2 + c < 0$, the proof becomes simple. We consider a point Q_m as in the proof. From (3) with $-ab\xi^2 + b^2 + c < 0$, we have $a\xi^2 - b > 0$, similarly we have $a\eta^2 - b > 0$. From the first we have $\dfrac{(2a\xi^2 - b)\eta + 2\xi\zeta}{b} - \eta = \dfrac{2(a\xi^2 - b)\eta + 2\xi\zeta}{b} > 0$, consequently $\dfrac{(2a\xi^2 - b)\eta + 2\xi\zeta}{b} > \eta$, from which we have $\varphi(\sigma Q_m) > \varphi(Q_m)$. Likewise, from the second we have $\varphi(\tau\sigma\tau Q_m) > \varphi(Q_m)$. From these relations it is clear that it suffices to consider only the case

$$\varphi(\sigma^{-1}Q_m) < \varphi(Q_m), \qquad \varphi(\tau\sigma^{-1}\tau Q_m) \leq \varphi(Q_m).$$

4. The Cases $b = -1,\ -2$ or -4

In this section, we examine the cases $b = -1,\ -2$ or -4. We state the results and give the proof only at the points in which the proof differs essentially from the previous one. We preserve the notations for the case $b > 0$, except for the permutation σ and T^b_{ac}.

In the case $n = 0$, we can solve equation (3) by the theory of binary quadratic forms (see [4] or [5]), the integral solutions of which are algorithmically computable. Thus we define *a trivial solution* of equation (2) as an integral solution such that $xy(-abx^2 + b^2 + c)(-aby^2 + b^2 + c) = 0$ or (only if $c = 0$) $x^2 = y^2$. (Note that it always holds that $(ax^2 - b)(ay^2 - b) \neq 0$ in this case.) [1]

We define σ as

$$\sigma(x,\ y,\ z) := \left(x,\ \frac{(2ax^2 - b)y + 2xz}{-b},\ \frac{2x(a^2x^2 - ab)y + (2ax^2 - b)z}{-b}\right).$$

Since

$$\varepsilon_n = \frac{2an^2 - b + 2n\sqrt{a^2n^2 - ab}}{-b},$$

is a unit with norm $+1$ in the ring of integers of $\mathbb{Q}(\sqrt{a^2n^2 - ab})$, σ is a permutation on S^b_{ac} , F^b_{ac} or C_n and satisfies lemmas and corollaries in *Sec.1.* We can prove the following in the same way as in *Lemma 3.*

Lemma 6. *Let $n > 0$. For a point P_0 on C_n, put $P_1 = \sigma P_0$, and let $\overset{\frown}{P_0P_1}$ be an arc of C_n, in which P_1 is contained and P_0 is not .*

(i) *If $-abn^2 + b^2 + c < 0$, let $P_0 = (y_0,\ -z_0)$ be a point on C_n^{+y} such that $\sigma P_0 = \rho_3 P_0$, $z_0 \geq 0$. Then*

$$C_n^{+y} = \bigcup_{i \in \mathbf{Z}} \sigma^i \overset{\frown}{P_0P_1}.$$

(ii) *If $-abn^2 + b^2 + c > 0$, let $P_0 = (-y_0,\ z_0)$ be a point on C_n^{+z} such that $\sigma P_0 = \rho_2 P_0$, $y_0 \geq 0$. Then*

$$C_n^{+z} = \bigcup_{i \in \mathbf{Z}} \sigma^i \overset{\frown}{P_0P_1}.$$

Also we can prove the following in the same way as in *Lemma 4.*

Lemma 7. *Let $n > 0$.*

I

(i) *If $-abn^2 + b^2 + c < 0$, define*

[1] Finding all trivial solutions with $x = 0$ or $y = 0$ amounts to solving a Pell equation and, in that sense, these solutions are not trivial in a strict sense.

$$E_{ac}^{bn} = \left\{ (n, y, z) \in C_n^{+y} \,\middle|\, \sqrt{\frac{abn^2 - b^2 - c}{a^2n^2 - ab}} \le y \le \sqrt{\frac{b^2 + c}{ab} - n^2} \right\}.$$

Then $C_n^{+y} = G_2 E_{ac}^{bn}$.

(ii) *If* $-abn^2 + b^2 + c > 0$, *define* E_{ac}^{bn} *as*

$$\left\{ (n, y, z) \in C_n^{+z} \,\middle|\, -n\sqrt{\frac{-abn^2 + b^2 + c}{-abn^2 + b^2}} < y \le n\sqrt{\frac{-abn^2 + b^2 + c}{-abn^2 + b^2}} \right\}.$$

Then $C_n^{+z} = G_2 E_{ac}^{bn}$.

II *If* P *is any point in* E_{ac}^{bn} *and* σP, $\sigma^{-1}P$ *do not belong to* $H_1 P$, *then*

$$\varphi(\sigma P) > \varphi(P), \quad \varphi(\sigma^{-1}P) > \varphi(P),$$

respectively. Moreover, if P *is any point in* E_{ac}^{bn}, *while* $Q = (n, y, z)$ *any point not belonging to* E_{ac}^{bn}, *then, unless* $Q \in H_1 P$

$$\varphi(Q) > \varphi(P).$$

Theorem 3. *Let* $b = -1, -2, -4$ *and let* T_{ac}^b *be the set of integral trivial solutions of equation (2). Define*

$$R_1 = \left\{ (x, y, z) \in S_{ac}^b \,\middle|\, 0 < x \le y \,,\, x^2 + y^2 \le \frac{b^2 + c}{ab}, z \ge 0 \right\},$$

and if $c > 0$,

$$R_2 = \left\{ (x, y, z) \in S_{ac}^b \,\middle|\, 0 < x \le y \le x\sqrt{\frac{-abx^2 + b^2 + c}{-abx^2 + b^2}}, z \ge 0 \right\}.$$

(i) *Put* $R_{ac}^b = R_2 \cup T_{ac}^b$ *if* $c \ge 0$ *and* $R_{ac}^b = R_1 \cup T_{ac}^b$ *if* $c < 0$. *Then the set of all integral solutions of (2) coincides with* GR_{ac}^b.

(ii) *If* $(x, y, z) \in R_1$ *then*

$$0 < x \le \sqrt{\frac{b^2 + c}{2ab}} \,,\ x \le y \le \sqrt{\frac{b^2 + c}{ab}}.$$

If $(x, y, z) \in R_2 (c > 0)$ *then, either* $x \ne y$, *in which case*

$$0 < x < \frac{c + \sqrt{c^2 + 16ab^3}}{-4ab} \,,\ x < y \le x\sqrt{\frac{-abx^2 + b^2 + c}{-abx^2 + b^2}},$$

or $x = y$ *and* $x \le \sqrt{(b + c)/a}$. *In paticular,* R_1, R_2 *are at most finite and algorithmically computable.*

Replacing the case "$-abx_0^2+b^2+c>0$ or $-aby_0^2+b^2+c>0$" in the proof of *Theorem 1* with "$-abx_0^2+b^2+c<0$ or $-aby_0^2+b^2+c<0$" and the case "$-abx_0^2+b^2+c<0$ and $-aby_0^2+b^2+c<0$" with "$-abx_0^2+b^2+c>0$ and $-aby_0^2+b^2+c>0$", and using *Lemma 7* instead of *Lemma 4*, we can prove this in the same way as in *Theorem 1*.

Proposition 2. *Let $b=-1,-2,-4$. For any points A, B belonging to $R^b_{ac}\backslash T^b_{ac}$, it holds that if $A \sim B$ then $A=B$.*

Proof. The proof is similar to that of *Proposition 1* and we give only a sketch of it. We preserve the definitions and notations in the proof of *Proposition 1*. For a point $P=(x,y,z)\in R^b_{ac}\setminus T^b_{ac}$ with $x,y>0, z\geq 0$, unless $\sigma P, \tau\sigma\tau P\in HP$, we have

$$\varphi(\sigma P)>\varphi(P), \qquad \varphi(\tau\sigma\tau P)>\varphi(P).$$

Consequently if P_m is a point such that $\varphi(P_m)$ is maximal in the sequence of points from A to B, then we may assume

$$\varphi(\sigma^{-1}P_m)<\varphi(P_m), \qquad \varphi(\tau\sigma^{-1}\tau P_m)\leq\varphi(P_m).$$

From these inequalities we obtain

$$0<\zeta-a\xi\eta<-b. \tag{23}$$

If $b=-1$ this is a contradiction. If $b=-2$ we have $\zeta-a\xi\eta=1$, hence $S=(\xi,\eta-\xi,a\xi(\xi-\eta)+1)$, $T=(\xi-\eta,\eta,a\eta(\eta-\xi)+1)$, from which we have

$$S=\rho_2\tau\sigma T \qquad \textit{or equivalently} \qquad T=\rho_1\tau(\tau\sigma\tau)S, \tag{24}$$

hence, there is a new sequence of points from A to B where the number of P's decreases by one. In the case $b=-4$, from (23) and $\zeta^2-a^2\xi^2\eta^2\equiv 0(mod\ 4)$ we have $\zeta-a\xi\eta=2$, hence we obtain the relation (24) and come to the same result. And if $n=1$ we are led to a contradiction in the same way as in the proof of *Proposition 1*. Thus if we suppose $g\notin H$ then we are led to a contradiction. Consequently $g\in H$, hence we arrive at $A=B$. □

5. Examples

In *Table 1* and *2*, we show R^b_{ac} for the cases $a=2$, $b=\pm1$, $-85\leq c\leq 85$, $c\neq 0$, which we have obtained by using *UBASIC*.

Theorem 5. *Let $a>2$, $b=1$, $c=-1$. Then equation (2) has only one solution* $(0,0,0)$.

Proof. It is obvious that $T^1_{a-1}=\{(0,0,0)\}$ and $R_1=\{(0,0,0)\}$, hence we have $R^1_{a-1}=\{(0,0,0)\}$. Therefore by *Theorem 1* we obtain $S^1_{a,-1}=GR^1_{a,-1}=\{(0,0,0)\}$. □

Table 1. R^1_{2c} of $(2x^2-1)(2y^2-1)=z^2-c$, for $-85 \le c \le 85$, $c \neq 0$

c	x	y	z	c	x	y	z	c	x	y	z	c	x	y	z
-85	4	6	46	-33	3	3	16		1	2	5	53	0	3	6
-83	2	3	6	-31	1	4	0	19	1	3	6		0	5	2
-81	1	7	4	-30	1	4	1	21	0	3	2	56	0	2	7
-80	1	9	9	-27	1	4	2	23	0	2	4	56	0	4	5
-78	1	8	7	-24	1	5	5	24	0	0	5	57	1	2	8
-75	4	5	38		2	2	5		1	1	5		2	5	20
-73	2	4	12	-22	1	4	3	25	2	3	12	58	0	5	3
-72	1	7	5	-21	2	4	14	26	0	1	5	63	0	0	8
-71	1	6	0	-19	2	3	10		0	3	3		1	1	8
-70	1	6	1	-17	1	3	0	29	1	2	6		4	4	32
	2	3	7	-16	1	3	1	31	0	4	0	64	1	3	9
-67	1	6	2	-15	1	4	4	32	0	2	5	65	0	1	8
-64	3	3	15	-13	1	3	2		0	4	1		0	5	4
-63	1	8	8		2	2	6		1	3	7	66	0	3	7
-62	1	6	3	-8	1	3	3		2	2	9	67	0	4	6
-61	1	7	6	-7	1	2	0	33	0	3	4		3	5	30
	4	4	30	-6	1	2	1		1	4	8	69	1	4	10
-56	2	6	21	-3	1	2	2	35	0	0	6	71	0	2	8
-55	1	6	4	-1	0	0	0		0	4	2		0	6	0
	2	3	8		1	1	0		1	1	6	72	0	6	1
-54	2	5	17	1	0	1	0		3	3	18		1	5	11
-51	3	6	34	2	0	1	1	40	0	4	3		3	3	19
	3	5	28	3	0	0	2	42	0	3	5	73	1	6	12
-48	1	5	1		1	1	2		1	2	7	74	0	5	5
	1	7	7	5	0	1	2	37	0	1	6		2	2	11
-49	1	5	0	7	0	2	0	39	2	4	16		2	4	17
	2	2	0	8	0	0	3	43	0	2	6		1	2	9
	2	2	1		0	2	1	47	0	4	4	75	0	6	2
	2	4	13		1	1	3		1	3	8	77	2	3	14
-46	1	6	5	9	1	2	4	48	0	0	7	79	2	6	24
-45	1	5	2	10	0	1	3		1	1	7	80	0	0	9
	2	2	2	11	0	2	2	49	0	5	0		0	4	7
-43	3	4	22	15	0	0	4		3	4	24		0	6	3
-40	1	5	3		1	1	4	50	0	1	7		1	1	9
	2	2	3		2	2	8		0	5	1	81	0	3	8
-38	2	3	9	16	0	2	3		1	4	9		4	5	40
-35	1	6	6	17	0	1	4		2	3	13	82	0	1	9
-33	1	5	4		0	3	0	51	1	5	10	83	1	3	10
	2	2	4	18	0	3	1		2	2	10	85	0	5	6

Table 2. R_{2c}^{-1} of $(2x^2+1)(2y^2+1)=z^2-c$, for $-85 \le c \le 85$, $c \ne 0$

c	x	y	z	c	x	y	z	c	x	y	z	c	x	y	z
-85	0	7	4	-50	0	5	1	-8	1	1	1	45	0	3	8
	1	4	4		1	4	7	-5	0	2	2		1	4	12
	4	5	40		2	3	11		1	1	2	46	0	1	7
-82	0	9	9	-48	0	6	5	-3	0	1	0	48	0	0	7
-81	2	6	24		1	3	3	-2	0	1	1		0	4	9
	2	2	0	-47	0	5	2	-1	0	0	0	49	0	5	10
-80	0	8	7	-45	2	2	6	1	0	1	2		3	4	26
	2	2	1	-42	0	5	3	3	0	0	2	54	1	2	9
-77	2	2	2	-41	1	3	4	6	0	1	3		2	3	15
-75	1	6	12		2	4	16	7	0	2	4	55	0	2	8
-74	0	7	5	-37	0	6	6		1	1	4		3	5	32
	1	4	5		3	3	18	8	0	0	3		1	1	8
-73	0	6	0	-35	0	5	4	9	1	2	6	57	3	6	38
-72	0	6	1		1	4	8	13	0	1	4	61	0	1	8
	1	5	9	-33	0	4	0	15	0	0	4	62	0	3	9
	2	4	15	-32	0	4	1	16	0	2	5	63	0	0	8
	2	2	3		1	3	5		1	1	5		2	2	12
	3	3	17		2	2	7	17	0	3	6	64	1	3	11
-71	2	3	10	-29	0	4	2	19	2	2	10		2	4	19
-69	0	6	2	-27	1	2	0	22	0	1	5	67	0	6	10
	3	5	30		2	3	12		1	2	7		4	4	34
-65	0	8	8	-26	0	5	5	24	0	0	5	70	0	5	11
	2	2	4		1	2	1		1	3	9		1	4	13
	4	4	32	-24	0	4	3	25	2	3	14		2	5	23
-64	0	6	3	-23	1	2	2	27	0	2	6	71	0	6	12
-63	0	7	6	-21	1	3	6		2	4	18	72	0	2	9
	1	4	6	-19	0	3	0		1	1	6		1	5	15
-59	2	5	20	-18	0	3	1	30	0	3	7		2	6	27
-57	0	6	4		1	2	3	31	0	4	8		1	1	9
	1	3	0	-17	0	4	4	33	0	1	6	73	1	2	10
-56	1	3	1		2	2	8	35	0	0	6	78	0	1	9
	2	2	5	-15	0	3	2	37	1	2	8	80	0	0	9
-53	1	5	10	-11	1	2	4	39	3	3	20		3	3	21
	1	3	2	-10	0	3	3	40	0	2	7	81	0	3	10
-51	0	5	0	-9	0	2	0		1	1	7		4	5	42
	3	4	24		1	1	0		2	2	11	85	2	3	16
-50	0	7	7	-8	0	2	1	43	1	3	10	82	0	1	9

Note. The solution $(0, \eta, \zeta)$ such that $\zeta + \eta\sqrt{2} = (z_0 + y_0\sqrt{2})(3+2\sqrt{2})^k$, $k \ge 0$, $k \in \mathbb{Z}$ is expressed by $(0, y_0, z_0)$.

By *Theorem 3* we can prove the following analogously.

Theorem 6. *Let* $b = -1$, $c = -1$, *and let* a *be not a square. Then equation (2) has only one solution* $(0, 0, 0)$.

Acknowledgement. The author would like to thank the referee for giving much advice. He made the author a number of proposals for the purpose of making the paper more easily readable. In paticular, *Theorem 1* and its proof as they finally appeared are owed to him. The author also would like to thank *Dr. Shin-ichi Katayama* for suggesting this problem and for giving the idea of permutations on the set of all real or integral solutions. Finally the author would like to thank *John Plant* for checking the English in the paper.

References

1. Kashihara, K.: The diophantain equation $x^2 - 1 = (y^2 - 1)(z^2 - 1)$. Res. Rep. Anan College Tech. **26**, 119–130 (in Japanese) 1990
2. Mordell, L. J.: Diophantain equations. London & New York, Academic Press, 1969
3. Katayama, S. & Kashihara, K.: On the structure of the integer solutions of $z^2 = (x^2 - 1)(y^2 - 1) + a$. J. Math. Tokushima Univ. **24**, 1-11 1990
4. Takagi, T.: Elementary theory of numbers, 2nd ed. Tokyo, Kyoritsu, (in Japanese) 1971
5. Borevich, Z.I. & Shafarevich, I.R.: Number theory. London & New York, Academic Press, 1971
6. Katayama,S.: On Products of Consecutive Integers. Proc. Japan Acad. **66**, Ser.A, No.10, 305-306 1990
7. Kida, Y.: UBASIC 86. Tokyo, Nihonhyoronsha, 1990

Kenji Kashihara
Department of Mathematics
Anan College of Technology
265 Aoki Minobayashi-cho
Anan-shi Tokushima 774 Japan

This article was processed by the author
using the Springer-Verlag TEX mamath macro package 1990.

(Received October 23, 1992;
in revised form May 27, 1993)