ACTA ARITHMETICA
109.2 (2003)

On the solutions of certain diagonal quadratic equations and Lang's conjecture

by

Hizuru Yamagishi (Saitama)

1. Introduction. In this paper, we consider rational solutions of two types of systems of diagonal quadratic equations. First, we describe our motivation for concerning them. The following is Büchi's problem.

Problem 1.1. *Does there exist an algorithm to determine*, *given* $m, n \in \mathbb{N}$, $A = (a_{ij})_{ij} \in M_{m,n}(\mathbb{Z})$, *and* $\mathbf{b} \in \mathbb{Z}^m$, *whether there exist* $x_1, \ldots, x_n \in \mathbb{Z}$ *satisfying the equations*

$$\sum_{j=1}^{n} a_{ij} x_j^2 = b_i, \quad i = 1, \ldots, m\ ?$$

When Problem 1.1 is solved negatively, we immediately have a negative solution to Hilbert's tenth problem. On the other hand, Matiyasevich's work implies a negative answer to Problem 1.1 if we have a solution of the following n square problem (see [1]).

Problem 1.2 (n square problem). *There exists a positive integer* n *such that the set of integral solutions of*

$$x_i^2 - 2x_{i+1}^2 + x_{i+2}^2 = 2, \quad i = 1, \ldots, n-2,$$

coincides with the set of integral solutions of

$$(-1)^{\varepsilon_1} x_1 = (-1)^{\varepsilon_i} x_i - (i-1), \quad i = 2, 3, \ldots, n,$$

where $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n = 0$ *or* 1.

In [1], Paul Vojta showed that the following Conjecture 1.3 on rational points on surfaces of general type implies a solution of the n square problem.

Conjecture 1.3. *Let* X *be a nonsingular projective algebraic variety of general type*, *defined over a number field* k. *Then there exists a proper*

2000 *Mathematics Subject Classification*: 11D09, 14G05.
Supported by JSPS Research Fellowships for Young Scientists and by Grant-in-Aid for JSPS Fellows.

Zariski-closed subset Z of X such that for all number fields K containing k, $X(K)\backslash Z(K)$ is finite.

On the other hand, we showed in [3] that construction of elliptic curves whose Mordell–Weil rank is at least a given positive integer is reduced to finding rational points on certain varieties, and in [2] that Conjecture 1.3 implies the boundedness of Mordell–Weil ranks of a certain family of elliptic curves by connecting a part of results in [1] to the rank problem for elliptic curves. In order to show the latter, we generalized the algebraic varieties in [1]. By using this result and generalizing an argument in [1], we now show that there exist no nontrivial solutions of certain types of systems of equations.

In Sections 2 and 3, we describe our systems of equations and the theorem related to their solutions.

2. Certain systems of Diophantine equations. Let k be a number field. Let $\{\alpha_i\}$ $(i = 0, 1, 2, \ldots)$ be an infinite sequence of elements of k. Let $d_{(i,j)} = \alpha_i - \alpha_j$ for any pair (i, j), and $d_i = d_{(i+1,i)}$. We assume that

(i) $\alpha_i \neq \alpha_j$ (if $i \neq j$),
(ii) $\alpha_0 = 0$,
(iii) the sequence $\{d_i\}$ is cyclic with period $m \geq 1$.

Let $X_n \in \mathbb{P}^n$ be a variety defined by the equations

$$d_{i+1}x_i^2 - d_{(i+2,i)}x_{i+1}^2 + d_i x_{i+2}^2 = d_i d_{i+1} d_{(i+2,i)} x_0^2, \qquad i = 1, \ldots, n-2, \tag{1}$$

and let L_n be the union of 2^n lines (called *trivial lines*) defined by the equations

$$(-1)^{\varepsilon_1} x_1 = (-1)^{\varepsilon_i} x_i - d_{(i,1)} x_0, \qquad i = 2, \ldots, n, \qquad \varepsilon_1, \ldots, \varepsilon_n = 0 \text{ or } 1. \tag{2}$$

Note that $L_n \subset X_n$. For (1) is expressed as

$$\begin{vmatrix} 0 & 1 & 1 & 1 \\ 0 & \alpha_i & \alpha_{i+1} & \alpha_{i+2} \\ 1 & \alpha_i^2 & \alpha_{i+1}^2 & \alpha_{i+2}^2 \\ x_0^2 & x_i^2 & x_{i+1}^2 & x_{i+2}^2 \end{vmatrix} = 0, \qquad i = 1, \ldots, n-2 \tag{3}$$

(expand along the last row), and points on (2) are expressed as

$$\begin{cases} x_0 = s, \quad x_1 = (-1)^{\varepsilon_1} t, \\ (-1)^{\varepsilon_i} x_i = t + d_{(i,1)} s, \quad i = 2, 3, \ldots, n, \end{cases} \tag{4}$$

where $(s, t) \in \mathbb{P}^1$. Now $x_i^2 = (t + d_{(i,1)}s)^2 = (s\alpha_1 - t)^2 - 2s(\alpha_1 s - t)\alpha_i + s^2\alpha_i^2$ $(i = 1, \ldots, n)$. Substitute (4) for x_i in (3), and add $-(s\alpha_1 - t)^2 \times$ (the first row), $2s(\alpha_1 s - t) \times$ (the second row), and $-s^2 \times$ (the third row) to the fourth row. Then the determinant is 0.

THEOREM 2.1. *If there exists an integer* $n_0 \geq 8$ *such that Conjecture* 1.3 *holds for* $X_{n_0}(k)$, *then there exists an integer* $n \geq n_0$ *such that the set of rational points on* X_n *coincides with the set of rational points on* L_n.

REMARK 2.2. The main theorem (Theorem 0.5) of [1] concerns the case $\alpha_i = i$.

Proof of Theorem 2.1. Let g_i $(i = 1, \ldots, n-2)$ be the left hand side of (3). Put $\alpha_i = 1/\beta_i$, $x_i = Y_i/\beta_i$ $(i = 1, \ldots, n)$, $\beta_0 = \alpha_0$, $x_0 = Y_0$. Then (3) becomes

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \beta_0 & \beta_i & \beta_{i+1} & \beta_{i+2} \\ \beta_0^2 & \beta_i^2 & \beta_{i+1}^2 & \beta_{i+2}^2 \\ Y_0^2 & Y_i^2 & Y_{i+1}^2 & Y_{i+2}^2 \end{vmatrix} = 0, \qquad i = 1, \ldots, n-2. \tag{5}$$

By an argument similar to that in [2], we see that for integers $n \geq 8$, the only curves on X_n of genus 0 or 1 are the 2^n lines defined by (2).

Next, let $n_0 \geq 8$ be an integer such that Conjecture 1.3 holds for $X_{n_0}(k)$. Then the number m_0 of rational points on $X_{n_0} - L_{n_0}$ is finite. Let $\bar{i}$ be the remainder of an integer i modulo m. Then $d_{\bar{i}} = \alpha_{i+1} - \alpha_i$ for any i by assumption (iii). We show that all k-rational points on $X_{n_0+m_0m}$ are on a trivial line or $x_0 = 0$. Note that if $\overline{i-j} = 0$ then the equations $g_i = 0$ and $g_j = 0$ are the same equations.

For any i with $0 \leq i \leq m_0$, the projection map $\Phi_i : \mathbb{P}^{n_0+m_0m} \to \mathbb{P}^{n_0}$ defined by

$$(x_0, x_1, x_2, \ldots, x_{n_0+m_0m}) \mapsto (x_0, x_{1+im}, x_{2+im}, \ldots, x_{n_0+im})$$

$(i = 0, 1, \ldots, m_0)$ restricts to a morphism $\phi_i : X_{n_0+m_0m} \to X_{n_0}$. Let $X_{n,\,x_0=0} = \{(x_i) \in X_n; x_0 = 0\}$. Then one can check that

$$\phi_i^{-1}(L_{n_0}) \subset L_{n_0+m_0m}, \qquad \phi_i^{-1}(X_{n_0,\,x_0=0}) \subset X_{n_0+m_0m,\,x_0=0}.$$

Let $W_n = X_n - L_n \cup X_{n,\,x_0=0}$. Then it follows that $\phi_i(W_{n_0+m_0m}) \subset W_{n_0}$. We show that $W_{n_0+m_0m}(k) = \emptyset$. Suppose, on the contrary, that $W_{n_0+m_0m}(k) \neq \emptyset$ and let $P = (x_0, x_1, \ldots, x_{n_0+m_0m}) \in W_{n_0+m_0m}(k)$. We will show that the $m_0 + 1$ points $\phi_i(P)$ $(i = 0, 1, \ldots, m_0)$ are all distinct. This contradicts the assumption on m_0. Suppose that there exist integers u, v $(0 \leq u < v \leq m_0)$ such that $\phi_u(P) = \phi_v(P)$. Then

$$x_{1+um}^2 = x_{1+vm}^2 \quad \text{and} \quad x_{2+um}^2 = x_{2+vm}^2.$$

Since the coefficients of g_{um} and g_{vm} coincide, these equalities imply $x_{um}^2 = x_{vm}^2$. This in turn implies $x_{um-1}^2 = x_{vm-1}^2$. Hence by downward induction we see that

$$x_1^2 = x_{l+1}^2,$$
$$x_2^2 = x_{l+2}^2,$$
$$\vdots$$

where $l = (v-u)m$. Then

$$\begin{cases} g_i(x_0, x_i, x_{i+1}, x_{i+2}) = 0, & i = 1, \dots, l-2, \\ g_{l-1}(x_0, x_{l-1}, x_l, x_1) = 0, \\ g_l(x_0, x_l, x_1, x_2) = 0. \end{cases}$$

Dividing both sides of $g_i = 0$ $(i = 1, \dots, l)$ by $d_i d_{i+1} x_0^2$, and letting $y_i = (x_i/x_0)^2$ $(i = 1, \dots, l)$, we obtain a system of linear equations in $y_1, \dots, y_l$ of the form

$$(6) \qquad Ay = b, \quad y = {}^{\mathrm{t}}(y_1, \dots, y_l), \quad b = {}^{\mathrm{t}}(b_1, \dots, b_l),$$

where $A = (a_{i,j})_{1 \le i,j \le l}$ with

$$\begin{aligned} &a_{i,i} = \frac{1}{d_i}, \quad a_{i,i+1} = -\frac{d_{(i+2,i)}}{d_i d_{i+1}}, \quad a_{i,i+2} = \frac{1}{d_{i+1}}, \quad i = 1, \dots, l-2, \\ &a_{l-1,1} = \frac{1}{d_l}, \quad a_{l-1,l-1} = \frac{1}{d_{l-1}}, \quad a_{l-1,l} = -\frac{d_{(l+1,l-1)}}{d_{l-1} d_l}, \\ &a_{l,1} = -\frac{d_{(l+2,l)}}{d_l d_{l+1}}, \quad a_{l,2} = \frac{1}{d_{l+1}}, \quad a_{l,l} = \frac{1}{d_l}, \\ &a_{i,j} = 0 \quad \text{for other } i, j, \\ &b_i = d_{(i+2,i)}, \quad i = 1, \dots, l. \end{aligned}$$

Since the sum of the columns of A is the 0-vector, the rank of A is less than l. Let C be the matrix obtained from A by replacing the lth column by b, that is,

$$\begin{pmatrix} \frac{1}{d_1} & -\frac{d_{(3,1)}}{d_1 d_2} & \frac{1}{d_2} & 0 & \dots & 0 & 0 & 0 & d_{(3,1)} \\ 0 & \frac{1}{d_2} & -\frac{d_{(4,2)}}{d_2 d_3} & \frac{1}{d_3} & \dots & 0 & 0 & 0 & d_{(4,2)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \dots & \frac{1}{d_{l-3}} & -\frac{d_{(l-1,l-3)}}{d_{l-3} d_{l-2}} & \frac{1}{d_{l-2}} & d_{(l-1,l-3)} \\ 0 & 0 & 0 & 0 & \dots & 0 & \frac{1}{d_{l-2}} & -\frac{d_{(l,l-2)}}{d_{l-2} d_{l-1}} & d_{(l,l-2)} \\ \frac{1}{d_l} & 0 & 0 & 0 & \dots & 0 & 0 & \frac{1}{d_{l-1}} & d_{(l+1,l-1)} \\ -\frac{d_{(l+2,l)}}{d_l d_{l+1}} & \frac{1}{d_{l+1}} & 0 & 0 & \dots & 0 & 0 & 0 & d_{(l+2,l)} \end{pmatrix}.$$

We compute the determinant of C. We add the first, second, $\dots$, and $(l-1)$th row to the lth row. Noting that

$$d_{l+1} = d_1, \quad d_{(l+1,1)} = d_{(l+2,2)},$$

we find that the lth row is

$$(0, 0, \ldots, 0, 2d_{(l+1,1)}).$$

Expanding the determinant of C along the lth column, we find that it is $2d_{(l+1,1)}$ times

$$\begin{vmatrix} \frac{1}{d_1} & -\frac{d_{(3,1)}}{d_1 d_2} & \frac{1}{d_2} & 0 & \ldots & 0 & 0 & 0 \\ 0 & \frac{1}{d_2} & -\frac{d_{(4,2)}}{d_2 d_3} & \frac{1}{d_3} & \ldots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \ldots & \frac{1}{d_{l-3}} & -\frac{d_{(l-1,l-3)}}{d_{l-3} d_{l-2}} & \frac{1}{d_{l-2}} \\ 0 & 0 & 0 & 0 & \ldots & 0 & \frac{1}{d_{l-2}} & -\frac{d_{(l,l-2)}}{d_{l-2} d_{l-1}} \\ \frac{1}{d_l} & 0 & 0 & 0 & \ldots & 0 & 0 & \frac{1}{d_{l-1}} \end{vmatrix}.$$

Expanding this along the first column, we see that

$$|C| = 2d_{(l+1,1)} \left(\frac{1}{d_1 \ldots d_{l-1}} + (-1)^l \frac{1}{d_l} D(l-2) \right)$$

where $D(l-2)$ is the determinant

$$\begin{vmatrix} -\frac{d_{(3,1)}}{d_1 d_2} & \frac{1}{d_2} & 0 & \ldots & 0 & 0 & 0 \\ \frac{1}{d_2} & -\frac{d_{(4,2)}}{d_2 d_3} & \frac{1}{d_3} & \ldots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \ldots & \frac{1}{d_{l-3}} & -\frac{d_{(l-1,l-3)}}{d_{l-3} d_{l-2}} & \frac{1}{d_{l-2}} \\ 0 & 0 & 0 & \ldots & 0 & \frac{1}{d_{l-2}} & -\frac{d_{(l,l-2)}}{d_{l-2} d_{l-1}} \end{vmatrix}$$

$$= \begin{vmatrix} -\frac{1}{d_1} - \frac{1}{d_2} & \frac{1}{d_2} & 0 & \ldots & 0 & 0 & 0 \\ \frac{1}{d_2} & -\frac{1}{d_2} - \frac{1}{d_3} & \frac{1}{d_3} & \ldots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \ldots & \frac{1}{d_{l-3}} & -\frac{1}{d_{l-3}} - \frac{1}{d_{l-2}} & \frac{1}{d_{l-2}} \\ 0 & 0 & 0 & \ldots & 0 & \frac{1}{d_{l-2}} & -\frac{1}{d_{l-2}} - \frac{1}{d_{l-1}} \end{vmatrix}.$$

(Note that $d_{(i+2,\,i)} = d_i + d_{i+1}$ for any i.) This determinant can be simplified as follows.

LEMMA 2.3.

$$D(l) = (-1)^l \frac{d_1 + d_2 + \ldots + d_{l+1}}{d_1 d_2 \ldots d_{l+1}}.$$

Proof. We prove this by induction. If $l = 1$, then

$$D(1) = -\frac{1}{d_1} - \frac{1}{d_2} = -\frac{d_1 + d_2}{d_1 d_2}.$$

Assume that the lemma holds for $l - 1 \geq 1$. Then

$$D(l) = \begin{vmatrix} -\frac{1}{d_1} - \frac{1}{d_2} & \frac{1}{d_2} & 0 & \dots & 0 & 0 & 0 \\ \frac{1}{d_2} & -\frac{1}{d_2} - \frac{1}{d_3} & \frac{1}{d_3} & \dots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \dots & \frac{1}{d_{l-1}} & -\frac{1}{d_{l-1}} - \frac{1}{d_l} & \frac{1}{d_l} \\ 0 & 0 & 0 & \dots & 0 & \frac{1}{d_l} & -\frac{1}{d_l} - \frac{1}{d_{l+1}} \end{vmatrix}.$$

Add the first, second, ..., $(l-1)$th column to the lth column of $M(l)$ to obtain

$$D(l) = \begin{vmatrix} -\frac{1}{d_1} - \frac{1}{d_2} & \frac{1}{d_2} & 0 & \dots & 0 & 0 & -\frac{1}{d_1} \\ \frac{1}{d_2} & -\frac{1}{d_2} - \frac{1}{d_3} & \frac{1}{d_3} & \dots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \dots & \frac{1}{d_{l-1}} & -\frac{1}{d_{l-1}} - \frac{1}{d_l} & 0 \\ 0 & 0 & 0 & \dots & 0 & \frac{1}{d_l} & -\frac{1}{d_{l+1}} \end{vmatrix}.$$

Expanding along the lth column yields

$$\begin{aligned} D(l) &= (-1)^l \frac{1}{d_1 d_2 \dots d_l} - \frac{1}{d_{l+1}} D(l-1) \\ &= (-1)^l \frac{1}{d_1 d_2 \dots d_l} - (-1)^{l-1} \frac{d_1 + d_2 + \dots + d_l}{d_1 d_2 \dots d_{l+1}} \\ &\qquad\qquad\qquad\qquad\text{(by induction assumption)} \\ &= (-1)^l \frac{d_1 + d_2 + \dots + d_{l+1}}{d_1 d_2 \dots d_{l+1}}. \ \blacksquare \end{aligned}$$

By Lemma 2.3, it follows that

$$\begin{aligned} |C| &= 2d_{(l+1,1)} \left(\frac{1}{d_1 d_2 \dots d_{l-1}} + (-1)^l \frac{1}{d_l} (-1)^{l-2} \frac{d_{(l,1)}}{d_1 d_2 \dots d_{l-1}} \right) \\ &= 2d_{(l+1,1)} \frac{d_l + d_{(l,1)}}{d_1 d_2 \dots d_{l-1}} = \frac{2d_{(l+1,1)}^2}{d_1 d_2 \dots d_{l-1}} \neq 0. \end{aligned}$$

Hence the rank of C is l. So $\operatorname{rank}(A) < \operatorname{rank}(C)$, which implies that there exist no solutions of (6). Therefore $\phi_i(P) \neq \phi_j(P)$ $(i \neq j)$. ■

3. Other systems of Diophantine equations. In this section, we consider another kind of systems of Diophantine equations. Notation is the same as in Section 2, i.e. k is a number field, $d_{(i,j)} = \alpha_i - \alpha_j$ for any pair (i,j), and $d_i = d_{(i+1,i)}$. Let $\{\alpha_i\}$ $(i = 0, 1, 2, \dots)$ be an infinite sequence of elements of k such that

(i) $\alpha_i \neq \alpha_j$ (if $i \neq j$),
(ii) $\alpha_0 = 1$,
(iii) the sequence $\{\alpha_{i+1}/\alpha_i\}$ is cyclic with period $m \geq 1$.

Let X_n be a variety defined by the equations

$$(7)\quad \alpha_{i+1}\alpha_{i+2}d_{i+1}x_i^2 - \alpha_i\alpha_{i+2}d_{(i+2,i)}x_{i+1}^2 + \alpha_i\alpha_{i+1}d_ix_{i+2}^2 = d_id_{i+1}d_{(i+2,i)}x_0^2, \quad i = 1, \ldots, n-2,$$

and L_n be the union of 2^n lines (called *trivial lines*) defined by the equations

$$(8)\quad (-1)^{\varepsilon_1}\alpha_ix_1 = (-1)^{\varepsilon_i}\alpha_1x_i - d_{(i,1)}x_0, \quad i = 2, 3, \ldots, n, \quad \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n = 0 \text{ or } 1.$$

THEOREM 3.1. *If there exists an integer* $n_0 \geq 8$ *such that Conjecture* 1.3 *holds for* $X_{n_0}(k)$, *then there exists an integer* $n \geq n_0$ *such that the set of rational points on* X_n *coincides with the set of rational points on* L.

Proof. Note that (7) is expressed as

$$(9)\quad \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & \alpha_i & \alpha_{i+1} & \alpha_{i+2} \\ 0 & \alpha_i^2 & \alpha_{i+1}^2 & \alpha_{i+2}^2 \\ x_0^2 & x_i^2 & x_{i+1}^2 & x_{i+2}^2 \end{vmatrix} = 0, \quad i = 1, \ldots, n-2$$

(expand along the last row). Let g_i $(i = 1, \ldots, n-2)$ be the left hand side of (9). Notation being as in the proof of Theorem 2.1, suppose that there exists a $P = (x_0, x_1, \ldots, x_{n_0+m_0m}) \in W_{n_0+m_0m}(k)$. We show that the m_0+1 points $\phi_i(P)$ are all distinct. By an argument similar to that in the proof of Theorem 2.1, we obtain again the equations

$$(10)\quad \begin{cases} g_i(x_0, x_i, x_{i+1}, x_{i+2}) = 0, & i = 1, \ldots, l-2, \\ g_{l-1}(x_0, x_{l-1}, x_l, x_1) = 0, \\ g_l(x_0, x_l, x_1, x_2) = 0. \end{cases}$$

Dividing the both sides of $g_i = 0$ $(i = 1, \ldots, l)$ by $\alpha_{i+1}\alpha_{i+2}x_0^2$, and letting $y_i = (x_i/x_0)^2$ $(i = 1, \ldots, l)$, we obtain a system of linear equations in $y_1, \ldots, y_l$ of the form

$$(11)\quad Ay = b, \quad y = {}^{\mathrm{t}}(y_1, \ldots, y_l), \quad b = {}^{\mathrm{t}}(b_1, \ldots, b_l),$$

where $A = (a_{i,j})_{1\leq i,j\leq l}$ with

$$a_{i,i} = d_{i+1}, \quad a_{i,i+1} = -\frac{d_{(i+2,i)}\alpha_i}{\alpha_{i+1}}, \quad a_{i,i+2} = \frac{d_i\alpha_i}{\alpha_{i+2}}, \quad i = 1, \ldots, l-2,$$

$$a_{l-1,1} = \frac{d_{l-1}\alpha_{l-1}}{\alpha_{l+1}}, \quad a_{l-1,l-1} = d_l, \quad a_{l-1,l} = -\frac{d_{(l+1,l-1)}\alpha_{l-1}}{\alpha_l},$$

$$a_{l,1} = -\frac{d_{(l+2,l)}\alpha_l}{\alpha_{l+1}}, \quad a_{l,2} = \frac{d_l\alpha_l}{\alpha_{l+2}}, \quad a_{l,l} = d_{l+1},$$

$$a_{i,j} = 0 \quad \text{for other } i, j,$$

$$b_i = \frac{d_i d_{i+1} d_{(i+2,i)}}{\alpha_{i+1}\alpha_{i+2}}, \quad i = 1, \ldots, l.$$

We compute the determinant of A. Factoring the common factor α_i out of the ith row, we have

$$|A| = \alpha_1 \ldots \alpha_l \times \begin{vmatrix} \frac{d_2}{\alpha_1} & -\frac{d_{(3,1)}}{\alpha_2} & \frac{d_1}{\alpha_3} & 0 & \ldots & 0 & 0 & 0 \\ 0 & \frac{d_3}{\alpha_2} & -\frac{d_{(4,2)}}{\alpha_3} & \frac{d_2}{\alpha_4} & \ldots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \ldots & \frac{d_{l-1}}{\alpha_{l-2}} & -\frac{d_{(l,l-2)}}{\alpha_{l-1}} & \frac{d_{l-2}}{\alpha_l} \\ \frac{d_{l-1}}{\alpha_{l+1}} & 0 & 0 & 0 & \ldots & 0 & \frac{d_l}{\alpha_{l-1}} & -\frac{d_{(l+1,l-1)}}{\alpha_l} \\ -\frac{d_{(l+2,l)}}{\alpha_{l+1}} & \frac{d_l}{\alpha_{l+2}} & 0 & 0 & \ldots & 0 & 0 & \frac{d_{l+1}}{\alpha_l} \end{vmatrix}.$$

Factoring the common factor $1/\alpha_i$ out of the ith column shows that $|A|$ equals

$$\begin{vmatrix} d_2 & -d_{(3,1)} & d_1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & d_3 & -d_{(4,2)} & d_2 & \ldots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \ldots & d_{l-1} & -d_{(l,l-2)} & d_{l-2} \\ \frac{d_{l-1}\alpha_1}{\alpha_{l+1}} & 0 & 0 & 0 & \ldots & 0 & d_l & -d_{(l+1,l-1)} \\ -\frac{d_{(l+2,l)}\alpha_1}{\alpha_{l+1}} & \frac{d_l\alpha_2}{\alpha_{l+2}} & 0 & 0 & \ldots & 0 & 0 & d_{l+1} \end{vmatrix}.$$

Noting that $\frac{\alpha_1}{\alpha_{l+1}} = \frac{\alpha_2}{\alpha_{l+2}} \left(= \frac{1}{\alpha_l}\right)$, and letting r be this value, we add the first, second, $\ldots$, and $(l-1)$th column to the lth column to find that

$$|A| = \begin{vmatrix} d_2 & -d_{(3,1)} & d_1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & d_3 & -d_{(4,2)} & d_2 & \ldots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \ldots & d_{l-1} & -d_{(l,l-2)} & 0 \\ d_{l-1}r & 0 & 0 & 0 & \ldots & 0 & d_l & d_{l-1}(r-1) \\ -d_{(l+2,l)}r & d_l r & 0 & 0 & \ldots & 0 & 0 & -d_{l+1}(r-1) \end{vmatrix}$$

$$= (r-1)\begin{vmatrix} d_2 & -d_{(3,1)} & d_1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & d_3 & -d_{(4,2)} & d_2 & \ldots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \ldots & d_{l-1} & -d_{(l,l-2)} & 0 \\ d_{l-1}r & 0 & 0 & 0 & \ldots & 0 & d_l & d_{l-1} \\ -d_{(l+2,l)}r & d_l r & 0 & 0 & \ldots & 0 & 0 & -d_{l+1} \end{vmatrix}.$$

Adding the lth column $\times (-r)$ to the first column shows that

$$|A| = (r-1)\begin{vmatrix} d_2 & -d_{(3,1)} & d_1 & 0 & \dots & 0 & 0 & 0 \\ 0 & d_3 & -d_{(4,2)} & d_2 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & d_{l-1} & -d_{(l,l-2)} & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & d_l & d_{l-1} \\ -d_l r & d_l r & 0 & 0 & \dots & 0 & 0 & -d_{l+1} \end{vmatrix}$$

$$= (r-1)\begin{vmatrix} d_2 & -d_1 & d_1 & 0 & \dots & 0 & 0 & 0 \\ 0 & d_3 & -d_{(4,2)} & d_2 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & d_{l-1} & -d_{(l,l-2)} & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & d_l & d_{l-1} \\ -d_l r & 0 & 0 & 0 & \dots & 0 & 0 & -d_{l+1} \end{vmatrix}$$

(add the first column to the second).

We similarly repeat adding the ith column ($i = 2, 3, \dots, l-2$) to the $(i+1)$th column to obtain

$$|A| = (r-1)\begin{vmatrix} d_2 & -d_1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & d_3 & -d_2 & 0 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & d_{l-1} & -d_{l-2} & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & d_l & d_{l-1} \\ -d_l r & 0 & 0 & 0 & \dots & 0 & 0 & -d_{l+1} \end{vmatrix}.$$

Expanding along the first column gives

$$\begin{aligned} |A| &= (r-1)(-d_2 \dots d_{l+1} + (-1)^{l+1}(-d_l r)(-1)^l d_1 \dots d_{l-1}) \\ &= (r-1) d_2 \dots d_l(-d_{l+1} + d_1 r) \\ &= (r-1) d_2 \dots d_l(-d_1/r + d_1 r) \\ &= d_1 \dots d_l (r-1)^2 (r+1)/r. \end{aligned}$$

Since $\alpha_l^2 = \alpha_{2l} \neq \alpha_0 = 1$, we have $\alpha_l \neq \pm 1$. So $|A| \neq 0$. Therefore (11) has unique solution. On the other hand,

$$y = {}^{\mathrm{t}}(y_1, y_2, \dots, y_l) = {}^{\mathrm{t}}(1, 1, \dots, 1)$$

is a solution of (11). Therefore the solutions of (10) are

$$(x_0, x_1, \dots, x_l) = (1, \pm 1, \pm 1, \dots, \pm 1),$$

and hence

$$(x_0, x_{1+im}, \dots, x_{n_0+im}) = (1, \pm 1, \pm 1, \dots, \pm 1).$$

Because every point of these is on L_{n_0}, it cannot be equal to $\phi_i(P)$. Therefore $\phi_i(P) \neq \phi_j(P)$ $(i \neq j)$. ∎

References

[1] P. Vojta, *Diagonal quadratic forms and Hilbert's tenth problem*, in: Contemp. Math. 270, Amer. Math. Soc., Providence, RI, 2000, 261–274.

[2] H. Yamagishi, *Boundedness of Mordell–Weil ranks of certain elliptic curves and Lang's conjecture*, preprint.

[3] —, *A unified method of construction of elliptic curves with high Mordell–Weil rank*, Pacific J. Math. 191 (1999), 189–200.

Department of Natural Sciences
Tokyo Denki University
Hatoyama, Saitama, 350-0394, Japan
E-mail: hizuru@u.dendai.ac.jp

Received on 5.4.2002
and in revised form on 5.8.2002 (4257)