Pacific Journal of Mathematics

ON ELLIPTIC CURVES OF RANK FOUR WITH THREE-DIVISION RATIONAL POINT

Hizuru Yamagishi

Volume 206 No. 1 September 2002

PACIFIC JOURNAL OF MATHEMATICS
Vol. 206, No. 1, 2002

ON ELLIPTIC CURVES OF RANK FOUR WITH THREE-DIVISION RATIONAL POINT

Hizuru Yamagishi

A universal family of elliptic curves of rank 4 with 3-division rational points is constructed. The base space is shown to be an elliptic $K3$ surface whose group of sections is of infinite order. Thus we obtain infinitely many such elliptic curves with mutually distinct j-invariants.

1. Introduction.

In [**5**], we have reduced the problem of constructing elliptic curves of rank n ($n \geq 1$) with generators to the problem of finding rational points on a certain variety V_n using the theory of twist. Moreover we have obtained all elliptic curves of at least rank n ($1 \leq n \leq 7$), by parametrizing all rational points on V_n.

The aim of this paper is to construct a universal family of elliptic curves of at least rank 4 with 3-division rational points by applying our previous results. When we treat such problems, it seems that the condition, existence of a 3-division rational point, is classified as a special type. Therefore this condition is one of the characteristics of this paper. Furthermore, by the universality of V_4, the extra condition for elliptic curves to have 3-division rational points should give rise to a subvariety of V_4. Our results will determine the structure of the subvariety W_4 quite explicitly. More precisely we will see that W_4 is a $K3$ surface with many lines on it. Using these lines, we can provide W_4 with a structure of elliptic surface and we find the rank of the group of its sections is at least 1. Thus we obtain a universal family of elliptic curves with 3-division rational points whose rank is at least 4, which is prametrized by an elliptic $K3$ surface with infinitely many rational curves. By universal family we mean that every elliptic curve of rank 4 with a 3-division rational point *is* a member of our family. We are aware that there are several attempts to construct some examples of such elliptic curves. But the universal nature of our result assures us that any such examples live in our family.

This paper is organized as follows.

In Section 2, we review the theory of twist and the defining equation of the base space in the case of rank ≥ 5 in [**5**].

In Section 3, the equation of the base space for the case of rank 4 is derived from that for the case of rank 5. It is shown to be rational threefold and its rational points are parametrized.

In Section 4, we determine the subvariety of the base space, which corresponds to the elliptic curves with nontrivial 3-division point. We show that it has the structure of an elliptic surface of rank ≥ 1.

In the final Section 5, we construct an example of an elliptic curve of rank ≥ 4 with 3-division rational point by our method.

2. Twist.

We recall the theory of twist developed in [**5**]. Let E be an elliptic curve over a number field k defined by the equation:

$$E:\ y^2 = ax^3 + bx^2 + cx + d, \tag{1}$$

and let $f(x)$ be the right hand side of (1). For integers $n \geq 2$, let V_n be the variety defined by the equations

$$V_n:\ y_i^2 = f(x_1)f(x_{i+1}), \qquad i = 1, \ldots, n-1.$$

Since V_n is birational to the quotient variety of E^n by the action of $(-id, \ldots, -id)$, the degree of the field extension $k(E^n)/k(V_n)$ is equal to 2. The following result is fundamental.

Theorem 2.1 ([**2**, §4])**.** *Let $E_{f(x_1)}$ denote the quadratic twist of E associated to the extension $k(E^n)/k(V_n)$. Suppose $End_k(E) \cong \mathbb{Z}$. Then the defining equation of $E_{f(x_1)}$ is given by*

$$E_{f(x_1)}:\ f(x_1)y^2 = f(x),$$

and the rank of $E_{f(x_1)}(k(V_n))$ is n. Its generators are given by $(x_1, 1)$, $(x_{i+1}, y_i/f(x_1))$ $(i = 1, \ldots, n-1)$.

By Theorem 3.1 in [**5**], any given elliptic curve of rank n is obtained by specialization at a certain rational point on V_n.

In order to investigate the rational points on V_n, we put $x_i = \alpha_{i-1}$ $(i = 1, \ldots, n)$, and we regard them as independent variables. We denote $k(\alpha_0, \ldots, \alpha_{n-1})$ by K and regard V_n as a variety over K. Then for $n \geq 5$, V_n is expressed as follows.

Theorem 2.2 ([**5**] Theorem 3.6)**.** *For $n \geq 5$, V_n is K-birational to the variety over K defined by the equations*

$$\begin{vmatrix} 1 & 1 & 1 & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_i \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_i^2 \\ \alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & \alpha_i^3 \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 & Y_i^2 \end{vmatrix} = 0, \qquad i = 4, \ldots, n-1$$

in the projective $(n-1)$*-space* $\mathbb{P}^{n-1}$ *with coordinate* $(Y_0, \ldots, Y_{n-1})$.

3. On the base space of generic family of rank 4.

In [**5**], there are marked differences between the way of treating with V_4 and that of V_n $(n \geq 5)$. But for our purpose, it is convenient to express V_4 in a similar form to V_n $(n \geq 5)$.

Theorem 3.1. *V_4 is K-birational to $\mathbb{P}^3$. More precisely the K-rational points on V_4 are parametrized by the coordinate $(Y_0,\ Y_1,\ Y_2,\ Y_3)$ of $\mathbb{P}^3$ as follows:*

$$(a,\ b,\ c,\ d,\ y_1,\ y_2,\ y_3) = (\bar{a},\ \bar{b},\ \bar{c},\ \bar{d},\ \bar{e}Y_0Y_1,\ \bar{e}Y_0Y_2,\ \bar{e}Y_0Y_3)$$

$$\textit{where}\ \ \bar{a} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 \end{vmatrix},\ \ \bar{b} = -\begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 \end{vmatrix},$$

$$\bar{c} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \\ \alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 \end{vmatrix},\ \ \bar{d} = -\begin{vmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \\ \alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 \end{vmatrix},$$

$$\bar{e} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \\ \alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 \end{vmatrix}.$$

Proof. It is enough to show that the existence of the birational map of V_4 to $\mathbb{P}^3$. Let φ be the map of V_4 to $\mathbb{P}^3$ given by

$$(a,\ b,\ c,\ d,\ y_1,\ y_2,\ y_3) \mapsto (f(\alpha_0),\ y_1,\ y_2,\ y_3),$$

and ψ be of $\mathbb{P}^3$ to V_4 given by

$$(Y_0,\ Y_1,\ Y_2,\ Y_3) \mapsto (\bar{a},\ \bar{b},\ \bar{c},\ \bar{d},\ \bar{e}Y_0Y_1,\ \bar{e}Y_0Y_2,\ \bar{e}Y_0Y_3).$$

For any element $(a,\ b,\ c,\ d,\ y_1,\ y_2,\ y_3) \in V_4$,

$$\begin{aligned}
&\psi \circ \varphi(a,\ b,\ c,\ d,\ y_1,\ y_2,\ y_3)\\
&= \psi(f(\alpha_0),\ y_1,\ y_2,\ y_3)\\
&= \left(\begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \\ f(\alpha_0)^2 & y_1^2 & y_2^2 & y_3^2 \end{vmatrix}, \begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 \\ f(\alpha_0)^2 & y_1^2 & y_2^2 & y_3^2 \end{vmatrix}, \right.\\
&\qquad \begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \\ \alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 \\ f(\alpha_0)^2 & y_1^2 & y_2^2 & y_3^2 \end{vmatrix}, \begin{vmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \\ \alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 \\ f(\alpha_0)^2 & y_1^2 & y_2^2 & y_3^2 \end{vmatrix},\\
&\qquad \left. f(\alpha_0)\bar{e}y_1,\ f(\alpha_0)\bar{e}y_2,\ f(\alpha_0)\bar{e}y_3 \right).
\end{aligned}$$

Note that $y_i^2 = f(\alpha_0)f(\alpha_i)$ $(i = 1,\ 2,\ 3)$, and divide each coordinate by $f(\alpha_0)\bar{e}$. Then the first-coordinate of this becomes

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \\ f(\alpha_0) & f(\alpha_1) & f(\alpha_2) & f(\alpha_3) \end{vmatrix} \times \frac{1}{\bar{e}}. \tag{2}$$

Adding $(-b \times (\text{the third row}) - c \times (\text{the second row}) - d \times (\text{the first row}))$ to the fourth row of the matrix of the determinant in (2), we find the value of (2) to be equal to a. By a similar row transformation the i-th coordinate $(i = 2,\ 3,\ 4)$ becomes $b,\ c,\ d$, respectively, so $\psi \circ \varphi = id_{V_4}$. Conversely for any element $(Y_0,\ Y_1,\ Y_2,\ Y_3) \in \mathbb{P}^3$,

$$\begin{aligned}
&\varphi \circ \psi(Y_0,\ Y_1,\ Y_2,\ Y_3)\\
&= \varphi(\bar{a},\ \bar{b},\ \bar{c},\ \bar{d},\ \bar{e}Y_0Y_1,\ \bar{e}Y_0Y_2,\ \bar{e}Y_0Y_3)\\
&= (\bar{a}{\alpha_0}^3 + \bar{b}{\alpha_0}^2 + \bar{c}\alpha_0 + \bar{d},\ \bar{e}Y_0Y_1,\ \bar{e}Y_0Y_2,\ \bar{e}Y_0Y_3).
\end{aligned} \tag{3}$$

Since $\bar{e}{Y_0}^2 = \bar{a}{\alpha_0}^3 + \bar{b}{\alpha_0}^2 + \bar{c}\alpha_0 + \bar{d}$, the rightmost side of (3) is $(\bar{e}Y_0^2,\ \bar{e}Y_0Y_1,\ \bar{e}Y_0Y_2,\ \bar{e}Y_0Y_3)$. It means that $\varphi \circ \psi = id_{\mathbb{P}^3}$. Consequently these maps are inverse to each other.

It follows from this theorem that the equation of the elliptic curve which corresponds to a point $(Y_0,\ Y_1,\ Y_2,\ Y_3) \in \mathbb{P}^3$ is given by

$$\bar{e}y^2 = \bar{a}x^3 + \bar{b}x^2 + \bar{c}x + \bar{d}, \tag{4}$$

and that the coordinates of four rational points on it are $(\alpha_i,\ Y_i)$ $(i = 0,\ 1,\ 2,\ 3)$. One can check this fact easily by tracing the map ψ. Moreover we recall the following result which shows the universality of the variety V_4:

Theorem 3.2. *Any elliptic curve over k with four k-rational points comes from a k-rational point of V_4.*

4. Base space of the family of rank 4 with three-division rational point.

The equation of an elliptic curve with 3-division rational points is expressed in general as

$$y^2 = ax^3 + (bx + c)^2, \tag{5}$$

where the coordinate of a 3-division point is $(0,\ c)$. Therefore the condition that the elliptic curve defined by (4) has a 3-division rational point is

$$\bar{b}/\bar{e} = Z_1^2,\ \bar{c}/\bar{e} = 2Z_1Z_2,\ \bar{d}/\bar{e} = Z_2^2. \tag{6}$$

This is transformed as follows.

Lemma 4.1. *The variety W defined by Equation* (6) *is a $K3$ surface.*

Moreover this is K-birational to the elliptic surface W_4 over $\mathbb{P}^1$ with coordinate $(\lambda,\ \mu)$ defined by the following simultaneous equation:

$$\begin{aligned}
&-(\alpha_1^3\lambda^2 - \alpha_0^3\mu^2)^2Y_2^2 \\
&+\alpha_2^2(\alpha_1^6\lambda^4 - 4\alpha_0\alpha_1^4\alpha_2\lambda^3\mu + 4\alpha_0^3\alpha_1^2\alpha_2\lambda^2\mu^2 + 4\alpha_0^2\alpha_1^3\alpha_2\lambda^2\mu^2 \\
&\qquad - 2\alpha_0^3\alpha_1^3\lambda^2\mu^2 - 4\alpha_0^4\alpha_1\alpha_2\lambda\mu^3 + \alpha_0^6\mu^4)Z_1^2 \\
&+2\alpha_2(\alpha_1^6\lambda^4 - 2\alpha_0\alpha_1^3\alpha_2^2\lambda^3\mu - 2\alpha_1^4\alpha_2^2\lambda^3\mu \\
&\qquad + 4\alpha_0^3\alpha_1\alpha_2^2\lambda^2\mu^2 + 4\alpha_0\alpha_1^3\alpha_2^2\lambda^2\mu^2 - 2\alpha_0^3\alpha_1^3\lambda^2\mu^2 \\
&\qquad - 2\alpha_0^3\alpha_1\alpha_2^2\lambda\mu^3 - 2\alpha_0^4\alpha_2^2\lambda\mu^3 + \alpha_0^6\mu^4)Z_1Z_2 \\
&+(\alpha_1^6\lambda^4 - 4\alpha_1^3\alpha_2^3\lambda^3\mu - 2\alpha_0^3\alpha_1^3\lambda^2\mu^2 + 4\alpha_0^3\alpha_2^3\lambda^2\mu^2 + 4\alpha_1^3\alpha_2^3\lambda^2\mu^2 \\
&\quad - 4\alpha_0^3\alpha_2^3\lambda\mu^3 + \alpha_0^6\mu^4)Z_2^2 = 0,
\end{aligned} \tag{7}$$

$$
\begin{aligned}
(8)\qquad & -(\alpha_1^3\lambda^2-\alpha_0^3\mu^2)^2Y_3^2\\
&+\alpha_3^2(\alpha_1^6\lambda^4-4\alpha_0\alpha_1^4\alpha_3\lambda^3\mu+4\alpha_0^3\alpha_1^2\alpha_3\lambda^2\mu^2+4\alpha_0^2\alpha_1^3\alpha_3\lambda^2\mu^2\\
&\qquad -2\alpha_0^3\alpha_1^3\lambda^2\mu^2-4\alpha_0^4\alpha_1\alpha_3\lambda\mu^3+\alpha_0^6\mu^4)Z_1^2\\
&+2\alpha_3(\alpha_1^6\lambda^4-2\alpha_0\alpha_1^3\alpha_3^2\lambda^3\mu-2\alpha_1^4\alpha_3^2\lambda^3\mu\\
&\qquad +4\alpha_0^3\alpha_1\alpha_3^2\lambda^2\mu^2+4\alpha_0\alpha_1^3\alpha_3^2\lambda^2\mu^2-2\alpha_0^3\alpha_1^3\lambda^2\mu^2\\
&\qquad -2\alpha_0^3\alpha_1\alpha_3^2\lambda\mu^3-2\alpha_0^4\alpha_3^2\lambda\mu^3+\alpha_0^6\mu^4)Z_1Z_2\\
&+(\alpha_1^6\lambda^4-4\alpha_1^3\alpha_3^3\lambda^3\mu-2\alpha_0^3\alpha_1^3\lambda^2\mu^2+4\alpha_0^3\alpha_3^3\lambda^2\mu^2+4\alpha_1^3\alpha_3^3\lambda^2\mu^2\\
&\quad -4\alpha_0^3\alpha_3^3\lambda\mu^3+\alpha_0^6\mu^4)Z_2^2=0.
\end{aligned}
$$

Proof. Since the equations in (6) are quadric forms in $Y_0,\ Y_1,\ Y_2,\ Y_3,\ Z_1,\ Z_2$, W is a $(2,\ 2,\ 2)$-complete intersection in $\mathbb{P}^5$. By Jacobian criterion, one can check that it is nonsingular, so it is a $K3$ surface. Moreover the first equation of (6) $\bar{e}Z_1^2-\bar{b}=0$, is expressed as

$$
\begin{vmatrix}
1 & 1 & 1 & 1 & 0\\
\alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & 0\\
\alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & 1\\
\alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & 0\\
Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 & Z_1^2
\end{vmatrix}=0.
$$

Similarly, the second and third equations are also expressed as

$$
\begin{vmatrix}
1 & 1 & 1 & 1 & 0\\
\alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & 1\\
\alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & 0\\
\alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & 0\\
Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 & 2Z_1Z_2
\end{vmatrix}=0,\quad
\begin{vmatrix}
1 & 1 & 1 & 1 & 1\\
\alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & 0\\
\alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & 0\\
\alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & 0\\
Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 & Z_2^2
\end{vmatrix}=0.
$$

This simultaneous equation is equivalent to the inequality

$$
(9)\qquad \operatorname{rank}\begin{pmatrix}
1 & 1 & 1 & 1 & 0 & 0 & 1\\
\alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & 0 & 1 & 0\\
\alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & 1 & 0 & 0\\
\alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & 0 & 0 & 0\\
Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 & Z_1^2 & 2Z_1Z_2 & Z_2^2
\end{pmatrix}<5
$$

by Proposition 4.2 which is stated later. By several elementary transformation, this matrix S_1 becomes

$$S_1\to S_2$$

where

$$S_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 \\ 0 & 0 & 0 & C_0 & C_1 & C_2 & C_3 \end{pmatrix},$$

$$C_0 = Y_0^2 - \alpha_0^2 Z_1^2 - 2\alpha_0 Z_1 Z_2 - Z_2^2,$$
$$C_1 = Y_1^2 - \alpha_1^2 Z_1^2 - 2\alpha_1 Z_1 Z_2 - Z_2^2,$$
$$C_2 = Y_2^2 - \alpha_2^2 Z_1^2 - 2\alpha_2 Z_1 Z_2 - Z_2^2,$$
$$C_3 = Y_3^2 - \alpha_3^2 Z_1^2 - 2\alpha_3 Z_1 Z_2 - Z_2^2.$$

Consequently (9) is equivalent to $\operatorname{rank} S_2 < 5$, i.e.,

$$\operatorname{rank} \begin{pmatrix} \alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 \\ C_0 & C_1 & C_2 & C_3 \end{pmatrix} < 2.$$

Applying Proposition 4.2 again, we obtain the equations

$$\begin{vmatrix} \alpha_0^3 & \alpha_i^3 \\ C_0 & C_i \end{vmatrix} = 0, \qquad i = 1,\ 2,\ 3. \tag{10}$$

Therefore the variety W is defined by the equations

$$\alpha_0^3 Y_i^2 - \alpha_i^3 Y_0^2 - \alpha_0^3(\alpha_i Z_1 + Z_2)^2 + \alpha_i^3(\alpha_0 Z_1 + Z_2)^2 = 0, \qquad i = 1,\ 2,\ 3.$$

Further the variety W is K-birational to W_4. In fact, let ρ be a map of W_4 to W defined by

$$\rho : (Y_2,\ Y_3,\ Z_1,\ Z_2,\ \lambda,\ \mu) \mapsto$$
$$\Bigg(\frac{-\alpha_0(\alpha_1^3\lambda^2 - 2\alpha_0^2\alpha_1\lambda\mu + \alpha_0^3\mu^2)Z_1 - (\alpha_1^3\lambda^2 - 2\alpha_0^3\lambda\mu + \alpha_0^3\mu^2)Z_2}{-\alpha_1^3\lambda^2 + \alpha_0^3\mu^2},$$
$$\frac{\alpha_1(\alpha_1^3\lambda^2 - 2\alpha_0\alpha_1^2\lambda\mu + \alpha_0^3\mu^2)Z_1 + (\alpha_1^3\lambda^2 - 2\alpha_1^3\lambda\mu + \alpha_0^3\mu^2)Z_2}{-\alpha_1^3\lambda^2 + \alpha_0^3\mu^2},$$
$$Y_2,\ Y_3,\ Z_1,\ Z_2 \Bigg).$$

Then this map is K-birational. Consequently the assertion of the lemma follows.

Remark. By (10), W contains 16 lines defined by the equations

$$Y_i = (-1)^{\varepsilon_i}(\alpha_i Z_1 + Z_2), \qquad \varepsilon_i = 0 \text{ or } 1,\ i = 0,\ 1,\ 2,\ 3$$

which we denote by $\ell(\varepsilon_0\varepsilon_1\varepsilon_2\varepsilon_3)$. The rank of the intersection matrix is 11, however, so these are not independent in Néron-Severi group of W.

Remark. In the above lemma, α_i $(i = 0,\ 1,\ 2,\ 3)$ are assumed to be independent variables. But W is still a $K3$ surface even if we assume only that $\alpha_i \in k^*$ are distinct.

Proposition 4.2. *Let $m < n$, and let $\mathbf{a}_1, \ldots, \mathbf{a}_n$ be column vectors of size m. Suppose that any m vectors of these are linearly independent. Then the simultaneous equation*

$$\begin{vmatrix} \mathbf{a}_1 & \ldots & \mathbf{a}_m & \mathbf{a}_i \\ Y_1^2 & \ldots & Y_m^2 & Y_i^2 \end{vmatrix} = 0, \qquad i = m+1, \ldots, n$$

is equivalent to the inequality

$$\operatorname{rank} \begin{pmatrix} \mathbf{a}_1 & \ldots & \mathbf{a}_n \\ Y_1^2 & \ldots & Y_n^2 \end{pmatrix} \leq m. \tag{11}$$

Proof. Inequality (11) means that each vector $\begin{pmatrix} \mathbf{a}_i \\ x_i \end{pmatrix}$ $(i = m+1,\ m+2, \ldots, n)$ is expressed as a linear combination of $\begin{pmatrix} \mathbf{a}_1 \\ x_1 \end{pmatrix}, \ldots, \begin{pmatrix} \mathbf{a}_m \\ x_m \end{pmatrix}$. Therefore

$$m = \operatorname{rank} \begin{pmatrix} \mathbf{a}_1 & \mathbf{a}_2 & \ldots & \mathbf{a}_m \\ x_1 & x_2 & \ldots & x_m \end{pmatrix} = \operatorname{rank} \begin{pmatrix} \mathbf{a}_1 & \mathbf{a}_2 & \ldots & \mathbf{a}_{n-1} & \mathbf{a}_n \\ x_1 & x_2 & \ldots & x_{n-1} & x_n \end{pmatrix}.$$

The converse is clear.

Lemma 4.3. *The rank of the group $ES(K)$ which consists of the sections on elliptic surface W_4 over $\mathbb{P}^1$ is greater than or equal to* 1.

Proof. It is sufficient to prove this when $\alpha_i = i+1$ $(i = 0, \ldots, 3)$. Then singular fibers are checked to be of type I_4 in Kodaira symbol at $(\lambda,\ \mu) = (0,\ 1)$ and $(1,\ 0)$, I_2 at $(3 \pm i\sqrt{23},\ 16)$ and $(1 \pm i\sqrt{7},\ 8)$, and I_1 at the roots of $(4096\lambda^8 - 1187840\lambda^7\mu + 1544192\lambda^6\mu^2 + 670720\lambda^5\mu^3 + 263296\lambda^4\mu^4 + 83840\lambda^3\mu^5 + 24128\lambda^2\mu^6 - 2320\lambda\mu^7 + \mu^8)$. These values of $(\lambda,\ \mu)$ are given by the poles of j-invariant of the generic fiber (see Lemma 4.4). The 16 lines $l(\varepsilon_0\varepsilon_1\varepsilon_2\varepsilon_3) \subset W$ mentioned above are transformed into W_4 by the birational map in Lemma 4.1 as follows: Lines $l(00\varepsilon_2\varepsilon_3)$ $(\varepsilon_2,\ \varepsilon_3 = 0$ or $1)$ are sections, $l(01\varepsilon_2\varepsilon_3)$ (respectively $l(10\varepsilon_2\varepsilon_3)$) are four $\mathbb{P}^1$s which constitute the singular fiber at $(\lambda,\ \mu) = (1,\ 0)$ (respectively $(0,\ 1)$), and $l(11\varepsilon_2\varepsilon_3)$ are exceptional. We now show that the rank of $ES(K)$ is at least 1 by using the sections $l(00\varepsilon_2\varepsilon_3)$. We will check this by looking at their intersection points with the singular fiber at $(\lambda,\ \mu) = (3 + i\sqrt{23},\ 16)$. Let C_1 (respectively C_2) denote the curve defined by (7) (respectively (8)) with $(\lambda,\ \mu) = (3 + i\sqrt{23},\ 16)$. Then C_1 (respectively C_2) intersects with $l(0000)$ and $l(0001)$ (respectively $l(0010)$ and $l(0011)$). The equation of C_1 is given by

$$-i\sqrt{23}Y_2 + 21Z_1 + 25Z_2 = 0, \tag{12}$$

$$23Y_3^2 + 1168Z_1^2 + 2632Z_1Z_2 + 1513Z_2^2 = 0, \tag{13}$$

and hence is isomorphic to a conic in $\mathbb{P}^2$ with coordinate $(Y_3,\ Z_1,\ Z_2)$. Let $i=\sqrt{-1}$ and $k_1=\mathbb{Q}(\sqrt{23},\ \sqrt{73},\ i)$. Then by using k_1-rational point $(Y_2,\ Y_3,\ Z_1,\ Z_2)=(-21i,\ 4i\sqrt{73},\ \sqrt{23},\ 0)$, we can parametrize k_1-rational points of C_1 by

$$\begin{aligned}(Y_2,Y_3,Z_1,Z_2)=\Big(&i\sqrt{23}(-483t^2+200i\sqrt{23}\sqrt{73}t+34027),\\ &-4(23i\sqrt{23}\sqrt{73}t^2+15134t-1513i\sqrt{23}\sqrt{73}),\\ &23(23t^2+1513),\\ &-184(i\sqrt{23}\sqrt{73}t+329)\Big).\end{aligned}$$

Let $C_1\cap l(0000)=P_1$, $C_1\cap l(0001)=P_2$ and $C_1\cap C_2=\{P_3,\ P_4\}$. Then the values t_i $(i=1,\ \ldots,\ 4)$, of the parameter t at P_i are

$$\begin{aligned}t_1&=-\frac{8}{3}-\frac{1}{3}\sqrt{73}-\frac{1}{3}i\sqrt{23}+\frac{11}{69}i\sqrt{23}\sqrt{73},\\ t_2&=\frac{8}{3}-\frac{1}{3}\sqrt{73}+\frac{1}{3}i\sqrt{23}+\frac{11}{69}i\sqrt{23}\sqrt{73},\\ t_3&=\frac{1}{21}i\sqrt{671}+\frac{100}{483}i\sqrt{23}\sqrt{73},\\ t_4&=-\frac{1}{21}i\sqrt{671}+\frac{100}{483}i\sqrt{23}\sqrt{73}.\end{aligned}$$

Let σ be an automorphism of $\mathbb{P}^1$ given by

$$\sigma : t\mapsto= \frac{(t-t_3)(t_2-t_4)}{(t-t_4)(t_2-t_3)},$$

which maps $P_2,\ P_3$, and P_4 to $1,\ 0$, and ∞ respectively.

Then

$$\sigma(t_1)=\left(-27413i\sqrt{671}+53009i\sqrt{23}+2785\sqrt{23}\sqrt{671}-966395\right)/1119744.$$

Since the absolute value of $\sigma(t_1)$ is found to be $(347-\sqrt{23}\sqrt{671})/324\neq 1$, $\sigma(t_1)$ is not a root of unity. Hence P_1 is of infinite order on the singular fiber at $(\lambda,\ \mu)=(3+i\sqrt{23},\ 16)$. Therefore $l(0000)$ provides us with a section of infinite order of the elliptic surface. Thus the rank of $ES(K)$ is at least 1.

Lemma 4.4. *The j-invariant of the generic fiber of W_4 with $\alpha_i = i+1$ $(i = 0,\ 1,\ 2,\ 3)$ is*

$$\begin{aligned}
&(4096\lambda^8 - 1187840\lambda^7\mu + 22777856\lambda^6\mu^2 - 12600320\lambda^5\mu^3 \\
&\quad + 7562368\lambda^4\mu^4 - 1575040\lambda^3\mu^5 + 355904\lambda^2\mu^6 \\
&\quad - 2320\lambda\mu^7 + \mu^8)^3 \\
&/(429981696\lambda^4\mu^4(8\lambda^2 - 2\lambda\mu + \mu^2)^2(8\lambda^2 - 3\lambda\mu + \mu^2)^2 \\
&\quad (4096\lambda^8 - 1187840\lambda^7\mu + 1544192\lambda^6\mu^2 + 670720\lambda^5\mu^3 \\
&\quad\quad + 263296\lambda^4\mu^4 + 83840\lambda^3\mu^5 + 24128\lambda^2\mu^6 - 2320\lambda\mu^7 + \mu^8)).
\end{aligned}$$

In particular, the elliptic surface W_4 is nontrivial.

Proof. We transform the equation of the generic fiber which is given by (7) and (8) to the canonical form. Let

$$\begin{aligned}
x &= Z_1 - t(\lambda - \mu), \\
y &= Y_3 - t(2\lambda - 3\mu), \\
z &= Y_2 - t(\lambda - 2\mu), \\
t &= Z_2/(-2\lambda + \mu).
\end{aligned}$$

Then we see that it has a rational point $(x,\ y,\ z,\ t) = (0,\ 0,\ 0,\ 1)$. Hence by the standard method (see e.g., [**1**]), the $(2,\ 2)$-intersection is transformed into the quartic form with a rational point P, and into a Weierstrass form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, where

$$\begin{aligned}
a_1 &= (\lambda - 2\mu)(8\lambda^3 + 20\lambda^2\mu - 19\lambda\mu^2 + 2\mu^3) \\
&\qquad (-128\lambda^5 + 3520\lambda^4\mu - 2880\lambda^3\mu^2 + 832\lambda^2\mu^3 - 178\lambda\mu^4 + 3\mu^5) \\
&\qquad /(6\lambda\mu(2\lambda - \mu)(2\lambda - 3\mu)^2(8\lambda^2 - \mu^2)(8\lambda^2 - 3\lambda\mu + \mu^2)), \\
a_3 &= 16(\lambda - 2\mu)(8\lambda^2 - 2\lambda\mu + \mu^2) \\
&\qquad (8\lambda^3 + 20\lambda^2\mu - 19\lambda\mu^2 + 2\mu^3)^6 \\
&\qquad (-16\lambda^4 - 32\lambda^3\mu + 90\lambda^2\mu^2 + 19\lambda\mu^3 + 6\mu^4) \\
&\qquad /(9\lambda^2\mu^2(2\lambda - \mu)^3(2\lambda - 3\mu)^6(8\lambda^2 - \mu^2)^3(8\lambda^2 - 3\lambda\mu + \mu^2)^3), \\
a_2 &= (8\lambda^3 + 20\lambda^2\mu - 19\lambda\mu^2 + 2\mu^3)^2 \\
&\quad (40960\lambda^{10} - 801792\lambda^9\mu + 2912256\lambda^8\mu^2 - 5442048\lambda^7\mu^3 \\
&\qquad + 7104000\lambda^6\mu^4 - 6047408\lambda^5\mu^5 + 3165264\lambda^4\mu^6 \\
&\qquad - 1097752\lambda^3\mu^7 + 266680\lambda^2\mu^8 - 34067\lambda\mu^9 + 1481\mu^{10}) \\
&\quad /(6\lambda\mu(2\lambda - \mu)^2(2\lambda - 3\mu)^4(8\lambda^2 - \mu^2)^2(8\lambda^2 - 3\lambda\mu + \mu^2)^2),
\end{aligned}$$

$$
\begin{aligned}
a_4 &= 16(8\lambda^2 - 2\lambda\mu + \mu^2)(8\lambda^3 + 20\lambda^2\mu - 19\lambda\mu^2 + 2\mu^3)^7 \\
&\quad (1024\lambda^9 + 640\lambda^8\mu - 15040\lambda^7\mu^2 + 31568\lambda^6\mu^3 - 37424\lambda^5\mu^4 \\
&\qquad + 35216\lambda^4\mu^5 - 19284\lambda^3\mu^6 + 10869\lambda^2\mu^7 - 6561\lambda\mu^8 + 914\mu^9) \\
&\quad /(9\lambda^2\mu^2(2\lambda - \mu)^4(2\lambda - 3\mu)^8(8\lambda^2 - \mu^2)^4(8\lambda^2 - 3\lambda\mu + \mu^2)^4), \\
a_6 &= 0.
\end{aligned}
$$

The j-invariant is computed to be the value in the statement of Lemma 4.4.

Theorem 4.5. *There are infinitely many elliptic surfaces $\pi_{(\lambda,\ \mu)} : \mathbf{E}_{(\lambda,\ \mu)} \to C_{(\lambda,\ \mu)}$, $(\lambda,\ \mu) \in \mathbb{P}^1(K)$, such that, for infinitely many $(\lambda,\ \mu)$:*

(i) *$\mathbf{E}_{(\lambda,\ \mu)}$, $C_{(\lambda,\ \mu)}$, and $\pi_{(\lambda,\ \mu)}$ are defined over K,*
(ii) *$\pi_{(\lambda,\ \mu)} : \mathbf{E}_{(\lambda,\ \mu)} \to C_{(\lambda,\ \mu)}$ is not isotrivial, namely the j-invariant of its fibers is nonconstant,*
(iii) *$C_{(\lambda,\ \mu)}$ is an elliptic curve with infinitely many K-rational points $P^n_{(\lambda,\ \mu)}$ $(n = 1,\ 2, \dots)$,*
(iv) *the fiber $\pi^{-1}_{(\lambda,\ \mu)}(P^n_{(\lambda,\ \mu)})$ is an elliptic curve of K-rank ≥ 4 with non-trivial 3-division K-rational points.*

Proof. Since (4) defines of a family of elliptic curves $\pi : \mathbf{E} \to \mathbb{P}^3$, we denote by $\pi' : \mathbf{E}' \to W$ the family of elliptic curves obtained from pulling back π along the natural projection $\alpha : W \to \mathbb{P}^3$. And let $C_{(\lambda,\ \mu)}$ denote the fiber of the elliptic surface $p : W \to \mathbb{P}^1$, and let $\pi_{(\lambda,\ \mu)} : \mathbf{E}_{(\lambda,\ \mu)} \to C_{(\lambda,\ \mu)}$ be the restriction of $\pi' : \mathbf{E}' \to W$ to $C_{(\lambda,\ \mu)} \subset W$. Recall that we have a section $P : \mathbb{P}^1 \to W$ of infinite order. It follows from Silverman's theorem ([**4**]) that rational point on $C_{(\lambda,\ \mu)}$ such that the specialization map for $\pi_{(\lambda,\ \mu)}$ is not injective has bounded height. Let $P_{(\lambda,\ \mu)} = P \cap C_{(\lambda,\ \mu)}$, then $P_{(\lambda,\ \mu)}$ is of infinite order at infinitely many $(\lambda,\ \mu)$, this implies that there is an integer $n_0 (\geq 1)$ such that for any integer $n \geq n_0$, $nP_{(\lambda,\ \mu)}$ gives injective specialization map. Letting $P^n_{(\lambda,\ \mu)} = (n + n_0)P_{(\lambda,\ \mu)}$ $(n = 1,\ 2,\ \dots)$, we see that Properties (i), (iii), (iv) hold true. Finally, we show that these families $\pi_{(\lambda,\ \mu)} : \mathbf{E}_{(\lambda,\ \mu)} \to C_{(\lambda,\ \mu)}$ satisfy Property (ii). Since $\pi' : \mathbf{E}' \to W$ is a pull-back of $\pi : \mathbf{E} \to W$, we have only to check that the j-invariant map of the fibers of $\pi|_{\alpha(C_{(\lambda,\ \mu)})}$ is nonconstant. We show this by specialization. Put $\alpha_i = i + 1$ $(i = 0,\ 1,\ 2,\ 3)$ and $(\lambda,\ \mu) = (3,\ 1)$. Then the value j_1 of j-invariant of the elliptic curve $\pi^{-1}_{(3,\ 1)}(2P_{(3,\ 1)})$ is found to be

$$
\begin{aligned}
j_1 = &-2^{14} \cdot 7^3 \cdot 19^3 \cdot 1570879^3 \cdot 4760715067931192217073 \\
&/(3^9 \cdot 5^{12} \cdot 11^3 \cdot 13^3 \cdot 67 \cdot 109^3 \cdot 179^3 \cdot 331^3 \cdot 499 \cdot 701 \\
&\cdot 10867 \cdot 79715743^3 \cdot 298760704699).
\end{aligned}
$$

On the other hand, the coordinate of the $3P_{(3,\ 1)}$ is

$$\begin{aligned}&(Y_0,\ Y_1,\ Y_2,\ Y_3,\ Z_1,\ Z_2)\\ &= \big(-2568087260400701976860 1,\ 60334008325736285093543,\\ &\quad 8493000884139970879754 3,\ -9685394130574570750619 1,\\ &\quad -4789234848907261418383 6,\ 16389422432073597934975\big),\end{aligned}$$

hence the equation of the elliptic curve $\pi^{-1}_{(3,\ 1)}(3P_{(3,\ 1)})$ is

$$\begin{aligned}y^2 = &-33292713244950929678791545801876109189830012 0x^3\\ &+ 22936770437987759107160413184673021684036748 96x^2\\ &- 15698558613029855754626838319318144492481282 00x\\ &+ 26861316765695724991686170137443258432825062 5.\end{aligned}$$

Let j_2 be the value of j-invariant of this elliptic curve. The elliptic curve has a good reduction at $p = 23$, and its equation becomes

$$y^2 = 19x^3 + x^2 + 9x + 3,$$

so $j_2 = 19$ and on the other hand $j_1 = 21$. Consequently j_2 is different from j_1. Let $C_{j_i} = \{P \in W; j(\pi^{-1}(P)) = j_i\} \subset W$ $(i = 1,\ 2)$. The above computation shows that each curve C_{j_i} $(i = 1,\ 2)$ has a horizontal component in the elliptic surface W. We see that $\pi_{(\lambda,\ \mu)}$ is nonconstant.

Theorem 4.6. *The construction by Theorem* 4.5 *is universal. That is, any elliptic curve of rank* ≥ 4 *with* 3*-division rational point is constructed by this method.*

Proof. As we have seen in [**5**], every elliptic curve of rank ≥ 4 comes from a rational point of V_4. Moreover, by the explanation given in the beginning of Section 4, any elliptic curve with 3-division point can be transformed to the form (5). Hence every elliptic curve of rank ≥ 4 with 3-division rational point arises as a rational point of W.

5. Example.

In this section, we give an example which belongs to our family.

Theorem 5.1. *The elliptic curve defined by the equation*

$$\begin{aligned}(14)\qquad y^2 = &\,x^3 + x^2 - 13261886323348785049798769366 5x\\ &+ 18733773131738750737283986787748862815262400\end{aligned}$$

belongs to our family. The rank of its Mordell-Weil group is at least 4*, its independent four points are*

$$\begin{aligned}(15)\qquad &(192389110733795,\ 583400181207775449375),\\ &(223557713735045,\ 508706369557047894375),\\ &(254726316736295,\ 1216676657039879660625),\\ &(285894919737545,\ 2046116787778740909375),\end{aligned}$$

and its 3*-division rational point is*

$$(16)\qquad (161220507732545, -1242314173258336839375).$$

The conductor is

$$\begin{aligned}&336097604736051248141403751202579296152060\\ &= 2^2\cdot 3\cdot 5\cdot 11\cdot 13\cdot 67\cdot 109\cdot 179\cdot 331\cdot 499\cdot 701\\ &\quad\cdot 10867\cdot 79715743\cdot 298760704699.\end{aligned}$$

Proof. Put $\alpha_i = i+1$ $(i = 0,\ 1,\ 2,\ 3)$ and $(\lambda,\ \mu) = (3,\ 1)$. Then, the point $P_{(3,\ 1)}$ does not give an elliptic curve because it is a quadric curve. The coordinate of $2P_{(3,\ 1)}$ is

$$\begin{aligned}&(Y_0,\ Y_1,\ Y_2,\ Y_3,\ Z_1,\ Z_2)\\ &= \big(62391865/156689676,\ 163211155/470069028,\\ &\quad 390353285/470069028,\ -218822425/156689676,\\ &\quad -54980765/117517257,\ 398578715/470069028\big).\end{aligned}$$

It follows from (4) that the equation of the corresponding elliptic curve $\pi^{-1}_{(3,\ 1)}(2P_{(3,\ 1)})$ is

$$\begin{aligned}(17)\qquad 12y^2 = {}&\frac{201816906250}{1192290917103}x^3 + \frac{12091538079940900}{4603435230934683}x^2\\ &- \frac{43828325326833950}{4603435230934683}x + \frac{158864992051051225}{18413740923738732},\end{aligned}$$

and four rational points are

$$\begin{aligned}&(1,\ 62391865/156689676),\ (2,\ 163211155/470069028),\\ &(3,\ 390353285/470069028),\ (4,\ 218822425/156689676).\end{aligned}$$

Transforming (17) into the minimal form, we obtain Equation (14), four rational points in (15), and the 3-division rational point in (16). The regulator of four points in (15) is found to be equal to 973.328878874..., hence these points are independent.

References

[1] J.W.S. Cassels, *Lectures on Elliptic Curves*, London Mathematical Society Student Texts, **24**, Cambridge University Press, 1991, MR 92k:11058, Zbl 0752.14033.

[2] F. Hazama, *Rational points on certain abelian varieties over function fields*, J. Number Theory, **5**0 (1995), 278-285, MR 96b:14019, Zbl 0838.14024.

[3] ———, *Picard numbers of certain complete intersection surfaces*, in 'Algebraic cycles and related topics' (Ed. F. Hazama), World Scientific, 1995, 23-36, MR 97m:14045, Zbl 0861.14042.

[4] J. Silverman, *Lower bounds for height functions*, Duke Math. J., **5**1 (1984), 395-403, MR 87d:11039, Zbl 0579.14035.

[5] H. Yamagishi, *A unified method of construction of elliptic curves with high Mordell-Weil rank*, Pacific J. Math., **1**91 (1999), 189-200, MR 2001a:11092.

Received November 6, 2000 and revised January 28, 2002. The author was supported by JSPS Research Fellowships for Young Scientists.

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