Available at WWW.MATHEMATICSWEB.ORG
POWERED BY SCIENCE @ DIRECT

Journal of Number Theory 100 (2003) 295–306

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

Boundedness of Mordell–Weil ranks of certain elliptic curves and Lang's conjecture

Hizuru Yamagishi[1]

Tokyo Denki University, Department of Natural Sciences, Hatoyama, Saitama 350-0394, Japan

Received 29 November 2001; revised 19 July 2002
Communicated by D. Goss

Abstract

In this paper, we show that a special case of Lang's conjecture on rational points on surfaces of general type implies that there exist only finitely many elliptic curves, when the x-coordinates of n rational points are specified with $n \geqslant 8$.

Keywords: Elliptic curves; Mordell–Weil rank; Lang's conjecture

1. Introduction

There exists the following 'folklore' conjecture in the study of rational points on elliptic curves (see [3], for example):

Conjecture 1.1. *There exist elliptic curves defined over the rational field* **Q** *of arbitrarily large rank.*

As is seen in [5,6,8–10], the theory of twists, developed in [7], provides us with a unified view point for the construction of elliptic curves of high Mordell–Weil rank. In this paper we show that if we assume a version of Lang's conjecture, then the theory gives us a useful tool to find some constraints on the form of elliptic curves of high Mordell–Weil rank. The version of the Lang's conjecture we have in mind is the following.

E-mail address: hizuru@u.dendai.ac.jp.
[1] Supported by JSPS Research Fellowships for Young Scientists and by Grant-in-Aid for JSPS Fellows.

0022-314X/03/$ - see front matter
doi:10.1016/S0022-314X(02)00126-9

Conjecture 1.2 ([4]). *Let X be a smooth projective algebraic variety of general type, defined over a number field k. Then there exists a proper Zariski-closed subset Z of X such that for all number fields K containing k, $X(K)\backslash Z(K)$ is finite.*

Paul Vojta proved in [4] that if Conjecture 1.2 holds in the case where X is a surface, then the only rational points on a certain projective variety are on lines which are naturally contained in the variety.

Inspired by Vojta's result, we show the following.

Theorem 1.3. *Let K be a finitely generated field over* $\mathbf{Q}$. *Let $n \geqslant 8$ be an integer and let α_i $(i = 0, \dots, n)$ be fixed elements of K. Suppose Conjecture* 1.2 *holds for k a finitely generated field over* $\mathbf{Q}$ (cf. [2]). *Then there are only finitely many elliptic curves of the form $y^2 = ax^4 + bx^2 + c$ $(a, b, c \in K)$ which have α_i as the x-coordinates of some K-rational points. In particular the Mordell–Weil ranks of such elliptic curves are bounded.*

2. Universal family for elliptic curves with some rational points

In this section, we show that all elliptic curves with a certain form are obtained by similar arguments to the ones used in [5,7,8,10].

First, we construct an elliptic curve with ℓ rational points defined over the function field of an algebraic variety. Let E be an elliptic curve over a number field k defined by the equation

$$E : y^2 = ax^4 + bx^2 + c, \tag{1}$$

and let $f(x)$ be the right-hand side of (1). Then the equation of E^ℓ is

$$y_i^2 = f(x_i) \quad (i = 1, \dots, \ell).$$

Let ι_i be the involution on the i^{th} factor E of E^ℓ defined by $\iota_i((x_i, y_i)) = (x_i, -y_i)$ $(i = 1, \dots, \ell)$, and put $V_\ell = E^\ell / \langle (\iota_1, \dots, \iota_\ell) \rangle$, so that the defining equation of V_ℓ is

$$y_i^2 = f(x_1) f(x_{i+1}) \quad (i = 1, \dots, \ell - 1).$$

Let $E_{f(x_1)}$ denote the twist of E by the quadratic extension $k(E^\ell)/k(V_\ell)$. Then we see by a similar argument to [1] that $E_{f(x_1)}$ is defined by the equation

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

and it has at least ℓ rational points

$$(x_1, 1), \ (x_{i+1}, y_i / f(x_1)) \quad (i = 1, \dots, \ell - 1). \tag{3}$$

Moreover, we can show the following.

Theorem 2.1. *Let E be a given elliptic curve defined by the equation*

$$E : y^2 = ax^4 + bx^2 + c,$$

and let $(\alpha_i,\ \beta_i)$ $(i = 1, \dots, \ell,\ \beta_1 \neq 0)$ be rational points on E. Let $E_{f(x_1)}$ be the twist of E by $k(E^\ell)/k(V_\ell)$. Then E with these rational points is obtained by specializing $E_{f(x_1)}$ at the point

$$(x_1, \dots, x_\ell, y_1, \dots, y_{\ell-1}) = (\alpha_1, \dots, \alpha_\ell,\ \beta_1\beta_2, \dots, \beta_1\beta_\ell) \quad \text{on } V_\ell.$$

Proof. Let $x_i = \alpha_i$ $(i = 1, \dots, \ell)$. Then the elliptic curve $E_{f(x_1)}$: $f(x_1)y^2 = f(x)$ is isomorphic to $y^2 = f(x)$ by the map $E_{f(x_1)} \to E$: $(x, y) \mapsto (x,\ \beta_1 y)$. The ℓ points on $E_{f(x_1)}$ given in (3) are $(\alpha_1, 1)$ $(\alpha_{i+1}, \beta_{i+1}/\beta_1)$ $(i = 1, \dots, \ell - 1)$, and these points map to (α_i, β_i) $(i = 1, \dots, \ell)$. □

From now on, we focus our attention on the variety V_ℓ. In order to investigate the rational points on V_ℓ, put $x_{i+1} = \alpha_i$ $(i = 0, \dots, \ell - 1)$, and denote $k(\alpha_0, \alpha_1, \dots, \alpha_{\ell-1})$ by K. One of our ideas is that we regard V_ℓ as a subvariety of the projective space $\mathbf{P}_K^{\ell+1}$ with coordinates a, b, c, y_i $(i = 1, \dots, \ell - 1)$. From this view point we can show V_ℓ is K-birational to an algebraic surface defined by equations of much simpler form.

Given $n + 1$ distinct elements $\alpha_i \in K$ $(0 \leqslant i \leqslant n)$, let W_n be a subvariety of $\mathbf{P}^n(K)$ defined by the equations

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_i^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 & \alpha_i^4 \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_i^2 \end{vmatrix} = 0 \quad (i = 3, \dots, n).$$

We put $W_2 = \mathbf{P}^2(K)$, by convention. By the jacobian criterion one can check that W_n is a nonsingular complete $(2,\ 2, \dots, 2)$-intersection surface.

Theorem 2.2. *Suppose that $f(\alpha_0) \neq 0$. Then V_{n+1} is K-birationally equivalent to W_n for any $n \geqslant 2$.*

Proof. The map $\varphi : V_{n+1} \to W_n$,

$$(a, b, c, y_1, \dots, y_n) \mapsto (f(\alpha_0), y_1, \dots, y_n)$$

is birational. Because the inverse map of φ is

$$\varphi^{-1} : W_n \to V_{n+1},$$

$$(Y_0, \dots, Y_n) \mapsto \left(\begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix}, - \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix}, \right.$$
$$\left. \begin{vmatrix} \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix}, Y_0 Y_1 D, \dots, Y_0 Y_n D \right), \tag{4}$$

where

$$D = \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \end{vmatrix}. \qquad \square$$

Remark 2.3. There exist 2^n lines on W_n defined by

$$(Y_0, Y_1, \dots, Y_n) = (s + t\alpha_0^2, (-1)^{\varepsilon_1}(s + t\alpha_1^2), \dots, (-1)^{\varepsilon_n}(s + t\alpha_n^2)),$$

where $\varepsilon_i = 0$ or 1. The defining equations of these are

$$\begin{aligned} (-1)^{\varepsilon_1} Y_1 &= (-1)^{\varepsilon_2} \frac{\alpha_1^2 - \alpha_0^2}{\alpha_2^2 - \alpha_0^2} Y_2 + \frac{\alpha_2^2 - \alpha_1^2}{\alpha_2^2 - \alpha_0^2} Y_0 \\ &= \cdots \\ &= (-1)^{\varepsilon_i} \frac{\alpha_1^2 - \alpha_0^2}{\alpha_i^2 - \alpha_0^2} Y_i + \frac{\alpha_i^2 - \alpha_1^2}{\alpha_i^2 - \alpha_0^2} Y_0 \\ &= \cdots \\ &= (-1)^{\varepsilon_n} \frac{\alpha_1^2 - \alpha_0^2}{\alpha_n^2 - \alpha_0^2} Y_n + \frac{\alpha_n^2 - \alpha_1^2}{\alpha_n^2 - \alpha_0^2} Y_0, \end{aligned} \tag{5}$$

where $\varepsilon_i = 0$ or 1 $(i = 1, \dots, n)$.

They have also a determinantal expression

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_i^2 \\ Y_0 & (-1)^{\varepsilon_1} Y_1 & (-1)^{\varepsilon_i} Y_i \end{vmatrix} = 0 \ \ (i = 2, 3, \dots, n),$$

where $\varepsilon_i = 0$ or 1 $(i = 1, \dots, n)$.

They will be called the trivial lines on W_n.

3. The connection to the result of Vojta

In [4], Vojta investigates the rational points on the variety X_n defined by

$$x_i^2 - 2x_{i+1}^2 + x_{i+2}^2 = 2x_0^2 \quad (i = 1, \dots, n-2). \tag{6}$$

Moreover, the 2^n lines on X_n defined by

$$\pm x_1 = \pm x_2 - x_0 = \pm x_3 - 2x_0 = \cdots = \pm x_n - (n-1)x_0 \tag{7}$$

play an important role for his purpose. These lines is called trivial lines. In this section, we show that the variety X_n $(n \geqslant 2)$ is a special case of the variety $\tilde{X}_n$ defined by the equations

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \beta_0 & \beta_1 & \beta_2 & \beta_i \\ \beta_0^2 & \beta_1^2 & \beta_2^2 & \beta_i^2 \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_i^2 \end{vmatrix} = 0 \quad (i = 3, \dots, n). \tag{8}$$

Note that W_n is obtained from $\tilde{X}_n$ by letting $\beta_i = \alpha_i^2$.

Lemma 3.1. *Let m and n $(m \leqslant n)$ be integers and $\mathbf{a}_0, \dots, \mathbf{a}_n$ be column vectors of size m. Suppose that any m vectors of these are linearly independent. Then the following three conditions are equivalent*:

(i) $rank\begin{pmatrix} \mathbf{a}_0 & \mathbf{a}_1 & \cdots & \mathbf{a}_{n-1} & \mathbf{a}_n \\ x_0 & x_1 & \cdots & x_{n-1} & x_n \end{pmatrix} = m,$

(ii) $\begin{vmatrix} \mathbf{a}_0 & \mathbf{a}_1 & \cdots & \mathbf{a}_{m-1} & \mathbf{a}_i \\ x_0 & x_1 & \cdots & x_{m-1} & x_i \end{vmatrix} = 0 \quad (i = m, m+1, \dots, n),$

(iii) $\begin{vmatrix} \mathbf{a}_0 & \mathbf{a}_i & \mathbf{a}_{i+1} & \cdots & \mathbf{a}_{i+m-1} \\ x_0 & x_i & x_{i+1} & \cdots & x_{i+m-1} \end{vmatrix} = 0 \quad (i = 1, 2, \dots, n-m+1).$

Proof. It is clear that (i) implies (ii) and (iii).

Condition (ii) means that each vector $\begin{pmatrix} \mathbf{a}_i \\ x_i \end{pmatrix}$ $(i = m,\ m+1, \dots, n)$ is expressed as a linear combination of $\begin{pmatrix} \mathbf{a}_0 \\ x_0 \end{pmatrix}, \dots, \begin{pmatrix} \mathbf{a}_{m-1} \\ x_{m-1} \end{pmatrix}$. Therefore

$$m = rank\begin{pmatrix} \mathbf{a}_0 & \mathbf{a}_1 & \cdots & \mathbf{a}_{m-1} \\ x_0 & x_1 & \cdots & x_{m-1} \end{pmatrix} = rank\begin{pmatrix} \mathbf{a}_0 & \mathbf{a}_1 & \cdots & \mathbf{a}_{n-1} & \mathbf{a}_n \\ x_0 & x_1 & \cdots & x_{n-1} & x_n \end{pmatrix}.$$

Hence (ii) implies (i).

Next, from (iii) with $i = 1$, we obtain

$$rank\begin{pmatrix} \mathbf{a}_0 & \mathbf{a}_1 & \cdots & \mathbf{a}_m \\ x_0 & x_1 & \cdots & x_m \end{pmatrix} = m.$$

By (iii) with $i = 2$, $\begin{pmatrix} \mathbf{a}_{m+1} \\ x_{m+1} \end{pmatrix}$ is expressed as a linear combination of $\begin{pmatrix} \mathbf{a}_0 \\ x_0 \end{pmatrix}, \begin{pmatrix} \mathbf{a}_2 \\ x_2 \end{pmatrix}, \ldots, \begin{pmatrix} \mathbf{a}_m \\ x_m \end{pmatrix}$. Thus

$$rank\begin{pmatrix} \mathbf{a}_0 & \mathbf{a}_1 & \cdots & \mathbf{a}_{m+1} \\ x_0 & x_1 & \cdots & x_{m+1} \end{pmatrix} = m.$$

Repeat this with $i = 3$ to $n - m + 1$, then (i) is obtained. □

Through this lemma, we can relate X_n with $\tilde{X}_n$.

Theorem 3.2. *X_n is the variety which arises by putting $\beta_0 = 0$, $\beta_i = 1/i$, $Y_0 = x_0$, $Y_i = x_i/i$ $(i = 1, 2, \ldots, n)$ in the equation of $\tilde{X}_n$.*

Remark 3.3. Similarly, by substituting $\beta_0 = 0$, $\beta_i = 1/i$, $Y_0 = x_0$, $Y_i = x_i/i$ $(i = 1, \ldots, n)$ into (5), (7) is obtained.

Proof. Let A be a matrix

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ \beta_0 & \beta_1 & \beta_2 & \beta_3 & \beta_4 & \cdots & \beta_n \\ \beta_0^2 & \beta_1^2 & \beta_2^2 & \beta_3^2 & \beta_4^2 & \cdots & \beta_n^2 \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 & Y_4^2 & \cdots & Y_n^2 \end{pmatrix}.$$

By Lemma 3.1, (8) is equivalent to

$$rank\,(A) = 3.$$

Let $\beta_0 = 0$, $\beta_i = 1/i$, $Y_0 = x_0$, $Y_i = x_i/i$ $(i = 1, \ldots, n)$, then

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 1/2 & 1/3 & 1/4 & \cdots & 1/n \\ 0 & 1/1^2 & 1/2^2 & 1/3^2 & 1/4^2 & \cdots & 1/n^2 \\ x_0^2 & (x_1/1)^2 & (x_2/2)^2 & (x_3/3)^2 & (x_4/4)^2 & \cdots & (x_n/n)^2 \end{pmatrix}.$$

Multiply the i^{th} column by $(i-1)^2$ $(i = 2, \ldots, n+1)$, and exchange the first row with the third row. Then A becomes

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 1^2 & 2^2 & 3^2 & 4^2 & \cdots & n^2 \\ x_0^2 & x_1^2 & x_2^2 & x_3^2 & x_4^2 & \cdots & x_n^2 \end{pmatrix}.$$

Let us denote this matrix by B. By Lemma 3.1,

$$rank(B) = 3$$

is equivalent to

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

By expanding this determinant along the 4th row, we obtain (6). $\square$

4. Curves on W_n of genus 0 or 1

In this section, we show that for $n \geqslant 8$, the curves on W_n of genus 0 or 1 are only the trivial lines by extending a part of results in [4] to the case of W_n.

We recall $W_2 = \mathbf{P}^2$. The rational maps $\mathbf{P}^i \to \mathbf{P}^{i-1}$ defined by $(Y_0, Y_1, \ldots, Y_i) \mapsto (Y_0, Y_1, \ldots, Y_{i-1})$ $(i = 3, 4, \ldots, n)$ define morphisms $\tilde{\pi}_i : W_i \to W_{i-1}$ $(i = 3, 4, \ldots, n)$ which form a chain

$$\mathbf{P}^2 = W_2 \stackrel{\tilde{\pi}_3}{\leftarrow} W_3 \stackrel{\tilde{\pi}_4}{\leftarrow} \cdots \stackrel{\tilde{\pi}_n}{\leftarrow} W_n.$$

The morphism $\tilde{\pi}_i$ is finite, is of degree 2, and is ramified along the curve $\tilde{C}_i$ on W_i defined by $Y_i = 0$. The $\tilde{C}_i$ is nonsingular and the image of $\tilde{C}_n$ in $W_2 = \mathbf{P}^2$ is the curve

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_2^2 & \alpha_n^2 \\ \alpha_0^4 & \alpha_2^4 & \alpha_n^4 \end{vmatrix} Y_1^2 - \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_n^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_n^4 \end{vmatrix} Y_2^2 = \begin{vmatrix} 1 & 1 & 1 \\ \alpha_1^2 & \alpha_2^2 & \alpha_n^2 \\ \alpha_1^4 & \alpha_2^4 & \alpha_n^4 \end{vmatrix} Y_0^2,$$

i.e.

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_n^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 & \alpha_n^4 \\ Y_0^2 & Y_1^2 & Y_2^2 & 0 \end{vmatrix} = 0.$$

The map $\psi : W_2 \to X_2$, defined by

$$(Y_0, Y_1, Y_2) \mapsto (-(\alpha_2^2 - \alpha_1^2)Y_0, (\alpha_2^2 - \alpha_0^2)Y_1, (\alpha_1^2 - \alpha_0^2)Y_2),$$

gives an isomorphism. We obtain the following $\tilde{\omega}_2$ by pulling back ω_2 in [4, (2.5)] along ψ

$$\begin{aligned} \tilde{\omega}_2 = & (\alpha_2^2 - \alpha_0^2)^2 Y_1 Y_2 \, dY_1 \otimes dY_1 \\ & + ((\alpha_2^2 - \alpha_1^2)^2 - (\alpha_2^2 - \alpha_0^2)^2 Y_1^2 - (\alpha_1^2 - \alpha_0^2)^2 Y_2^2) \, dY_1 \otimes dY_2 \\ & + (\alpha_1^2 - \alpha_0^2)^2 Y_1 Y_2 \, dY_2 \otimes dY_2. \end{aligned}$$

Then the next lemma holds.

Lemma 4.1. *The only $\tilde{\omega}_2$-integral curves on W_2 are*

(i) *the coordinate axes* $Y_0 = 0, \ Y_1 = 0, \ Y_2 = 0,$

(ii) *the four trivial lines* $\pm Y_1 = \pm \dfrac{\alpha_1^2 - \alpha_0^2}{\alpha_2^2 - \alpha_0^2} Y_2 - \dfrac{\alpha_2^2 - \alpha_1^2}{\alpha_2^2 - \alpha_0^2} Y_0,$

(iii) *the smooth conics*

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \tilde{c} \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 & \tilde{c}^2 \\ Y_0^2 & Y_1^2 & Y_2^2 & 0 \end{vmatrix} = 0, \quad \tilde{c} \in \mathbf{C} \backslash \{\alpha_0^2, \ \alpha_1^2, \ \alpha_2^2\}.$$

Proof. These are obtained by transforming the equations in [4, Lemma 2.7] by ψ. The relation of c in [4] with $\tilde{c}$ in this Lemma is given by

$$c = \frac{(\alpha_1^2 - \alpha_0^2)(\tilde{c} - \alpha_2^2)}{(\alpha_2^2 - \alpha_1^2)(\tilde{c} - \alpha_0^2)}. \qquad \square$$

Hence by the argument in [4] we obtain the following theorem.

Theorem 4.2. *Let $n \geqslant 8$ be an integer. Then the only curves on W_n of genus* 0 *or* 1 *are the trivial lines.*

5. The rational points on W_n and elliptic curves

In this section, we show that the K-rational points on the trivial lines of W_n are exceptional points for our construction of elliptic curves. Thereafter we prove our main theorem.

Lemma 5.1. *Let $P = (Y_0, Y_1, \dots, Y_n)$ be a point on W_n. Suppose $Y_0 \neq 0$. The elliptic curve given by P is K-isomorphic to the elliptic curve $\tilde{E}_{f(x_1)}$ defined by the equation*

$$\begin{aligned}\tilde{E}_{f(x_1)} : &\begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \end{vmatrix} y^2 \\ &= \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix} x^4 - \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix} x^2 + \begin{vmatrix} \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix},\end{aligned}$$

which is obtained by expanding

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & x^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 & x^4 \\ Y_0^2 & Y_1^2 & Y_2^2 & y^2 \end{vmatrix} = 0$$

along the fourth column.

Proof. By the map φ^{-1} in (4), a K-rational point $(Y_0, Y_1, \dots, Y_n)$ on W_n goes to

$$(a, b, c) = \left(\begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix}, -\begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix}, \begin{vmatrix} \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix} \right) \in \mathbf{P}^2.$$

Therefore, the elliptic curve $E_{f(x_1)}$ which corresponds to the point is

$$\begin{aligned}&\left(\begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix} x_1^4 - \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix} x_1^2 + \begin{vmatrix} \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix} \right) y^2 \\ &= \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix} x^4 - \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix} x^2 + \begin{vmatrix} \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix} \qquad (9)\end{aligned}$$

by (2). Since $\alpha_0 = x_1$, the coefficient of y^2 in (9) is

$$-\begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_0^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 & \alpha_0^4 \\ Y_0^2 & Y_1^2 & Y_2^2 & 0 \end{vmatrix} = -\begin{vmatrix} 1 & 1 & 1 & 0 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & 0 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 & 0 \\ Y_0^2 & Y_1^2 & Y_2^2 & -Y_0^2 \end{vmatrix}$$
$$= \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \end{vmatrix} Y_0^2.$$

Therefore, by the isomorphism $E_{f(x_1)} \to \tilde{E}_{f(x_1)} : (\hat{x}, \hat{y}) \mapsto (\hat{x}, \hat{y}Y_0)$, $E_{f(x_1)}$ is K-isomorphic to $\tilde{E}_{f(x_1)}$. $\square$

In view of Theorem 4.2, the following lemma is crucial.

Lemma 5.2. *The K-rational points on the trivial lines of W_n are exceptional for constructing elliptic curves with $n+1$ rational points, namely they do not correspond to any elliptic curves.*

Proof. Every rational point $(Y_0, Y_1, \ldots, Y_n) = (s + t\alpha_0^2, (-1)^{\varepsilon_1}(s + t\alpha_1^2), \ldots, (-1)^{\varepsilon_n}(s + t\alpha_n^2))$, $\varepsilon_i = 0$ or 1 $(i = 1, \ldots, n)$ on the trivial lines in Remark 2.3 corresponds to the curve defined by

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & x^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 & x^4 \\ (s + t\alpha_0^2)^2 & (s + t\alpha_1^2)^2 & (s + t\alpha_2^2)^2 & y^2 \end{vmatrix} = 0$$

by Lemma 5.1. Add (the first row) $\times (-s^2)$ + (the second row) $\times (-2st)$ + (the third row) $\times (-t^2)$ to the 4th row. Then we obtain

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & x^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 & x^4 \\ 0 & 0 & 0 & y^2 - (s + tx^2)^2 \end{vmatrix} = 0.$$

Since

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \end{vmatrix} \neq 0,$$

we have $y^2 - (s + tx^2)^2 = 0$. This is product of two quadratics, therefore our lemma is proved. □

Proof of Theorem 1.3. By Theorems 2.1 and 2.2, all elliptic curves which are stated in this theorem corresponds to K-rational points on W_n. But any K-rational points on trivial lines do not give any elliptic curves by Lemma 5.2. Therefore if Conjecture 1.2 for k a finitely generated field over $\mathbf{Q}$ holds for W_n, then there are only finite K-rational points on W_n which correspond to elliptic curve. □

Remark 5.3. All elliptic curves with nontrivial two-torsion point are obtained by using the method of construction in Section 2. For each elliptic curve of this type is expressed as follows without loss of generality:

$$E_1\colon\ y^2 = x^3 + gx^2 + hx \quad \text{where } (0,0) \text{ gives a two-torsion point.}$$

Moreover, E_1 is birationally equivalent to the elliptic curve E_2 defined by the equation

$$E_2\colon\ y^2 = x^4 - 2gx^2 + g^2 - 4h,$$

by the birational map $E_1 \to E_2 : (x_0, y_0) \mapsto (y_0/x_0, 2x_0 + g - y_0^2/x_0^2)$.

Acknowledgments

The author thanks Professor Fumio Hazama for his useful advice.

References

[1] F. Hazama, Rational points on certain abelian varieties over function fields, J. Number Theory 50 (2) (1995) 278–285.
[2] S. Lang (Ed.), Number Theory III, Encyclopaedia of Mathematical Sciences, Vol. 60, Springer, Berlin, 1991.
[3] J. Silverman, The Arithmetic of Elliptic Curves, GTM 106, Springer, Berlin, 1992.
[4] P. Vojta, Diagonal quadratic forms and Hilbert's tenth problem, Contemp. Math. 270 (2000) 261–274.
[5] H. Yamagishi, On the existence of elliptic curves of Mordell–Weil rank 6 with 4 parameters, J. Algebra 181 (2) (1996) 558–564.
[6] H. Yamagishi, On certain twisted families of elliptic curves of rank 8, Manuscripta Math. 95 (1998) 1–10.
[7] H. Yamagishi, A unified method of construction of elliptic curves with high Mordell–Weil rank, Pacific J. Math. 191 (1) (1999) 189–200.
[8] H. Yamagishi, On the existence of families of elliptic curves of rank four with all two-torsion points, Far East J. Math. Sci. (FJMS) 3 (5) (2001) 803–823.

[9] H. Yamagishi, Construction of families of elliptic curves of rank 6 with a nontrivial two-torsion point, Far East J. Math. Sci. (FJMS) 4 (1) (2002) 129–135.

[10] H. Yamagishi, On elliptic curves of rank four with three-division rational point, Pacific J. Math. 206 (1) (2002) 231–244.