Pacific Journal of Mathematics

A UNIFIED METHOD OF CONSTRUCTION OF ELLIPTIC CURVES WITH HIGH MORDELL–WEIL RANK

Hizuru Yamagishi

Volume 191 No. 1 November 1999

PACIFIC JOURNAL OF MATHEMATICS
Vol. 191, No. 1, 1999

A UNIFIED METHOD OF CONSTRUCTION OF ELLIPTIC CURVES WITH HIGH MORDELL–WEIL RANK

Hizuru Yamagishi

By using the twist theory, we reduce 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. By parametrizing all rational points on V_n ($1 \leq n \leq 7$), we get all elliptic curves of at least rank n ($n \leq 7$).

1. Introduction.

The purpose of this paper is to describe a unified method of construction of elliptic curves with given Mordell-Weil rank, and to show it is powerful enough to produce every known example in principle. In view of the fact that there is no general algorithm to give an elliptic curve with high rank, our method might shed a light on this area of active research.

The main ingredient in this paper is the twist theory as is developed in [**3**]. One of our main theorems says that the twists give us every elliptic curve with high Mordell-Weil rank. Once this is established, we naturally come to consider a variety V_n parametrizing a family of elliptic curves with a given rank n, and we show that almost every rational point on this variety gives an elliptic curve with rank $\geq n$. Thus our method should provide us with every known example as a rational point on it. We will show that this is indeed the case.

In this paper, we parametrize the rational points on V_n in each case of $n = 1$ to 7. As is mentioned above parametrizing the rational points on V_n is equivalent to getting every elliptic curve of rank at least n ($n \leq 7$). Moreover, the variety V_n is expected to be useful for solving other problems. For example, in [**5**] it is used to construct a family of elliptic curves of rank 2 with given j-invariant. Moreover in [**6**], it is used to give a family of elliptic curves of rank 6 with a nontrivial rational two-torsion point. The point which is worthy of special mention is that we get very easily the equation of any elliptic curve which corresponds to a rational point on V_n.

The present paper is organized as follows. In Section 2, we show every elliptic curve with generators comes from a twist. Then for each rank n we define the variety V_n mentioned above, which plays a very important role throughout the paper, and construct a generic elliptic curve with its generators as a generic fiber of a certain family of elliptic curves parametrized by V_n. Furthermore we show that we can get a given elliptic curve by specializing this family at a certain rational point on V_n. In Section 3, we focus our attention on the structure of V_n. In each case of rank 1 to 7, we show V_n is rational and obtain a parametric representation of all rational points of V_n. For the case of rank ≥ 5, we define another variety which is birational to V_n, and parametrize rational points on V_n in these cases using this variety. The concrete proof is given only for the case of rank 6, because it is the most typical and richest and the other cases are treated more easily. In Section 4, for a given elliptic curve with generators whose rank ≤ 7, we specify the values of the parameters which are used in Section 3 to express the rational points of V_n. As an application, we reconstruct the example of rank 7 due to Grunewald and Zimmert [**2**] in Section 5.

I would like to express my gratitude to Professor Fumio Hazama for his useful advice. And I also thank Professor Kenneth A. Ribet and Professor Robert Coleman for their stimulating conversation.

2. Generic case and its specialization.

In this section, we construct an elliptic curve with rank n defined over the function field of an algebraic variety. Let E be an elliptic curve over a field k of characteristic $\neq 2$ defined by the following equation

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

and let $f(x)$ be the right hand side of the equation of E. Then we can express E^n by the simultaneous equation:

$$y_i^2 = f(x_i) \qquad (i = 1, \dots, n).$$

Let ι_i the involution on E^n defined by $\iota((x_i, y_i)) = (x_i - y_i)$ $(i = 1, \dots, n)$ and put $V_n = E^n/\langle(\iota_1, \dots, \iota_n)\rangle$, then the function field of V_n is the set of the invariant elements of the function field of E^n under the action of $\langle(\iota_1, \dots, \iota_n)\rangle$. Consequently,

$$k(V_n) = k(E^n)^{\langle(\iota_1,\dots,\iota_n)\rangle} = k(y_1y_2, \dots, y_1y_n, x_1, \dots, x_n).$$

Since $(y_1y_{i+1})^2 = f(x_1)f(x_{i+1})$ holds for $i = 1, \dots, n-1$, we find that V_n is defined by

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

(Here we rename y_1y_{i+1} as y_i.) Let E_b be the twist of E by the quadratic extension $k(E^n)/k(V_n)$. It is defined by the equation

$$f(x_1)y^2 = f(x)$$

(see [**3**, §4]). Let $E_b(k(V_n))$ be the group of $k(V_n)$-rational points on E_b.

Theorem 2.1 (Hazama)**.** *If* $\mathrm{End}_k(E) \cong \mathbb{Z}$*, then the rank of* $E_b(k(V_n))$ *is* n*, and its generators are the following:*

$$(x_1, 1) \quad \left(x_{i+1},\ \frac{y_i}{f(x_1)}\right) \qquad (i = 1, \dots, n-1).$$

Now, we can obtain a given elliptic curve with its generators by specializing the above twisted generic elliptic curve at a certain k-rational point on V_n as follows:

Proposition 2.2. *Let* E *be a given elliptic curve defined by the following equation*

$$E : y^2 = ax^3 + bx^2 + cx + d,$$

and let (α_i, β_i) $(i = 1, \dots, n)$ *be its independent generators. Let* E_b *be the twist of* E *by* $k(E^n)/k(V_n)$*. Then* E *with these generators is obtained by specialization at the point* $(x_1, \dots, x_n,\ y_1, \dots, y_{n-1}) = (\alpha_1, \dots, \alpha_n,\ \beta_1\beta_2, \dots, \beta_1\beta_n)$ *on* V_n*.*

Proof. Put $x_i = \alpha_i$ $(i = 1, \dots, n)$. Then $E_b : f(x_1)y^2 = f(x)$ is isomorphic to $y^2 = f(x)$ by the map $(x, y) \mapsto (x, \beta_1 y)$. Here the generators of twisted elliptic curve become $(\alpha_1, 1)$, $\left(\alpha_{i+1}, \frac{\beta_{i+1}}{\beta_1}\right)$ $(i = 1, \dots, n-1)$. Therefore they are mapped to (α_i, β_i) $(i = 1, \dots, n-1)$. □

3. The structure of the base space.

In this section, we investigate the structure of the variety V_n defined in Section 1 in each case.

The case of rank 1 is slightly different from the other cases, and can be treated easily. More precisely, the twisted elliptic curve

$$E_b : f(x_1)y^2 = ax^3 + bx^2 + cx + d, \tag{3}$$

has a rational point $(x_1, 1) \in E_b(k(x_1))$, and it follows from Theorem 2.1 that it is of rank one as an elliptic curve over $k(x_1)$. But a generalization opposed to a specialization decreases the rank of an elliptic curve, hence E_b regarded as an elliptic curve over $k(x_1, a, b, c, d)$ is of rank 1.

As is seen from this argument for the case of rank 1, it is natural to regard V_n defined by (2) $(n \geq 2)$ as an algebraic variety defined over $K = k(x_1, \dots, x_n)$. Therefore V_n is a 3-dimensional subvariety in the projective $n+2$ space $\mathbb{P}^{n+2}$ with coordinates $(a, b, c, d, y_1, \dots, y_{n-1})$, and E_b is regarded as a generic fiber of the elliptic fiber space defined by Equation (3) over V_n.

Case of rank 2. Our V_2 is defined by one quadratic equation with a rational point $P_1\ (a,b,c,d,y_1) = (0,0,0,1,1)$, hence V_2 is K-rational and we can parametrize K-rational points on V_2 as follows:

Theorem 3.1. *V_2 is rational, in fact, each K-rational point on V_2 is expressed as*

$$((S+T)p_1,\ (S+T)p_2,\ (S+T)p_3,\ (S+T)p_4 - ST,\ -ST),$$

where $(p_1,p_2,p_3,p_4) \in \mathbb{P}^3$ and

$$S = p_1x_1^3 + p_2x_1^2 + p_3x_1 + p_4, \quad T = p_1x_2^3 + p_2x_2^2 + p_3x_2 + p_4.$$

Case of rank 3. We recall two results which will be frequently used later. The first of them is classical and well-known (see [**1**], for example), but in view of the fundamental role played by it, we recall its proof.

Lemma 3.2. *Let V be a complete intersection of l quadrics in $\mathbb{P}^{l-1}$ defined over k. Suppose that it contains a linear subvariety W k-isomorphic to $\mathbb{P}^{l-1}$. Then V is k-rational.*

Proof. There is a k-linear subvariety L k-isomorphic to $\mathbb{P}^n$ such that the intersection of W and L is empty. For any point P on $L(k)$, let M be the variety spanned by $\{P\}$ and W, which is k-isomorphic to $\mathbb{P}^l$. Then we can express the intersection of the variety defined by i-th equation of V and M as the union of W and a k-linear subvariety $W_i \cong \mathbb{P}^{l-1}$. Since W_i $(i = 1,\dots,l)$ are in M, we get a k-rational point Q as intersection of W_i $(i = 1,\dots,l)$. The map $\varphi : L \to V$ defined by $\varphi(P) = Q$ gives a birational map from $L(\cong \mathbb{P}^{n-l})$ to V. □

The next result is from an elementary linear algebra:

Lemma 3.3. *Let N be a given $n \times (n+1)$ matrix and we denote the matrix removed i-th column by N_i. The homogeneous equation*

$$N \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \\ \lambda_{n+1} \end{pmatrix} = 0$$

in $\mathbb{P}^n$ has a unique solution if N is of full rank. And then the solution is

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_i \\ \vdots \\ \lambda_{n+1} \end{pmatrix} = \begin{pmatrix} \det(N_1) \\ \vdots \\ (-1)^{i+1}\det(N_i) \\ \vdots \\ (-1)^{n+2}\det(N_{n+1}) \end{pmatrix}.$$

Now we show that V_3 is birational to $\mathbb{P}^3$. As V_3 is a $(2,2)$-intersection in $\mathbb{P}^5$ with coordinates (a,b,c,d,y_1,y_2) and contains a line W defined by the equations $x_1^2a + x_1b + c = 0$, $d = y_1 = y_2 = 0$, therefore we can apply Lemma 3.2 and 3.3. Note that W is spanned by $S_1 = (1,0,-x_1^2,0,0,0)$, $S_2 = (0,1,-x_1,0,0,0)$. By a direct computation based on the map φ in the proof of Lemma 3.2, we obtain the following:

Theorem 3.4. *V_3 is rational. Every K-rational point on V_3 is given by*

$$(\lambda + \nu p_1,\ \mu,\ -\lambda x_1^2 - \mu x_1,\ \nu p_2,\ \nu p_3,\ \nu p_4),$$

where $(p_1,p_2,p_3,p_4) \in \mathbb{P}^3$ and

$$\begin{aligned}
&(\lambda,\mu,\nu)\\
&= \big(x_1^3x_2x_3(x_3-x_2)(x_1x_3-x_2x_3+x_1x_2)p_1^2\\
&\quad -(x_3-x_2)(x_1^4-(x_2+x_3)x_1^3-x_1x_2x_3(x_2+x_3)+x_2^2x_3^2)p_1p_2\\
&\quad +(x_3-x_2)(x_2-x_1+x_3)p_2^2-x_3(x_3-x_1)p_3^2+x_2(x_2-x_1)p_4^2,\\
&\quad -x_1^5x_2x_3(x_3^2-x_2^2)p_1^2\\
&\quad -x_1^2(x_1+x_2)(x_1+x_3)(x_3-x_2)(x_2+x_3-x_1)p_1p_2\\
&\quad -(x_3(x_3^2-x_1^2)-x_2(x_2^2-x_1^2))p_2^2+x_3(x_3^2-x_1^2)p_3^3-x_2(x_2^2-x_1^2)p_4^2,\\
&\quad x_2x_3(p_1x_1^3+p_2)(x_3-x_1)(x_2-x_1)(x_3-x_2)\big) \in \mathbb{P}^2.
\end{aligned}$$

Case of rank 4. In this case, V_4 contains the plane W defined by the equations $x_1^3a + x_1^2b + x_1c + d = 0$, $y_1 = y_2 = y_3 = 0$. Hence by a similar argument to the one employed in the case of rank 3, we obtain the following:

Theorem 3.5. *V_4 is rational. Every K-rational point on V_4 is expressed as*

$$(\lambda + \rho p_1,\ \mu,\ \nu,\ -(\lambda x_1^3 + \mu x_1^2 + \nu x_1),\ \rho p_2,\ \rho p_3,\ \rho p_4),$$

where $(p_1,p_2,p_3,p_4) \in \mathbb{P}^3$ and

$$\begin{aligned}
&(\lambda,\mu,\nu,\rho)\\
&= \big(-x_1^3p_1^2(x_3-x_2)(x_4-x_2)(x_4-x_3)\\
&\qquad \cdot(x_1^2(x_2+x_3+x_4)-x_1(x_2x_3+x_3x_4+x_2x_4)+x_2x_3x_4)\\
&\quad +p_2^2(x_3-x_2)(x_4-x_1)(x_4-x_3)\\
&\quad -(x_2-x_1)((x_4-x_1)(x_4-x_2)p_3^2-(x_3-x_1)(x_3-x_2)p_4^2)\big),\\
&\quad x_1^6p_1^2(x_3-x_2)(x_4-x_2)(x_4-x_3)(x_2+x_3+x_4)\\
&\quad -p_2^2(x_3-x_1)(x_4-x_1)(x_4-x_3)(x_1+x_3+x_4)\\
&\quad +p_3^2(x_2-x_1)(x_4-x_1)(x_4-x_2)(x_1+x_2+x_4)
\end{aligned}$$

$$
\begin{aligned}
&- p_4^2(x_2-x_1)(x_3-x_1)(x_3-x_2)(x_1+x_2+x_3),\\
&- x_1^6p_1^2(x_3-x_2)(x_4-x_2)(x_4-x_3)(x_2x_3+x_3x_4+x_2x_4)\\
&+ p_2^2(x_3-x_1)(x_4-x_1)(x_4-x_3)(x_1x_3+x_3x_4+x_1x_4)\\
&- p_3^2(x_2-x_1)(x_4-x_1)(x_4-x_2)(x_1x_2+x_2x_4+x_1x_4)\\
&+ p_4^2(x_2-x_1)(x_3-x_1)(x_3-x_2)(x_1x_2+x_2x_3+x_1x_3),\\
&p_1x_1^3(x_2-x_1)(x_3-x_1)(x_3-x_2)(x_4-x_1)(x_4-x_2)(x_4-x_3)\big).
\end{aligned}
$$

Before proceeding to the case of rank ≥ 5, we state the following theorem. It can be proved by a similar argument to the one for [**4**, Theorem 2.1].

Theorem 3.6. *Let V_n be the algebraic variety over K defined by* (2) *where we regard a, b, c, d and y_i $(i = 1, \dots, n-1,\ n \geq 5)$ as variables. Then V_n is K-birational to the variety $\bar{V}_n$ defined by the equations*

$$\begin{vmatrix} 0 & 1 & 2 & 3 & i \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 & Y_i^2 \end{vmatrix} = 0 \qquad (i = 4, \dots, n-1)$$

in $\mathbb{P}^{n-1}$ with coordinate $(Y_0, \dots, Y_{n-1})$, where we write $\begin{vmatrix} 0 & 1 & 2 & 3 & i \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 & Y_i^2 \end{vmatrix}$ for the determinant $\begin{vmatrix} 1 & 1 & 1 & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_i \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_i^2 \\ \alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & \alpha_i^3 \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 & Y_i^2 \end{vmatrix}$ $(i = 4, \dots, n-1)$, and $\alpha_i = x_{i+1}$ $(i = 0, \dots, n-1)$.

Case of rank 5. In this case, $\bar{V}_5$ in Theorem 3.6 is defined by one quadric equation with a rational point $P_1 = (1, 1, 1, 1, 1)$. Hence we have the following theorem which is similar to Theorem 3.1:

Theorem 3.7. *$\bar{V}_5$ is rational. Every K-rational point on $\bar{V}_5$ is expressed as*

$$(2p_1S - T,\ 2p_2S - T,\ 2p_3S - T,\ 2p_4S - T,\ -T),$$

where $(p_1, p_2, p_3, p_4) \in \mathbb{P}^3$ and

$$S = \begin{vmatrix} 0 & 1 & 2 & 3 & 4 \\ p_1 & p_2 & p_3 & p_4 & 0 \end{vmatrix}, \quad \begin{vmatrix} 0 & 1 & 2 & 3 & 4 \\ p_1^2 & p_2^2 & p_3^2 & p_4^2 & 0 \end{vmatrix}.$$

Case of rank 6. In this case, $\bar{V}_6$ is a $(2,2)$-intersection in $\mathbb{P}^5$ and contains a line W which is spanned by $S_1 = (1, 1, 1, 1, 1, 1)$, $S_2 = (\alpha_0, \dots, \alpha_5)$. Therefore, we can apply Lemma 3.2. Let L be a linear subspace spanned by

$$
\begin{aligned}
S_3 &= (\alpha_4-\alpha_5,\ 0,\ 0,\ 0,\ \alpha_5-\alpha_0,\ \alpha_0-\alpha_4),\\
S_4 &= (\ 0,\ \alpha_4-\alpha_5,\ 0,\ 0,\ \alpha_5-\alpha_1,\ \alpha_1-\alpha_4),\\
S_5 &= (\ 0,\ 0,\ \alpha_4-\alpha_5,\ 0,\ \alpha_5-\alpha_2,\ \alpha_2-\alpha_4),\\
S_6 &= (\ 0,\ 0,\ 0,\ \alpha_4-\alpha_5,\ \alpha_5-\alpha_3,\ \alpha_3-\alpha_4).
\end{aligned}
$$

For any point $P = p_1S_3 + p_2S_4 + p_3S_5 + p_4S_6$ on L, the point on M is represented by the form $\lambda S_1 + \mu S_2 + \nu P$. We denote the i-th coordinate of P by $P(i-1)$. Then the equation of $W_1 \cap W_2$ is easily seen to be

$$N \begin{pmatrix} \lambda \\ \mu \\ \nu \end{pmatrix} = 0,$$

where N is a 2×3-matrix (N_{ij}) defined by

$$\begin{aligned}
N_{11} &= 2 \begin{vmatrix} 0 & 1 & 2 & 3 & 4 \\ P(0) & P(1) & P(2) & P(3) & P(4) \end{vmatrix}, \\
N_{12} &= 2 \begin{vmatrix} 0 & 1 & 2 & 3 & 4 \\ \alpha_0 P(0) & \alpha_1 P(1) & \alpha_2 P(2) & \alpha_3 P(3) & \alpha_4 P(4) \end{vmatrix}, \\
N_{13} &= \begin{vmatrix} 0 & 1 & 2 & 3 & 4 \\ P(0)^2 & P(1)^2 & P(2)^2 & P(3)^2 & P(4)^2 \end{vmatrix}, \\
N_{21} &= 2 \begin{vmatrix} 0 & 1 & 2 & 3 & 5 \\ P(0) & P(1) & P(2) & P(3) & P(5) \end{vmatrix}, \\
N_{22} &= 2 \begin{vmatrix} 0 & 1 & 2 & 3 & 5 \\ \alpha_0 P(0) & \alpha_1 P(1) & \alpha_2 P(2) & \alpha_3 P(3) & \alpha_5 P(5) \end{vmatrix}, \\
N_{23} &= \begin{vmatrix} 0 & 1 & 2 & 3 & 5 \\ P(0)^2 & P(1)^2 & P(2)^2 & P(3)^2 & P(5)^2 \end{vmatrix}.
\end{aligned}$$

Then by Lemma 3.3,

$$\begin{pmatrix} \lambda \\ \mu \\ \nu \end{pmatrix} = \begin{pmatrix} \det(N_1) \\ -\det(N_2) \\ \det(N_3) \end{pmatrix},$$

where N_i is the 2×2-matrix with the i-th column removed from N. Hence the point on $\bar{V}_6$ which corresponds to P is $\lambda S_1 + \mu S_2 + \nu P$, where $(\lambda, \mu, \nu) = (\det(N_1), -\det(N_2), \det(N_3))$. Hence we have the following:

Theorem 3.8. *$\bar{V}_6$ is rational. Every K-rational point on $\bar{V}_6$ is expressed as*

$$\begin{aligned}
\Big(& \lambda + \mu\alpha_0 + \nu p_1(\alpha_4 - \alpha_5), \quad \lambda + \mu\alpha_1 + \nu p_2(\alpha_4 - \alpha_5), \\
& \lambda + \mu\alpha_2 + \nu p_3(\alpha_4 - \alpha_5), \quad \lambda + \mu\alpha_3 + \nu p_4(\alpha_4 - \alpha_5), \\
& \lambda + \mu\alpha_4 + \nu \sum_{i=0}^{3} p_{i+1}(\alpha_5 - \alpha_i), \ \lambda + \mu\alpha_5 + \nu \sum_{i=0}^{3} p_{i+1}(\alpha_i - \alpha_4) \Big)
\end{aligned}$$

where $(p_1, p_2, p_3, p_4) \in \mathbb{P}^3$,

$$(\lambda, \mu, \nu) = (N_{12}N_{23} - N_{13}N_{22}, -N_{11}N_{23} + N_{13}N_{21}, N_{11}N_{22} - N_{12}N_{21})$$

with N_{ij} as above.

Case of rank 7. In this case, $\bar{V}_7$ is a $(2,2,2)$-intersection in $\mathbb{P}^6$. Unfortunately, this is not rational and only unirational [**1**]. To remedy this situation, we consider

$$E : y^2 = ax^4 + bx^3 + cx^2 + dx + e$$

instead of (1). Let $f(x)$ be the right hand side of the equation of E and V_7 the variety defined by the equation

$$y_i^2 = f(x_1)f(x_{i+1}) \qquad (i = 1, \dots, 6).$$

Repeating a similar argument to the one given above, we obtain the variety which is birational to V_7 defined by the equation,

$$\begin{vmatrix} 0 & 1 & 2 & 3 & 4 & i \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 & Y_4^2 & Y_i^2 \end{vmatrix} = 0 \qquad (i = 5, 6, 7).$$

We call this $\bar{V}_7$. This is in $\mathbb{P}^7$ and its dimension is 4. Note that $\bar{V}_7$ contains a plane W spanned by $S_1 = (1, \dots, 1)$, $S_2 = (\alpha_0, \dots, \alpha_7)$, $S_3 = (\alpha_0^2, \dots, \alpha_7^2)$. Hence we are in the same situation as the case of rank 6. Thus we have the following theorem which can be proved similarly:

Theorem 3.9. *$\bar{V}_7$ is rational. Every K-rational point on $\bar{V}_7$ is expressed as*

$$\begin{aligned} &\big(\lambda + \mu\alpha_0 + \nu\alpha_0^2,\ \lambda + \mu\alpha_1 + \nu\alpha_1^2,\ \lambda + \mu\alpha_2 + \nu\alpha_2^2, \\ &\lambda + \mu\alpha_3 + \nu\alpha_3^2 + \rho p_1,\ \lambda + \mu\alpha_4 + \nu\alpha_4^2 + \rho p_2,\ \lambda + \mu\alpha_5 + \nu\alpha_5^2 + \rho p_3, \\ &\lambda + \mu\alpha_6 + \nu\alpha_6^2 + \rho p_4,\ \lambda + \mu\alpha_7 + \nu\alpha_7^2 + \rho p_5\big), \end{aligned}$$

where $(p_1, p_2, p_3, p_4, p_5) \in \mathbb{P}^4$ and

$$(\lambda, \mu, \nu) = (\det(N_1), -\det(N_2), \det(N_3), -\det(N_4))$$

with N_i $(i = 1, \dots, 4)$ as following:

$$\begin{aligned} N_{11} &= 2\begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 0 & p_1 & p_2 & p_3 \end{vmatrix}, \\ N_{12} &= 2\begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 0 & \alpha_3 p_1 & \alpha_4 p_2 & \alpha_5 p_3 \end{vmatrix}, \\ N_{13} &= 2\begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 0 & \alpha_3^2 p_1 & \alpha_4^2 p_2 & \alpha_5^2 p_3 \end{vmatrix}, \\ N_{14} &= \begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 0 & p_1^2 & p_2^2 & p_3^2 \end{vmatrix}, \\ N_{21} &= 2\begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 6 \\ 0 & 0 & 0 & p_1 & p_2 & p_4 \end{vmatrix}, \\ N_{22} &= 2\begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 6 \\ 0 & 0 & 0 & \alpha_3 p_1 & \alpha_4 p_2 & \alpha_6 p_4 \end{vmatrix}, \\ N_{23} &= 2\begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 6 \\ 0 & 0 & 0 & \alpha_3^2 p_1 & \alpha_4^2 p_2 & \alpha_6^2 p_4 \end{vmatrix}, \end{aligned}$$

$$N_{24} = \begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 6 \\ 0 & 0 & 0 & p_1^2 & p_2^2 & p_4^2 \end{vmatrix},$$

$$N_{31} = 2\begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 7 \\ 0 & 0 & 0 & p_1 & p_2 & p_5 \end{vmatrix},$$

$$N_{32} = 2\begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 7 \\ 0 & 0 & 0 & \alpha_3 p_1 & \alpha_4 p_2 & \alpha_7 p_5 \end{vmatrix},$$

$$N_{33} = 2\begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 7 \\ 0 & 0 & 0 & \alpha_3^2 p_1 & \alpha_4^2 p_2 & \alpha_7^2 p_5 \end{vmatrix},$$

$$N_{34} = \begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 7 \\ 0 & 0 & 0 & p_1^2 & p_2^2 & p_5^2 \end{vmatrix}.$$

Remark 3.10. In the case of $n \leq 4$, one can write down immediately the defining equation of elliptic curve which corresponds to a point on V_n. In the case of $n \geq 5$, let $P = (\bar{y}_0, \ldots, \bar{y}_{n-1})$ be a rational point on $\bar{V}_n$. Then, the defining equation of the elliptic curve which corresponds to P is

$$\begin{vmatrix} 1 & 1 & 1 & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & x \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & x^2 \\ \alpha_0^3 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & x^3 \\ \bar{y}_0^2 & \bar{y}_1^2 & \bar{y}_2^2 & \bar{y}_3^2 & y^2 \end{vmatrix} = 0.$$

This is obtained by tracing the birational map between V_n and $\bar{V}_n$.

4. The value of the parameter which corresponds to a given elliptic curve.

In view of Proposition 2.2, every elliptic curve with rank n should correspond to a point of V_n. In this section, we give the values of the parameters for this point of V_n $(2 \leq n \leq 7)$. let E be an elliptic curve defined by the following equation

$$y^2 = ax^3 + bx^2 + cx + d$$

with independent generators (x_i, y_i) $(i = 1, \ldots, r,\ 2 \leq r \leq 7)$. Then we have the values of parameters as follows:

$r = 2$

$$(p_1, p_2, p_3, p_4) = (a, b, c, d - y_1 y_2),$$

$r = 3$

$$(p_1, p_2, p_3, p_4) = \left(\frac{a x_1^2 + b x_1 + c}{x_1^2}, d, y_1 y_2, y_1 y_3 \right),$$

$r = 4$

$$(p_1, p_2, p_3, p_4) = \left(\frac{y_1}{x_1^3}, y_2, y_3, y_4 \right),$$

$r = 5$

$$(p_1, p_2, p_3, p_4) = (y_1 - y_5, y_2 - y_5, y_3 - y_5, y_4 - y_5),$$

$r = 6$

$$\begin{aligned} p_j &= -\left(\sum_{i=1}^{6}(x_6 - x_{i+1})\right)\left(\sum_{i=1}^{6} x_{i+1}(x_6 - x_{i+1})\right)\left(\sum_{i=1}^{6} y_{i+1}(x_5 - x_{i+1})\right) \\ &\quad + \left(\sum_{i=1}^{6}(x_5 - x_{i+1})\right)\left(\sum_{i=1}^{6} x_{i+1}(x_6 - x_{i+1})\right)\left(\sum_{i=1}^{6} y_{i+1}(x_6 - x_{i+1})\right) \\ &\quad - \left(\sum_{i=1}^{6}(x_5 - x_{i+1})\right)\left(\sum_{i=1}^{6} x_{i+1}(x_6 - x_{i+1})\right)\left(\sum_{i=1}^{6} y_{i+1}(x_6 - x_{i+1})\right) \\ &\quad + \left(\sum_{i=1}^{6}(x_6 - x_{i+1})\right)\left(\sum_{i=1}^{6} x_{i+1}(x_5 - x_{i+1})\right)\left(\sum_{i=1}^{6} y_{i+1}(x_6 - x_{i+1})\right) \\ &\quad + x_j \left(\sum_{i=1}^{6}(x_6 - x_{i+1})\right)\left(\left(\sum_{i=1}^{6}(x_6 - x_{i+1})\right)\left(\sum_{i=1}^{6} y_{i+1}(x_5 - x_{i+1})\right)\right. \\ &\qquad \left. - \left(\sum_{i=1}^{6}(x_5 - x_{i+1})\right)\left(\sum_{i=1}^{6} y_{i+1}(x_6 - x_{i+1})\right)\right) \\ &\quad + y_j \left(\sum_{i=1}^{6}(x_6 - x_{i+1})\right)\left(\left(\sum_{i=1}^{6}(x_5 - x_{i+1})\right)\left(\sum_{i=1}^{6} x_{i+1}(x_6 - x_{i+1})\right)\right. \\ &\qquad \left. - \left(\sum_{i=1}^{6}(x_6 - x_{i+1})\right)\left(\sum_{i=1}^{6} x_{i+1}(x_5 - x_{i+1})\right)\right), \end{aligned}$$

$(j = 1, \ldots, 4)$.

In the case $r = 7$, let E be an elliptic curve defined by the following equation

$$y^2 = ax^4 + bx^3 + cx^2 + dx + e$$

with independent generators (x_i, y_i) $(i = 1, \dots, 8)$. Then the values of the parameters are given by the formula

$$\begin{aligned} p_i = {} & (x_3 - x_2)(y_1(x_2x_3 - x_3x_{i+3} - x_2x_{i+3} + x_{i+3}^2) - y_{i+3}x_2x_3) \\ & - (x_3 - x_1)(y_2(x_1x_3 - x_3x_{i+3} - x_1x_{i+3} + x_{i+3}^2) - y_{i+3}x_1x_3) \\ & + (x_2 - x_1)(y_3(x_1x_2 - x_2x_{i+3} - x_2x_{i+3} + x_{i+3}^2) - y_{i+3}x_1x_2), \\ & (i = 1, \dots, 5). \end{aligned}$$

5. Examples.

In the previous sections, we have given a parametric representation of V_n $(1 \leq n \leq 7)$. Therefore we will get as many elliptic curves with specified rank as we like by specialization at rational points on V_n. As an example, we give the values of parameters which enable one to obtain the elliptic curve with rank 7 in [**2**, Corollary C]. The elliptic curve is

$$y^2 = x^3 - 1717730532x + 27401746395780$$

with generators

$$(24144,\ 56466),\ (23562,\ 97182),\ (23736,\ 50022),\ (24840,\ 245430),$$
$$(25422,\ 404082),\ (23793,\ 34119),\ (26121,\ 596187).$$

The values of the parameters are

$$\begin{aligned} (p_1, p_2, p_3, p_4, p_5) = (&47822467248393469632, \\ &66206014691795224675,\ 104521834162171114920, \\ &76522282208132178600,\ 101559585548776675320), \end{aligned}$$

$$\begin{aligned} & (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) \\ & = \left(\frac{1}{234},\ -\frac{1}{348},\ -\frac{1}{174},\ \frac{1}{930},\ \frac{1}{1512},\ -\frac{1}{117},\ \frac{1}{2211},\ 0\right). \end{aligned}$$

References

[1] P.A. Beauville, *Variétés de Prym et Jacobiennes Intermédiaires*, Ann. Scient Éc. Norm. Sup., **4** (1977), 309-391.

[2] F.J. Grunewald and R. Zimmert, *Über einige rationale elliptische Kurven mit freien Rang* ≥ 8, J. Reine. Angew. Math., **296** (1977), 100-107.

[3] F. Hazama, *Rational points on certain abelian varieties over function fields*, J. Number Theory, **50** (1995), 278-285.

[4] H. Yamagishi, *On abelian surfaces with rank* 12 *associated to certain* $K3$ *surfaces*, in 'Algebraic cycles and related topics', Ed. F. Hazama, World Scientific, (1995), 93-102.

[5] ———, *Geometric construction of elliptic curves with given Mordell-Weil rank and* j*-invariant*, (submitted to Proceedings of the American Mathematical Society).

[6] ———, *A construction of families of elliptic curves of rank* 6 *with a nontrivial two-torsion point*, (submitted to Journal of Number Theory).

Received February 5, 1998 and revised June 24, 1998.

Tokyo Denki University
Saitama, 350-0394
Japan
E-mail address: hizuru@j.dendai.ac.jp