# POINTS DEFINED OVER CYCLIC QUARTIC EXTENSIONS ON AN ELLIPTIC CURVE AND GENERALIZED KUMMER SURFACES

Masato KUWATA
*Kanagawa Institute of Technology*
*1030 Shimo-Ogino*
*Atsugi-shi, Kanagawa,*
*243-0292 Japan*
kuwata@gen.kanagawa-it.ac.jp

## 1. Introduction

Let $E$ be an elliptic curve over a number field $k$. By the Mordell-Weil theorem the group $E(K)$ of $K$-rational points on $E$, where $K/k$ is a finite extension of $k$, is a finitely generated abelian group. We fix $E/k$ once and for all, and we study the behavior of the rank of the group $E(K)$ as $K$ varies through a certain family. We are particularly interested in the family $\mathcal{F}_k(G)$ of all Galois extensions $K/k$ whose Galois group $\mathrm{Gal}(K/k)$ is isomorphic to a prescribed finite group $G$. In this article we focus on the case $G = \mathbb{Z}/4\mathbb{Z}$.

One case that has been well studied is the case where $G = \mathbb{Z}/2\mathbb{Z}$. If an elliptic curve $E/k$ is given by the Weierstrass equation $y^2 = x^3 + Ax + B$, and $d$ is a nonzero element of $k$, the quadratic twist of $E$ by $d$, denoted by $E_d$, is given by the equation $dy^2 = x^3 + Ax + B$. Since we have the relation $\operatorname{rank} E(k(\sqrt{d})) = \operatorname{rank} E(k) + \operatorname{rank} E_d(k)$, studying the behavior of the rank of $E(k(\sqrt{d}))$, as $k(\sqrt{d})$ varies through $\mathcal{F}_k(\mathbb{Z}/2\mathbb{Z})$, is equivalent to studying the family $\{E_d(k) \mid d \in k^\times/(k^\times)^2\}$. In this case it is very easy to find values of $d$ such that $\operatorname{rank} E_d(k)$ is positive. Indeed, take any integer $m$ in $k$, and write $m^3 + Am + B = dl^2$, then for almost all $m$, the point $(m, l) \in E_d(k)$ is of infinite order.

[received: July, 12; accepted in revised form: August, 15, 2002]

If $k$ is the field of rational numbers $\mathbb{Q}$, our problem is conjecturally equivalent to the vanishing of the quadratic twists of the $L$-function of $E$ (see [5] for more detail). Let $L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}$ be the $L$-function of $E/\mathbb{Q}$, and let $\chi : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times$ be a Dirichlet character of order 2. The twist of $L(E,s)$ by $\chi$ is given by $L(E,s,\chi) = \sum_{n=1}^{\infty} \chi(n) a_n n^{-s}$. In this case we have a functional equation that relates $L(E, 2-s, \chi)$ and $L(E,s,\chi)$, and this functional equation forces $L(E,1,\chi)$ to vanish for at least one half of quadratic characters.

When $\chi$ runs through Dirichlet characters of order $n$, there is no a priori reason that the twist $L(E,s,\chi)$ vanishes for infinitely many $\chi$'s. However, numerical experiments seem to suggest that $L(E,s,\chi)$ vanishes quite often when the order of the character is small (see [2]).

If $n$ is greater than 2, we do not dispose of an obvious method to find a point on $E$ defined over some cyclic extension of degree $n$. It turns out that we have a higher dimensional analogue of $E_d$ that is a variety over $k$ whose $k$-rational point corresponds to a point on $E$ defined over some cyclic extension $K/k$ of degree $n$. When $G = \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$, this variety is a surface which belongs to the class of surfaces called *generalized Kummer surfaces*. Earlier, we obtained some results for the case $G = \mathbb{Z}/3\mathbb{Z}$ by studying this surface (see [4]). When $G = \mathbb{Z}/4\mathbb{Z}$, it turns out that we have a stronger result:

**Theorem 1.1.** *Let $E$ be an elliptic curve over a number field $k$. Then there exist infinitely many cyclic quartic extensions $K/k$ such that* $\operatorname{rank} E(K)$ *is strictly greater than* $\operatorname{rank} E(K_2)$*, where $K_2$ is the unique intermediate quadratic extension of $k$ in $K$.*

**Corollary 1.2.** *Let $F_{k,G} = \bigcup_{K \in \mathcal{F}_k(G)} K$ be the compositum of all the Galois extensions of $k$ whose Galois group is isomorphic to $G$. Then the quotient group $E(F_{k,\mathbb{Z}/4\mathbb{Z}})/E(F_{k,\mathbb{Z}/2\mathbb{Z}})$ is not finitely generated.*

To prove our theorem we find a $k$-rational curve contained in the generalized Kummer surface in question, and write down its equation explicitly.

The author would like to thank Professor Hershy Kisilevsky and Dr. Jack Fearnley for useful conversations. He would also thank Professors Katsuya Miyake and Ki-ichiro Hashimoto for giving me an opportunity to present an earlier version of this paper at the conference "Galois theory and Modular forms" at the Tokyo Metropolitan University.

## 2. A generalized Kummer surface

Let $E$ be an elliptic curve over $k$. Consider the automorphism $\rho$ of $E \times E$ given by

$$\begin{array}{rccc} \rho & : & E \times E & \longrightarrow & E \times E \\ & & (P, Q) & \longmapsto & (Q, -P). \end{array}$$

It is easy to see that $\rho$ is of order 4, and $\rho^2$ is the multiplication-by-$(-1)$ map. Let $X$ be the quotient of $E \times E$ by the group $\langle \rho \rangle$ generated by $\rho$, and let $\widetilde{X}$ be its minimal non-singular model obtained by blowing-ups. $\widetilde{X}$ is a generalized Kummer surface (cf. Katsura [3], Bertin [1]). In particular $\widetilde{X}$ is a $K3$ surface.

The set of fixed points of $\rho$ consists of the four points of the form $(T, T)$, where $T$ is a 2-torsion point. The set of fixed points of $\rho^2$ consists of the sixteen points of the form $(T, S)$, where $T$ and $S$ are 2-torsion points. Thus $\rho$ acts freely away from these sixteen points. We denote by $X^\circ$ the open set of $X$ obtained by removing the image of these sixteen points in $X$.

**Lemma 2.1.** *If the equivalence classes* $[P, Q]$ *is in the set of* $k$*-rational points* $X^\circ(k)$*, then* $(P, Q)$ *satisfies one of the following*:

(1) $P$ *and* $Q$ *are defined over* $k$.

(2) $P$ *and* $Q$ *are both defined over some quadratic extension* $k(\sqrt{d})/k$. *If* $\tau \in \mathrm{Gal}(k(\sqrt{d})/k)$ *is the generator, then we have* $\tau(P) = -P$ *and* $\tau(Q) = -Q$.

(3) $P$ *and* $Q$ *are both defined over some cyclic quartic extension* $K/k$. *If we choose a suitable generator* $\sigma \in \mathrm{Gal}(K/k)$*, then we have* $\sigma(P) = Q$ *and* $\sigma(Q) = -P$.

*Proof.* Let $P$ and $Q$ be points on $E(\bar{k})$, and suppose that $[P, Q] \in X^\circ(k)$. If $\sigma$ is an element of $\mathrm{Gal}(\bar{k}/k)$, then $(\sigma(P), \sigma(Q))$ is one of the following four pairs: $(P, Q)$, $\rho(P, Q) = (Q, -P)$, $\rho^2(P, Q) = (-P, -Q)$ or $\rho^3(P, Q) = (-Q, P)$. Note that these four pairs are distinct since $[P, Q]$ is in $X^\circ$. We can therefore define a map $\psi : \mathrm{Gal}(\bar{k}/k) \to \langle \rho \rangle$. Since the automorphism $\rho$ is defined over $k$, it commutes with any element of $\mathrm{Gal}(\bar{k}/k)$. Thus, if $\sigma_1(P, Q) = \rho^i(P, Q)$ and $\sigma_2(P, Q) = \rho^j(P, Q)$, then $\sigma_1\big(\sigma_2(P, Q)\big) = \sigma_1\big(\rho^j(P, Q)\big) = \rho^i\big(\rho^j(P, Q)\big) = \rho^{i+j}(P, Q)$. This shows that the map $\psi$ is a homomorphism.

Let $K$ be the Galois extension of $k$ corresponding to $\ker \psi$ via Galois theory. Then $\mathrm{Gal}(K/k)$ is isomorphism to a subgroup of $\langle \rho \rangle$. If $\mathrm{Gal}(K/k) = \{\mathrm{id}\}$, then $K = k$, and both $P$ and $Q$ are defined over $k$. This is the case (1).

If $\mathrm{Gal}(K/k) \simeq \langle\rho^2\rangle$, then $K$ is a quadratic extension of $k$. Let $\tau \in \mathrm{Gal}(\bar{k}/k)$ be an element whose image in $\mathrm{Gal}(K/k)$ generates $\mathrm{Gal}(K/k)$. Then $\psi(\tau) = \langle\rho^2\rangle$. This shows that $\tau(P,Q) = \rho^2(P,Q) = (-P,-Q)$. This is the case (2).

If $\mathrm{Gal}(K/k) \simeq \langle\rho\rangle$, then $K$ is a cyclic quartic extension. Let $\sigma \in \mathrm{Gal}(\bar{k}/k)$ be an element whose image in $\mathrm{Gal}(K/k)$ maps to $\rho$ by $\psi$. Then we have $\sigma(P,Q) = (Q,-P)$. This implies that $Q = \sigma(P)$ and $\sigma^2(P) = \sigma(Q) = -P$. This is the case (3). □

Conversely, if we have a point $P$ defined over some cyclic quartic extension of $k$, we have the following.

**Lemma 2.2.** *Let $P$ be a point whose field of definition is a cyclic quartic extension $K/k$. Let $\sigma$ be a generator of $\mathrm{Gal}(K/k)$. Define $P' = P - \sigma^2(P)$. Then $[P', \sigma(P')]$ is in $X(k)$. Furthermore, if $E$ does not have a $k$-rational 2-torsion point, then $[P', \sigma(P')]$ is in $X^\circ(k)$.*

*Proof.* First, note that $P'$ is not $O$. Otherwise, we have $P = \sigma^2(P)$, which is a contradiction to the fact that the field of definition of $P'$ is $K$. We see easily that $\sigma^2(P') = -P'$, which implies that $\sigma(P', \sigma(P')) = (\sigma(P'), \sigma^2(P')) = (\sigma(P'), -P') = \rho(P', \sigma(P'))$. This shows that $[P', \sigma(P')]$ is in $X(k)$.

Suppose that $[P', \sigma(P')]$ is not in $X^\circ(k)$. Then $P'$ is a 2-torsion point of $E$. Moreover, $P'$ is defined over the intermediate quadratic extension $K_2$ between $K$ and $k$, since we have $\sigma^2(P') = -P' = P'$. Then we see that either $P'$ itself or $P' + \sigma(P')$ is a $k$-rational 2-torsion point of $E$. □

## 3. Equation of the surface $X$

In this section we will write down an equation of $X$ in order to study $X$ in detail. We first fix an equation of $E$:

$$E : y^2 = x^3 + Ax + B. \tag{1}$$

For simplicity of exposition, we assume $AB \neq 0$ throughout. Let $k(E \times E)$ be the function field of $E \times E$. Then $k(E \times E)$ may be written as $k(x_1, x_2, y_1, y_2)$, where $(x_1, y_1)$ and $(x_2, y_2)$ both satisfy the equation (1). The automorphism induced by $\rho$ on $k(E \times E)$, also denoted by $\rho$, satisfies

$$\rho(x_1) = x_2, \quad \rho(x_2) = x_1, \quad \rho(y_1) = y_2, \quad \rho(y_2) = -y_1.$$

Let $Y$ be the quotient surface $E \times E/\langle\rho^2\rangle = E \times E/\{\pm 1\}$, which is a singular model of the Kummer surface associated with $E \times E$.

**Lemma 3.1.** *The function field $k(Y)$ of the quotient surface $Y$ is the subfield of $k(E \times E)$ generated by $x_1$, $x_2$ and $y = y_1/y_2$, which satisfy the equation*

$$(x_2^3 + Ax_2 + B)y^2 = x_1^3 + Ax_1 + B. \tag{2}$$

*Furthermore, the automorphism $\rho$ acts on $k(Y)$ by*

$$\rho(x_1) = x_2, \quad \rho(x_2) = x_1, \quad \rho(y) = -\frac{1}{y}.$$

*Proof.* It is easy to see that the elements $x_1$, $x_2$ and $y = y_1/y_2$ are fixed by the automorphism $\rho^2$ and thus belong to $k(Y)$. Also, it is easy to see that $x_1$, $x_2$ and $y$ satisfy the equation (2). We thus need to show that these three elements generate $k(Y)$. To see this it suffices to show that the degree of extension $[k(E \times E) : k(Y)]$ is 2. The element $y_1$ is a root of the quadratic equation in $T$ with coefficients in $k(Y)$:

$$T^2 - x_1^3 - Ax_1 - B = 0.$$

Thus, we have $[k(E \times E) : k(Y)] \leq 2$. The fact that $y_1$ and $y_2$ are independent in $k(E \times E)$ implies that $k(E \times E) \neq k(Y)$. Thus, we conclude $[k(E \times E) : k(Y)] = 2$. The action of $\rho$ on $y$ is given by

$$\rho(y) = \frac{\rho(y_1)}{\rho(y_2)} = \frac{y_2}{-y_1} = -\frac{1}{y}.$$

□

**Proposition 3.2.** *The function field $k(X)$ of the quotient surface $X = E \times E/\langle\rho\rangle$ is the subfield of $k(E \times E)$ generated by*

$$\xi = x_1 + x_2, \quad \eta = x_2 y - \frac{x_1}{y}, \quad t = y - \frac{1}{y},$$

*which satisfy the equation*

$$-t\xi^3 + 3\xi^2\eta + \eta^3 + A\left(t^2 + 4\right)\eta + Bt\left(t^2 + 4\right) = 0. \tag{3}$$

*Proof.* First, we can easily verify that the elements $\xi$, $\eta$ and $t$ are fixed by the automorphism $\rho$, and thus belong to $k(X)$. It is easy to see that $k(\xi, \eta, y) = k(x_1, x_2, y) = k(Y)$. This shows that $k(Y)$ is a quadratic extension of $k(\xi, \eta, t)$ obtained by adding $y$ satisfying $y^2 - ty - 1 = 0$.

To obtain a relation among $\xi$, $\eta$ and $t$, we first express the equation (2) in terms of $\xi$, $\eta$ and $y$, and then we eliminate $y$ using the relation $y^2 - ty - 1 = 0$. □

## 4. Rational curves on the surface $X$

In this section we show that there exist infinitely many parametrized curves defined over $k$ on the surface $X$. This allows us to show that there are infinitely many different cyclic quartic extensions such that the Mordell-Weil group over it increases from that over $k$.

Looking at the equation (2), we notice that the surface $Y = E \times E/\{\pm 1\}$ can be regarded as a family of cubic curves in the $x_1x_2$-plane parametrized by $y$. The projective model of this plane curve defined over $k(y)$ intersects with the line at infinity at three points. These are not defined over $k(y)$, but one of them is defined over the extension $k(\sqrt[3]{y})$. Writing $u = \sqrt[3]{y}$, we obtain a plane cubic curve defined over $k(u)$ given by

$$(x_2^3 + Ax_2 + B)u^6 = x_1^3 + Ax_1 + B \tag{4}$$

with a $k(u)$-rational point at infinity. The tangent line at this point intersects with the third point $P$ (see Figure 1), which is again $k(u)$-rational.

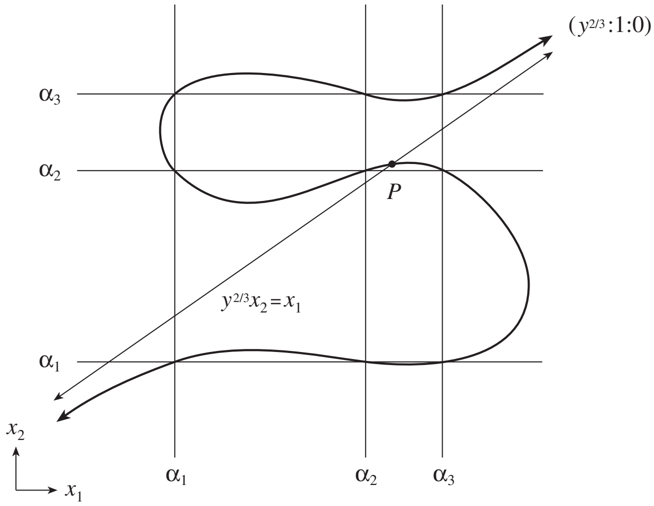


*Figure 1.* Plane cubic curve $(x_2^3 + Ax_2 + B)y^2 = x_1^3 + Ax_1 + B$.
(Here, $\alpha_1$,$\alpha_2$ and $\alpha_3$ are the three roots of $x^3 + Ax + B = 0$.)

A simple calculation shows that the coordinates of $P$ are given by

$$(x_1, x_2) = \left( \frac{-B(u^4 + u^2 + 1)}{A(u^2 + 1)}, \frac{-B(u^4 + u^2 + 1)}{Au^2(u^2 + 1)} \right). \tag{5}$$

In other words the triple cover $Y'$ of $Y$ defined by the equation (4) has a $k$-rational parametrized curve. The automorphism of $\rho$ on $Y$ can be lifted to the automorphism of $Y'$ by defining

$$\rho' : (x_1, x_2, u) \mapsto (x_2, x_1, -1/u).$$

It is easy to see that the parametrized curve obtained above is stable under the action of $\rho$. We have a commutative diagram:

$$\begin{tikzcd} Y' \arrow[r] \arrow[d, "\rho'"'] & Y \arrow[d, "\rho"] \\ Y' \arrow[r] & Y \end{tikzcd}$$

Let $X'$ be the quotient $Y'/\langle\rho\rangle$. The diagram above induce the diagram:

$$\begin{tikzcd} Y' \arrow[r] \arrow[d] & Y \arrow[d] \\ X' \arrow[r] & X \end{tikzcd}$$

**Proposition 4.1.** *The function field of the quotient $X' = Y'/\langle\rho\rangle$ is the subfield of $k(E \times E)$ generated by*

$$\xi = x_1 + x_2, \quad \eta = x_2 u^3 - \frac{x_1}{u^3}, \quad s = u - \frac{1}{u},$$

*which satisfy the equation*

$$\begin{aligned} &- s(s^2+3)\xi^3 + 3\xi^2\eta + \eta^3 \\ &\qquad + A(s^2+1)^2(s^2+4)\eta + Bs(s^2+1)^2(s^2+3)(s^2+4) = 0. \quad (6) \end{aligned}$$

*The covering map $X' \to X$ is given by $(\xi, \eta, s) \mapsto (\xi, \eta, s^3 + 3s)$.*

*Proof.* The proof goes similarly to that of Proposition 3.2. The last part is a consequence of the simple calculation

$$s^3 = \left(u - \frac{1}{u}\right)^3 = u^3 - \frac{1}{u^3} - 3\left(u - \frac{1}{u}\right) = y - \frac{1}{y} - 3s = t - 3s.$$

□

We think of the equation (6) as that of a cubic curve in $\xi\eta$-plane over the function field $k(s)$. This curve has two rational points, one at infinity and the other coming from $P$ on $Y$. Calculations show that the latter has coordinates

$$(\xi, \eta) = \left(\frac{-B(s^2+3)}{A}, \frac{-Bs(s^2+3)}{A}\right).$$

Choosing the point at infinity $(1 : s : 0)$ as the origin, we regard $X'$ as the elliptic curve over $k(s)$.

**Proposition 4.2.** *The equation* (6) *is transformed to the Weierstrass form*

$$\begin{aligned} Y^2 = {} & X^3 - 48A^2(s^2+4)^2 X \\ & - 16(s^2+4)^3\big((4A^3+27B^2)s^2(s^2+3)^2 + 8A^3\big) \end{aligned} \tag{7}$$

*by the transformation*

$$\begin{aligned} X &= \frac{4(s^2+4)}{(s\xi-\eta)}\Big(As(s^2+2)\xi + A(2s^2+1)\eta + 3Bs(s^2+1)(s^2+3)\Big), \\ Y &= \frac{12s(s^2+4)}{(s\xi-\eta)^2}\Big(3B(s^2+3)\big(s(s^2+2)\xi^2 - 2\xi\eta - s\eta^2\big) \\ &\qquad + 2A(s^2+1)^2(s^2+4)\big(A\eta + Bs(s^2+3)\big)\Big). \end{aligned}$$

*The point* $(\xi,\eta) = \big(-B(s^2+3)/A, -Bs(s^2+3)/A\big)$ *is transformed to*

$$\begin{aligned} (X,Y) = \Bigg(&\frac{4}{A^2}\big((A^3+9B^2)(s^2+3)^2 - A^3\big), \\ &\frac{36B(s^2+3)}{A^3}\big((A^3+6B^2)(s^2+3)^2 - A^3\big),\Bigg) \end{aligned} \tag{8}$$

*which is of infinite order.*

*Proof.* Converting to the Weierstrass form is standard and straight forward. The elliptic surface given by (7) has the following types of singular fibers under the condition $AB \neq 0$.

- $\mathrm{I}_0^*$ at $s^2+4=0$,
- $\mathrm{I}_2$ at $s(s^2+3)=0$,
- $\mathrm{I}_1$ at $(4A^3+27B^2)s^2(s^2+3)^2 + 16A^3 = 0$.

If the point given by (8) is a torsion point, its specialization at each fiber is a torsion point of the same order. Since a fiber of type $\mathrm{I}_0^*$ is isomorphic to $\mathbb{G}_a \times (\mathbb{Z}/2\mathbb{Z})^2$ as an algebraic group, its torsion points are of order 2. Since the $Y$-coordinate of the point (8) is not 0, it is not a point of order 2, and thus it is of infinite order. □

A $k(s)$-rational point on the elliptic curve (7) is one-to-one correspondence with a $k(s)$-rational point $(\xi(s), \eta(s))$ on the plane curve (6), which in turn gives a parametrized curve $(\xi(s), \eta(s), s^3+3s)$ on the surface $X$. Since Proposition 4.2 gives us infinitely many $k(s)$-rational points on (7), we have infinitely many $k$-rational parametrized curve on $X$.

## 5. Points on $E$ defined over cyclic quartic extensions

We have seen that the surface $X$ has a $k$-rationally parametrized curve

$$(\xi, \eta, t) = \left( \frac{-B(s^2+3)}{A}, \frac{-Bs(s^2+3)}{A}, s^3 + 3s \right) \tag{9}$$

with parameter $s$. This gives a point on $E$ defined over a quartic extension of $k(s)$.

**Lemma 5.1.** *Let $v$ be a root of the quadratic equation in $T$ with $k(u)$-coefficients*:

$$A(u^2+1)T^2 + A^3Bu^4(u^2+1)^2 + B^3(u^4+u^2+1)^3 = 0.$$

*Then $k(v)$ is a cyclic quartic extension of $k(s)$, and the elliptic curve $E$ has four $k(v)$-rational points*

$$\begin{aligned}(x, y) = &\left( \frac{-B(u^4+u^2+1)}{A(u^2+1)}, \pm \frac{v}{A(u^2+1)} \right), \\ &\left( \frac{-B(u^4+u^2+1)}{Au^2(u^2+1)}, \pm \frac{v}{Au^3(u^2+1)} \right).\end{aligned}$$

*Proof.* We have seen that the point on $X$ given by (9) comes from the point $P$ on the Kummer surface $Y$. We obtain four points in the lemma by taking the preimage of $P$ in $E \times E$. The arguments in §2 show that the field of definition of these points, $k(v)$, is a cyclic quartic extension of $k(s)$. This may be seen directly as $v$ satisfies the following quartic equation in $T$ with $k[s]$-coefficients

$$\begin{aligned}&A^2(s^2+4)T^4 \\ &\quad + AB(s^2+4)(s^4+3s^2+1)\big(A^3(s^2+4) + B^2(s^2+3)^3\big)T^2 \\ &\qquad + B^2\big(A^3(s^2+4) + B^2(s^2+3)^3\big)^2 = 0. \end{aligned} \tag{10}$$

□

*Proof of Theorem* 1.1. First we show that the points obtained in Lemma 5.1 are of infinite order. If we let

$$d(u) = -\frac{A^3Bu^4(u^2+1)^2 + B^3(u^4+u^2+1)^3}{A(u^2+1)},$$

then the points in Lemma 5.1 may be considered as $k(u)$-rational point on the twisted curve

$$E_{d(u)} : d(u)y^2 = x^3 + Ax + B.$$

If we regard this elliptic curve over $k(u)$ as an elliptic surface over $k$, then the only singular fibers it has are of Kodaira type $\mathrm{I}_0^*$. This implies that the only possible torsion $k(u)$-rational points are points of order 2. However, our points are clearly not of order 2 since the $y$-coordinates are not 0.

Since $k(v)/k(u)$-trace of the $k(v)$-points in Lemma 5.1 are $O$, we see that the intersection between the subgroup generated by these $k(v)$-points and the group $E(k(u))$ is $\{O\}$. Thus we have $\operatorname{rank} E(k(v)) > \operatorname{rank} E(k(u))$.

By specializing $s$ to different values of $k$, we obtain infinitely many points on $E$ defined over the splitting field of (10). By Hilbert's irreducibility theorem these are cyclic quartic extensions for infinitely many values of $s$. Also, by a theorem of Silverman [6] on the specialization of a family of elliptic curves, points on an elliptic curve obtained by specializing a point of infinite order is once again of infinite order except for a finite number of values. This completes the proof. $\square$

*Proof of Corollary* 1.2. Since points on $E$ whose field of definition are different quartic extensions are clearly independent, the assertion follows immediate from the theorem. $\square$

**Remark 5.2.** The discriminant of the equation (10) is given by

$$16A^6B^6s^4(s^2+4)^3(s^4+5s^2+5)^4\big(A^3(s^2+4)+B^2(s^2+3)^3\big)^6.$$

## 6. Elliptic curve with 2-torsion

If the elliptic curve $E$ in question has a 2-torsion point, then the surface $X$ has more $k$-rational curves on it. In this section we show explicit results for the case where $E$ has three $k$-rational 2-torsion points. Other cases can be worked out similarly.

Let us fix the equation of $E$ as

$$E: y^2 = (x-c)(x-d)(x+c+d).$$

Then the equation (3) of $X$ becomes

$$-t\xi^3 + 3\xi^2\eta + \eta^3 - (c^2+cd+d^2)(t^2+4)\eta + cd(c+d)t(t^2+4) = 0.$$

We regard this as a cubic curve in the $\xi\eta$-plane over $k(t)$. We have several obvious $k(t)$-rational points, for example,

$$P_1 = (2c, ct), \quad P_2 = (2d, dt), \quad P_3 = (-2c-2d, -ct-dt).$$

These correspond to 2-torsion points on $E \times E$. The tangent line at $P_1$ intersects with the curve at $Q = (-c, ct)$. This gives four points on $E$ given by

$$\left(-\frac{c}{2} + \frac{3ct}{2\sqrt{t^2+4}}, \sqrt{\frac{3c}{8}\Big((c+2d)^2 - \frac{9c^2t^2}{t^2+4}\Big)\Big(1 - \frac{t}{\sqrt{t^2+4}}\Big)}\right),$$
$$\left(-\frac{c}{2} - \frac{3ct}{2\sqrt{t^2+4}}, \sqrt{\frac{3c}{8}\Big((c+2d)^2 - \frac{9c^2t^2}{t^2+4}\Big)\Big(1 + \frac{t}{\sqrt{t^2+4}}\Big)}\right).$$

These are defined over the cyclic quartic extension that is the splitting field of the equation

$$\begin{aligned} T^4 &+ 3c(t^2+4)\big((2c+d)(c-d)t^2 - (c+2d)^2\big)T^2 \\ &\qquad + 9c^2(t^2+4)\big((2c+d)(c-d)t^2 - (c+2d)^2\big)^2 = 0. \end{aligned}$$

By considering tangent lines at other points, we obtain more points defined over similar cyclic quartic extensions.

**Remark 6.1.** Choosing $P_1 = (2c, ct)$ as the origin, the equation of $X$ may be converted to the Weierstrass form.

$$\begin{aligned} Y^2 &= X^3 - 48(c^2+cd+d^2)(t^2+4)X \\ &\quad + 16(t^2+4)^3\big((c-d)^2(c+2d)^2(2c+d)^2t^2 + 8(c^2+cd+d^2)\big)^3. \end{aligned}$$

The rank of the Mordell-Weil group of this elliptic curve over $k(t)$ is 2 or 3 depending on whether or not $E$ has complex multiplication. If $E$ does not have complex multiplication, then the Mordell-Weil group is generated by the images of $P_2$ and $P_3$.

## References


[1] J. Bertin, *Réseaux de Kummer et surfaces de K3*, Invent. Math. **93** (1988), 267–284.

[2] J. Fearnley, *Vanishing and non-vanishing of L-series of elliptic curves twisted by Dirichlet characters*, Ph.D. thesis, Concordia University, 2001.

[3] T. Katsura, *Generalized Kummer surfaces and their unirationality in characteristic p*, J. Fac. Sci., Univ. Tokyo, Sect. IA **34** (1987), 1–41.

[4] M. Kuwata, *Points defined over cyclic cubic extensions on an elliptic curve and generalized Kummer surfaces*, preprint.

[5] D. E. Rohrlich, *The vanishing of certain Rankin-Selberg convolutions*, in "Automorphic forms and analytic number theory (Montreal, PQ, 1989)," Univ. Montréal, Montreal, QC, 123–133, 1990.

[6] J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–251.