Math. J. Okayama Univ. **47** (2005), 85–97

QUADRATIC TWISTS OF AN ELLIPTIC CURVE AND MAPS FROM A HYPERELLIPTIC CURVE

Masato KUWATA

Abstract. For an elliptic curve E over a number field k, we look for a polynomial $f(t)$ such that $\operatorname{rank} E^{f(t)}(k(t))$ is at least 3. To do so, we construct a family of hyperelliptic curves $C : s^2 = f(t)$ over k of genus 3 such that $J(C)$ is isogenous to $E_1 \times E_2 \times E_3$, and we give an example of C and E such that $J(C)$ is isogenous to $E \times E \times E$ over $\mathbf{Q}(\sqrt{-3})$.

1. Introduction

Let E be an elliptic curve over a number field k given by a Weiererstrass equation $y^2 = x^3 + ax + b$. The quadratic twist of E by $d \in k^\times/(k^\times)^2$ is the elliptic curve given by $dy^2 = x^3 + ax + b$, which we denote by E^d. For a given elliptic curve E, it is natural to ask how the rank of the Mordell-Weil group $E^d(k)$ varies as d changes. In particular, we would like to find d such that the rank is as large as possible. In order to construct a family of such d's we look for a polynomial $f(t) \in k[t]$ such that $\operatorname{rank} E^{f(t)}(k(t))$ is as large as possible, while keeping the degree of f as small as possible. This is equivalent to look for a hyperelliptic curve $C : s^2 = f(t)$ that admits many independent maps to E, while keeping its genus $g(C)$ as small as possible.

Two maps φ_1 and φ_2 from C to E are said to be independent if the pullbacks of the regular differential $\omega_E = dx/y$ by φ_1^* and by φ_2^* are independent in $H^0(C, \Omega_{C/k})$. If there are n independent maps from a hyperelliptic curve C to a given elliptic curve E, then the Jacobian $J(C)$ is isogenous to $E^n \times A$, where A is an abelian variety. Curves with splitting Jacobian are of interest in many different contexts, and many various are known (see for example, [1], [2], [3], [4], [5], [6], [7], [8], [10]). In particular, Rubin-Silverberg [10] constructs a hyperelliptic curve of genus 5 whose Jacobian $J(C)$ is isogenous to $E^3 \times A$, where A is an abelian surface. In this paper we constructs hyperelliptic curves of genus 3 whose Jacobian $J(C)$ is isogenous to the product of three elliptic curves.

Note in passing that our interests lie not just hyperelliptic curves but those whose quotient by the hyperelliptic involution is isomorphic to $\mathbf{P}^1$ over k. This distinction makes a difference when the genus is greater than 2.

In §2 we gather results for the case where the genus of C is 2. Many of our constructions are already known; some are classical and explicit, while others are known only theoretically. Howe-Leprévost-Poonen [5] also treats this problem systematically in a different context. We make everything as explicit as possible. Rubin-Silverberg [10] also gives some explicit results, some of which are similar to ours.

In §3 we construct hyperelliptic curves of genus 3 that admit maps to elliptic curves. Given two elliptic curves E_1 and E_2 with rational 4-torsion points, we construct a hyperelliptic curve C of genus 3 with two maps $\varphi_i : C \to E_i$ ($i = 1, 2$) of degree 2. Then the Jacobian $J(C)$ of C is isogenous to $E_1 \times E_2 \times E_3$ with a third elliptic curve E_3. We vary E_1 and E_2 in such a way that they are isomorphic, and find the case where E_3 is also isomorphic. Note that there are many examples of nonhyperelliptic curves of genus 3 whose Jacobian is isogenous to the product $E \times E \times E$. However, the condition that C is hyperelliptic is essential for our application.

The author would like to thank the referee for pointing out the work of Rubin and Silverberg. He also thank Prof. Kazuo Matsuno for useful conversations.

2. Curves of genus 2

In this section we consider (hyperelliptic) curves of genus 2 that admit two independent maps of degree 2 to a given elliptic curve E.

Let C be such a curve of genus 2. If $\varphi : C \to E$ is a map of degree 2, then C admits an automorphism of order 2, which exchanges points in the inverse image of a point in E. If $\sigma : C \to C$ is such an automorophism, then $C/\langle\sigma\rangle \cong E$, and $C/\langle\iota \circ \sigma\rangle$, where ι is the hyperelliptic involution, is once again an elliptic curve. We are particularly interested in the case where $C/\langle\iota \circ \sigma\rangle$ is isomorphic to E itself, or isogenous to E.

2.1. **Rational 2-torsion point.**

Let E be the elliptic curve over k given by

$$E : y^2 = x(x^2 + Ax + B), \quad A, B \in \mathbf{Q}, \quad AB \neq 0.$$

If we put $x = \lambda t^2 + \mu$, then we obtain a curve of genus 2

$$C : y^2 = (\lambda t^2 + \mu)\big((\lambda t^2 + \mu)^2 + A(\lambda t^2 + \mu) + B\big).$$

Let σ be the involution of C given by $(t, y) \mapsto (-t, y)$. The map $\varphi_1 : (t, y) \mapsto (\lambda t^2 + \mu, y)$ is the quotient map $C \to C/\langle\sigma\rangle \cong E$.

Let ι be the hyperelliptic involution $(t, y) \mapsto (t, -y)$. The involution $\tau \circ \iota$ fixes the function t^2 and y/t. Letting $x' = 1/t^2$ and $y' = y/t^3$, we obtain from the equation of C

$$F : y'^2 = (\lambda + \mu x')\big((\lambda + \mu x')^2 + Ax'(\lambda + \mu x') + Bx'^2\big).$$

This is the quotient elliptic curve $C/\langle\tau \circ \iota\rangle$. We look for conditions on λ and μ such that $C/\langle\tau \circ \iota\rangle$ is isomorphic to E once again. Now we look for a map from the x-line to the x'-line which sends the three roots of the right hand side of the above equation to the three roots of $x(x^2 + Ax + B)$.

A straightforward calculation shows that if $\mu = -B/A$, then $x \mapsto x' = A(\lambda - x)/B$ gives such a map. Thus, putting $\mu = -B/A$, and simplifying the formulas as much as possible, we obtain the following

Proposition 2.1. *Let E be the elliptic curve given by $y^2 = x(x^2+Ax+B)$, and let C_λ be the family of curves of genus 2 parametrized by λ given by*

$$C_\lambda : s^2 = A(\lambda A t^2 - B)\big(\lambda^2 A^2 t^4 + \lambda A(A^2 - 2B)t^2 + B^2\big).$$

Then C_λ admits the involution $\sigma : (t, s) \mapsto (-t, s)$, and the quotient $C_\lambda/\langle\sigma\rangle$ equals E with the quotient map $\varphi_1 : C_\lambda \to E$ given by

$$\varphi_1 : (t, s) \longmapsto \left(\frac{\lambda A t^2 - B}{A}, \frac{s}{A^2}\right).$$

Furthermore, the quotient $C_\lambda/\langle\sigma \circ \tau\rangle$ is $E^{-\lambda A/B}$, the quadratic twist of E by $-\lambda A/B$. The quotient map $\varphi_2 : C_\lambda \to E^{-\lambda A/B}$ is given by

$$\varphi_2 : (t, s) \longmapsto \left(\frac{-B(\lambda A t^2 - B)}{\lambda A^2 t^2}, \frac{B^2 s}{\lambda^2 A^4 t^3}\right).$$

Corollary 2.2 (cf. Rubin-Silverberg[10, Cor. 3.3])**.** *Let $f(t)$ be the polynomial*

$$f(t) = -A(t^2+1)\big(Bt^4 + (2B - A^2)t^2 + B\big),$$

and let $E^{f(t)}$ be the elliptic cureve over $k[t]$ given by

$$f(t)\, y^2 = x(x^2 + Ax + B).$$

Then the Mordell-Weil group $E^{f(t)}(k(t))$ has two independent points:

$$P_1 = \left(\frac{-B(t^2+1)}{A}, \frac{B}{A^2}\right), \quad P_2 = \left(\frac{-B(t^2+1)}{At^2}, \frac{B}{A^2t^3}\right).$$

Proof. We put $\lambda = -B/A$ in the proposition. The image of $(t, 1)$ by φ_i gives a point in $E^{f(t)}$. The independence of P_1 and P_2 follows from the fact that φ_1 and φ_2 are independent maps by construction. $\square$

Corollary 2.3. *Let E be the elliptic curve given by $y^2 = x(x^2 + Ax + B)$, and let d_0 be any element in $k^\times/(k^\times)^2$. Then there are infinitely many $d \in k^\times/(k^\times)^2$ such that both $E^d(k)$ and $E^{dd_0}(k)$ have positive rank.*

Proof. We put $\lambda = -d_0B/A$ in the proposition. Then two maps in the proposition give points of infinite order in $E^{f(t)}(k(t))$ and $E^{d_0f(t)}(k(t))$, respectively. It suffices to specialize t to various values in k. $\square$

2.2. **Elliptic curves whose 2-torsion points are defined over a cyclic extension.** Let $k(E[2])$ be the extension of k over which all the 2-torsion points of E are defined. As is remarked after Corollary 7 in [5], if the Galois group $\mathrm{Gal}(k(E[2])/k)$ is isomorphic to A_3(= cyclic group of order 3), then we can construct a curve C of genus 2 with two independent maps. We give an explicit family of such curves of genus 2.

Let E be the elliptic curve over k given by

$$y^2 = x^3 - ux^2 + (u-3)x + 1, \quad u \in \mathbf{Q}.$$

Note that $x^3 - ux^2 + (u-3)x + 1$ is a generic polynomial of cyclic cubic extensions (see Serre [11, p. 1]). The linear transformation $x \mapsto 1/(1-x)$ permutes the three roots of $x^3 - ux^2 + (u-3)x + 1$, and it sends 1 to ∞.

So, consider the map $\bar{\varphi}_1 : t \mapsto x = \lambda t^2 + 1$, which ramifies at the points over $x = 1$ and $x = \infty$. Define C_λ to be the pull-back of E by $\bar{\varphi}_1$:

$$C_\lambda : s^2 = \lambda^3 t^6 - \lambda^2 (u-3)t^4 - \lambda u t^2 - 1. \tag{1}$$

Proposition 2.4. *Let C_λ be the family of hyperelliptic curves defined by (1). Then there are two independent maps $\varphi_1 : C_\lambda \to E$ and $\varphi_2 : C_\lambda \to E^\lambda$ given by*

$$\varphi_1 : (t,s) \mapsto (\lambda t^2 + 1, s), \quad \varphi_2 : (t,s) \longmapsto \left(-\frac{1}{\lambda t^2}, \frac{s}{\lambda^2 t^3}\right).$$

Proof. Let σ be the automorphism of C_λ defined by $(t,s) \mapsto (-t,s)$. Then φ_1 is nothing but the quotient map $C_\lambda \to C_\lambda/\langle\sigma\rangle$. The map φ_2, which is obtained by lifting the composition of $t \mapsto x = \lambda t^2 + 1$ and $x \mapsto 1/(x-1)$, is the quotient map $C_\lambda \to C_\lambda/\langle \sigma \circ \iota\rangle$, where ι is the hyperelliptic involution on C_λ. □

Corollary 2.5. *Let $f(t)$ be the polynomial*

$$f(t) = t^6 - (u-3)t^4 - ut^2 - 1,$$

and let $E^{f(t)}$ be the elliptic cureve over $k[t]$ given by

$$f(t)\, y^2 = x^3 - ux^2 + (u-3)x + 1.$$

Then the Mordell-Weil group $E^{f(t)}(k(t))$ has two independent points:

$$P_1 = (t^2 + 1, 1), \quad P_2 = \left(-\frac{1}{t^2}, \frac{1}{t^3}\right).$$

Proof. It suffices to let $\lambda = 1$ in Proposition 2.4. □

2.3. **Elliptic curves with an isogeny of odd degree.** Suppose an elliptic curve $E : y^2 = x^3 + Ax + B$ is isogenous over k to another elliptic curve $E' : Y^2 = X^3 + A'X + B'$ with an isogeny $\psi : E \to E'$ of odd degree. Then ψ induces an isomorphism $E[2](\bar{k}) \to E'[2](\bar{k})$. As is shown in [5, Corollary 7], we can construct a curve of genus 2 over k whose Jacobian is $(2, 2)$-isogenous to $E \times E'$ under these circumstances.

An explicit construction goes as follows. Once we fix equations of E and E' as above, the isomorphism $E[2](\bar{k}) \to E'[2](\bar{k})$ induces an isomorphism from the x-line to the X-line. To be precise, there is a liniear transformation $h : x \mapsto X = (px + q)/(rx + s)$ over k which maps the three roots of $x^3 + Ax + B = 0$ to the three roots of $X^3 + A'X + B = 0$. Let α be the point on the x-line satisfying $h(\alpha) = \infty$, define $\bar{\varphi}_1$ to be the map $t \mapsto x = \mu t^2 + \alpha$, and define C_μ to be the pull-back of E by $\bar{\varphi}_1$:

$$\begin{array}{ccc} C_\mu & \xrightarrow{\varphi_1} & E \\ \downarrow & & \downarrow \\ \mathbf{P}^1_t & \xrightarrow{\bar{\varphi}_1} & \mathbf{P}^1_x = E/\{\pm 1\}. \end{array}$$

C_μ is a double cover of the t-line ramifying at the six points which are the inverse image of the three roots of $x^3 + Ax + B = 0$ by $\bar{\varphi}_1$. Also define C'_μ to be the pull-back of E' by the map $\bar{\varphi}_2 = h \circ \bar{\varphi}_1$. Now it is easy to see that C'_μ is a double cover of the t-line ramifying at the same six points as C_μ. It turns out that by choosing a suitable μ we can make C_μ and C'_μ isomorphic. Let C be this isomorphic curve of genus 2. Then C admits two maps to E; one is φ_1, and the other is the lift of $\bar{\varphi}_2$ composed with the dual isogeny $\psi' : E' \to E$. In particular the Jacobian $J(C)$ is isogenous to $E \times E$.

In the following we will work out in detail for the cases of isogenies of degree 3 and 5. First we start consider the elliptic curve

$$E : y^2 = x^3 - 9(u + 3)(3u + 1)x + 18(u + 3)(3u^2 + 6u - 1). \tag{2}$$

It is isogenous to

$$E' : Y^2 = X^3 - 27(u + 27)(u + 3)X + 54(u + 3)(u^2 - 54u - 243) \tag{3}$$

by an isogeny of degree 3. Here we give the formula for the dual isogeny $\psi' : E' \to E$, which we will need later:

$$\psi : (X, Y) \longmapsto \left(\frac{X^3 + 9(u + 3)\big(2X^2 + 3(19u + 9)X + 48u(5u + 27)\big)}{9(X + 9u + 27)^2}, \right.$$
$$\left. \frac{\big(X^3 + 27(u + 3)\big(X^2 - (7u - 27)X + 11u^2 - 270u + 243\big)\big)Y}{27(X + 9u + 27)^3} \right).$$

By straight forward calculations we find that the linear transformation

$$h : x \mapsto X = -3\frac{(2u+9)x - 6(u+3)^2}{x - 3(u+2)}$$

sends three roots of $x^3 - 9(u+3)(3u+1)x + 18(u+3)(3u^2+6u-1) = 0$ to those of $X^3 - 27(u+27)(u+3)X + 54(u+3)(u^2-54u-243) = 0$.

Proposition 2.6. *Let C be the curve of genus 2 given by*

$$C : s^2 = -t^6 + 9(u+2)t^4 - 9(2u+9)t^2 + 9u.$$

Then we have a map φ_1 from C to the elliptic curve E given by (2) and a map φ_2 to E' given by (3). They are independent and given by

$$\begin{aligned} \varphi_1 &: (s,t) \longmapsto (x,y) = \bigl(-t^2 + 3(u+2), s\bigr), \\ \varphi_2 &: (s,t) \longmapsto (X,Y) = \left(\frac{-3(2u+9)t^2 + 9u}{t^2}, \frac{9us}{t^3}\right). \end{aligned}$$

Proof. We follow the strategy explained earlier, and find that the twisting factor μ in this case equals -1. □

Corollary 2.7 (cf. Rubin-Silverberg[10, Cor. 3.5])**.** *Let $f(t)$ be the polynomial*

$$f(t) = -t^6 + 9(u+2)t^4 - 9(2u+9)t^2 + 9u,$$

and let $E^{f(t)}$ be the elliptic cureve over $k[t]$ given by

$$f(t)\, y^2 = x^3 - 9(u+3)(3u+1)x + 18(u+3)(3u^2+6u-1).$$

Then the Mordell-Weil group $E^{f(t)}(k(t))$ has two independent points:

$$\begin{aligned} P_1 &= \bigl(-t^2 + 3(u+2), 1\bigr), \\ P_2 &= \Bigl(-\frac{(6u+19)t^6 - 9(5u+14)t^4 + 27t^2 - 9u}{t^2(t^2+3)^2}, \\ &\qquad \frac{(27u+80)t^6 - 9(5u+16)t^4 + 9ut^2 + 9u}{t^3(t^2+3)^3}\Bigr). \end{aligned}$$

Proof. The second point P_2 is obtained from the map $\psi' \circ \varphi_2$. □

Next we consider the curve

$$E : y^2 = x^3 - 3(u^2+1)(u^2-6u+4)x + 2(u^2+1)^2(u^2-9u+19), \tag{4}$$

which is isogenous to

$$E' : Y^2 = X^3 - 3(u^2+1)(u^2+114u+124)X + 2(u^2+1)^2(u^2-261u-2501). \tag{5}$$

by an isogeny of degree 5. Since the actual formula for the isogeny is too complicated and of little interest, we omit it. We find that the linear transformation

$$h : x \longmapsto X = -\frac{(8u^2+72u-13)x - 8(u^2+1)(u^2+6u-32)}{4x-4u^2+12u+5}$$

sends three roots of $x^3-3(u^2+1)(u^2-6u+4)x+2(u^2+1)^2(u^2-9u+19) = 0$ to those of $X^3-3(u^2+1)(u^2+114u+124)X+2(u^2+1)^2(u^2-261u-2501) = 0$.

Proposition 2.8. *Let C be the curve of genus 2 given by*

$$C : s^2 = -3t^6 + 3(4u^2-12u-5)t^4 - 3(8u^2+72u-13)t^2 + 3(2u-11)^2$$

There exits a map φ_1 from C to the elliptic curve E given by (4) and a map φ_2 to E' given by (5). They are given by

$$\begin{aligned}\varphi_1 : (s,t) &\longmapsto (x,y) = \left(-\frac{3t^2-4u^2+12u+5}{4}, \frac{3s}{8}\right),\\ \varphi_2 : (s,t) &\longmapsto (X,Y)\\ &\qquad = \left(-\frac{(8u^2+72u-13)t^2-3(2u-11)^2}{4t^2}, \frac{3(2u-11)^2 s}{8t^3}\right).\end{aligned}$$

Proof. We follow the strategy explained earlier, and find that the twisting factor μ in this case equals $-3/4$. ☐

Corollary 2.9. *Let $f(t)$ be the polynomial*

$$f(t) = -3t^6 + 3(4u^2-12u-5)t^4 - 3(8u^2+72u-13)t^2 + 3(2u-11)^2,$$

and let $E^{f(t)}$ be the elliptic cureve over $k[t]$ given by

$$f(t)\,y^2 = x^3 - 3(u^2+1)(u^2-6u+4)x + 2(u^2+1)^2(u^2-9u+19).$$

Then the Mordell-Weil group $E^{f(t)}(k(t))$ has two independent points:

$$\begin{aligned}P_1 &= \left(-\frac{3t^2-4u^2+12u+5}{4}, \frac{3}{8}\right),\\ P_2 &= \left(\frac{p(t)}{d(t)^2}, \frac{q(t)}{d(t)^3}\right),\end{aligned}$$

where

$$\begin{aligned}p(t) = &-(32u^4-64u^3+148u^2-76u+107)t^{10}\\ &+5(112u^4-96u^3-72u^2-24u-205)t^8\\ &+10(128u^4-864u^3+196u^2-732u-283)t^6\\ &+10(2u-11)(2u-1)(52u^2-72u+73)t^4\\ &+5(2u-11)^2(8u^2-72u+29)t^2+3(2u-11)^4,\end{aligned}$$

$$
\begin{aligned}
q(t) = &-3(160u^5 - 240u^4 + 400u^3 - 440u^2 + 242u - 211)t^{12} \\
&+ 6(160u^5 + 880u^4 - 432u^3 + 2072u^2 - 478u + 1315)t^{10} \\
&+ 9(2u - 11)(48u^4 + 32u^3 - 280u^2 - 88u - 293)t^8 \\
&- 12(2u - 11)(144u^4 + 464u^3 + 1216u^2 + 684u + 487)t^6 \\
&+ 3(2u - 11)^2(232u^3 + 444u^2 - 338u - 171)t^4 \\
&- 18(2u - 11)^4(2u - 1)t^2 - 3(2u - 11)^5, \\
d(t) = &\, 2t\big((2u + 1)t^4 + 10(2u - 1)t^2 + 5(2u - 11)\big).
\end{aligned}
$$

Remark 2.10. It is possible to obtain similar formulas for the curve that admits an isogeny of degree 7:

$$
\begin{aligned}
y^2 = x^3 &- 3(u^2 + 3)(9u^2 - 48u + 43)x \\
&+ 2(u^2 + 3)(27u^4 - 216u^3 + 522u^2 - 584u + 747),
\end{aligned}
$$

or the curve that admits an isogeny of degree 13:

$$
\begin{aligned}
y^2 = x^3 &- 3(u^2 + 1)(4u^2 - 2u + 7)(4u^4 - 10u^3 + 11u^2 - 10u + 4)x \\
&+ 2(u^2 + 1)^2(4u^2 - 2u + 7) \\
&\times (16u^6 - 64u^5 + 124u^4 - 168u^3 + 149u^2 - 77u + 23).
\end{aligned}
$$

The results are too complicated, and thus we do not write them down here.

3. Hyperelliptic curves of genus 3

In this section we construct a hyperelliptic curve C of genus 3 starting from two given elliptic curves E_1 and E_2 such that C admits maps of degree 2 to each of E_1 and E_2. Then the Jacobian $J(C)$ is isogenous to the product $E_1 \times E_2 \times E_3$ with a third elliptic curve E_3. We will then determine E_3 explicitly.

Our strategy is to find a curve of geometric genus 0 on the Kummer surface S obtained from the quotient $E_1 \times E_2/\{\pm 1\}$. A section of an elliptic fibration on $S \to \mathbf{P}^1$ is a curve of arithmetic genus 0, and thus geometric genus 0. An irreducible singular fiber of an elliptic fibration is also a curve of geometric genus 0, though its arithmetic genus is 1. Here we use such a singular curve for our construction. The difficulty lies in the fact that singular fibers of type I_1 or II in an elliptic fibration are rarely defined over the base field.

Oguiso [9] classified all the elliptic fibrations on the Kummer surface S with a section. We find that one of the fibrations admits a singular fiber of type I_1 defined over the base field k if E_1 and E_2 satisfy a certain condition.

Let F_u be the elliptic curve defined over $k(u)$ given by the equation

$$F_u : y^2 = x\big(x^2 - 2(u-2)x + u^2\big).$$

This curve has a $k(u)$-rational 4-torsion point $(u, 2u)$. In fact, this is the universal elliptic curve with a 4-torsion point.

Take two distinct elements λ and μ in k, and consider two elliptic curves:

$$\begin{aligned} E_1 &: y^2 = x\big(x^2 - 2(\lambda-2)x + \lambda^2\big), \\ E_2 &: y^2 = x\big(x^2 - 2(\mu-2)x + \mu^2\big). \end{aligned} \tag{6}$$

Let S be the Kummer surface associated to the product $E_1 \times E_2$. A singular affine model of S is given by the equation

$$z\big(z^2 - 2(\mu-2)z + \mu^2\big)\, y^2 = x\big(x^2 - 2(\lambda-2)x + \lambda^2\big). \tag{7}$$

One of the elliptic fibrations on S classified by Oguiso [9] is given by the map $(x, y, z) \mapsto zy/x$. Setting $v = zy/x$, we obtain

$$v\mu^2 y^2 - \big(x^2 + 2\big((\mu-2)v^2 - (\lambda-2)\big)x + \lambda^2\big)y + x^2 v^3 = 0.$$

By setting

$$Y = 2v\mu^2 y - \big(x^2 + 2\big((\mu-2)v^2 - (\lambda-2)\big) + \lambda^2\big),$$

we have

$$Y^2 = \big(x^2 - 2(2v^2 + \lambda - 2)x + \lambda^2\big)\big(x^2 + 2\big(2(\mu-1)v^2 - (\lambda-2)\big)x + \lambda^2\big).$$

The discriminant of the right hand side with respect to x is

$$2^{16}\mu^4\lambda^4 v^8 (v-1)(v+1)(v^2 + \lambda - 1)\big((\mu-1)v^2 + 1\big)\big((\mu-1)v^2 - \lambda + 1\big).$$

From this we see that the elliptic fibration $(x, y, z) \mapsto zy/x$ has a singular fiber of type I_1 at $v = \pm 1$. In other words, the intersection of (7) and $x = \pm zy$ is a curve of geometric genus 0. It is easy to obtain a parametrization of the intersection of (7) and $x = \pm zy$ with parameter t:

$$(x, y, z) = \left(\frac{t(\mu t + \lambda)}{t+1}, t^2, \frac{\mu t + \lambda}{t(t+1)}\right).$$

We thus obtain a map $f : \mathbf{P}^1 \to E_1 \times E_2/\{\pm 1\}$. Let C be the curve that makes the following diagram commutative:

$$\begin{array}{ccc} C & \xrightarrow{\tilde{f}} & E_1 \times E_2 \\ \big\downarrow & & \big\downarrow \\ \mathbf{P}^1 & \xrightarrow{f} & E_1 \times E_2/\{\pm 1\} \end{array}$$

C is the hyperelliptic curve given by the equation

$$C : s^2 = t(t+1)(\mu t + \lambda)\big(\mu^2 t^4 + 4\mu t^3 - 2(\lambda\mu - 2\lambda - 2\mu)t^2 + 4\lambda t + \lambda^2\big). \tag{8}$$

The discriminant of the right hand side is

$$2^{12}\mu^6\lambda^{12}(\lambda-\mu)^{12}(\lambda-1)^2(\mu-1)^2$$

Thus, C is a curve of genus 3 as long as $\lambda, \mu \neq 0, 1$ and $\lambda \neq \mu$. The above commutative diagram shows that C admits maps $\varphi_1 : C \to E_1$ and $\varphi_2 : C \to E_2$ given by

$$\varphi_1 : (t,s) \longmapsto (x,y) = \left(\frac{t(\mu t+\lambda)}{t+1}, \frac{s}{(t+1)^2}\right),$$

$$\varphi_2 : (t,s) \longmapsto (x,y) = \left(\frac{(\mu t+\lambda)}{t(t+1)}, \frac{s}{t^2(t+1)^2}\right).$$

Theorem 3.1. *Let λ and μ be two distinct elements of $k \setminus \{0,1\}$, and let C be the hyperelliptic curve given by the equation* (8). *Then C admits two automorphisms σ and τ given by*

$$\sigma : (t,s) \longmapsto \left(-\frac{\mu t+\lambda}{\mu(t+1)}, \frac{s(\lambda-\mu)^2}{\mu^2(t+1)^4}\right),$$

$$\tau : (t,s) \longmapsto \left(-\frac{\lambda(t+1)}{\mu t+\lambda}, \frac{s\lambda^2(\lambda-\mu)^2}{(\mu t+\lambda)^4}\right).$$

The quotients $C/\langle\sigma\rangle$ and $C/\langle\tau\rangle$ are birationally equivalent to E_1 and E_2 given by (6), *respectively. The quotient $C/\langle\sigma\circ\tau\rangle$ is birationally equivalent to the elliptic curve E_3 given by*

$$E_3 : y^2 = (x+\lambda+\mu)(x^2+4x-4\lambda\mu+4\lambda+4\mu),$$

and the quotient map $\varphi_3 : C \to E_3$ is given by

$$\varphi_3 : (t,s) \longmapsto (x,y) = \left(\mu t+\frac{\lambda}{t}, \frac{s}{t^2}\right).$$

The Jacobian $J(C)$ of the hyperelliptic curve C is $(2,2,2)$*-isogenous to the product of elliptic curve $E_1 \times E_2 \times E_3$.*

Proof. A map that exchanges points in the inverse image $\varphi_1^{-1}(P)$ of each point $P \in E_1$ is an automorphism of C. σ is nothing but this automorphism. Similarly, τ is the automorphism obtained by exchanging the inverse image $\varphi_2^{-1}(P)$. Thus, the quotients $C/\langle\sigma\rangle$ and $C/\langle\tau\rangle$ are birationally equivalent to E_1 and E_2, respectively.

The automorphism $\sigma\circ\tau$ is given by

$$\sigma\circ\tau : (t,s) \longmapsto \left(\frac{\lambda}{\mu t}, \frac{s\lambda^2}{\mu^2 t^4}\right).$$

In the function field $k(C) = k(t,s)$, two elements

$$x = \mu t + \frac{\lambda}{t}, \quad \text{and} \quad y = \frac{s}{t^2}$$

are invariant under $\sigma \circ \tau$. Using elimination theory, it is easy to see that these x and y satisfy the equation of E_3.

Since three elliptic curves E_1, E_2, E_3 are generically not isomorphic, three maps φ_1, φ_2, φ_3 are independent. Therefore, the Jacobian $J(C)$ of the hyperelliptic curve C is $(2,2,2)$-isogenous to the product $E_1 \times E_2 \times E_3$. □

The j-invariants of E_i are:

$$j_1 = -\frac{16(\lambda^2 - 16\lambda + 16)^3}{\lambda^4(\lambda - 1)},$$
$$j_2 = -\frac{16(\mu^2 - 16\mu + 16)^3}{\mu^4(\mu - 1)},$$
$$j_3 = \frac{16\big((\lambda-\mu)^2 + 16(\lambda-1)(\mu-1)\big)^3}{(\lambda-\mu)^4(\lambda-1)(\mu-1)}.$$

If $\mu = \lambda/(\lambda-1)$, then $j_1 = j_2$. However, when $\mu = \lambda/(\lambda-1)$, E_2 is isomoprphic to the quadratic twist

$$E_1^{1-\lambda} : (1-\lambda)y^2 = x\big(x^2 - 2(\lambda-2)x + \lambda^2\big).$$

Thus, if we set $\lambda = 1 - \nu^2$ and $\mu = 1 - 1/\nu^2$, then E_1 and E_2 are isomorphic over k, and their j-invariants are

$$j_1 = j_2 = \frac{16(\nu^4 + 14\nu^2 + 1)^3}{\nu^2(\nu^2 - 1)^4}. \tag{9}$$

Then the j-invariant of E_3 is given by

$$j_3 = \frac{16(\nu^8 + 14\nu^4 + 1)^3}{\nu^4(\nu^4 - 1)^4}. \tag{10}$$

Proposition 3.2. *If k contains a root of the equation*

$$\begin{aligned}(\nu^2 - \nu + 1)(\nu^2 + \nu + 1)(\nu^3 + \nu^2 + 3\nu - 1)\\ (\nu^3 - \nu^2 + 3\nu + 1)(\nu^3 - 3\nu^2 - \nu - 1)(\nu^3 + 3\nu^2 - \nu + 1)\\ (\nu^4 - 4\nu^3 + 10\nu^2 - 4\nu + 1)(\nu^4 + 4\nu^3 + 10\nu^2 + 4\nu + 1) = 0,\end{aligned}$$

then there exists a hyperelliptic curve C over k whose Jacobian is $(2,2,2)$-isogenous to the product $E \times E \times E$ over at most a quadratic extension of k.

Proof. The above equation is obtained by equating (9) and (10). If ν is a root, then all three elliptic curves E_1, E_2 and E_3 have the same j-invariant. Since E_1 and E_2 are isomorphic, we can make E_3 isomorphic to these by at most a quadratic extension of k. $\square$

Example 3.3. If we put $\nu = \zeta_3$, a primitive cube root of unity, then all three elliptic curves E_i are isomorphic. After a suitable change of coordinates over $\mathbf{Q}(\zeta_3)$, we obtain

$$\begin{aligned} E_1 \cong E_2 \cong E_3 : y^2 &= x(x^2 - 2x - 3), \\ C : s^2 &= t(t^6 + 7t^3 + 8). \end{aligned}$$

The maps $C \to E_i$ are defined over $\mathbf{Q}(\zeta_3)$; they are given by

$$\begin{aligned} \varphi_1 : (t,s) &\longmapsto \left(\frac{\zeta_3^2(t-1)(t+1+\zeta_3)}{t-\zeta_3}, \frac{s}{(t-\zeta_3)^2} \right), \\ \varphi_2 : (t,s) &\longmapsto \left(\frac{3\zeta_3^2(t+1+\zeta_3)}{(t-1)(t-\zeta_3)}, \frac{3\zeta_3 s}{(t-1)^2(t-\zeta_3)^2} \right), \\ \varphi_3 : (t,s) &\longmapsto \left(\frac{t^2+t+1}{t-1}, \frac{s}{(t-1)^2} \right). \end{aligned}$$

Example 3.4. Putting $\lambda = 4$ and $\mu = 4/3$, we obtain

$$\begin{aligned} E_1 : y^2 &= x(x^2 - 4x + 16), \\ E_2 : y^2 &= x\Big(x^2 + \frac{4}{3}x + \frac{16}{9}\Big), \\ E_3 : y^2 &= x(x+4)\Big(x + \frac{16}{3}\Big). \end{aligned}$$

In this case E_1 is a quadratic twist of E_2 by -3. The conductor of E_2 and the conductor of E_3 are both 72. In fact, E_2 is isogenous to E_3 with the isogeny given by

$$(x,y) \mapsto \left(\frac{(3x-4)^2}{9x}, \frac{y(9x^2-16)}{9x^2} \right).$$

The curve C is given by

$$s'^2 = 3t(t+1)(t+3)(t^2+3)(t^2+3t+3),$$

where $s' = 9s/8$. In this cace C is isogenous to $E_2^{(-3)} \times E_2 \times E_2$ over $\mathbf{Q}$ and thus isogenous to $E_2 \times E_2 \times E_2$ over $\mathbf{Q}(\sqrt{-3})$. The curve C in this example is a quadratic twist by -3 of the curve in the previous example.

Question 3.5. Can we choose λ and μ such that E_1, E_2 and E_3 are all isogenous to each other over $\mathbf{Q}$?

References

[1] Gerhard Frey, *On elliptic curves with isomorphic torsion structures and corresponding curves of genus* 2, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995, pp. 79–98.

[2] Gerhard Frey and Ernst Kani, *Curves of genus* 2 *covering elliptic curves and an arithmetical application*, Arithmetic algebraic geometry (Texel, 1989), Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 153–176.

[3] Everett W. Howe, *Constructing distinct curves with isomorphic Jacobians in characteristic zero*, Internat. Math. Res. Notices (1995), no. 4, 173–180 (electronic).

[4] ———, *Plane quartics with Jacobians isomorphic to a hyperelliptic Jacobian*, Proc. Amer. Math. Soc. **129** (2001), no. 6, 1647–1657 (electronic).

[5] Everett W. Howe, Franck Leprévost, and Bjorn Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), no. 3, 315–364.

[6] Ernst Kani, *The existence of curves of genus two with elliptic differentials*, J. Number Theory **64** (1997), no. 1, 130–161.

[7] ———, *The number of curves of genus two with elliptic differentials*, J. Reine Angew. Math. **485** (1997), 93–121.

[8] Robert M. Kuhn, *Curves of genus* 2 *with split Jacobian*, Trans. Amer. Math. Soc. **307** (1988), no. 1, 41–49.

[9] Keiji Oguiso, *On Jacobian fibrations on the Kummer surfaces of the product of non-isogenous elliptic curves*, J. Math. Soc. Japan **41** (1989), no. 4, 651–680.

[10] Karl Rubin and Alice Silverberg, *Rank frequencies for quadratic twists of elliptic curves*, Experiment. Math. **10** (2001), no. 4, 559–569.

[11] Jean-Pierre Serre, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992, Lecture notes prepared by Henri Damon [Henri Darmon], With a foreword by Darmon and the author.

MASATO KUWATA
FACULTY OF ECONOMICS,
CHUO UNIVERSITY,
742-1 HIGASHINAKANO, HACHIOJI-SHI, TOKYO 192-0393, JAPAN
e-mail address: kuwata@tamacc.chuo-u.ac.jp

(*Received February 26, 2005*)