J. Math. Soc. Japan
Vol. 54, No. 2, 2002

Elliptic curves from sextics

By Mutsuo Oka

(Received Oct. 4, 2000)

Abstract. Let $\mathcal{N}$ be the moduli space of sextics with 3 $(3,4)$-cusps. The quotient moduli space $\mathcal{N}/G$ is one-dimensional and consists of two components, $\mathcal{N}_{\text{torus}}/G$ and $\mathcal{N}_{\text{gen}}/G$. By quadratic transformations, they are transformed into one-parameter families C_s and D_s of cubic curves respectively. First we study the geometry of $\mathcal{N}_\varepsilon/G$, $\varepsilon = $ torus, gen and their structure of elliptic fibration. Then we study the Mordell-Weil torsion groups of cubic curves C_s over $\boldsymbol{Q}$ and D_s over $\boldsymbol{Q}(\sqrt{-3})$ respectively. We show that C_s has the torsion group $\boldsymbol{Z}/3\boldsymbol{Z}$ for a generic $s \in \boldsymbol{Q}$ and it also contains subfamilies which coincide with the universal families given by Kubert [**Ku**] with the torsion groups $\boldsymbol{Z}/6\boldsymbol{Z}$, $\boldsymbol{Z}/6\boldsymbol{Z}+\boldsymbol{Z}/2\boldsymbol{Z}$, $\boldsymbol{Z}/9\boldsymbol{Z}$, or $\boldsymbol{Z}/12\boldsymbol{Z}$. The cubic curves D_s has torsion $\boldsymbol{Z}/3\boldsymbol{Z}+\boldsymbol{Z}/3\boldsymbol{Z}$ generically but also $\boldsymbol{Z}/3\boldsymbol{Z}+\boldsymbol{Z}/6\boldsymbol{Z}$ for a subfamily which is parametrized by $\boldsymbol{Q}(\sqrt{-3})$.

1. Introduction.

Let $\mathcal{N}_3$ be the moduli space of sextics with 3 $(3,4)$-cusps as in [**O2**]. For brevity, we denote $\mathcal{N}_3$ by $\mathcal{N}$. A sextic C is called *of a torus type* if its defining polynomial f has the expression $f(x,y) = f_2(x,y)^3 + f_3(x,y)^2$ for some polynomials f_2, f_3 of degree 2, 3 respectively. We denote by $\mathcal{N}_{\text{torus}}$ the component of $\mathcal{N}$ which consists of curves of a torus type and by $\mathcal{N}_{\text{gen}}$ the curves of a general type ($=$ not of a torus type). We denote the dual curve of C by C^*. Let $G = PGL(3,\boldsymbol{C})$. The quotient moduli space is by definition the quotient space of the moduli space by the action of G.

In §2, we study the quotient moduli space $\mathcal{N}/G$. We will show that $\mathcal{N}/G$ is one dimensional and it has two components $\mathcal{N}_{\text{torus}}/G$ and $\mathcal{N}_{\text{gen}}/G$ which consist of sextics of a torus type and sextics of a general type respectively. After giving normal forms of these components C_s, $s \in \boldsymbol{P}^1(\boldsymbol{C})$ and D_s, $s \in \boldsymbol{P}^1(\boldsymbol{C})$, we show that the family C_s *contains a unique sextic* C_{54} *which is self dual* (Theorem 2.8) and C_{54} *has an involution which is associated with the Gauss map* (Proposition 2.12).

In section 3, we study the structure of the elliptic fibrations on the components $\mathcal{N}_\varepsilon/G$, $\varepsilon = $ torus, gen which are represented by the normal families C_s, $s \in \boldsymbol{P}^1(\boldsymbol{C})$ and D_s, $s \in \boldsymbol{P}^1(\boldsymbol{C})$. Using a quadratic transformation we write these

2000 *Mathematics Subject Classification*. Primary 14H10; Secondary 14H52, 14H20.
Key Words and Phrases. Sextics, dual curves, elliptic curves, Mordell-Weil torsion.

families by smooth cubic curves C_s and D_s which are defined by the following cubic polynomials.

$$C_s : x^3 - \frac{1}{4}s(x-1)^2 + sy^2 = 0$$

$$\begin{aligned} D_s : -8x^3 + 1 + (s+35)y^2 - 6x^2 + 3x - 6\sqrt{-3}y - 3\sqrt{-3}x \\ - 6\sqrt{-3}x^2 - 12\sqrt{-3}xy + (s-35)xy = 0 \end{aligned}$$

We show that C_s, $s \in \boldsymbol{P}^1(\boldsymbol{C})$ (respectively D_s, $s \in \boldsymbol{P}^1(\boldsymbol{C})$) *has the structure of rational elliptic surfaces* X_{431} (resp. X_{3333}) in the notation of [**Mi-P**].

In section 4, we study their torsion subgroups of the Mordell-Weil group of the cubic families C_s and D_s. The family C_s is defined over $\boldsymbol{Q}$ and D_s is defined over quadratic number field $\boldsymbol{Q}(\sqrt{-3})$. Both families enjoy beautiful arithmetic properties. We will show that *the torsion group* $(C_s)_{\mathrm{tor}}(\boldsymbol{Q})$ *is isomorphic to* $\boldsymbol{Z}/3\boldsymbol{Z}$ *for a generic* $s \in \boldsymbol{Q}$ *but it has subfamilies* $C_{\varphi_6(u)}$, $C_{\varphi_{6,2}(r)}$, $C_{\varphi_9(t)}$ *and* $C_{\varphi_{12}(v)}$, $u, r, t, v \in \boldsymbol{Q}$ *for which the Mordell-Weil torsion group are* $\boldsymbol{Z}/6\boldsymbol{Z}$, $\boldsymbol{Z}/6\boldsymbol{Z} + \boldsymbol{Z}/2\boldsymbol{Z}$, $\boldsymbol{Z}/9\boldsymbol{Z}$ *and* $\boldsymbol{Z}/12\boldsymbol{Z}$ *respectively*. Each of these groups is parametrized by a rational function with $\boldsymbol{Q}$ coefficients which is defined over $\boldsymbol{Q}$ and this parametrization coincides, up to a linear fractional change of parameter, to the universal family given by Kubert in [**Ku**].

As for $(D_s)_{\mathrm{tor}}(\boldsymbol{Q}(\sqrt{-3}))$, we show that $(D_s)_{\mathrm{tor}}(\boldsymbol{Q}(\sqrt{-3}))$ *is generically isomorphic to* $\boldsymbol{Z}/3\boldsymbol{Z} + \boldsymbol{Z}/3\boldsymbol{Z}$ *but it also takes* $\boldsymbol{Z}/3\boldsymbol{Z} + \boldsymbol{Z}/6\boldsymbol{Z}$ *for a subfamily* $D_{\xi_6(t)}$ *parametrized by a rational function with coefficients in* $\boldsymbol{Q}$ *and defined on* $\boldsymbol{Q}(\sqrt{-3})$.

2. Normal forms of the moduli $\mathcal{N}$.

We consider the submoduli $\mathcal{N}^{(1)}$ of the sextics whose cusps are at $O := (0,0)$, $A := (1,1)$ and $B := (1,-1)$. As every sextic in $\mathcal{N}$ can be represented by a curve in $\mathcal{N}^{(1)}$ by the action of G, we have $\mathcal{N}/G \cong \mathcal{N}^{(1)}/G^{(1)}$ where $G^{(1)}$ is the stabilizer of $\mathcal{N}^{(1)} : G^{(1)} := \{g \in G; g(\mathcal{N}^{(1)}) = \mathcal{N}^{(1)}\}$. By an easy computation, we see that $G^{(1)}$ is the semi-direct product of the group $G_0^{(1)}$ and a finite group $\mathcal{K}$, isomorphic to the permutation group $\mathcal{S}_3$ where $G_0^{(1)}$ is defined by

$$G_0^{(1)} := \left\{ M = \begin{pmatrix} a_1 & a_2 & 0 \\ a_2 & a_1 & 0 \\ a_1 - a_3 & a_2 & a_3 \end{pmatrix} \in G;\ a_3(a_1^2 - a_2^2) \neq 0 \right\}.$$

Note that $G_0^{(1)}$ is normal in $G^{(1)}$ and $g \in G_0^{(1)}$ fixes singular points pointwise. The isomorphism $\mathcal{K} \cong \mathcal{S}_3$ is given by identifying $g \in \mathcal{K}$ as the permutation of three singular locus O, A, B. We will study the normal forms of the quotient moduli $\mathcal{N}/G \cong \mathcal{N}^{(1)}/G^{(1)}$.

Lemma 2.1. *For a given line $L := \{y = bx\}$ with $b^2 - 1 \neq 0$, there exists $M \in G_0^{(1)}$ such that L^M is given by $x = 0$.*

Proof. By an easy computation, the image of L by the action of M^{-1}, where M is as above, is defined by $(a_1 - ba_2)y + (a_2 - ba_1)x = 0$. Thus we take $a_1 = ba_2$. Then $a_1^2 - a_2^2 = a_2^2(b^2 - 1) \neq 0$ by the assumption. □

Lemma 2.2. *The tangent cone at O is not $y \pm x = 0$ for $C \in \mathcal{N}^{(1)}$.*

Proof. Assume for example that $y - x = 0$ is the tangent cone of C at O. The intersection multiplicity of the line $L_1 := \{y - x = 0\}$ and C at O is 4 and thus $L_1 \cdot C \geq 7$, an obvious contradiction to Bezout theorem. □

Let $\mathcal{N}^{(2)}$ be the subspace of $\mathcal{N}^{(1)}$ consisting of curves $C \in \mathcal{N}^{(1)}$ whose tangent cone at O is given by $x = 0$. Let $G^{(2)}$ be the stabilizer of $\mathcal{N}^{(2)}$. By Lemma 2.1 and Lemma 2.2, we have the isomorphism:

Corollary 2.3. $\mathcal{N}^{(1)}/G^{(1)} \cong \mathcal{N}^{(2)}/G^{(2)}$.

It is easy to see that $G^{(2)}$ is generated by the group $G_0^{(2)} := G^{(2)} \cap G_0^{(1)}$ and an element τ of order two which is defined by $\tau(x, y) = (x, -y)$. Note that

$$G_0^{(2)} = \left\{ M = \begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_1 & 0 \\ a_1 - a_3 & 0 & a_3 \end{pmatrix} \in G_0^{(1)};\ a_1 a_3 \neq 0 \right\}.$$

For $C \in \mathcal{N}^{(2)}$, we associate complex numbers $b(C)$, $c(C) \in \mathbf{C}$ which are the directions of the tangent cones of C at A, B respectively. This implies that the lines $y - 1 = b(C)(x - 1)$ and $y + 1 = c(C)(x - 1)$ are the tangent cones of C at A and B respectively. We have shown that $C \in \mathcal{N}_{\text{torus}}^{(2)}$ if and only if $b(C) + c(C) = 0$ and otherwise C is of a general type and they satisfy $c(C)^2 + 3c(C) - b(C)c(C) + 3 - 3b(C) + b(C)^2 = 0$ (§4, [**O2**]).

We consider the subspaces:

$$\mathcal{N}_{\text{torus}}^{(3)} := \{C \in \mathcal{N}_{\text{torus}}^{(2)};\ b(C) = 0\}, \quad \mathcal{N}_{\text{gen}}^{(3)} := \{C \in \mathcal{N}_{\text{gen}}^{(2)};\ b(C) = c(C) = \sqrt{-3}\}$$

and we put $\mathcal{N}^{(3)} := \mathcal{N}_{\text{torus}}^{(3)} \cup \mathcal{N}_{\text{gen}}^{(3)}$.

Remark. The common solution of both equations: $b + c = c^2 + 3c - bc + 3 - 3b + b^2 = 0$ is $(b, c) = (1, -1)$ and in this case, C degenerates into two non-reduced lines $(y^2 - x^2)^2 = 0$ and a conic.

Lemma 2.4. *Assume that $C \in \mathcal{N}^{(2)}$. Then there exist a unique $C' \in \mathcal{N}^{(3)}$ and an element $g \in G^{(2)}$ such that $C^g = C'$. This implies that*

$$\mathcal{N}_{\text{torus}}/G \cong \mathcal{N}_{\text{torus}}^{(2)}/G^{(2)} \cong \mathcal{N}_{\text{torus}}^{(3)}, \quad \mathcal{N}_{\text{gen}}/G \cong \mathcal{N}_{\text{gen}}^{(2)}/G^{(2)} \cong \mathcal{N}_{\text{gen}}^{(3)}.$$

Proof. Assume that $C \in \mathcal{N}^{(1)}_{\text{torus}}$, $b + c = 0$. Consider an element $g \in G_0^{(1)}$,

$$g^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 - a_3 & 0 & a_3 \end{pmatrix}.$$

The image L_A^g is given by $y - x + xa_3 - a_3 - bxa_3 + ba_3 = 0$. Thus we can solve the equation $a_3(1 - b) - 1 = 0$ in a_3 uniquely as $a_3 = 1/(1 - b)$ as $b \neq 1$. Thus $g \in G_0^{(1)}$ is unique if it fixes the singular points pointwise and thus C' is also unique. It is easy to see that the stabilizer of $\mathcal{N}^{(3)}_{\text{torus}}$ is the cyclic group of order two generated by τ, as C' is even in y (see the normal form below) and $C'^{\tau} = C'$ for any $C' \in \mathcal{N}^{(3)}_{\text{torus}}$. Thus we have $\mathcal{N}^{(2)}_{\text{torus}}/G^{(2)} \cong \mathcal{N}^{(3)}_{\text{torus}}$.

Consider the case $C \in \mathcal{N}^{(2)}_{\text{gen}}$. Then the images of the tangent cones at A, B by the action of g are given by $y - x + xa_3 - a_3 - bxa_3 + ba_3 = 0$ and $y + x - xa_3 + a_3 - cxa_3 + ca_3 = 0$ respectively. Assume that $b(C^g) = c(C^g)$. Then we need to have $a_3(1 - b) - 1 = a_3(-1 - c) + 1$, which has a unique solution in a_3, if $(\star)$ $b - c - 2 \neq 0$. Assume that $c^2 + 3c - bc + 3 - 3b + b^2 = 0$ and $b - c - 2 = 0$. Then we get $(b, c) = (1, -1)$ which is excluded as it corresponds to a non-reduced sextic. Thus the condition $(\star)$ is always satisfied. Put $(b', c') := (b(C^g), c(C^g))$. They satisfy the equality $c'^2 + 3c' - b'c' + 3 - 3b' + b'^2 = 0$ and $b' = c'$. Thus we have either $b' = c' = \sqrt{-3}$ or $b' = c' = -\sqrt{-3}$. However in the second case, $(C^g)^{\tau}$ belongs to the first case. Thus $b' = c' = \sqrt{-3}$ and $C^g \in \mathcal{N}^{(3)}_{\text{gen}}$ as desired. □

2.1. Normal forms of curves of a torus type.

In [**O2**], we have shown that a curve in $\mathcal{N}^{(1)}_{\text{torus}}$ is defined by a polynomial $f(x, y)$ which is expressed by a sum $f_2(x, y)^3 + sf_3(x, y)^2$ where $f_2(x, y)$ is a smooth conic passing through O, A, B and $f_3(x, y) = (y^2 - x^2)(x - 1)$.

Proposition 2.5. *The direction of the tangent cones at O, A and B are the same with the tangent line of the conic $f_2(x, y) = 0$ at these points.*

This is immediate as the multiplicity of $f_3(x, y)^2$ at O, A, B are 4. Assume that $C \in \mathcal{N}^{(3)}_{\text{torus}}$, that is, the tangent cones of C at O, A and B are given by $x = 0$, $y - 1 = 0$ and $y + 1 = 0$ respectively. Thus the conic $f_2(x, y) = 0$ is also uniquely determined as $f_2(x, y) = y^2 + x^2 - 2x$. Therefore $\mathcal{N}^{(3)}_{\text{torus}}$ is one-dimensional and it has the representation

$$C_s : f_{\text{torus}}(x, y, s) := f_2(x, y)^3 + sf_3(x, y)^2 = 0. \tag{2.6}$$

For $s \neq 0, 27, \infty$, C_s is a sextic with three $(3, 4)$-cusps, while C_{27} obtains a node. If $g \in G^{(2)}$ fixes the tangent lines $y \pm 1 = 0$, then $g = e$ or τ. As $C_s^{\tau} = C_s$, this implies that $C_s^g = C_s$. Thus $C_s \neq C_t$ if $s \neq t$.

2.2. Normal form of sextics of a general type.

For the moduli $\mathcal{N}_{\mathrm{gen}}$ of sextics of a general type, we start from the expression given in §4.1, [**O2**]. We may assume $b = c = \sqrt{-3}$. Then the parametrization is given by

$$f_{\mathrm{gen}}(x, y, s) := f_0(x, y) + sf_3(x, y)^2, \quad f_3(x, y) = (y^2 - x^2)(x - 1)$$

where s is equal to a_{06} in [**O2**] and f_0 is the sextic given by

$$\begin{aligned}(2.7) \quad f_0(x, y) := {} & y^6 + y^5(6\sqrt{-3} - 6\sqrt{-3}x) + y^4(35 - 76x + 38x^2) \\ & + y^3(-24\sqrt{-3}x + 36\sqrt{-3}x^2 - 12\sqrt{-3}x^3) \\ & + y^2(-94x^2 + 200x^3 - 103x^4) \\ & + y(24\sqrt{-3}x^3 - 42\sqrt{-3}x^4 + 18\sqrt{-3}x^5) + 64x^3 - 133x^4 + 68x^5.\end{aligned}$$

Let $D_s := \{f_{\mathrm{gen}}(x, y, s) = 0\}$ for each $s \in \boldsymbol{C}$. Observe that $D_0 = \{f_0(x, y) = 0\}$ is a sextic with three $(3, 4)$-cusps and of a general type. For the computation of dual curves using Maple V, it is better to take the substitution $y \mapsto y\sqrt{-3}$ to make the equation to be defined over $\boldsymbol{Q}$. Summarizing the discussion, we have

THEOREM 2.8. *The quotient moduli space $\mathcal{N}/G$ is one dimensional and it has two components.*

(1) *The component $\mathcal{N}_{\mathrm{torus}}/G$ has the normal forms $C_s = \{f(x, y, s) = 0\}$ where $f(x, y, s) = f_2(x, y)^3 + sf_3(x, y)^2$, $f_2(x, y) = y^2 + x^2 - 2x$ and $f_3(x, y) = (y^2 - x^2) \cdot (x - 1)$. The curve C_{54} is a unique curve in $\mathcal{N}/G$ which is self-dual.*

(2) *The component $\mathcal{N}_{\mathrm{gen}}/G$ has the normal form*: $f_{\mathrm{gen}}(x, y, s) = f_0(x, y) + sf_3(x, y)^2$ *where f_3 is as above and the sextic $f_0(x, y) = 0$ is contained in $\mathcal{N}_{\mathrm{gen}}$. This component has no self-dual curve.*

PROOF OF THEOREM 2.8. We need only prove the assertion for the dual curves. The proof will be done by a direct computation of dual curves using the method of §2, [**O2**] and the above parametrizations. We use Maple V for the practical computation. Here is the recipe of the proof. Let X^*, Y^*, Z^* be the dual coordinates of X, Y, Z and let $(x^*, y^*) := (X^*/Z^*, Y^*/Z^*)$ be the dual affine coordinates.

(1) Compute the defining polynomials of the dual curves C_s^* and D_s^* respectively, using the method of Lemma 2.4, [**O2**]. Put $g_{\mathrm{torus}}(x^*, y^*, s)$ and $g_{\mathrm{gen}}(x^*, y^*, s)$ the defining polynomials.

(2) Let $G_\varepsilon(X^*, Y^*, Z^*, s)$ be the homogenization of $g_\varepsilon(x^*, y^*, s)$, $\varepsilon =$ torus or gen. Compute the discriminant polynomials $\Delta_{Y^*} G_\varepsilon$ which is a homogeneous polynomial in X^*, Z^* of degree 30 (cf. Lemma 2.8, [**O1**]). Recall that the mul-

tiplicity in $\Delta_{Y^*} G_\varepsilon$ of the pencil $X^* - \eta Z^* = 0$ passing through a singular point is generically given by $\mu + m - 1$ where μ is the Milnor number and m is the multiplicity of the singularity ([**O2**]). Thus the contribution from a $(3,4)$-cusp is 8. Thus if C_s^* has three $(3,4)$-cusps, it is necessary that $\Delta_{Y^*}(G) = 0$ has three linear factors with multiplicity ≥ 8.

(3-1) For the curves of a general type, an easy computation shows that it is not possible to get a degeneration into a sextic with 3 $(3,4)$-cusps by the above reason.

(3-2) For the curves of a torus type, we can see that $s = 54$ is the only parameter such that $C_s^* \in \mathcal{N}$. Thus it is enough to show that $C_{54}^* \cong C_{54}$.

(4) The dual curve C_{54}^* of C_{54} is defined by the homogeneous polynomial

$$\begin{aligned} G(X^*, Y^*, Z^*) := {} & 128{X^*}^5 Z^* + 1376{X^*}^4{Z^*}^2 - 192{X^*}^3{Y^*}^2 Z^* \\ & + 4664{X^*}^3{Z^*}^3 - 2{X^*}^2{Y^*}^4 - 1584{X^*}^2{Y^*}^2{Z^*}^2 \\ & + 7090{X^*}^2{Z^*}^4 + 58X^*{Y^*}^4 Z^* - 3060X^*{Y^*}^2{Z^*}^3 \\ & + 5050X^*{Z^*}^5 + {Y^*}^6 + 349{Y^*}^4{Z^*}^2 - 1725{Y^*}^2{Z^*}^4 + 1375{Z^*}^6. \end{aligned}$$

We can see that C_{54}^* is isomorphic to C_{54} as $(C_{54}^*)^A = C_{54}$ where

$$A = \begin{pmatrix} -4/3 & 0 & -5/3 \\ 0 & 1 & 0 \\ -5/3 & 0 & -13/3 \end{pmatrix}.$$

2.3. Involution τ on C_{54}.

For a later purpose, we change the coordinates of $\boldsymbol{P}^2$ so that the three cusps of C_s are at $O_Z := (0,0,1)$, $O_Y := (0,1,0)$, $O_X := (1,0,0)$. A new normal form in the affine space is given by $C_s : f_2(x,y)^3 + s f_3(x,y)^2 = 0$ where $f_2(x,y) := xy - x + y$ and $f_3(x,y) := -xy$. In particular, C_{54} is defined by

$$f(x,y) = (xy - x + y)^3 + 54x^2y^2 = 0. \tag{2.9}$$

In this coordinate, C_{54}^* is defined by

$$\begin{aligned} & -28y^3 - 17x^4y^2 - 17x^2y^4 - 28x^3y^3 - 2y^5 + 1788x^3y + 1788x^2y \\ & - 17y^4 - 17x^4 + 262xy + 1788x^2y^3 - 1788xy^2 - 262xy^4 + 1788xy^3 \\ & - 1788x^3y^2 - 8166x^2y^2 + 28x^3 + 262x^4y - 2x^5y - 2xy^5 + 1 \\ & - 17y^2 - 17x^2 + 2x^5 + 2x - 2y + x^6 + y^6 = 0. \end{aligned}$$

It is easy to see that $(C_{54}^*)^{A_1} = C_{54}$ where

$$A_1 := \begin{pmatrix} -1/3 & 7/3 & -1/3 \\ 7/3 & -1/3 & 1/3 \\ -1/3 & 1/3 & -7/3 \end{pmatrix}.$$

For a given $A \in GL(3, \boldsymbol{C})$, we denote the automorphism defined by the right multiplication of A by φ_A. Let $F(X, Y, Z)$ be the homogenization of $f(x, y)$. Then the Gauss map $\mathrm{dual}_{C_{54}} : C_{54} \to C_{54}^*$ is defined by

$$\mathrm{dual}_{C_{54}}(X, Y, Z) = (F_X(X, Y, Z), F_Y(X, Y, Z), F_Z(X, Y, Z))$$

where F_X, F_Y, F_Z are partial derivatives. We define an isomorphism $\tau : C_{54} \to C_{54}$ by the composition $\varphi_{A_1} \circ \mathrm{dual}_{C_{54}}$. Then τ is the restriction of the rational mapping: $\Psi : \boldsymbol{C}^2 \to \boldsymbol{C}^2$, $(x, y) \mapsto (x_d, y_d)$ and

(2.10)

$$\begin{cases} x_d := \dfrac{-y^3+4x^2-x^2y^3+4x^3y^2-8x^3y-4x^2y^2-8xy-4xy^2-2xy^3+109x^2y+4y^2+4x^3}{-4y^3+x^2-4x^2y^3+4x^3y^2-8x^3y-109x^2y^2-2xy-4xy^2-8xy^3+4x^2y+y^2+4x^3} \\ y_d := -\dfrac{-4y^3+4x^2-4x^2y^3+x^3y^2-2x^3y-4x^2y^2-8xy-109xy^2-8xy^3+4x^2y+4y^2+x^3}{-4y^3+x^2-4x^2y^3+4x^3y^2-8x^3y-109x^2y^2-2xy-4xy^2-8xy^3+4x^2y+y^2+4x^3}. \end{cases}$$

Observe that τ is defined over $\boldsymbol{Q}$. C_{54} has three flexes of order 2 at $F_1 := (1, -1/4, 1)$, $F_2 := (1/4, -1, 1)$, $F_3 := (4, -4, 1)$ and τ exchanges flexes and cusps:

$$\text{(2.11)} \qquad \begin{cases} \tau(O_X) = F_1, \ \tau(O_Y) = F_2, \ \tau(O_Z) = F_3, \\ \tau(F_1) = O_X, \ \tau(F_2) = O_Y, \ \tau(F_3) = O_Z. \end{cases}$$

Furthermore we assert that

Proposition 2.12. *The morphism τ is an involution on C_{54}.*

Proof. By the definition of τ and Lemma 2.13 below, we have ($C := C_{54}$):

$$\tau \circ \tau = (\varphi_{{}^tA_1^{-1}} \circ \mathrm{dual}_C)^2 = (\mathrm{dual}_{C^{A_1}} \circ \varphi_{A_1}) \circ (\varphi_{{}^tA_1^{-1}} \circ \mathrm{dual}_C) = \mathrm{id}$$

as A_1 is a symmetric matrix. □

Let C be a given irreducible curve in $\boldsymbol{P}^2$ defined by a homogeneous polynomial $F(X, Y, Z)$ and let $B \in GL(3, \boldsymbol{C})$. Then C^B is defined by $G(X, Y, Z) := F((X, Y, Z)B^{-1})$.

Lemma 2.13. *Two curves $(C^B)^*$ and $(C^*)^{{}^tB^{-1}}$ coincide and the following diagram commutes.*

$$\begin{array}{ccc} C & \xrightarrow{\mathrm{dual}_C} & C^* \\ \Big\downarrow \varphi_B & & \Big\downarrow \varphi_{{}^tB^{-1}} \\ C^B & \xrightarrow{\mathrm{dual}_{C^B}} & (C^B)^* \end{array}$$

Proof. The first assertion is the same as Lemma 2, [**O2**]. The second assertion follows from the following equalities. Let $(a,b,c) \in C$.

$$\begin{aligned} \mathrm{dual}_{C^B}(\varphi_B(a,b,c)) &= (G_X(\varphi_B(a,b,c)), G_Y(\varphi_B(a,b,c)), G_Z(\varphi_B(a,b,c))) \\ &= (F_X(a,b,c), F_Y(a,b,c), F_y(a,b,c)){}^tB^{-1} \\ &= \varphi_{{}^tB^{-1}}(\mathrm{dual}_C(a,b,c)) \end{aligned}$$
□

In section 5, we will show that τ is expressed in a simple form as a cubic curve.

3. Structure of elliptic fibrations.

We consider the elliptic fibrations corresponding to the above normal forms. For this purpose, we first take a linear change of coordinates so that three lines defined by $f_3(x,y) = 0$ changes into lines $X = 0$, $Y = 0$ and $Z = 0$. The corresponding three cusps are now at $O_Z = (0,0,1)$, $O_Y = (0,1,0)$, $O_X = (1,0,0)$ in $\boldsymbol{P}^2$. Then we take the quadratic transformation which is a birational mapping of $\boldsymbol{P}^2$ defined by $(X,Y,Z) \mapsto (YZ, ZX, XY)$. Geometrically this is the composition of blowing-ups at O_X, O_Y, O_Z and then the blowing down of three lines which are strict transform of $X, Y, Z = 0$. It is easy to see that our sextics are transformed into smooth cubics for which $X = 0$, $Y = 0$ and $Z = 0$ are tangent lines of the flex points. Those flexes are the image of the $(3,4)$-cusps. We take a linear change of coordinates so that the flex on $Z = 0$ is moved at $O := (0,1,0)$ with the tangent $Z = 0$. Then the corresponding families are described by the families given by $\{h_{\mathrm{torus}}(x,y,s) = 0; s \in \boldsymbol{P}^1\}$ and $\{h_{\mathrm{gen}}(x,y,s) = 0, s \in \boldsymbol{P}^1\}$ where

$$\begin{cases} C_s : h_{\mathrm{torus}}(x,y,s) := x^3 - \dfrac{1}{4}s(x-1)^2 + sy^2, \\ D_s : h_{\mathrm{gen}}(x,y,s) := -8x^3 + 1 + (s+35)y^2 - 6x^2 + 3x \\ \qquad -6\sqrt{-3}y - 3\sqrt{-3}x - 6\sqrt{-3}x^2 - 12\sqrt{-3}xy + (s-35)xy. \end{cases}$$

Let $H_\varepsilon(X,Y,Z,S,T) = h_\varepsilon(X/Z, Y/Z, S/T)Z^3T$ for $\varepsilon =$ torus, gen. We consider the elliptic surface associated to the canonical projection $\pi : S_\varepsilon \to \boldsymbol{P}^1$ where S_ε is the hypersurface in $\boldsymbol{P}^1 \times \boldsymbol{P}^2$ which is defined by $H_\varepsilon(X,Y,Z,S,T) = 0$.

Case I. Structure of $S_{\mathrm{torus}} \to \boldsymbol{P}^1$. For simplicity, we use the affine coordinate $s = S/T$ of $\{T \neq 0\} \subset \boldsymbol{P}^1$ and denote $\pi^{-1}(s)$ by C_s. We see that the singular fibers are $s = 0, 27, \infty$. C_∞ consists of three lines, isomorphic to I_3 in Kodaira's notation, [**Ko**]. C_{27} obtains a node and this fiber is denoted by I_1 in [**Ko**]. The fiber C_0 is a line with multiplicity 3. The surface S_{torus} has three singular points on the fiber C_0 at $(X, Y, Z) = (0, 1/2, 1), (0, -1/2, 1), (0, 1, 0)$. Each singularity is an A_2-singularity. We take minimal resolutions at these points. At each point, we need two $\boldsymbol{P}^1$ as exceptional divisors and let $p : \tilde{S}_{\text{torus}} \to S_{\text{torus}}$ be the resolution map. The composition $\tilde{\pi} := \pi \circ p : \tilde{S}_{\text{torus}} \to \boldsymbol{P}^1$ is the corresponding elliptic surface. Now it is easy to see that $\widetilde{C_0} := \tilde{\pi}^{-1}(0)$ is a singular fiber with 7 irreducible components, which is denoted by IV^* in [**Ko**]. Here we used the following lemma. The elliptic surface $\tilde{S}_{\text{torus}}$ is rational and denoted by X_{431} in [**Mi-P**].

Assume that the surface $V := \{(s, x, y) \in \boldsymbol{C}^3; f(s, x, y) = 0\}$ has an A_2 singularity at the origin where $f(s, x, y) := sx + y^3 + sx \cdot h(s, x, y)$ where $h(O) = 0$. Consider the minimal resolution $\pi : \tilde{V} \to V$ and let $\pi^{-1}(O) = E_1 \cup E_2$. It is well-known that $E_1 \cdot E_2 = 1$ and $E_i^2 = -2$ for $i = 1, 2$.

Lemma 3.1. *Consider a linear form $\ell(s, x, y) = as + bx + cy$ and let L' be the strict transform of $\ell = 0$ to $\tilde{V}$.*

(1) *Assume that $b = c = 0$ and $a \neq 0$. Then $(\pi^*\ell) = 3L' + 2E_1 + E_2$ and $L' \cdot E_1 = 1$ and L' does not intersect with E_2, under a suitable ordering of E_1 and E_2.*

(2) *Assume that $abc \neq 0$. Then we have $(\pi^*\ell) = L' + E_1 + E_2$ and $L' \cdot E_i = 1$ for $i = 1, 2$.*

The proof is immediate from a direct computation.

Case II. Structure of $S_{\text{gen}} \to \boldsymbol{P}^1$. Now consider the elliptic surface S_{gen}. Put $D_s = \pi^{-1}(s)$. The singular fibers are at $s = -35, -53 + 6\sqrt{-3}, -53 - 6\sqrt{-3}$ and $s = \infty$. The fiber $s = \infty$ is already I_3 and S_{gen} is smooth on this fiber. On the other hand, S_{gen} has an A_2-singularity on each fiber D_s, $s = -35, -53 + 6\sqrt{-3}$, $-53 - 6\sqrt{-3}$. Let $p : \tilde{S}_{\text{gen}} \to S_{\text{gen}}$ be the minimal resolution map and we consider the composition $\tilde{\pi} := \pi \circ p : \tilde{S}_{\text{gen}} \to \boldsymbol{P}^1$ as above. Then using (2) of Lemma 3.1, we see that $\tilde{\pi} : \tilde{S}_{\text{gen}} \to \boldsymbol{P}^1$ has four singular fibers and each of them is I_3 in the notation [**Ko**]. This elliptic surface is also rational and denoted as X_{3333} in [**Mi-P**].

4. Torsion group of C_s and D_s.

Consider an elliptic curve C defined over a number field K by a Weierstrass short normal form: $y^2 = h(x), h(x) = x^3 + Ax + B$. The j-invariant is defined by $j(C) = -1728(4A)^3/\Delta$ with $\Delta = -16(4A^3 + 27B^2)$. We study the torsion group of the Mordell-Weil group of C which we denote by $C_{\text{tor}}(K)$ hereafter.

Recall that a point of order 3 is geometrically a flex point of the complex curve C ([**Si**]) and its locus is defined by $f(x, y) = \mathcal{F}(f)(x, y) = 0$ where $f(x, y)$ is the defining polynomial of C and $\mathcal{F}(f) := f_{x,x}f_y^2 - 2f_{x,y}f_xf_y + f_{y,y}f_x^2 = 0$ ([**O1**]). In our case, $\mathcal{F}(f) = 24xy^2 - 18x^4 - 12x^2A - 2A$. The unit of the group is given by the point at infinity $O := (0, 1, 0)$ and the inverse of $P = (\alpha, \beta) \in C$ is given by $(\alpha, -\beta)$ and we denote it by $-P$. For a later purpose, we prepare two easy propositions. Consider a line $L(P, m)$ passing through $-P$ defined by $y = m(x - \alpha) - \beta$. The x-coordinates of two other intersections with C are the solution of $q(x) := f(x, m(x - \alpha) - \beta)/(x - \alpha)$ which is a polynomial of degree 2 in x. Let $\Delta_x q$ be the discriminant of q in x. Note that $\Delta_x q$ is a polynomial in m.

(A) When does a point $Q \in C$ exist such that $2Q = P$.

Assume that a K point $Q = (x_1, y_1)$ satisfies $2Q = P$. Geometrically this implies that the tangent line T_QC passes through $-P$.

Proposition 4.1. *There exists a K-point Q with $2Q = P$ if and only if m is a K-solution of $\Delta_x q(m) = 0$ and x_1 is the multiple solution of $q(x) = 0$. If P is a flex point, $\Delta_x q(m) = 0$ contains a canonical solution which corresponds to the tangent line at P and $m = -f_x(\alpha, \beta)/f_y(\alpha, \beta)$. For any K-solution m with $m \neq -f_x(\alpha, \beta)/f_y(\alpha, \beta)$, the order of Q is equal to $2 \cdot$ order P.*

(B) When does a point $Q \in C$ exist such that $3Q = P$.

Assume that a K-point $Q = (x_1, y_1)$ satisfies $3Q = P$. Put $Q' := 2Q$ and put $Q' = (x_2, y_2)$. Let T_QC be the tangent line at Q. Then T_QC intersects C at $-Q'$. Then $-3Q$ is the third intersection of C and the line L which passes through Q, Q'. Thus three points $-P, Q, Q'$ are colinear. Write L as $y = m(x - \alpha) - \beta$. Then x_1, x_2 are the solutions of $q(x) = 0$. Thus we have

$$x_2 = -\mathrm{coeff}(q, x)/\mathrm{coeff}(q, x^2) - x_1, \quad y_1 = m(x_1 - \alpha) - \beta \tag{4.2}$$

where $\mathrm{coeff}(q, x^i)$ is the coefficient of x^i in $q(x)$. Let $L_Q(x, y)$ be the linear form defining T_QC and let $R(x)$ be the resultant of $f(x, y)$ and $L_Q(x, y)$ in y. Put $R_1(x) := R(-\mathrm{coeff}(q, x)/\mathrm{coeff}(q, x^2) - x)$. Then by the above consideration, $x = x_1$ is a common solution of $q(x) = R_1(x) = 0$. Let $R_2(m)$ be the resultant of $q(x)$ and $R_1(x)$. Note that if $\Delta_x q(m) = 0$, L is tangent to C at Q and $R_2(m) = 0$. In this case, $2Q = P$.

Proposition 4.3. *Assume that there exists a K-point Q with $3Q = P$ and order $Q = 3 \cdot$ order P and let m be as above. Then $R_2(m) = 0$ and $\Delta_x q(m) \neq 0$. Moreover x_1 is given as a common solution of $q(x) = R_1(x) = 0$.*

Actually one can show that $R_2(m)$ is divisible by $(\Delta_x q)^2$.

4.1. Cubic family associated with sextics of a torus type.

We have observed that the family C_s for $s \in \boldsymbol{Q}$ is defined over $\boldsymbol{Q}$. First, recall that C_s is defined by

$$C_s : x^3 - \frac{1}{4}s(x-1)^2 + sy^2 = 0 \tag{4.4}$$

and the Weierstrass normal form is given by $C_s : y^2 = x^3 + a(s)x + b(s)$ where

$$a(s) = -\frac{1}{48}s^4 + \frac{1}{2}s^3, \quad b(s) = -\frac{1}{24}s^5 + \frac{1}{4}s^4 + \frac{1}{864}s^6. \tag{4.5}$$

Put $\Sigma := \{0, 27, \infty\}$. This corresponds to singular fibers. We have two sections of order 3: $s \mapsto ((1/12)s^2, \pm(1/2)s^2)$. Put $P_1 := ((1/12)s^2, (1/2)s^2)$. Thus the torsion group is at least $\boldsymbol{Z}/3\boldsymbol{Z}$. By [**Ma**], the possible torsion group which has an element of order 3 is one of $\boldsymbol{Z}/3\boldsymbol{Z}$, $\boldsymbol{Z}/6\boldsymbol{Z}$, $\boldsymbol{Z}/2\boldsymbol{Z}+\boldsymbol{Z}/6\boldsymbol{Z}$, $\boldsymbol{Z}/9\boldsymbol{Z}$, or $\boldsymbol{Z}/12\boldsymbol{Z}$. The j-invariant of C_s is given by

$$j(C_s) := j_{\text{torus}}(s), \quad j_{\text{torus}}(s) := s(s-24)^3/(s-27). \tag{4.6}$$

(1) Assume that $(C_s)_{\text{tor}}(\boldsymbol{Q})$ has an element of order 6, say $P_2 := (\alpha_2, \beta_2) \in C_s \cap \boldsymbol{Q}^2$. We may assume that $P_2 + P_2 = P_1$. By Proposition 4.1, this implies that $x = \alpha_2$ must be the multiple solution of

$$q(x) := s^4 - 36s^3 - 72ms^2 - 6xs^2 - 6s^2m^2 + 72m^2x - 72x^2 = 0.$$

As $-f_x(-P_1)/f_y(-P_1) = -s/2$, we must have $m \neq -s/2$ and thus

$$\Delta_x' q := \Delta_x q/(2m+s) = s^3 - 32s^2 - 2ms^2 - 4m^2 s + 8m^3 = 0. \tag{4.7}$$

The curve $\Delta_x'(q) = 0$ is a rational curve and we can parametrize $\Delta_x' q = 0$ as $s = \varphi_6(u)$, $m = \varphi_6(u)u$ where

$$\varphi_6(u) := 32/(1+2u)(2u-1)^2. \tag{4.8}$$

The point P_2 is parametrized as

$$P_2 = \left(\frac{128}{3}\frac{-1+12u^2}{(2u+1)^2(-1+2u)^4}, \frac{512(6u+1)}{(-1+2u)^5(2u+1)^2}\right) \tag{4.9}$$

where $u \in \boldsymbol{Q}$. We put $A_6 := \{s = \varphi_6(u); u \in \boldsymbol{Q}\}$ and $\Sigma_6 := \varphi^{-1}(\Sigma)$. Note that $\Sigma_6 = \{-1/2, 1/2, 5/6, -1/6\}$.

(1-2) Assume that we are given $s = \varphi(u)$ and we consider the case when (4.7) has three rational solutions in m for a fixed s. This is the case if $\varphi_6(u) = \varphi_6(v)$ has two rational solutions different from u. This is also equivalent to $(C_s)_{\text{tor}}(\boldsymbol{Q})$ has $\boldsymbol{Z}/2\boldsymbol{Z}+\boldsymbol{Z}/2\boldsymbol{Z}$ as a subgroup. The equation is given by the conic

(4.10) $$Q : 4u^2 - 2u + 4uv - 1 - 2v + 4v^2 = 0.$$

By an easy computation, Q is rational and it has a parametrization as follows.

(4.11) $$u = \varphi_2(r) := \frac{-36 + 5r^2}{6(12 + r^2)}, \quad v(r) := -\frac{1}{6}\frac{(r^2 + 24r - 36)}{(12 + r^2)}.$$

The generators are P_2 of order 6 and $R = (\gamma, 0)$ of order 2 where

$$\gamma := -\frac{81}{4}\frac{(r^4 - 48r^3 + 72r^2 - 432)(12 + r^2)^4}{(r^2 - 36)^4 r^4}.$$

Put $\varphi_{6,2}(r) := \varphi_6(\varphi_2(r))$, which is given explicitly as

$$\varphi_{6,2}(r) = 27(12 + r^2)/r^2(r - 6)^2(r + 6)^2.$$

We define a subset $A_{6,2}$ of A_6 by the image $\varphi_{6,2}(\boldsymbol{Q})$. Put $\Sigma_{6,2} := \varphi_{6,2}^{-1}(\Sigma)$. It is given by $\Sigma_{6,2} = \{0, \pm 2, \pm 6\}$.

(2) Assume that there exists a rational point $P_3 = (\alpha_3, \beta_3)$ of order 9 such that $3P_3 = P$. By Proposition 4.3, this is the case if and only if

$$\begin{aligned}R_3(m,s) := {} & 512m^9 + 768m^8 s - 512m^6 s^3 - 1536m^6 s^2 - 192s^4 m^5 \\ & - 6144m^5 s^3 - 6528m^4 s^4 + 96s^5 m^4 - 12288m^3 s^4 \\ & - 2048m^3 s^5 + 64s^6 m^3 + 480s^6 m^2 - 15360s^5 m^2 \\ & - 6144s^6 m + 384s^7 m - 6s^8 m + 56s^8 - 512s^6 - 768s^7 - s^9 = 0\end{aligned}$$

has a rational solution. Here R_3 is $R_2/(\Delta_x q)^2(s + 2m)s^4$ up to a constant multiplication. Again we find that the curve $\{(m,s) \in \boldsymbol{C}^2; R_3(m,s) = 0\}$ is rational and we can parametrize this curve as $s = \varphi_9(t)$, $m = \psi_9(t)$ where

(4.12) $$\begin{cases} \varphi_9(t) := -\dfrac{1}{8}\dfrac{(-1 + 9t^2 - 3t + 3t^3)^3}{t^3(t-1)^3(t+1)^3} \\ \psi_9(t) := \dfrac{1}{16}\dfrac{(-1 + 9t^2 - 3t + 3t^3)^2(-t + t^3 + 1 + 7t^2)}{t^3(t-1)^3(t+1)^3}. \end{cases}$$

The generator $P_3 = (\alpha_3, \beta_3)$ is given by

$$\begin{cases} \alpha_3 = \dfrac{1}{768}\dfrac{(1 - 18t + 15t^2 - 12t^3 + 15t^4 + 30t^5 + 33t^6)(9t^2 - 1 + 3t^3 - 3t)^4}{(t-1)^6(t+1)^6 t^6} \\ \beta_3 = -\dfrac{1}{512}\dfrac{(1 + 3t^2)(9t^2 - 1 + 3t^3 - 3t)^6}{(t-1)^5(t+1)^7 t^8}. \end{cases}$$

We put $A_9 := \{\varphi_9(t); t \in \boldsymbol{Q}\}$ and $\Sigma_9 := \varphi_9^{-1}(\Sigma) = \{0, 1, -1\}$.

(3) Assume that $s \in A_6$ and $(C_s)_{\mathrm{tor}}(\boldsymbol{Q})$ has an element $P_4 = (\alpha_4, \beta_4) \in C_s \cap \boldsymbol{Q}^2$ of order 12. Then we may assume that $P_4 + P_4 = P_2$. This implies that the tangent line at P_4 passes through $-P_2$. Write this line as $y = n(x - \alpha_2) - \beta_2$. By the same discussion as above, the equality $\Gamma(n_1, u) = 0$ holds where Γ is the polynomial defined by

$$\begin{aligned}(4.13)\qquad \Gamma(u, n_1) := {} & -786432u^4 - 98304n_1u^3 - 524288u^3 + 393216u^2 \\ & - 16384n_1u^2 - 3072n_1^2u^2 + 131072u + 24576n_1u \\ & + 4096n_1 + 16384 + 256n_1^2 + n_1^4\end{aligned}$$

and $n = n_1/(2u+1)(2u-1)^2$. Again we find that $\Gamma = 0$ is a rational curve and we have a parametrization: $u = u(v)$ and $n_1 = n_1(v)$ where

$$(4.14)\qquad u(v) = -\frac{1}{2}\frac{(v^4 + 2v^2 + 5)}{(v^4 - 6v^2 - 3)}, \quad n_1(v) = -16\frac{(2v^2 - 4v^3 - 4v + v^4 - 3)}{(v^4 - 6v^2 - 3)}$$

$$(4.15)\qquad s = \varphi_{12}(v) := \varphi_6(u(v)), \quad \varphi_{12}(v) := -\frac{(v^4 - 3 - 6v^2)^3}{(v-1)^4(1+v)^4(1+v^2)}.$$

The generator of the torsion group $\boldsymbol{Z}/12\boldsymbol{Z}$ is $P_4 = (\alpha_4, \beta_4)$ where

$$\begin{cases} \alpha_4 := \dfrac{1}{12}\dfrac{(v^8 - 12v^7 + 24v^6 - 36v^5 + 42v^4 + 12v^3 + 36v - 3)(v^4 - 6v^2 - 3)^4}{(v-1)^8(v+1)^8(v^2+1)^2} \\ \beta_4 := -\dfrac{1}{2}\dfrac{(v^4 - 6v^2 - 3)^6 v(v^2+3)}{(v-1)^7(v+1)^{11}(v^2+1)^2}. \end{cases}$$

We put $A_{12} := \{\varphi_{12}(v); v \in \boldsymbol{Q}\}$. By definition, $A_{12} \subset A_6$. The singular fibers $\Sigma_{12} := \varphi^{-1}(\Sigma)$ is given by $\{0, \pm 1\}$. Summarizing the above discussion, we get

THEOREM 4.16. *The j-invariant is given by* $j_{\mathrm{torus}}(s) = s(s-24)^3/(s-27)$ *and the Mordell-Weil torsion group of* C_s *is given as follows.*

$$(C_s)_{\mathrm{tor}}(\boldsymbol{Q}) = \begin{cases} \boldsymbol{Z}/3\boldsymbol{Z}, & s \in \boldsymbol{Q} - A_6 \cup A_9 \cup \Sigma \\ \boldsymbol{Z}/6\boldsymbol{Z}, & s = \varphi_6(u) \in A_6 - A_{6,2} \cup A_{12}, \ u \in \boldsymbol{Q} - \Sigma_6 \\ \boldsymbol{Z}/6\boldsymbol{Z} + \boldsymbol{Z}/2\boldsymbol{Z}, & s = \varphi_{6,2}(r) \in A_{6,2}, \ r \in \boldsymbol{Q} - \Sigma_{6,2} \\ \boldsymbol{Z}/9\boldsymbol{Z}, & s = \varphi_9(t) \in A_9, \ t \in \boldsymbol{Q} - \Sigma_9 \\ \boldsymbol{Z}/12\boldsymbol{Z}, & s = \varphi_{12}(v) \in A_{12}, \ v \in \boldsymbol{Q} - \Sigma_{12} \end{cases}$$

4.2. Comparison with Kubert family.

In [**Ku**], Kubert gave parametrizations of the moduli of elliptic curves defined over $\boldsymbol{Q}$ with given torsion groups which have an element of order ≥ 4. His family starts with the normal form:

(4.17) $$E(b,c) : y^2 + (1-c)xy - by = x^3 - bx^2.$$

We first eliminate the linear term of y and then the coefficient of x^2. Let $K_w(b,c)$ be the Weierstrass short normal form, which is obtained in this way. The j-invariant is given by

$$j(E(b,c)) = \frac{(1 - 8bc^2 - 8cb - 4c + 16b + 6c^2 + 16b^2 - 4c^3 + c^4)^3}{b^3(3c^2 - c - 3c^3 - 8bc^2 + b - 20cb + c^4 + 16b^2)}.$$

For a given elliptic curve E defined over K with Weierstrass normal form $E : y^2 = x^3 + ax + b$ and a given $k \in K$, the change of coordinates $x \mapsto x/k^2$, $y \mapsto y/k^3$ changes the normal form into $y^2 = x^3 + ak^4x + bk^6$. We denote this operation by $\Psi_k(E)$.

1. Elliptic curves with the torsion group $\boldsymbol{Z}/6\boldsymbol{Z}$. This family is given by a parameter c with $b = c + c^2$.

2. Elliptic curves with the torsion group $\boldsymbol{Z}/6\boldsymbol{Z} + \boldsymbol{Z}/2\boldsymbol{Z}$. This family is given by a parameter c_1 with $b = c + c^2$ and $c = (10 - 2c_1)/(c_1^2 - 9)$.

3. Elliptic curves with the torsion group $\boldsymbol{Z}/9\boldsymbol{Z}$. The corresponding parameter is f and $b = cd$, $c = fd - f$, $d = f(f-1) + 1$.

4. Elliptic curves with the torsion group $\boldsymbol{Z}/12\boldsymbol{Z}$. The corresponding parameter is τ and $b = cd$, $c = fd - f$, $d = m + \tau$, $f = m/(1-\tau)$ and $m = (3\tau - 3\tau^2 - 1)/(\tau - 1)$.

Proposition 4.18. *Our family $C_{\varphi_6(u)}, C_{\varphi_{6,2}(r)}, C_{\varphi_9(t)}, C_{\varphi_{12}(v)}$ are equivalent to the respective Kubert families. More explicitly, we take the following change of parameters to make their j-invariants coincide with those of Kubert and then we take the change of coordinates of type Ψ_k to make the Weierstrass short normal forms to be identical with $K_w(x,y)$.*

1. *For $C_{\varphi_6(u)}$, take $u = -(c-1)/2(3c+1)$ and $k = c^2(c+1)/(3c+1)^2$.*
2. *For $C_{\varphi_{6,2}(r)}$, take $r = -12/(c_1 - 3)$ and $k = 4(-5 + c_1)^2(c_1 - 1)^2/(c_1^2 - 6c_1 + 21)^2/(c_1 - 3)(c_1 + 3)$.*
3. *For $C_{\varphi_9(t)}$, take $t = -f/(f-2)$ and $k = f^3(f-1)^3/(f^3 - 3f^2 + 1)^2$.*
4. *For $C_{\varphi_{12}(v)}$, take $v = -1/(2\tau - 1)$ and $k = (\tau - 1)\tau^4(-2\tau + 2\tau^2 + 1)(-1 + 2\tau)^2/(6\tau^4 - 12\tau^3 + 12\tau^2 - 6\tau + 1)^2$.*

We omit the proof as the assertion is immediate from a direct computation.

4.3. Involution on C_{54}.

We consider again the self dual curve $C := C_{54}$ (see §3). The Weierstrass normal form is $y^2 = x^3 - 98415x + 11691702$. Note that $54 \in A_6 - A_{12} \cup A_{6,2} \cup \Sigma$. In fact, $54 = \varphi_6(1/6)$ and $54 \notin A_{12} \cup A_{6,2}$. The j-invariant is 54000 and the torsion group $C_{\mathrm{tor}}(\boldsymbol{Q})$ is $\boldsymbol{Z}/6\boldsymbol{Z}$ and the generator is given by $P = (-81, 4374)$.

Other rational points are $2P = (243, -1458)$, $3P = (162, 0)$, $4P = (243, 1458)$, $5P = (-81, -4374)$, and $O = (0, 1, 0)$ (= the point at infinity). Recall that C has an involution τ which is defined by (2.10) in §3. To distinguish our original sextic and cubic, we put

$$C^{(6)} : (xy - x + y)^3 + 54x^2y^2 = 0, \quad C^{(3)} : y^2 = x^3 - 98415x + 11691702.$$

The identification $\Phi : C^{(3)} \to C^{(6)}$ is given by the rational mapping:

$$\Phi(x, y) = (-2916/(27x - 5103 - y), 2916/(y + 27x - 5103))$$

and the involution $\tau^{(3)}$ on $C^{(3)}$ is given by the composition $\Phi^{-1} \circ \tau \circ \Phi$. After a boring computation, $\tau^{(3)}$ is reduced to an extremely simple form in the Weierstrass normal form and it is given by $\tau^{(3)}(x, y) = (p(x, y), q(x, y))$ where

$$(4.19) \qquad p(x, y) := 81\frac{2x - 567}{x - 162}, \quad q(x, y) := -19683\frac{y}{(x - 162)^2}.$$

Note that C has another canonical involution ι which is an automorphism defined by $\iota : (x, y) \mapsto (x, -y)$. We can easily check that $\tau^{(3)} \circ \iota = \iota \circ \tau^{(3)}$. Note that $\tau^{(3)}(P) = 2P$, $\tau^{(3)}(2P) = P$, $\tau^{(3)}(3P) = O$, $\tau^{(3)}(O) = 3P$, $\tau^{(3)}(4P) = 5P$, $\tau^{(3)}(5P) = 4P$. Let $\eta : C \to C$ be the translation by the 2-torsion element $3P$ i.e., $\eta(x, y) = (x, y) + (162, 0)$. It is easy to see that $\tau^{(3)}$ is the composition $\iota \circ \eta$. That is $\tau^{(3)}(x, y) = (x, -y) + (162, 0)$ where the addition is the addition by the group structure of C_{54}. Thus

Theorem 4.20. *The involution τ on sextics $C^{(6)}$ is equal to the involution $\tau^{(3)}$ on $C^{(3)}$ which is defined by* (4.19) *and it is also equal to* $(x, y) \mapsto (x, -y) + (162, 0)$.

4.4. Cubic family associated with sextics of a general type.

We consider the family of elliptic D_s curves associated to the moduli of sextics of a general type with three $(3, 4)$-cusps. Recall that D_s is defined by the equation:

$$\begin{aligned} D_s : -8x^3 + 1 + sy^2 + 35y^2 - 6x^2 + 3x - 6\sqrt{-3}y - 3\sqrt{-3}x \\ - 6\sqrt{-3}x^2 - 12\sqrt{-3}xy + (s - 35)xy = 0. \end{aligned}$$

This family is defined over $\boldsymbol{Q}(\sqrt{-3})$. We change this polynomial into a Weierstrass normal form by the usual process killing the coefficient of y and then by killing the coefficient of x^2. A Weierstrass normal forms is given by $y^2 = x^3 + a(s)x + b(s)$ where

$$
(4.21)\quad \begin{cases} a(s) := -\dfrac{1}{768}(s+47)(s+71)(s^2+70s+1657) \\ b(s) := \dfrac{1}{55296}(s^2+70s+793)(s^4+212s^3+17502s^2 \\ \qquad\qquad\qquad\qquad + 648644s + 9038089). \end{cases}
$$

The singular fibers are $s = -35$, $-53 + 6\sqrt{-3}$, $-53 - 6\sqrt{-3}$ and $s = \infty$. Put $\Sigma = \{-35, -53 \pm 6\sqrt{-3}, \infty\}$. In this section, we consider the Modell-Weil torsion over the quadratic number field $\boldsymbol{Q}(\sqrt{-3})$. First we observe that this family has 8 sections of order three $\pm P_{3,i}$, $i = 1, \dots, 4$ where $P_{3,i}$ are given by

$$
(4.22)\qquad P_{3,1} := (x_{3,1}, y_{3,1}),\quad \begin{cases} x_{3,1} := 5041/48 + 71s/24 + s^2/48 \\ y_{3,1} := 2917/4 + 53s/2 + s^2/4, \end{cases}
$$

$$
(4.23)\quad P_{3,2} := (x_{3,2}, y_{3,2}),\quad \begin{cases} x_{3,2} := -2209/16 - 47s/8 - s^2/16 \\ y_{3,2} := \sqrt{-3}(s^2+106s+2917)(s+35)/144, \end{cases}
$$

$$
(4.24)\quad P_{3,3} := (x_{3,3}, y_{3,3}),\quad \begin{cases} x_{3,3} := s^2/48 + 793/48 + 35s/24 + (s+35)\sqrt{-3}/2 \\ y_{3,3} := (-1+\sqrt{-3})(s+35)(s+6\sqrt{-3}+53)/8, \end{cases}
$$

$$
(4.25)\quad P_{3,4} := (x_{3,4}, y_{3,4}),\quad \begin{cases} x_{3,4} := s^2/48 + 793/48 + 35s/24 - (s+35)\sqrt{-3}/2 \\ y_{3,4} := -(1+\sqrt{-3})(s+53-6\sqrt{-3})(s+35)/8. \end{cases}
$$

Thus they generate a subgroup isomorphic to $\boldsymbol{Z}/3\boldsymbol{Z} + \boldsymbol{Z}/3\boldsymbol{Z}$. We can take the generators $P_{3,1}, P_{3,2}$ for example. Thus by [**Ke-Mo**], $(D_s)_{\mathrm{tor}}(\boldsymbol{Q}(\sqrt{-3}))$ is isomorphic to one of the following.

(a) $\boldsymbol{Z}/3\boldsymbol{Z} + \boldsymbol{Z}/3\boldsymbol{Z}$, (b) $\boldsymbol{Z}/3\boldsymbol{Z} + \boldsymbol{Z}/6\boldsymbol{Z}$ and (c) $\boldsymbol{Z}/6\boldsymbol{Z} + \boldsymbol{Z}/6\boldsymbol{Z}$.

By the same discussion as in 5.1, there exists $P \in D_s$ with order 6 and $2P = P_{3,1}$ if and only if

$$
\Delta(s,m) := s^3 + 85s^2 - 4ms^2 - 568ms + 1555s - 16m^2s \\ - 1136m^2 - 15465 - 20164m + 64m^3 = 0.
$$

Fortunately the variety $\Delta = 0$ is again rational and we can parametrize it as

$$
(4.26)\quad s = \xi_6(t),\ \ \xi_6(t) := -(27t^3 - 1304t^2 + 17920t - 71680)/(t-8)(t-16)^2,
$$

$$
(4.27)\quad m = \psi(t),\quad \psi(t) := -(-128t^2 + 3t^3 + 1536t - 6144)/(t-8)(t-16)^2.
$$

It turns out that the condition for the existence of $Q \in D_s$ with $2Q = P_{3,2}$ is the same with the existence of P, $2P = P_{3,1}$. Assume that $s = \xi_6(t)$. Then by an easy computation, we get $P = (x_{6,1}, y_{6,1})$ and $Q = (x_{6,2}, y_{6,2})$ where

$$x_{6,1} := -\frac{1}{3}\frac{(-3072t^5+11796480t^2+86016t^4-1327104t^3-56623104t+113246208+47t^6)}{(t-8)^2(t-16)^4},$$

$$y_{6,1} := \frac{-4t^3(t^2-24t+192)(7t^2-144t+768)}{(t-16)^5(t-8)^2},$$

$$x_{6,2} := \frac{1}{3}\frac{(37t^6-2016t^5+40704t^4-294912t^3-1179648t^2+28311552t-113246208)}{(t-8)^2(t-16)^4},$$

$$y_{6,2} := -\frac{8}{7}\frac{\sqrt{-3}(t-12)(t-12-4\sqrt{-3})(7t-72+8\sqrt{-3})(7t-72-8\sqrt{-3})t(t-12+4\sqrt{-3})}{(t-16)^3(t-8)^3}.$$

It is easy to see by a direct computation that $3P = 3Q = (\alpha, 0)$ where

$$\alpha := -\frac{2}{3}\frac{(t^2-48t+384)(13t^4-528t^3+8064t^2-55296t+147456)}{(t-8)^2(t-16)^4},$$

and $Q - P = P_{3,3}$. Now we claim that

Claim 1. $(D_s)_{\mathrm{tor}}(\boldsymbol{Q}(\sqrt{-3})) = \boldsymbol{Z}/3\boldsymbol{Z} + \boldsymbol{Z}/6\boldsymbol{Z}$ with generators $P_{3,3}$ and P.

In fact, if the torsion is $\boldsymbol{Z}/6\boldsymbol{Z} + \boldsymbol{Z}/6\boldsymbol{Z}$, there exist three elements of order two. However $f_0(x) := f(x,0)$ factorize as $(x-\alpha)f_{0,0}(x)$ and their discriminants are given by

$$\Delta_x f_0 := \frac{2048t^6(t-12)^3(t^2-24t+192)^3(7t^2-144t+768)^6}{(t-8)^9(t-16)^{18}},$$

$$\Delta_x f_{0,0} := 165888(t-12)^3(t^2-24t+192)^3(t-8)^7(t-16)^8.$$

Consider quartic $Q_4 : g(t,v) := 165888(t-12)(t^2-24t+192)(t-8) - v^2 = 0$. Thus D_s has three two torsion elements if and only if the quartic $g(t,v) = 0$ has $\boldsymbol{Q}(\sqrt{-3})$-point (t_0, v_0) with $t_0 \neq 8, 16, 12, 12 \pm 4\sqrt{-3}$. The proof of Claim is reduces to:

Assertion 1. There are no such point on Q_4.

Proof. By an easy birational change of coordinates, $g(t,v) = 0$ is equivalent to the elliptic curve $C := \{x^3 + 1/16777216 - y^2 = 0\}$. We see that C has two elements of order three, $(0, \pm 1/4096)$ and three two-torsions $(-1/256, 0)$, $(1/512 - 1/512\sqrt{-3}, 0)$ and $(1/512 + 1/512\sqrt{-3}, 0)$. Again by [**Ke-Mo**], $C_{\mathrm{tor}}(\boldsymbol{Q}(\sqrt{-3})) = \boldsymbol{Z}/2\boldsymbol{Z} + \boldsymbol{Z}/6\boldsymbol{Z}$. As the rank of C is 0 ([**S-Z**]), there are exactly 12 points on

C. They correspond to either zeros or poles of $\Delta_x(f_0)$. This implies that the quartic Q_4 has no non-trivial points and thus C does not have three 2-torsion points. This completes the proof of the Assertion and thus also proves the Claim. □

Now we formulate our result as follows. Let $A_6 = \{s = \xi_6(t); t \in \boldsymbol{Q}(\sqrt{-3})\}$ and $\Sigma_6 := \xi_6^{-1}(\Sigma)$ is given by $\Sigma_6 = \{8, 16, 0, 12, 12 \pm 4\sqrt{-3}, (72 \pm 8\sqrt{-3})/7\}$.

THEOREM 4.28. *The Mordell-Weil torsion of D_s is given by*

$$(D_s)_{\text{tor}}(\boldsymbol{Q}(\sqrt{-3})) = \begin{cases} \boldsymbol{Z}/3\boldsymbol{Z} + \boldsymbol{Z}/3\boldsymbol{Z} & s \in \boldsymbol{Q}(\sqrt{-3}) - A_6 \cup \Sigma \\ \boldsymbol{Z}/6\boldsymbol{Z} + \boldsymbol{Z}/3\boldsymbol{Z} & s = \xi_6(t) \in A_6, \quad t \in \boldsymbol{Q}(\sqrt{-3}) - \Sigma_6. \end{cases}$$

The j-invariant is given by

$$j(D_s) = \frac{1}{64} \frac{(s+47)^3(s+71)^3(s^2+70s+1657)^3}{(s+35)^3(s^2+106s+2917)^3}.$$

4.5. Examples.

(A) First we consider the case of elliptic curves C_s. In the following examples, we give only the values of parameter s as the coefficients are fairly big. The corresponding Weierstrass normal forms are obtained by (4.5).

1. $s = 54$. The curve C_{54} with torsion group $\boldsymbol{Z}/6\boldsymbol{Z}$ has been studied in §4.3.

2. Take $r = 3$, $s = \varphi_{6,2}(3) = 343/9$. Then the torsion group is isomorphic to $\boldsymbol{Z}/6\boldsymbol{Z} + \boldsymbol{Z}/2\boldsymbol{Z}$ with generators $P_2 = (-55223/972, -588245/486)$ and $R = (88837/972, 0)$. The j-invariant is given by $7^3 \cdot 127^3/2^2 \cdot 3^6 \cdot 5^2$.

3. Take $t = -3$, $s = \varphi_9(-3) = 1/216$. Then the torsion group is isomorphic to $\boldsymbol{Z}/9\boldsymbol{Z}$ and the generator $P_3 = (289/559872, -7/419904)$. The j-invariant is $71^3 \cdot 73^3/2^9 \cdot 3^9 \cdot 7^3 \cdot 17$.

4. Take $v = 3$, $s = \varphi_{12}(3) = -27/80$. Then the torsion is isomorphic to $\boldsymbol{Z}/12\boldsymbol{Z}$ with generator $P_4 = (-2997/25600, -6561/102400)$. The j-invariant is $-11^3 \cdot 59^3/2^{12} \cdot 3 \cdot 5^3$.

(B) We consider elliptic curves D_s defined over $\boldsymbol{Q}(\sqrt{-3})$. The normal form is given by (4.21).

5. Take $s = 1$. Then $(D_1)_{\text{tor}}(\boldsymbol{Q}(\sqrt{-3})) = \boldsymbol{Z}/3\boldsymbol{Z} + \boldsymbol{Z}/3\boldsymbol{Z}$ and the generators are $(x_{3,1}, y_{3,1}) = (108, 756)$ and $(x_{3,2}, y_{3,2}) = (-144, 756\sqrt{-3})$. The j-invariant is $2^{15}3^3/7^3$.

6. Take $t = 4$ and $s = -299/9$. Then the torsion is isomorphic to $\boldsymbol{Z}/6\boldsymbol{Z} + \boldsymbol{Z}/3\boldsymbol{Z}$. The generators can be taken as $(x_{6,1}, y_{6,1}) = (-2351/243, -532/243)$ and $(x_{3,3}, y_{3,3}) = (8\sqrt{-3}/9 - 2171/243, -680/81 + 248\sqrt{-3}/81)$. The j-invariant is given by $5^3 \cdot 17^3 \cdot 31^3 \cdot 2203^3/2^6 \cdot 3^6 \cdot 7^3 \cdot 19^6$.

4.6. Appendix: Parametrization of rational curves.

Parametrizations of a rational curve are always possible and there exist even some programs to find a parametrization on Maple V. For the detail, see [**Ab-Ba**] and [**vH**] for example. In our case, it is easy to get a parametrization by a direct computation. For a rational curve with degree less than or equal four is easy. For other case, we first decrease the degree, using suitable birational maps. We give a brief indication. We remark here that the parametrization is unique up to a linear fractional change of the parameter.

(1) For the parametrization of $s^3 - 32s^2 - 2ms^2 - 4m^2s + 8m^3 = 0$, put $m = us$.

(2) For the parametrization of

$$\begin{aligned} R_3(m,s) := {} & 512m^9 + 768m^8s - 512m^6s^3 - 1536m^6s^2 - 192s^4m^5 \\ & - 6144m^5s^3 - 6528m^4s^4 + 96s^5m^4 - 12288m^3s^4 - 2048m^3s^5 \\ & + 64s^6m^3 + 480s^6m^2 - 15360s^5m^2 - 6144s^6m + 384s^7m \\ & - 6s^8m + 56s^8 - 512s^6 - 768s^7 - s^9 = 0 \end{aligned}$$

put successively $s = s_1/m_1$ and $m = 1/m_1$, then put $n_1 = n_2/s_1^2$, then $s_1 = s_2 - 2$ and $n_2 = n_4s_2$. This changes degree of our curve to be 6. Then $s_2 + s_3 - 4$ and $n_4 = n_5 + 2$ and $n_5 = n_6s_3$. This changes our curve into a quartic. Other computation is easy.

4.7. Further remark.

We would like to thank to Professor A. Silverberg who has kindly communicated us about the papers [**R-S1**] and [**R-S2**]. In [**R-S1**], a universal family for $\boldsymbol{Z}/3\boldsymbol{Z} + \boldsymbol{Z}/3\boldsymbol{Z}$ over $\boldsymbol{Q}(\sqrt{-3})$ is given as follows. $A(u) : y^2 = x^3 + a_0(u)x + b_0(u)$ where

$$a_0(u) = -27u(8 + u^3), \quad b_0(u) = -54(8 + 20u^3 - u^6)$$

and the subfamily, given by $u = (4 + \tau^3)/(3\tau^2)$, describes elliptic curves with torsion $\boldsymbol{Z}/6\boldsymbol{Z} + \boldsymbol{Z}/3\boldsymbol{Z}$ ([**R-S2**]). Again by an easy computation, we can show that by the change of parameter $s = -47 + 12u$ we can identify D_s and $A(u)$. Our subfamily for $\boldsymbol{Z}/6\boldsymbol{Z} + \boldsymbol{Z}/3\boldsymbol{Z}$ is also the same with that of [**R-S2**] by the fractional change of parameter: $t = 8(\tau - 2)/(\tau - 1)$.

We would like to thank H. Tokunaga for the valuable discussions and informations about elliptic fibrations and also to K. Nakamula and T. Kishi for the information about elliptic curves over a number field. I am also gratefull to SIMATH for many computations.

4.8. Appendix: Computation of dual curves C_s^* and D_s^*.

In Theorem 2.8, the dual curves C_s^* and D_s^* are defined by the following polynomials. C_s^* is defined by $g(x,y)=0$ where:

$$\begin{aligned} g := {} & -4s^3 - 729 - 4374x - 837s + 2187y^2 - 8748x^2 - 864sx^4 - 27sy^6 \\ & + 16s^3xy^2 - 32s^2x^5 - 112s^2x^4 - 24s^3x^2 - 4s^3x^4 - 2187y^4 \\ & - 16s^3x^3 - 16s^3x + 8s^3x^2y^2 - 24s^2x^2y^2 + 729y^6 - 5832x^3 \\ & - 2673sx^2 - 2214sx - 2160sx^3 - 260s^2x^3 - 424s^2x^2 - 356s^2x \\ & - 112s^2 + 68s^2x^3y^2 - 36s^2xy^4 + 972sxy^2 + 27sx^2y^4 - 1080sx^3y^2 \\ & - 810sx^2y^2 + 1242sxy^4 + 8s^3y^2 - 4s^3y^4 + 144s^2y^4 - 783sy^4 \\ & - 32s^2y^2 + 8748xy^2 - 4374xy^4 + 8748x^2y^2 + 1647sy^2 - 120s^2xy^2. \end{aligned}$$

For the dual curve of D_s, we first change the coordinates by $y \mapsto \sqrt{3}I$ so that D_s is defined by $f_1(x,y)=0$ where

$$\begin{aligned} f_1 := {} & 162y^5x - 216y^3x + 324y^3x^2 - 72yx^3 - 108y^3x^3 + 126yx^4 - 54yx^5 \\ & - 12y^2x^3s - 27y^6 - 162y^5 + 64x^3 - 133x^4 + 68x^5 + sx^6 + 315y^4 \\ & + 9y^4s - 684y^4x + 342y^4x^2 - 600y^2x^3 + 309y^2x^4 + x^4s - 2x^5s \\ & - 18y^4xs + 9y^4x^2s + 282y^2x^2 + 6y^2x^4s + 6y^2x^2s \end{aligned}$$

and the dual curve D_s^* is defined by

$$\begin{aligned} & 59011092000y^5x + 6633394206750y^3x + 2758312645200y^3x^2 \\ & \quad + 19978762090770yx^3 + 3718476720000yx^4 + 442161486099 \\ & \quad + 14031749711565x + 1533079825101y + 57301070400y^6 \\ & \quad + 327874701312y^5 + 36043875529317x^2 + 33637736054772x^3 \\ & \quad + 13114936771650x^4 + 1875661200000x^5 - 147317217894s \\ & \quad + 1495218073320y^3 + 840892247884y^4 + 2027895885759y^2 \\ & \quad - 9s^7 - 19567881s^4 - 792758961s^3 - 17398899090s^2 - 284688s^5 \\ & \quad - 2376s^6 + 892912667112xs - 891s^6y - 297s^6y^3 + 18099072s^3y^5 \\ & \quad + 1641408380640y^4x + 40192740000y^4x^2 + 5014174998000y^2x^3 \end{aligned}$$

$$+ 13471184352354\, y^2 x^2 + 624708869400\, y^2 x^3 s - 260721\, s^5 y^2 x$$
$$+ 313980192\, s^3 y^3 x^2 + 25325395200\, s^2 y x^4 + 1111553560851\, s\, y^2 x$$
$$+ 17158062\, s^4 y^2 x^2 + 447680160\, s^3 y^3 x + 1839668382\, s^3 y x^2$$
$$+ 349513914\, s^3 y^2 x + 310125896640\, s\, y^3 x^2 + 48690\, s^5 y^2 x^2$$
$$+ 1255966935678\, s\, y x + 13061376\, s^4 y^2 x^3 + 651732480\, s^3 y x^4$$
$$+ 3109968\, s^4 y^4 x + 13930477632\, s^2 y^3 x^2 + 41472\, s^5 y x^4 + 22680\, s^5 y^4 x$$
$$+ 227913552\, s^3 y^4 x + 857351568\, s^3 y^2 x^3 - 258309\, s^5 y x^2$$
$$+ 31851986040\, s^2 y^2 x^3 + 8284032\, s^4 y x^4 - 12\, s^7 y^2 x + 23328\, s^4 y^5 x$$
$$- 891648\, s^5 x + 576\, s^6 x^5 + 136512\, s^5 x^5 - 36\, s^7 x - 8649\, s^6 x$$
$$- 5193\, s^6 x^3 - 36\, s^7 x^3 + 123193007676\, s^2 x^2 + 100685283444\, s^2 x^4$$
$$+ 48478194\, s^4 x^4 + 366309\, s^5 x^4 - 54\, s^7 x^2 + 3855993059241\, x^3 s$$
$$+ 1053\, s^5 x^3 + 15541496150580\, y x + 3825792\, s^3 y^5 x + 87264\, s^4 y^4 x^2$$
$$+ 6924960\, s^3 y^4 x^2 + 1553580078\, s^3 y^2 x^2 + 102908891178\, s^2 y x^3$$
$$- 594\, s^6 y x^3 + 2243063232\, s^3 y x^3 - 2823\, s^6 y^2 x - 8212278\, s^4 y^2 x$$
$$+ 193245024024\, y^4 x s + 5241726000\, y^4 x^2 s + 1514133147270\, y^2 x^2 s$$
$$+ 1972998\, s^4 y x^2 + 25533064350\, s^2 y^3 x - 442098\, s^5 y x - 750\, s^6 y^2 x^2$$
$$- 6\, s^7 y^2 x^2 + 408\, s^6 y^2 x^3 + 109656\, s^5 y^2 x^3 + 72\, s^6 y^4 x + 3568752\, s^4 y^3 x^2$$
$$- 2079\, s^6 y x^2 + 117157642245\, s^2 y x^2 - 470102076\, s^3 y x - 2376\, s^6 y x$$
$$+ 26298260280\, s^2 y x + 663862307760\, s\, y^3 x + 2280870105552\, s\, y x^3$$
$$- 198\, s^6 y^3 x - 15120\, s^5 y^3 x + 36673809381\, s^2 y^2 x + 487202688000\, s\, y x^4$$
$$+ 9212984712\, s^2 y^4 x + 2730186\, s^4 y^3 x - 28516212\, s^4 y x + 21735702\, s^4 y x^3$$
$$+ 68554643454\, s^2 y^2 x^2 + 29808\, s^5 y x^3 + 270950400\, s^2 y^4 x^2$$
$$+ 230247360\, s^2 y^5 x + 432\, s^5 y^4 x^2 + 6058281600\, s\, y^5 x + 16416\, s^5 y^3 x^2$$
$$+ 3070054921815\, s\, y x^2 + 3414088023336\, x^2 s - 195210\, s^5 y + 432\, s^5 y^5$$
$$- 194681718\, s^3 y^3 - 6\, s^7 y^2 + 1068775776\, s^2 y^5 - 17005221\, s^4 y - s^7 y^4$$

$$+ 212975424 s^2 y^6 + 36864 s^4 y^6 + 5608648080 s y^6 - 5371866 s^4 y^3$$
$$+ 976651446 s^2 y^4 + 144 s^5 y^6 + 3956832 s^3 y^6 - 2051776 s^4 y^4$$
$$- 43410095 s^3 y^4 - 442882878 s^3 y^2 - 13456455885 s^2 y + 74417206602 s y^2$$
$$- 718361460 s^3 y - 5373594108 s^2 y^2 - 1662 s^6 y^2 - 1576652661 s^2 y^3$$
$$- 13156989 s^4 y^2 + 76562957565 s y^3 + 144288 s^4 y^5 - 30512884194 s y$$
$$- 202446 s^5 y^2 - 290 s^6 y^4 - 35175 s^5 y^4 + 30086432208 s y^5 - 64503 s^5 y^3$$
$$+ 62584308983 y^4 s + 1784396469555 x^4 s + 298204200000 x^5 s$$
$$- 15510231 s^4 x^2 - 11106 s^6 x^2 - 835704 s^5 x^2 + 2996734833 s^3 x^4$$
$$- 9 s^7 x^4 + 216 s^6 x^4 + 1651193118 s^3 x^2 + 181976491107 s^2 x^3$$
$$+ 4757584653 s^2 x + 13305600 s^4 x^5 + 48152898 s^4 x^3 - 48064977 s^4 x$$
$$- 1179136260 s^3 x + 4348482318 s^3 x^3 + 684432000 s^3 x^5$$
$$+ 19633320000 s^2 x^5 + 12117831538440 y^2 x + 30098845732644 y x^2.$$

References

[Ab-Ba] S. S. Abhyankar and C. L. Bajaj, Automatic parametrization of rational curves and surfaces III: Algebraic plane curves, Comput. Aided Geom. Design, **5** (1988), 309–321.

[B-K] E. Brieskorn and H. Knörrer, Ebene Algebraische Kurven, Birkhäuser, 1981, Basel-Boston-Stuttgart.

[D] A. Degtyarev, Alexander polynomial of a curve of degree six, J. Knot Theory Ramifications, Vol. 3, No. 4, 439–454, 1994.

[vH] M. van Hoeij, Rational parametrizations of algebraic curves using a canonical divisor, J. Symbolic Comput., **11** (1996), 1–19.

[Ke-Mo] M. A. Kenku and F. Momose, Torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J., Vol. 109 (1988), 125–149.

[Ko] K. Kodaira, On compact analytic surfaces II, Ann. of Math., **77** (1963), 563–626 and III, Ann. of Math., **78** (1963), 1–40.

[Ku] D. S. Kubert, Universal bounds on the torsion of elliptic curves, Proc. London Math. Soc. (3), **33** (1976), 193–237.

[Ma] B. Mazur, Rational isogenies of prime degree, Invent. Math., **44** (1978), 129–162.

[Mi-P] R. Miranda and U. Persson, On Extremal Rational Elliptic Surfaces, Math. Z., **193** (1986), 537–558.

[N] M. Namba, Geometry of projective algebraic curves, Decker, New York, 1984.

[O1] M. Oka, Flex Curves and their Applications, Geom. Dedicata, Vol. 75 (1999), 67–100.

[O2] M. Oka, Geometry of cuspidal sextics and their dual curves, to appear in Adv. Stud. Pure Math., **29** (2000), Singularities and arrangements, Sapporo-Tokyo, 1998.

[R-S1] K. Rubin and A. Silverberg, Families of Elliptic Curves with Constant mod p Representations, in: Conference on Elliptic Curves and Modular Forms, Hong Kong, December

18–21, 1993, International Press, Cambridge, MA, 1995, 148–161; Second edition: Elliptic Curves, Modular Forms, & Fermat's Last Theorem, 1997.

[R-S2] K. Rubin and A. Silverberg, Mod 6 representations of elliptic curves, pp. 213–220 in: Automorphic Forms, Automorphic Representations, and Arithmetic, Proceedings of Symposia in Pure Mathematics, vol. 66, Part 1, eds. Robert S. Doran, Ze-Li Dou, George T. Gilbert, AMS, 1999.

[S-Z] U. Schneiders and H. G. Zimmer, The rank of elliptic curves upon quadratic extension, Computational number theory, 1989, 239–260.

[Si] J. H. Silverman, The Arithmetic of Elliptic Curves, Grad. Texts in Math., 106, Springer, New-York, 1986.

[W] R. Walker, Algebraic curves, Dover Publ. Inc., New York, 1949.

[Z] H. G. Zimmer, Torsion of elliptic curves over cubic and certain biquadratic number fields, Arithmetic geometry, 203–220, Comtemp. Math., 174, Amer. Math. Soc.

Mutsuo Oka

Department of Mathematics
Tokyo Metropolitan University
Minami-Ohsawa, Hachioji-shi
Tokyo 192-0397
Japan
E-mail: oka@comp.metro-u.ac.jp