TOKYO J. MATH.
VOL. 20, NO. 2, 1997

On Torsion Subgroups of Elliptic Curves with Integral j-Invariant over Imaginary Cyclic Quartic Fields

Toshiharu KISHI

Tokyo Metropolitan University

(Communicated by T. Ishikawa)

1. Introduction.

We are interested in the following problem.

PROBLEM. Determine all possible torsion subgroups $E_{tor}(K)$ of the K-rational points of an elliptic curve E defined over a number field K of a fixed degree $n=[K:\mathbf{Q}]$.

This problem has been studied by many people, such as Mazur, Kenku, Momose, Kamienny, Müller, Ströher, Zimmer, $\cdots$, for K of small degree over $\mathbf{Q}$. In this paper, we prove the following:

THEOREM. *Let K be an imaginary cyclic quartic field and E an elliptic curve over K. Suppose that*

1. *$f_2<4$ or $f_3<4$, where f_p is the residue degree of a prime ideal over p in the extension $K/\mathbf{Q}$; and*
2. *the j-invariant of E is an integer of K.*

Then, $E_{tor}(K)$ is isomorphic to one of the following ten groups:

$$E_{tor}(K)\cong\begin{cases}\mathbf{Z}/m\mathbf{Z} & (1\le m\le 8,\ m\ne 7)\\ \mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/2\mu\mathbf{Z} & (1\le\mu\le 3)\,.\end{cases}$$

All these groups do occur (as this is so already over the real quadratic subfield of K [10]).

Before further describing the contents of this paper, let us recall some history on this problem.

In the case of $n=1$ (i.e. $K=\mathbf{Q}$), this problem was solved by Mazur (see [9]).

THEOREM (Mazur).

$$E_{tor}(\mathbf{Q})\cong\begin{cases}\mathbf{Z}/m\mathbf{Z} & (1\le m\le 12,\ m\ne 11)\\ \mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/2\mu\mathbf{Z} & (1\le\mu\le 4)\,.\end{cases}$$

Received November 29, 1995

In solving the above problem for $n \geq 2$, Müller, Ströher and Zimmer ([10]) note that the order of $E_{tor}(K)$ is bounded by a constant number depending only on the degree n and the prime number p under $\mathfrak{p}$ when E has good or additive reduction modulo a prime ideal $\mathfrak{p}$, and prove the following theorem.

THEOREM (Müller, Ströher, Zimmer). *Let E be an elliptic curve with integral j-invariant over a quadratic field K. Then,*

$$E_{tor}(K) \cong \begin{cases} \mathbf{Z}/m\mathbf{Z} & (1 \leq m \leq 10, m \neq 9) \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mu\mathbf{Z} & (1 \leq \mu \leq 3) \\ \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}\,. \end{cases}$$

(Today the result without the assumption that j-invariant is integral is given by Kamienny, Kenku, Momose ([5], [6], [7]).)

Further, because of the integrality of j-invariant, they succeeded in listing all elliptic curves and ground fields where the torsion groups are isomorphic to one of the above groups except $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$, and $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

In the same way (i.e., with the assumption that j is integral), part of the cases of $n=3, 4$ have been computed (precisely, the case where the ground field is cubic is treated in [1] and the composite of two complex quadratic fields is in [3]).

Our method closely follows that of [10]. In the first place, we appeal to the reduction theory (§2) to obtain a first list (Theorem 1) of possible torsion subgroups of $E(K)$ under the assumption on K as in the above Theorem. To remove the possibility of certain cyclic subgroups of $E(K)$ of relatively large order (such as 13, 15, 16), we have to carry out long and tedious computations about the equations, called $E(b, c)$, of some explicitly parametrized elliptic curves with a specified K-rational point (§3). In particular, when the j-invariant is integral, we obtain some restrictive conditions on the coefficients of $E(b, c)$. These conditions give rise to "norm equations". Finally in Section 4, we solve these equations making use of the assumption of K as in the above Theorem to list possible equations $E(b, c)$ in different cases. As a result, we can exclude some of the groups listed in Section 1, thereby obtaining our Theorem.

2. Reduction theory.

Let K be a number field, $\mathfrak{p}$ a prime ideal of K, p the prime number under $\mathfrak{p}$, and let E be an elliptic curve defined over K.

Now we denote by $k_{\mathfrak{p}}$ the residue field of K with respect to $\mathfrak{p}$, $e_{\mathfrak{p}}$ (resp. $f_{\mathfrak{p}}$) the ramification index (resp. residue degree) of $\mathfrak{p}$ in the extension $K/\mathbf{Q}$ and $\tilde{E}(k_{\mathfrak{p}})$ the set of all $k_{\mathfrak{p}}$-rational points on the reduction $\tilde{E}$ of E modulo $\mathfrak{p}$.

Müller, Ströher and Zimmer show the following fact (see [10], Theorem 1).

FACT 1. *The order of the torsion subgroup $E_{tor}(K)$ satisfies the following divisibility relations.*

1. *If E has good reduction modulo $\mathfrak{p}$, then*

$$|E_{tor}(K)|\,\big|\,|\tilde{E}(k_{\mathfrak{p}})|\cdot p^{2t_{\mathfrak{p}}}, \quad \text{and } |\tilde{E}(k_{\mathfrak{p}})|\leq 1+p^{f_{\mathfrak{p}}}+2\sqrt{p^{f_{\mathfrak{p}}}}\,.$$

2. *If E has additive reduction modulo $\mathfrak{p}$, then*

$$|E_{tor}(K)|\,\big|\,12\cdot p^{2(t_{\mathfrak{p}}+1)}$$

where
$$t_{\mathfrak{p}}=\begin{cases}0 & (\textit{if } p-1>e_{\mathfrak{p}})\\ \max\{r\in\mathbf{N}\,;\,(p-1)p^{r-1}\leq e_{\mathfrak{p}}\} & (\textit{otherwise})\,.\end{cases}$$

Applying this to an elliptic curve over a quartic field, we obtain the following proposition.

PROPOSITION 1. *Let K be an imaginary cyclic quartic field, $v_{\mathfrak{p}}$ the normalized additive valuation of rank 1 associated with $\mathfrak{p}$ and E an elliptic curve over K. Suppose that*
1. *$f_2<4$ or $f_3<4$,*
2. *for each $i\in\{2,3\}$, there exists a prime ideal $\mathfrak{p}$ dividing i of K such that $v_{\mathfrak{p}}(j)\geq 0$.*

Then,

$$|E_{tor}(K)|\,\big|\,2^4\cdot 5,\ 6\cdot 5,\ 2^3\cdot 7,\ 3\cdot 7,\ 11,\ 13\,,\quad \textit{or}\ \ 2^6\cdot 3^2\,.$$

(Remark: the condition $v_{\mathfrak{p}}(j)\geq 0$ implies that E does not have multiplicative reduction modulo $\mathfrak{p}$.)

PROOF. Let, for each $i\in\{2,3\}$, $\mathfrak{p}_i$ be the prime ideal of K satisfying the above assumption 2. Note that $t_{\mathfrak{p}_2}\leq 3$ and $t_{\mathfrak{p}_3}\leq 1$.

o If $f_2<4$, then

$$\text{I.}\qquad |E_{tor}(K)|\,\Bigg|\begin{cases}|\tilde{E}(k_{\mathfrak{p}_2})|\cdot 2^6\leq 9\cdot 2^6 & \text{if } E \text{ has good red. mod } \mathfrak{p}_2\\ |\tilde{E}(k_{\mathfrak{p}_3})|\cdot 3^2\leq 100\cdot 3^2 & \text{if } E \text{ has good red. mod } \mathfrak{p}_3\,.\end{cases}$$

$$\text{II.}\qquad |E_{tor}(K)|\,\Bigg|\begin{cases}2^{10}\cdot 3 & \text{if } E \text{ has add. red. mod } \mathfrak{p}_2\\ 2^2\cdot 3^5 & \text{if } E \text{ has add. red. mod } \mathfrak{p}_3\,.\end{cases}$$

Let $E_{tor}^{(p)}(K)$ be the p-primary part of $E_{tor}(K)$ for a prime number p. Reduction mod $\mathfrak{p}_3$ shows that the order of $E_{tor}^{(2)}(K)$ satisfies $|E_{tor}^{(2)}(K)|\,|\,2^6$. Actually, according to [12], Prop. 3.1 (p. 176),

$$|E_{tor}^{(2)}(K)|\,\Bigg|\begin{cases}2^2 & \text{if } E \text{ has add. red. mod } \mathfrak{p}_3\\ |\tilde{E}(k_{\mathfrak{p}_3})|\leq 100 & \text{if } E \text{ has add. red. mod } \mathfrak{p}_3\,.\end{cases}$$

Thus, when $E_{tor}(K)$ does not contain any element of prime order $p\geq 5$,

$$|E_{tor}(K)|\,|\,2^6\cdot 3^2\,. \tag{i}$$

On the other hand, when $E_{tor}(K)$ contains an element P which has order $p\geq 5$, E has good red. mod $\mathfrak{p}_2$. Then, $|E_{tor}^{(p)}(K)|\leq 9$, so $p=5$ or 7. Further, for E also has good red.

mod $\mathfrak{p}_3$,

$$|E_{tor}^{(2)}(K)| \leq 100/p \quad \text{and} \quad |E_{tor}^{(3)}(K)| \leq 9/p\,.$$

Thus,

$$|E_{tor}(K)| \mid 2^4 \cdot 5 \quad \text{or} \quad 2^3 \cdot 7\,. \tag{ii}$$

o If $f_3 < 4$, then

I. $$|E_{tor}(K)| \left| \begin{cases} |\tilde{E}(k_{\mathfrak{p}_2})| \cdot 2^6 \leq 25 \cdot 2^6 & \text{if } E \text{ has good red. mod } \mathfrak{p}_2 \\ |\tilde{E}(k_{\mathfrak{p}_3})| \cdot 3^2 \leq 16 \cdot 3^2 & \text{if } E \text{ has good red. mod } \mathfrak{p}_3\,. \end{cases} \right.$$

II. $$|E_{tor}(K)| \left| \begin{cases} 2^{10} \cdot 3 & \text{if } E \text{ has add. red. mod } \mathfrak{p}_2 \\ 2^2 \cdot 3^5 & \text{if } E \text{ has add. red. mod } \mathfrak{p}_3\,. \end{cases} \right.$$

In the same way as in the case of $f_2 < 4$, reduction mod $\mathfrak{p}_3$ and $\mathfrak{p}_2$ shows

$$|E_{tor}^{(2)}(K)| \mid 2^4 \quad \text{and} \quad |E_{tor}^{(3)}(K)| \mid 3^2\,.$$

Thus, when $E_{tor}(K)$ does not contain any element of prime order $p \geq 5$,

$$|E_{tor}(K)| \mid 2^4 \cdot 3^2\,. \tag{iii}$$

On the other hand, when $E_{tor}(K)$ contains and element P which has prime order $p \geq 5$, $|E_{tor}^{(p)}(K)| \leq 16$. So $p = 5$, 7, 11 or 13. Furthermore,

$$|E_{tor}^{(2)}(K)| \leq 16/p\,, \qquad |E_{tor}^{(3)}(K)| \leq 25/p\,.$$

Thus,

$$|E_{tor}(K)| \mid 6 \cdot 5, 2 \cdot 7, 3 \cdot 7, 11 \quad \text{or} \quad 13\,. \tag{iv}$$

The proposition follows from the relations (i)–(iv).

In general, if $E_{tor}(K)$ has a subgroup which is isomorphic to $\mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z}$ (for an integer m), then K contains a primitive m-th root of unity. So, if K is an imaginary cyclic quartic field which is unequal to $\mathbf{Q}(\zeta_5)$ where ζ_5 is a primitive *fifth* root of unity, then

$$E_{tor}(K) \not\supseteq \mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} \qquad (\text{for } \forall m \geq 3)\,.$$

(Note that imaginary cyclic quartic fields do not contain any imaginary quadratic fields.) Therefore, the next theorem follows.

THEOREM 1. *Let K be an imaginary cyclic quartic field and E an elliptic curve over K. Suppose that*
1. *$f_2 < 4$ or $f_3 < 4$,*
2. *for each $i \in \{2, 3\}$, there exists a prime ideal $\mathfrak{p}$ dividing i of K such that $v_{\mathfrak{p}}(j) \geq 0$.*
Then, $E_{tor}(K)$ is isomorphic to a subgroup of one of the following groups.

$$\mathbf{Z}/64\mathbf{Z} \oplus \mathbf{Z}/9\mathbf{Z} \quad \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/32\mathbf{Z} \oplus \mathbf{Z}/9\mathbf{Z}$$
$$\mathbf{Z}/16\mathbf{Z} \oplus \mathbf{Z}/5\mathbf{Z} \quad \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/5\mathbf{Z} \quad \mathbf{Z}/6\mathbf{Z} \oplus \mathbf{Z}/5\mathbf{Z}$$
$$\mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/7\mathbf{Z} \quad \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/7\mathbf{Z} \quad \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/7\mathbf{Z}$$
$$\mathbf{Z}/11\mathbf{Z} \quad \mathbf{Z}/13\mathbf{Z}$$

We will study the groups which do not occur from the torsion subgroups of elliptic curves over quadratic fields in §4. For this purpose we quote the following result from [10] (Theorem 4 and tables).

FACT 2. *Let k be a real quadratic field and E an elliptic curve with integral j-invariant over k. Then, $E_{tor}(k)$ is isomorphic to one of the following groups. And all these groups occur.*

$$E_{tor}(k) \cong \begin{cases} \mathbf{Z}/m\mathbf{Z} & (1 \le m \le 8,\ m \ne 7) \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mu\mathbf{Z} & (1 \le \mu \le 3)\,. \end{cases}$$

3. Parametrization.

In this section, we study an elliptic curve E over a number field K whose torsion subgroup $E_{tor}(K)$ contains an element P of order $N \ge 4$.

Such an elliptic curve is isomorphic (over K) to the following curve, which is called *Tate's normal form* or *Kubert's $E(b, c)$-form* (cf. [4], Chapter 4, [8], and [10]).

$$E(b, c) : Y^2 + (1-c)XY - bY = X^3 - bX^2 \qquad (b \in K^\times, c \in K)\,,$$
$$P = (0, 0)\,.$$

Here,

$$j = \frac{(((1-c)^2 - 4b)^2 + 24b(1-c))^3}{b^3(((1-c)^2 - 4b)^2 + 8(1-c)^3 - 27b - 9(1-c)((1-c)^2 - 4b))}\,.$$

THEOREM 2. *Let $\mathfrak{p}$ be a prime ideal of K, O_K the ring of integers of K, U_K the group of units of K and $v_\mathfrak{p}$ the normalized additive valuation of rank 1 associated with $\mathfrak{p}$.*

Case 1. *If $N = 8$, then there exists $d \in K$ such that*

$$b = (2d-1)(d-1)\,, \qquad c = (2d-1)(d-1)d^{-1}\,.$$

Further, if $j \in O_K$, then the following four conditions are satisfied:

(1) $0 \le v_\mathfrak{p}(\varepsilon) \le \frac{5}{2} v_\mathfrak{p}(2) \qquad (\forall \mathfrak{p})$,

(2) $0 \le v_\mathfrak{p}(2-\varepsilon) \le 2v_\mathfrak{p}(2) \qquad (\forall \mathfrak{p})$,

(3) $1 - \varepsilon \in U_K$,

(4) $0 \le v_\mathfrak{p}(\varepsilon^2 - 8\varepsilon + 8) \le 5v_\mathfrak{p}(2) \qquad (\forall \mathfrak{p})$,

where $\varepsilon=d^{-1}$.

Case 2. *If* $N=16$, *then there exist* w *and* $x\in K$ *such that*

$$b=\frac{2FGJ}{(-1+x)H^2I^3}, \qquad c=\frac{-2FG}{(-1+x)HI^2}$$

where

$$\begin{aligned} F&=-1-x+x^2+x^3+w\,,\\ G&=-2+x-x^2+x^3+x^4+xw\,,\\ H&=1-3x+x^2+x^3+w\,,\\ I&=1-x+x^2+x^3+w\,,\\ J&=-4+4x-2x^2+4x^3+4x^4-4x^5-2x^6+(4x-2x^2-2x^3)w\,. \end{aligned}$$

Moreover, w *and* x *satisfy*

$$X_1(16): w^2=1-2x-x^2-x^4+2x^5+x^6\,.$$

Further, if $j\in O_K$, *then the following two conditions are satisfied*:

$$\begin{array}{ll} (1) & x\in U_K, \\ (2) & 0\le v_{\mathfrak{p}}(x+1)\le v_{\mathfrak{p}}(2) \qquad (\forall\mathfrak{p}). \end{array}$$

Case 3. *If* $N=9$, *then there exists* $f\in K$ *such that*

$$b=f(d-1)d\,,\quad c=f(d-1)\qquad \text{where}\quad d=f^2-f+1\,.$$

Further, if $j\in O_K$, *then the following two conditions are satisfied*:

$$\begin{array}{ll} (1) & f\in U_K, \\ (2) & f-1\in U_K. \end{array}$$

Case 4. *If* $N=6$ *then*

$$b=c(1+c)\,.$$

Further, if $j\in O_K$, *then the following three conditions are satisfied*:

$$\begin{array}{ll} (1) & 0\le v_{\mathfrak{p}}(\varepsilon)\le 2v_{\mathfrak{p}}(3) \qquad (\forall\mathfrak{p}), \\ (2) & 0\le v_{\mathfrak{p}}(1+\varepsilon)\le 3v_{\mathfrak{p}}(2) \qquad (\forall\mathfrak{p}), \\ (3) & (a)\ \ v_{\mathfrak{p}}(9+\varepsilon)=0 \qquad (\forall\mathfrak{p}\nmid 6), \\ & (b)\ \ v_{\mathfrak{p}}(9+\varepsilon)=v_{\mathfrak{p}}(1+\varepsilon) \qquad (\forall\mathfrak{p}\mid 2), \\ & (c)\ \ v_{\mathfrak{p}}(9+\varepsilon)=v_{\mathfrak{p}}(\varepsilon) \qquad (\forall\mathfrak{p}\mid 3), \end{array}$$

where $\varepsilon=c^{-1}$.

Case 5. *If* $N=12$ *then there exists* $\varepsilon\in K$ *such that*

$$b=\frac{(-2+\varepsilon)(-1+3\varepsilon-\varepsilon^2)}{(-1+\varepsilon)^4}, \qquad c=\frac{-1+3\varepsilon-\varepsilon^2}{(-1+\varepsilon)^3}\,.$$

Further, if $j \in O_K$, then the following three conditions are satisfied:

$$\begin{array}{lll} (1) & 0 \leq v_{\mathfrak{p}}(\varepsilon) \leq v_{\mathfrak{p}}(2) + \frac{1}{2} v_{\mathfrak{p}}(3) & (\forall \mathfrak{p}), \\ (2) & -1+\varepsilon \in U_K, & \\ (3) & (a)\ \ v_{\mathfrak{p}}(-\varepsilon+2)=0 & (\forall \mathfrak{p} \nmid 2), \\ & (b)\ \ v_{\mathfrak{p}}(-\varepsilon+2)=v_{\mathfrak{p}}(\varepsilon) & (\forall \mathfrak{p} \mid 2). \end{array}$$

Case 6. *If $N=5$ then*

$$b=c\,.$$

Further, if $j \in O_K$, then the following two conditions are satisfied:

$$\begin{array}{lll} (1) & b \in U_K, & \\ (2) & 0 \leq v_{\mathfrak{p}}(b^2-11b-1) \leq 3v_{\mathfrak{p}}(5) & (\forall \mathfrak{p}). \end{array}$$

Case 7. *If $N=10$ then there exists $\varepsilon \in K$ such that*

$$b=\frac{(\varepsilon-1)(\varepsilon-2)}{\varepsilon(-1+3\varepsilon-\varepsilon^2)^2}\,, \qquad c=\frac{(\varepsilon-1)(\varepsilon-2)}{\varepsilon(-1+3\varepsilon-\varepsilon^2)}\,.$$

Further, if $j \in O_K$, then the following three conditions are satisfied:

$$\begin{array}{lll} (1) & 0 \leq v_{\mathfrak{p}}(\varepsilon) \leq v_{\mathfrak{p}}(2) & (\forall \mathfrak{p}), \\ (2) & 0 \leq v_{\mathfrak{p}}(\varepsilon-2) \leq v_{\mathfrak{p}}(2) & (\forall \mathfrak{p}), \\ (3) & \varepsilon-1 \in U_K. & \end{array}$$

Case 8. *If $N=15$ then there exist $w, x \in K$ such that*

$$b=\frac{4xFGJ}{HI^2}\,, \qquad c=\frac{4xFG}{HI}\,,$$

where

$$\begin{aligned} F &= -4+x+w\,, \\ G &= -8-2x-x^2+2w\,, \\ H &= -8-6x-x^2+2w\,, \\ I &= 64+48x+12x^2+x^3+(-16-8x-x^2)w\,, \\ J &= 64+32x+16x^2+x^3+(-16-4x-x^2)w\,. \end{aligned}$$

Moreover, x and w satisfy

$$X_1(15):\ w^2=16+8x+5x^2+x^3\,.$$

Further, if $j \in O_K$, then the following two conditions are satisfied:

$$\begin{array}{ll} (1) & v_{\mathfrak{p}}(x)=0 \ \text{ or } \ 2v_{\mathfrak{p}}(2), \\ (2) & v_{\mathfrak{p}}(x+4)=0 \ \text{ or } \ 2v_{\mathfrak{p}}(2) \ \text{ or } \ 4v_{\mathfrak{p}}(2). \end{array}$$

Case 9. *If $N=7$, then there exists $d\in K$ such that*

$$b=d^2(d-1)\,,\qquad c=d(d-1)\,.$$

Further, if $j\in O_K$, then the following two conditions are satisfied:

$$\begin{aligned}&(1)\qquad d\in U_K,\\&(2)\qquad d-1\in U_K.\end{aligned}$$

Case 10. *If $N=11$ then there exist $w, x\in K$ such that*

$$b=\frac{(w-4+2x)(w-4)(w+4)}{128x}\,,\qquad c=\frac{(w-4+2x)(w-4)}{16x}\,.$$

Moreover, w and x satisfy

$$X_1(11): w^2=16-4x^2+x^3\,.$$

Further, if $j\in O_K$, then the following five conditions are satisfied:

$$\begin{aligned}&(1)\qquad 0\le v_{\mathfrak{p}}(x)\le 2v_{\mathfrak{p}}(2)\qquad (\forall\mathfrak{p}),\\&(2)\qquad 0\le v_{\mathfrak{p}}(x-4)\le 2v_{\mathfrak{p}}(2)\qquad (\forall\mathfrak{p}),\\&(3)\qquad v_{\mathfrak{p}}(w-4)=\tfrac{3}{2}v_{\mathfrak{p}}(x)\qquad (\forall\mathfrak{p}),\\&(4)\qquad v_{\mathfrak{p}}(w+4)=\tfrac{3}{2}v_{\mathfrak{p}}(x)\qquad (\forall\mathfrak{p}),\\&(5)\qquad v_{\mathfrak{p}}(w-4+2x)=\tfrac{3}{2}v_{\mathfrak{p}}(x)\qquad (\forall\mathfrak{p}).\end{aligned}$$

Case 11. *If $N=13$ then there exist $w, u\in K$ such that*

$$b=\frac{2(-1+u)u^2FI}{G^2H}\,,\qquad c=\frac{2(-1+u)u^2F}{GH}\,,$$

where

$$\begin{aligned}F&=1-2u+u^2+u^3+w\,,\\G&=1+u^2-u^3+w\,,\\H&=1-2u+3u^2-u^3+w\,,\\I&=1-u^2+u^3+w\,.\end{aligned}$$

Moreover, w and u satisfy

$$X_1(13): w^2=1-4u+6u^2-2u^3+u^4-2u^5+u^6\,.$$

Further, if $j\in O_K$, then the following two conditions are satisfied:

$$\begin{aligned}&(1)\qquad u\in U_K,\\&(2)\qquad u-1\in U_K.\end{aligned}$$

REMARK. In this theorem the Cases 1, 3–7 and 9–10 are quoted from [10], so we have only to prove Cases 2, 8 and 11. The equations of Cases 2, 8 and 11 are in fact equations of the universal family on the modular curves $X_1(16)$, $X_1(15)$ and $X_1(13)$, respectively, and are transformations of the equations given in Reichert [11].

PROOF. First, we show how to derive our equations from [11].

For an integer m, let x_{mP} be a X-coodinate of mP.

Case 2. Reichert [11] obtained

$$X_1(16) : (u^2+3u+2)V^2+(u^3+4u^2+4u)V-u=0$$

from the equation $x_{7P}=x_{-9P}$ by the birational transformations

$$(*)\qquad \begin{cases} b=cr\,, \quad c=s(r-1)\,, \\ m(1-s)=s(1-r)\,, \quad r-s=t(1-s)\,, \end{cases}$$

and

$$m=\frac{V^2+(u+1)V}{V^2+(u-1)V-u}\,, \qquad t=\frac{-1}{V-1}\,.$$

Further, by the transformations

$$V=\frac{2u}{w+u(u+2)^2}\,, \qquad u=x-1\,,$$

we arrive at

$$w^2=1-2x-x^2-x^4+2x^5+x^6\,.$$

Case 8. In the same way, Reichert's form is obtained from $x_{7P}=x_{-8P}$ by the birational transformations $(*)$ and

$$m=\frac{-V^2+(u^2-u)V+u^3}{-V^2+(u^2+u)V+u^3+u^2}\,, \qquad t=\frac{uV}{-V^2+(u^2+u)V+u^3+u^2}\,.$$

Further by the transformations

$$u=\frac{1}{4}x\,, \qquad V=\frac{1}{8}(w+x-4)\,,$$

we arrive at

$$w^2=16+8x+5x^2+x^3\,.$$

Case 11. The equation

$$X_1(13) : w^2=1-4u+6u^2-2u^3+u^4-2u^5+u^6$$

is obtained by the birational transformations $(*)$ and

$$m=\frac{V+u^3-u}{V}\,, \quad t=\frac{-u^2+u}{V}\,, \quad V=\frac{w}{2}-\frac{u^3-u^2-1}{2}\,.$$

Secondly, we prove the estimations of coefficient of $E(b, c)$. But it is really long and tedious, so we describe only Case 2: the rest can be proved by similar arguments.

Note that the following two lemmas are valid.

LEMMA 1. *$v_{\mathfrak{p}}(b)>0$ and $v_{\mathfrak{p}}(c)>0 \Rightarrow v_{\mathfrak{p}}(j)<0$.*

This follows easily from the formula for j given at the beginning of §3.

LEMMA 2. *$2v_{\mathfrak{p}}(c)<v_{\mathfrak{p}}(b)\leq 0 \Rightarrow v_{\mathfrak{p}}(j)<0$.*

PROOF.

$$\begin{aligned} 2v_{\mathfrak{p}}(c)<v_{\mathfrak{p}}(b)\leq 0 \Rightarrow v_{\mathfrak{p}}(j) &= 12v_{\mathfrak{p}}(c)-(3v_{\mathfrak{p}}(b)+4v_{\mathfrak{p}}(c)) \\ &= 8v_{\mathfrak{p}}(c)-3v_{\mathfrak{p}}(b) \\ &< 2v_{\mathfrak{p}}(c)<0 . \end{aligned}$$ □

Case 2. Put $F'=F(x, -w)$, $G'=G(x, -w)$, $H'=H(x, -w)$, $I'=I(x, -w)$, $J'=J(x, -w)$ for $F=F(x, w)$, $G=G(x, w)$, $H=H(x, w)$, $I=I(x, w)$, $J=J(x, w)$. Then

$$FF'=4(1-x)x(1+x)\,, \qquad GG'=4(1-x)(1+x^2)\,,$$
$$HH'=4(-1+x)x(1-2x-x^2)\,, \quad II'=4x^2\,, \quad JJ'=16(-1+x)^2\,.$$

(1) Now we prove that $j\in O_K \Rightarrow x\in U_K$. It is equivalent to the condition that $j\in O_K \Rightarrow v_{\mathfrak{p}}(x)=0$ $(\forall \mathfrak{p})$.

Suppose that $v_{\mathfrak{p}}(x)>0$ for some $\mathfrak{p}$. Then $v_{\mathfrak{p}}(w)=0$. Moreover, we know $v_{\mathfrak{p}}(F)+v_{\mathfrak{p}}(F')=v_{\mathfrak{p}}(FF')=2v_{\mathfrak{p}}(2)+v_{\mathfrak{p}}(x)$ and $v_{\mathfrak{p}}(F-F')=v_{\mathfrak{p}}(2)$. Thus $(v_{\mathfrak{p}}(F)+v_{\mathfrak{p}}(F'))/2>v_{\mathfrak{p}}(F-F')$, and so $v_{\mathfrak{p}}(F)\neq v_{\mathfrak{p}}(F')$. So we have the following two cases:

① $$v_{\mathfrak{p}}(F)=\begin{cases} v_{\mathfrak{p}}(2)+v_{\mathfrak{p}}(x) & (\text{if } v_{\mathfrak{p}}(F)>v_{\mathfrak{p}}(F')) \quad \cdots(\alpha) \\ v_{\mathfrak{p}}(2) & (\text{if } v_{\mathfrak{p}}(F)<v_{\mathfrak{p}}(F'))\,. \quad \cdots(\beta) \end{cases}$$

In the same way, comparing $v_{\mathfrak{p}}(G)$, $v_{\mathfrak{p}}(H)$, $\cdots$ with $v_{\mathfrak{p}}(G')$, $v_{\mathfrak{p}}(H')$, $\cdots$, respectively, we have the following:

② $$v_{\mathfrak{p}}(G)=v_{\mathfrak{p}}(G')=v_{\mathfrak{p}}(2)\,.$$

③ $$v_{\mathfrak{p}}(H)=\begin{cases} v_{\mathfrak{p}}(2)+v_{\mathfrak{p}}(x) & (\text{if } v_{\mathfrak{p}}(H)>v_{\mathfrak{p}}(H')) \quad \cdots(\alpha) \\ v_{\mathfrak{p}}(2) & (\text{if } v_{\mathfrak{p}}(H)<v_{\mathfrak{p}}(H'))\,. \quad \cdots(\beta) \end{cases}$$

④ $$v_{\mathfrak{p}}(I)=\begin{cases} v_{\mathfrak{p}}(2)+2v_{\mathfrak{p}}(x) & (\text{if } v_{\mathfrak{p}}(I)>v_{\mathfrak{p}}(I')) \quad \cdots(\alpha) \\ v_{\mathfrak{p}}(2) & (\text{if } v_{\mathfrak{p}}(I)<v_{\mathfrak{p}}(I'))\,. \quad \cdots(\beta) \end{cases}$$

⑤ $$v_{\mathfrak{p}}(J)=v_{\mathfrak{p}}(J')=2v_{\mathfrak{p}}(2)\,.$$

On the other hand we have $v_{\mathfrak{p}}(F-H)=v_{\mathfrak{p}}(F'-H')=v_{\mathfrak{p}}(2)$. This implies that ①-$\alpha$ (i.e. $v_{\mathfrak{p}}(F)=v_{\mathfrak{p}}(2)+v_{\mathfrak{p}}(x)$) and ③-$\alpha$ (i.e. $v_{\mathfrak{p}}(H)=v_{\mathfrak{p}}(2)+v_{\mathfrak{p}}(x)$) do not occur at the same time. Furthermore if $v_{\mathfrak{p}}(F)=v_{\mathfrak{p}}(2)$ and $v_{\mathfrak{p}}(H)=v_{\mathfrak{p}}(2)$, then we have $v_{\mathfrak{p}}(F')=v_{\mathfrak{p}}(2)+v_{\mathfrak{p}}(x)$ and $v_{\mathfrak{p}}(H')=v_{\mathfrak{p}}(2)+v_{\mathfrak{p}}(x)$, which is impossible. So ①-β and ③-β do not occur at the same time either. In the same way, the condition $v_p(F-I)=v_p(F'-I')=v_p(2)$ implies that ①-α⇒④-β and ①-β⇒④-α.

Therefore, the following two cases are possible.

case A. ①-α and ③-④-β. Then, $v_p(b)=v_p(x)>0$, $v_p(c)=v_p(x)>0$. So, according to Lemma 1, $v_p(j)<0$.

case B. ①-β and ③-④-α. Then, $v_p(b)=-8v_p(x)$, $v_p(c)=-5v_p(x)$. So, according to Lemma 2, $v_p(j)<0$.

Next, suppose that $v_p(x)<0$ for some $\mathfrak{p}$. Then we have the followings.

① $$v_p(F)=\begin{cases} v_p(2) & (\text{if } v_p(F)>v_p(F')) & \cdots(\alpha) \\ v_p(2)+3v_p(x) & (\text{if } v_p(F)<v_p(F'))\,. & \cdots(\beta) \end{cases}$$

② $$v_p(G)=\begin{cases} v_p(2)-v_p(x) & (\text{if } v_p(G)>v_p(G')) & \cdots(\alpha) \\ v_p(2)+4v_p(x) & (\text{if } v_p(G)<v_p(G'))\,. & \cdots(\beta) \end{cases}$$

③ $$v_p(H)=\begin{cases} v_p(2)+v_p(x) & (\text{if } v_p(H)>v_p(H')) & \cdots(\alpha) \\ v_p(2)+3v_p(x) & (\text{if } v_p(H)<v_p(H'))\,. & \cdots(\beta) \end{cases}$$

④ $$v_p(I)=\begin{cases} v_p(2)-v_p(x) & (\text{if } v_p(I)>v_p(I')) & \cdots(\alpha) \\ v_p(2)+3v_p(x) & (\text{if } v_p(I)<v_p(I'))\,. & \cdots(\beta) \end{cases}$$

⑤ $$v_p(J)=\begin{cases} 2v_p(2)-v_p(x) & (\text{if } v_p(J)>v_p(J')) & \cdots(\alpha) \\ 2v_p(2)+3v_p(x) & (\text{if } v_p(J)<v_p(J'))\,. & \cdots(\beta) \end{cases}$$

On the other hand we have the following conditions:

$$\begin{aligned} &v_p(x\cdot F-G)=v_p(x\cdot F'-G')=v_p(2)+v_p(x)\,,\\ &v_p(F-H)=v_p(F'-H')=v_p(2)+v_p(x)\,,\\ &v_p(F-I)=v_p(F'-I')=v_p(2)\,,\\ &HI+J=2F \quad \text{and} \quad H'I'+J'=2F'\,. \end{aligned}$$

Therefore, the following only two cases are possible.

case A. ①-②-③-④-⑤-α. Then, $v_p(b)=-2v_p(x)>0$, $v_p(c)=-v_p(x)>0$. So, $v_p(j)<0$.

case B. ①-②-③-④-⑤-β. Then, $v_p(b)=-6v_p(x)$, $v_p(c)=-9v_p(x)$. So, $v_p(j)<0$.

(2) To show that $j\in O_K \Rightarrow 0\le v_p(x+1)\le v_p(2)$ ($\forall\mathfrak{p}$), we put $y=x+1$. Then,

$$X_1(16): w^2=8y-12y^2+4y^3+4y^4-4y^5+y^6\,,$$

$$F=-2y^2+y^3+w\,, \qquad FF'=4(1-y)(-2+y)y\,,$$

$$G=-4+2y+2y^2-3y^3+y^4+(-1+y)w\,, \qquad GG'=4(2-y)(2-2y+y^2)\,,$$

$$H=4-2y-2y^2+y^3+w\,, \qquad HH'=4(-2+y)(-1+y)(2-y^2)\,,$$

$$I=2-2y^2+y^3+w\,,\qquad II'=4(-1+y)^2\,,$$
$$J=-8-4y+20y^2-12y^3-6y^4+8y^5-2y^6+2(1-y)(-2+y)(1+y)w\,,$$
$$JJ'=16(-2+y)^2\,.$$

Applying the above argument for these equations and polynomials, one can show $v_p(j)<0$ when $v_p(y)<0$ or $v_p(y)>v_p(2)$.

In this way, we can complete the proof. Q.E.D.

4. Solving norm equations.

In this section, let K be an imaginary cyclic quartic field which is unequal to the field $\mathbf{Q}(\zeta_5)$, where ζ_5 is a primitive 5th root of unity, and $k=\mathbf{Q}(\sqrt{D})$ the real quadratic field which is contained in K, where D is a square-free integer. (In the case $K=\mathbf{Q}(\zeta_5)$, the residue degrees f_2 and f_3 are equal to 4.)

We will apply Theorem 2 to elliptic curves E with integral j-invariant over K. At this time, the next fact is essential (see [2], Satz 15, p 320).

FACT 3. *Let K be an imaginary cyclic quartic field, k the real quadratic field which is contained in K and U_K (resp. U_k) the group of units of K (resp. k). Then*

$$[U_K : W_K U_k]=1\,,$$

where W_K is the group of all roots of unity contained in K.
Especially, if $K\neq\mathbf{Q}(\zeta_5)$, then $U_K=U_k$.

PROPOSITION 2. *Let K be an imaginary cyclic quartic field which is unequal to the field $\mathbf{Q}(\zeta_5)$, and E an elliptic curve with integral j-invariant over K. Then, $E_{tor}(K)$ does not have subgroups which are isomorphic to one of the following groups.*

1. $\mathbf{Z}/9\mathbf{Z}$, $\mathbf{Z}/12\mathbf{Z}$, $\mathbf{Z}/10\mathbf{Z}$, $\mathbf{Z}/7\mathbf{Z}$,
2. $\mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/8\mathbf{Z}$,
3. $\mathbf{Z}/16\mathbf{Z}$,
4. $\mathbf{Z}/15\mathbf{Z}$,
5. $\mathbf{Z}/11\mathbf{Z}$,
6. $\mathbf{Z}/13\mathbf{Z}$.

PROOF. *Cases* 1, 5 *and* 6. Suppose $E_{tor}(K)\geq\mathbf{Z}/m\mathbf{Z}$ ($m\in\{9, 12, 10, 7, 11, 13\}$). According to Theorem 2 and Fact 3, one can easily show that E has already defined over the real quadratic subfield k of K and $j\in O_k$, which contradicts Fact 2.

Case 2. Suppose $E_{tor}(K)\geq\mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/8\mathbf{Z}$. In particular, $E_{tor}(K)\geq\mathbf{Z}/8\mathbf{Z}$, and so according to Case 1 of Theorem 2, there exists ε ($\in K$) which satisfies the following three conditions:

$$\begin{array}{lll} (1) & N_{K/\mathbf{Q}}(\varepsilon)=\pm 2^n & 0\le n\le 10\,, \\ (2) & N_{K/\mathbf{Q}}(2-\varepsilon)=\pm 2^m & 0\le m\le 8\,, \\ (3) & 1-\varepsilon\in U_K=U_k\,. & \end{array}$$

From (3), we know the conditions (1) and (2) are equivalent to the following respectively.

$$\begin{array}{lll} (1)' & N_{k/\mathbf{Q}}(\varepsilon)=\pm 2^{n'} & 0\le n'\le 5\,, \\ (2)' & N_{k/\mathbf{Q}}(2-\varepsilon)=\pm 2^{m'} & 0\le m'\le 4\,. \end{array}$$

Müller, Ströher, Zimmer [10] solved these norm equations and got the following eight solutions.

$$\varepsilon=3\pm\sqrt{5}\,,\quad -1\pm\sqrt{5}\,,\quad 5\pm\sqrt{17}\,,\quad -3\pm\sqrt{17}\,.$$

By direct computations, we know the elliptic curves which are yielded by these solutions have only one K-rational point of order 2. This is a contradiction to our hypothesis.

Case 3. Suppose $E_{tor}(K)\geq\mathbf{Z}/16\mathbf{Z}$. According to Case 2 of Theorem 2, there exists an element x which satisfies the following two conditions:

$$\begin{array}{lll} (1) & x\in U_K=U_k\,, & \\ (2) & N_{K/\mathbf{Q}}(x+1)=\pm 2^n & 0\le n\le 4\,. \end{array}$$

By the condition (1), we can put x in the form

$$x=\alpha+\beta\sqrt{D}\,,\quad \alpha^2+D\beta^2=\pm 1 \qquad (\alpha,\beta\in\mathbf{Q})\,.$$

Further we remark that since $E_{tor}(K)\geq\mathbf{Z}/8\mathbf{Z}$, $D=5$ or 17 (see Proof of Case 2). Then we get the following as the solutions of the norm equations (2):

$$x=1\,,\quad \pm\frac{1}{2}\pm\frac{1}{2}\sqrt{5}\,,\quad -\frac{3}{2}\pm\frac{1}{2}\sqrt{5}\,,\quad \pm2\pm\sqrt{5}\,.$$

- $x=1$. This is a cusp.
- $x=\frac{1}{2}\pm\frac{1}{2}\sqrt{5}$, $-\frac{3}{2}\pm\frac{1}{2}\sqrt{5}$, $\pm2\pm\sqrt{5}$. Then $w^2=1-2x-x^2-x^4+2x^5+x^6>0$, so $w\notin K$.
- $x=-\frac{1}{2}\pm\frac{1}{2}\sqrt{5}\Rightarrow w^2=-5\pm2\sqrt{5}$. We have $N_{K/\mathbf{Q}}(F)=N_{K/\mathbf{Q}}(H)=N_{K/\mathbf{Q}}(I)=2^4$, $N_{K/\mathbf{Q}}(G)=2^4\cdot 11$, $N_{K/\mathbf{Q}}(J)=2^8\cdot 5^2$, $N_{K/\mathbf{Q}}(-1+x)=1$. Then, for a prime ideal $\mathfrak{p}$ of K which divides 11,

$$v_{\mathfrak{p}}(b)>0 \quad\text{and}\quad v_{\mathfrak{p}}(c)>0\,.$$

Therefore, according to Lemma 1 (in Proof of Theorem 2), $v_{\mathfrak{p}}(j)<0$, which contradicts the assumption $j\in O_K$.

Case 4. By virtue of the following Lemma, we can prove this case by the same method as Case 3.

LEMMA 3. *If $E_{tor}(K)\geq\mathbf{Z}/5\mathbf{Z}$, then in the $E(b,c)$-form of this elliptic curve E (cf.*

Case 6, *Thm* 2), b $(=c)$ *is one of the following*:

$$b=-7\pm 5\sqrt{2},\ \pm 5\pm 2\sqrt{6},\ 3\pm\sqrt{10},\ 18\pm 5\sqrt{13},\ 5\pm\sqrt{26},$$
$$6\pm\sqrt{37},\ 8\pm\sqrt{65},\ -57\pm 5\sqrt{130},\ 68\pm 5\sqrt{185}\ .$$

In particular, let $k=\mathbf{Q}(\sqrt{D})$ *be the real quadratic field contained in* K. *Then*,

$$D=2,\ 6,\ 10,\ 13,\ 26,\ 37,\ 65,\ 130,\ 185\ .$$

(This Lemma results from [10] (see Table 8) as in Case 2.)

By Proposition 2 and Theorem 1, we arrive at the following theorem.

THEOREM 3. *Let K be an imaginary cyclic quartic field and E an elliptic curve over K. Suppose that*

1. $f_2<4$ *or* $f_3<4$,
2. $j\in O_K$.

Then, $E_{tor}(K)$ is isomorphic to one of the following ten groups.

$$E_{tor}(K)\cong\begin{cases}\mathbf{Z}/m\mathbf{Z} & (1\leq m\leq 8,\ m\neq 7)\\ \mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/2\mu\mathbf{Z} & (1\leq\mu\leq 3)\end{cases}$$

REMARK. All these groups do occur (cf. Fact 2).

5. Closing remarks.

We wish to remove the assumption, $f_2<4$ or $f_3<4$, on the ground field K. At first, we need to evaluate the order of the torsion subgroup. One can prove the following proposition as in Proposition 1.

PROPOSITION 3. *Let K be an imaginary cyclic quartic field and E an elliptic curve over K. Suppose that*

> *For each $i\in\{2,3\}$, there exists a prime ideal $\mathfrak{p}$ dividing i of K such that $v_{\mathfrak{p}}(j)\geq 0$.*

Then, $E_{tor}(K)$ divides one of the following integers.

$$2^4\cdot 3\cdot 5,\quad 2^2\cdot 25,\quad 2^3\cdot 3\cdot 7,\quad 2^3\cdot 11,\quad 2^2\cdot 13$$
$$2^2\cdot 17,\quad 2^2\cdot 19,\quad 2^2\cdot 23,\quad 2^6\cdot 3^2\ .$$

Next, we have to solve the norm equations including the case where $K=\mathbf{Q}(\zeta_5)$ (cf. Prop. 2). The following is conjectured.

CONJECTURE. Let K be an imaginary cyclic quartic field and E an elliptic curve with integral j-invariant over K. Then, $E_{tor}(K)$ does not have subgroups which are isomorphic to one of the following groups.

$$\begin{array}{llll} \mathbf{Z}/16\mathbf{Z}\,, & \mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/8\mathbf{Z} & & \\ \mathbf{Z}/9\mathbf{Z}\,, & \mathbf{Z}/12\mathbf{Z}\,, & \mathbf{Z}/5\mu\mathbf{Z} & (\mu\geq 2) \\ \mathbf{Z}/7\mathbf{Z}\,, & \mathbf{Z}/11\mathbf{Z}\,, & \mathbf{Z}/13\mathbf{Z}\,. & \end{array}$$

(The cases of $\mathbf{Z}/9\mathbf{Z}$, $\mathbf{Z}/12\mathbf{Z}$, $\mathbf{Z}/5\mu\mathbf{Z}$ ($\mu\geq 2$), and $\mathbf{Z}/7\mathbf{Z}$ have been calculated.)

Thus, in order to get the result such as Theorem 3 for arbitrary imaginary cyclic quartic fields K, we have to study elliptic curves E such that $E_{tor}(K)\geq\mathbf{Z}/17\mathbf{Z}$, $\mathbf{Z}/19\mathbf{Z}$, or $\mathbf{Z}/23\mathbf{Z}$.

On the other hand, it is interesting to study how many elliptic curves (and ground fields) exist whose torsion subgroups are isomorphic to a given group of Theorem 3; this has been partially solved (see Proof of Cases 2, 4, Prop. 2).

ACKNOWLEDGMENT. I would like to thank Professor Ken Nakamula for guiding me to this problem and recommending some references. I am also grateful to Professor H. G. Zimmer for sending me some papers and teaching the latest works.

References

[1] G. W. FUNG, H. STRÖHER, H. C. WILLIAMS and H. G. ZIMMER, Torsion groups of elliptic curves with integral j-invariant over pure cubic fields, J. Number Theory **36** (1990), 12–45.

[2] H. HASSE, Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern, *Helmut Hasse Mathematische Abhandlungen III*, 289–379, Walter de Gruyter (1975).

[3] C. HOLLINGER and H. G. ZIMMER, Torsion groups of elliptic curves with integral j-invariant over multiquadratic fields, preprint.

[4] D. HUSEMÖLLER, *Elliptic Curves*, G. T. M. **111** (1986), Springer.

[5] S. KAMIENNY, Torsion points on elliptic curves, Bull. Amer. Math. Soc. (N.S.) **23** (1990), 371–373.

[6] S. KAMIENNY, Torsion points on elliptic curves and q-coefficients of modular forms, Invent. Math. **109** (1992), 221–229.

[7] M. A. KENKU and F. MOMOSE, Torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J. **109** (1988), 125–149.

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

[9] B. MAZUR, Rational points on modular curves, *Modular Functions of One Variable V*, Lecture Notes in Math. **601** (1977), 107–148, Springer.

[10] H. H. MÜLLER, H. STRÖHER and H. G. ZIMMER, Torsion groups of elliptic curves with integral j-invariant over quadratic fields, J. Reine Angew. Math. **397** (1989), 100–161.

[11] M. A. REICHERT, Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields, Math. Comp. **46** (1986), 637–658.

[12] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, G.T.M. **106** (1986), Springer-Verlag.

Present Address:
DEPARTMENT OF MATHEMATICS, TOKYO METROPOLITAN UNIVERSITY,
MINAMI-OHSAWA, HACHIOJI-SHI, TOKYO, 192–03 JAPAN.