Karino, K.
Osaka J. Math.
34 (1997), 703–715

NON-EXISTENCE OF ELLIPTIC CURVES WITH SMALL CONDUCTORS OVER IMAGINARY QUADRATIC FIELDS

KIYOSHI KARINO

(Received March 21, 1996)

1. Introduction

In this paper, I will use the term *elliptic curve* to mean an abelian variety of dimension 1, or, what is the same, an irreducible non-singular projective algebraic curve of genus 1 furnished with a rational point 0, the origin for the group law. Any such curve E defined over a field K (frequently denoted E/K) has a plane cubic model of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

where x and y are coordinates in the affine plane and the coefficients a_i are in our ground filed K. We call (1) a Weierstrass equation. We can simplify (1) by completing the square. Replacing (x, y) by $(2^{-2}x, 2^{-3}y - 2^{-3}a_1x - 2^{-1}a_3)$ gives an equation of the form

$$y^2 = x^3 + b_2x^2 + 8b_4x + 16b_6 \tag{2}$$

where

$$b_2 = {a_1}^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = {a_3}^2 + 4a_6.$$

We also define quantities

$$\begin{aligned} b_8 &= {a_1}^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2{a_3}^2 - {a_4}^2 \\ c_4 &= {b_2}^2 - 24b_4 \\ c_6 &= -{b_2}^3 + 36b_2b_4 - 216b_6 \\ \Delta &= -{b_2}^2b_8 - 8{b_4}^3 - 27{b_6}^2 + 9b_2b_4b_6 \\ j &= {c_4}^3\Delta^{-1} \end{aligned}$$

They are related by the following identities

$$4b_8 = b_2b_6 - {b_4}^2,\ 1728\Delta = {c_4}^3 - {c_6}^2.$$

Also, if $a_1 = a_3 = 0$, Then Δ is just 16 times the discriminant of the cubic polynomial $x^3 + a_2x^2 + a_4x + a_6$. Δ is called a discriminant of the curve (1). For another affine curve

$$y'^2 + a_1'x'y' + a_3'y' = x'^3 + a_2'x'^2 + a_4'x' + a_6' \tag{3}$$

related by

$$x = u^2x' + r \quad \text{and} \quad y = u^3y' + u^2sx' + t$$

where u, r, s, t are in K and $u \neq 0$. The following identities hold (using an obvious notation).

$$\begin{aligned}
&ua_1' = a_1 + 2s \\
&u^2a_2' = a_2 - sa_1 + 3r - s^2 \\
&u^3a_3' = a_3 + ra_1 + 2t \\
&u^4a_4' = a_4 + sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\
&u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \\
&u^2b_2' = b_2 + 12r \\
&u^4b_4' = b_4 + rb_2 + 6r^2 \\
&u^6b_6' = b_6 + 2rb_4 + r^2b_2 + 4r^3 \\
&u^8b_8' = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \\
&u^4c_4' = c_4 \\
&u^6c_6' = c_6 \\
&u^{12}\Delta' = \Delta \\
&j = j'.
\end{aligned}$$

If two elliptic curves E and E' are isomorphic, then $j = j'$; the converse is true over an algebraically closed filed K.

2. The case E has a rational 2-division point

We will use the following notation.

k : the Gauss number filed $\mathbb{Q}(\sqrt{-1})$

P : a prime ideal of k which divides 5

Q : a prime ideal of k which divides 2

π : an integer of k such that $Q||\pi$

The purpose of this part is to prove that there is no elliptic curve E/k of conductor P or P^2 with no rational 2-division point. Observe that it is sufficient to treat the case $P = (2 + \sqrt{-1})$. We will assume that there exists such an elliptic curve E/k. It has a global minimal Weierstrass equation since k has class number

1. Completing the square and translating 2-division point to the origin, we obtain an equation

$$E' : y^2 = x^3 + Ax^2 + Bx = x(x-\alpha)(x-\beta)$$

where A and B are integers of k and α and β are in $\mathbb{C}$. Let Δ and Δ' be the discriminant of E and E' respectively. Then,

$$16(\alpha\beta)^2(\alpha-\beta)^2 = \Delta' = 2^{12}\Delta = 2^{12}(2+\sqrt{-1})^n\varepsilon$$

where $1 \leq n \leq 11$ and ε is a unit of k. Putting $X = \alpha\beta$ and $Y = (\alpha-\beta)^2$, we gain the following

$$(4) \qquad X^2Y = 2^8(2+\sqrt{-1})^n\varepsilon \quad (X \text{ and } Y \text{ are integers of } k)$$

$$(5) \qquad A = \pm\sqrt{Y+4X}$$

We will solve the equation (1) for each n under the condition that (2) is in k. Observe that X and Y are of the forms

$$X = (1+\sqrt{-1})^r(2+\sqrt{-1})^s\varepsilon'$$
$$Y = (1+\sqrt{-1})^t(2+\sqrt{-1})^u\varepsilon''$$

where $2r+t = 16$, $2s+u = n$ and ε', ε'' are the units of k. The possibilities for X and Y are finite since $1 \leq n \leq 11$. By simple calculations, we gain the following lemma.

Lemma 2.1. *Up to isomorphism, there are* 11 *elliptic curves* E/k *with a rational* 2*-division point and conductor of the form* P^rQ^s *where* $1 \leq r \leq 2$ *and* $s \geq 0$ *as follows.*

$$(1) \qquad j = (1+\sqrt{-1})^6(63+32\sqrt{-1})^3\sqrt{-1}(2+\sqrt{-1})^{-1}$$
$$A = (1+\sqrt{-1})^3(4+\sqrt{-1}),\ B = (1+\sqrt{-1})^2$$

$$(2) \qquad j = (1+\sqrt{-1})^{15}(4-\sqrt{-1})^3\sqrt{-1}(2+\sqrt{-1})^{-1}$$
$$A = (1+\sqrt{-1})^3(2-\sqrt{-1}),\ B = (1+\sqrt{-1})^5$$

$$(3) \qquad j = (1+\sqrt{-1})^{12}(3+2\sqrt{-1})^3(2+\sqrt{-1})^{-2}$$
$$A = (1+\sqrt{-1})^5\sqrt{-1},\ B = (1+\sqrt{-1})^4(2+\sqrt{-1})\sqrt{-1}$$

$$(4) \qquad j = -27(1+\sqrt{-1})^{12}$$

$$A = 0,\ B = (1+\sqrt{-1})^4(2+\sqrt{-1})$$

(5) $$j = 27(1+\sqrt{-1})^{15}(4+3\sqrt{-1})^3\sqrt{-1}(2+\sqrt{-1})^{-3}$$
$$A = 3(1+\sqrt{-1})^3\sqrt{-1},\ B = (1+\sqrt{-1})^5$$

(6) $$j = -(1+\sqrt{-1})^{15}\sqrt{-1}$$
$$A = (1+\sqrt{-1})^3(2+\sqrt{-1}),\ B = (1+\sqrt{-1})^5(2+\sqrt{-1})\sqrt{-1}$$

(7) $$j = (1+\sqrt{-1})^6(-3+28\sqrt{-1})^3(2+\sqrt{-1})^4$$
$$A = (1+\sqrt{-1})(5+4\sqrt{-1}),\ B = -(1+\sqrt{-1})^7$$

(8) $$j = 3^3\cdot 11^3(1+\sqrt{-1})^6\sqrt{-1}$$
$$A = 3(1+\sqrt{-1})^3(2+\sqrt{-1})\sqrt{-1},\ B = (1+\sqrt{-1})^2(2+\sqrt{-1})^2$$

(9) $$j = -(1+\sqrt{-1})^{12}5^3$$
$$A = (1+\sqrt{-1})^5(2+\sqrt{-1})\sqrt{-1},\ B = (1+\sqrt{-1})^4(2+\sqrt{-1})^2\sqrt{-1}$$

(10) $$j = -(1+\sqrt{-1})^{12}(3-8\sqrt{-1})^3\sqrt{-1}(2+\sqrt{-1})^{-1}$$
$$A = (1+\sqrt{-1})^5(2+\sqrt{-1})\sqrt{-1},\ B = (1+\sqrt{-1})^4(2+\sqrt{-1})^2$$

(11) $$j = (1+\sqrt{-1})^{15}(2-\sqrt{-1})^3\sqrt{-1}(2+\sqrt{-1})^{-1}$$
$$A = (1+\sqrt{-1})^3(2+\sqrt{-1}),\ B = (1+\sqrt{-1})^5(2+\sqrt{-1})^2.$$

We will prepare the following lemma to pick up elliptic curves of prime power conductors.

Lemma 2.2. *Let $E : y^2 = x^3 + Ax^2 + Bx$ be an elliptic curvre over k where A and B are integers of k. Assume that its discriminant is $2^{12}D$ where D is integral and prime to 2. Then E has good reduction at Q if and only if A and B satisfy either of these sets of congruences.*

(1) $$A \equiv 2\alpha^2 \pmod{Q^6} \quad B \equiv \alpha^4 \pmod{Q^6}$$
(2) $$A \equiv \alpha^2 \pmod{Q^4} \quad B \equiv 0 \pmod{Q^8}$$

α is integral and prime to 2.

(3) $$A \equiv 0 \pmod{Q^5} \qquad B \equiv \pi^4 + 8\pi \pmod{Q^8}$$

$\pi^2 A - B \equiv \pi^4 + \pi^6 \pmod{Q^{10}}$ *or* $\pi^2 A - B \equiv 5\pi^4 + 4\pi^5 + \pi^6 \pmod{Q^{10}}$.

Proof. See [17, page 242]. □

Proposition 2.3. *There exists no elliptic curve E/k with a non-trivial 2-division point which is everywhere good reduction except for P.*

Proof. This is shown by non-solvability of the congruence equations of the above lemma. It is confirmed by case check. Since it is quite elementary, we do not write details, but indicate the outline of computations.

For the condition (1), $B \equiv \alpha^4 \pmod{Q^6}$ implies that $Q|\alpha$ since $Q|B$. But this contradicts that α is prime to 2. For the condition (2), B does not satisfy the congruence $B \equiv 0 \pmod{Q^8}$. For the condition (3), Put $\pi = (1+\sqrt{-1})$ and calculate $B - (\pi^4 + 8\pi)$, $\pi^2 A - B - (\pi^4 + \pi^6)$ and $\pi^2 A - B - (5\pi^4 + 4\pi^5 + \pi^6)$. □

Calculating c_4, we obtain the following corollaries.

Corollary 2.4. *There are 5 elliptic curves E/k with a rational 2-division point and conductor of the form PQ^r where $r \geq 1$ as follows.*

(1) $c_4 = 32(32 - 63\sqrt{-1})$ $\quad A = (1+\sqrt{-1})^3(4+\sqrt{-1})$
$\quad B = (1+\sqrt{-1})^2$

(2) $c_4 = -64(1+\sqrt{-1})(4-\sqrt{-1})$ $\quad A = (1+\sqrt{-1})^3(2-\sqrt{-1})$
$\quad B = (1+\sqrt{-1})^5$

(3) $c_4 = 64(-3 - 2\sqrt{-1})$ $\quad A = (1+\sqrt{-1})^5\sqrt{-1}$
$\quad B = (1+\sqrt{-1})^4(2+\sqrt{-1})\sqrt{-1}$

(4) $c_4 = 192(1+\sqrt{-1})(2-\sqrt{-1})^2\sqrt{-1}$ $\quad A = 3(1+\sqrt{-1})^3\sqrt{-1}$
$\quad B = (1+\sqrt{-1})^5$

(5) $c_4 = 32\sqrt{-1}(-3+28\sqrt{-1})$ $\quad A = (1+\sqrt{-1})(5+4\sqrt{-1})$
$\quad B = -(1+\sqrt{-1})^7$.

Corollary 2.5. *There are 6 elliptic curves E/k with a rational 2-division point and conductor of the form P^2Q^r where $r \geq 1$ as follows.*

(1) $c_4 = 192(2+\sqrt{-1})$ $\quad A = 0$
$\quad B = (1+\sqrt{-1})^4(2+\sqrt{-1})$

(2) $c_4 = 16(1+\sqrt{-1})^5(2+\sqrt{-1})$ $\quad A = (1+\sqrt{-1})^3(2+\sqrt{-1})$
$\quad B = (1+\sqrt{-1})^5(2+\sqrt{-1})\sqrt{-1}$

$$\begin{array}{lll}
(3) & c_4 = 33\cdot 32\sqrt{-1}(2+\sqrt{-1})^2 & A = 3(1+\sqrt{-1})^3(2+\sqrt{-1})\sqrt{-1} \\
 & & B = (1+\sqrt{-1})^2(2+\sqrt{-1})^2 \\
(4) & c_4 = -64(2+\sqrt{-1})^3(1+2\sqrt{-1}) & A = (1+\sqrt{-1})^5(2+\sqrt{-1})\sqrt{-1} \\
 & & B = (1+\sqrt{-1})^4(2+\sqrt{-1})^2\sqrt{-1} \\
(5) & c_4 = 64(2+\sqrt{-1})^2(3-8\sqrt{-1}) & A = (1+\sqrt{-1})^5(2+\sqrt{-1})\sqrt{-1} \\
 & & B = (1+\sqrt{-1})^4(2+\sqrt{-1})^2 \\
(6) & c_4 = 320(1+\sqrt{-1})(2+\sqrt{-1}) & A = (1+\sqrt{-1})^3(2+\sqrt{-1}) \\
 & & B = (1+\sqrt{-1})^5(2+\sqrt{-1})^2.
\end{array}$$

3. The Case E has no rational 2-division point

3.1. Preliminaries

We will use the following notation in this section.

k	:	a number field
$\mathfrak{m}$	:	an integral ideal of k
h_0	:	the class number of k
ϕ	:	the Euler function
$A_{\mathfrak{m}}$	:	the set of all the fractional ideals prime to $\mathfrak{m}$
$S_{\mathfrak{m}}$	:	$=\{(\alpha)\in A_{\mathfrak{m}} : \alpha\in k, \alpha\equiv 1 \pmod{\mathfrak{m}}\}$, the ray class in $A_{\mathfrak{m}}$
r_1	:	the number of real conjugate fields of k
E_k	:	all the units of k
E_k^0	:	$\{\varepsilon\in E_k : \varepsilon\equiv 1 \pmod{\mathfrak{m}}\}$
N	:	the absolute norm map of ideals
$N_{N/k}$	:	the relative norm map of ideals with respect to an extension K/k.

Lemma 3.1. *Let E/k be an elliptic curve without a rational 2-division point and B be a 2-division field of E. Then* $\mathrm{Gal}(B/k)\cong S_3$ *or* A_3.

Proof. By definition, $\mathrm{Gal}(B/k)$ is a subgroup of $\mathrm{Aut}(E[2]) = GL_2(\mathbb{Z}/2\mathbb{Z})$, which does not fix non-zero element of $E[2]$. Hence, the lemma follows. □

The following fact is well known.

Fact 3.2. *Let E be an elliptic curve over k and B be a n-division field of E. The prime ideal which ramifies in B/k divides n or the conductor of E.*

Lemma 3.3. *Given a prime ideal P of k. Let E/k be an elliptic curve everywhere good reduction except for P and B its 2-division field. Let $Q_1, \cdots, Q_n$ be all the prime ideals of k which divides 2 and ramify in B/k. Moreover assume that E has no rational 2-division point. Then* $\mathrm{Gal}(B/k) \cong S_3$, *if* $NP \not\equiv 1, 0 \pmod 3$, $NQ_i \not\equiv 1 \pmod 3$ *and* $h_0 \not\equiv 0 \pmod 3$.

Proof. Assume that $\mathrm{Gal}(B/k) \cong A_3$. Let K be a class field correspondent to $S_{\mathfrak{m}}$ where $\mathfrak{m} = P^e \prod_{i=1}^n Q_i^{e_i}$. By the Fact 3.2, B is a subfield of K for some $e, e_i \in \mathbb{N}$. Meanwhile, we have

$$\begin{aligned}[K : k] &= [A_{\mathfrak{m}} : S_{\mathfrak{m}}] \\ &= h_0 2^{r_1} \phi(\mathfrak{m})/[E_k : E_k^0] \\ &= NP^{e-1}(NP-1) \prod_{i=1}^n NQ_i^{e_i-1}(NQ_i - 1)/[E_k : E_k^0].\end{aligned}$$

Therefore, $[B : k] \not\equiv 0 \pmod 3$ since $[K : k] \not\equiv 0 \pmod 3$ by assumption. This is absurd. □

Lemma 3.4. *Let B/k be a Galois extension such that* $\mathrm{Gal}(B/k) \cong S_3$, *let K and $L^{(i)} (i = 1, 2, 3)$ be subfields of B such that $[K : k] = 2$ and $[L^{(i)} : k] = 3$ respectively and let P be a prime ideal of k which ramifies in B/k and* $\mathfrak{p}$ (resp. $\mathfrak{p}^{(i)}$, $\mathfrak{P}$) *be a prime ideal of K* (resp. $L^{(i)}$, B) *which divides P. Put* $\mathrm{Gal}(B/L^{(i)}) = \langle \tau_i \rangle$. *Then, we inertia* (resp. *decomposition*) *group of $\mathfrak{P}$ in B/k.*

(1)	$Z(\mathfrak{P}) = T(\mathfrak{P}) = S_3$	$P = \mathfrak{P}^6$	*in*	B
		$P = \mathfrak{p}^{(i)3}$	*in*	$L^{(i)}$
		$P = \mathfrak{p}^2$	*in*	K
(2)	$Z(\mathfrak{P}) = S_3, T(\mathfrak{P}) = A_3$	$P = \mathfrak{P}^3$	*in*	B
		$P = \mathfrak{p}^{(i)3}$	*in*	$L^{(i)}$
		$P = \mathfrak{p}$	*in*	K
(3)	$Z(\mathfrak{P}) = T(\mathfrak{P}) = A_3$	$P = (\mathfrak{P}_1\mathfrak{P}_2)^3$	*in*	B
		$P = \mathfrak{p}^{(i)3}$	*in*	$L^{(i)}$
		$P = \mathfrak{p}_1\mathfrak{p}_2$	*in*	K
(4)	$Z(\mathfrak{P}) = T(\mathfrak{P}) = \langle \tau_i \rangle$	$P = (\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3)^2$	*in*	B
		$P = \mathfrak{p}_1^{(i)}\mathfrak{p}_2^{(i)2}$	*in*	$L^{(i)}$
		$P = \mathfrak{p}^2$	*in*	K.

Proof. This lemma follows immediately from the fact that $T(\mathfrak{P}) \neq \{1\}$ and $Z(\mathfrak{P})/T(\mathfrak{P})$ is a cyclic group. □

Lemma 3.5. *Notation as Lemma* 3.4. *If* $Z(\mathfrak{P}) = T(\mathfrak{P}) = S_3$, *then* $\mathfrak{P}$ *divides* 3.

Proof. Let p a rational prime number divided by $\mathfrak{P}$ and $V(\mathfrak{P})$ be a first ramification group of $\mathfrak{P}$. $V(\mathfrak{P})$ must equal A_3 since the order of $V(\mathfrak{P})$ is a power of p and $T(\mathfrak{P})/V(\mathfrak{P})$ is a cyclic group. Therefore $p = 3$. □

Lemma 3.6. *Notation as Lemma* 3.4. *If* $Z(\mathfrak{P}) = T(\mathfrak{P}) = A_3$ *then,* $N\mathfrak{P} \neq 2$.

Proof. Assume that $N\mathfrak{P} = 2$, $V(\mathfrak{P})$ must equal A_3 since $[T(\mathfrak{P}) : V(\mathfrak{P})] | (N\mathfrak{P} - 1) = 1$. This contradicts the fact that the order of $V(\mathfrak{P})$ is a power of p. □

Lemma 3.7. *Let K/k be a Galois extension and P be a prime ideal of k. Let $\mathfrak{P}$ be a prime ideal of K which divides P and* e *its ramification index and let n be an integer such that $\mathfrak{P}^n || \mathfrak{D}_{K/k}$, here $\mathfrak{D}_{K/k}$ denotes the different of K/k. Then, we have*
(1) $n = e - 1$ *if* $(\mathfrak{P}, 1) = 1$.
(2) $e \leq n \leq e - 1 + e\nu_p(e)$ *if* $(\mathfrak{P}, 1) \neq 1$.
where $\nu_p(e)$ denotes P-index of e.

Proof. See [5, page 61, Vol. 2]. □

3.2. The case $k = \mathbb{Q}(\sqrt{-1})$

Let $k = \mathbb{Q}(\sqrt{-1})$. Hereafter till the end of this section, let P and Q be prime ideals of k which divides 5 and 2 respectively. Let $\mathfrak{P}$ (resp. $\mathfrak{p}$, $\mathfrak{p}^{(i)}$) be a prime ideal of $\mathfrak{P}$ (resp. K, $L^{(i)}$) which divides P and let $\mathfrak{Q}$ (resp. $\mathfrak{q}$, $\mathfrak{q}^{(i)}$) be a prime ideal of B (resp. K, $L^{(i)}$) which divides Q.

The following lemma is immediate from Lemma 3.3.

Lemma 3.8. *Let E/k be an elliptic curve having everywhere good reduction except at P and no rational 2-division point. Let B be a 2-division field of E. Then,* $\mathrm{Gal}(B/k) \cong S_3$.

Lemma 3.9. *Notation as above. Q ramifies in B/k as the case* (4) *in Lemma* 3.4.

Proof. Let K be a subfield of B such that $[K : k] = 2$. Only P and Q can ramify in K/k. So, K is a subfield of a class field correspondent to $S_\mathfrak{m}$ where

$\mathfrak{m} = P^r Q^s (r, s \in \mathbb{N})$. Then, we have

$$[A_{\mathfrak{m}} : S_{\mathfrak{m}}] = \begin{cases} 5^{r-1}2^s & \text{if} \quad r \geq 1 \quad \text{and} \quad s \geq 1 \\ 1 & \text{if} \quad r = 0 \quad \text{and} \quad 1 \leq s \leq 3 \\ 2^{s-3} & \text{if} \quad r = 0 \quad \text{and} \quad s \geq 4 \\ 5^{r-1} & \text{if} \quad r \geq 1 \quad \text{and} \quad s = 0. \end{cases}$$

So, $s \geq 1$ since $[K : k]$ divides $[A_{\mathfrak{m}} : S_{\mathfrak{m}}]$. Hence, Q ramifies as the case (1) or (4) in Lemma 3.4. But, by Lemma 3.5, Q can not ramify as the case (1). Therefore, Q ramifies as the case (4). □

Proposition 3.10. *There exists no elliptic curve E/k of conductor P without a rational 2-division point.*

Proof. Assume that there exists such an elliptic curve E. By a suitable transformation, we have an affine equation

$$E' : y^2 = x^3 + ax^2 + bx + c$$

where a, b, c are integers of k and the discriminant of E' equals $2^{12}(2 \pm \sqrt{-1})^m \varepsilon$ where $1 \leq m \leq 11$ and ε is a unit of k. Let B be a 2-division field of E. Let K and $L^{(i)} (i = 1, 2, 3)$ be subfields of B such that $[K : k] = 2$ and $[L^{(i)} : k] = 3$ respectively. Observe that the 2-division field and the conductor of E are the same as those of E'. By the assumption that E has multiplicative reduction at P, we have

$$x^3 + ax^2 + bx + c \equiv (x - \alpha)^2 (x - \beta) \pmod{P}$$

for suitable distinct integers of k α, β. So, $P = \mathfrak{p}_1^{(i)} \mathfrak{p}_2^{(i)2}$ in $L^{(i)}$ since $L^{(i)} = k(\gamma)$ where γ is a solution for the equation $x^3 + ax^2 + bx + c = 0$. Therefore, P ramifies as the case (4) in Lemma 3.4. Let $\mathfrak{D}_{B/k}$ be a different of B/k and d_B a discriminant of B. Then, we can put $\mathfrak{D}_{B/k} = (\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3)(\mathfrak{Q}_1 \mathfrak{Q}_2 \mathfrak{Q}_3)^m$. Let Δ be a discriminant of E. We have $K = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{(2 \pm \sqrt{-1})\varepsilon}))$ since P ramifies in K/k. Using the chain rule of differents, we have

$$|d_B| = N_{B/\mathbb{Q}}(\mathfrak{D}_{B/\mathbb{Q}}) = N_{k/\mathbb{Q}}(N_{B/k}(\mathfrak{D}_{B/k}) \cdot \mathfrak{D}_{k/\mathbb{Q}}^{[B:k]}) = 5^3 \cdot 2^{3m+12}$$

and

$$|d_B| = N_{B/\mathbb{Q}}(\mathfrak{D}_{B/k} \cdot \mathfrak{D}_{K/\mathbb{Q}}) = 5^3 \cdot |d_K|^3.$$

Hence, m must be even since the discriminant of $\sqrt{(2 \pm \sqrt{-1})\varepsilon}$ equals $2^8 \cdot 5$ or $2^{12} \cdot 5$. Meanwhile, we have $2 \leq m \leq 5$ by Lemma 3.7. Therefore, $m = 2, 4$.

According to [13, p. 17], $|d_B|^{(1/12)}$ must be larger than 7.412879... But, $(5^3 \cdot 2^{(3\cdot 4+12)})^{(1/12)} = 5.981395...$ This is a contradiction. □

Proposition 3.11. *There exists no elliptic curve E/k with conductor P^2 and no rational 2-division point.*

Proof. Assume that there exists no elliptic curve E. By a suitable transformation, we have an affine equation

$$E' : y^2 = x^3 + ax^2 + bx + c$$

where a, b, c are integers of k and the discriminant of E' equals $2^{12}(2 \pm \sqrt{-1})^m \varepsilon$ where $1 \leq n \leq 11$ and ε is a unit of k. Let B be a 2-division field of E. Let K and $L^{(i)}(i = 1, 2, 3)$ be subfields of B such that $[K : k] = 2$ and $[L^{(i)} : k] = 3$ respectively. By the assumption that E has additive reduction at P, we have

$$x^3 + ax^2 + bx + c \equiv (x - \alpha)^3 \pmod{P}$$

for a suitable integer of k, α. Therefore, $P = \mathfrak{p}^{(i)3}$ in $L^{(i)}$. Let Δ be a discriminant of E and ζ_8 be a primitive 8th root of unity. Then, we have $K = k(\sqrt{\Delta}) = \mathbb{Q}(\zeta_8)$ since P does not ramify in K/k. Hence, $P = \mathfrak{p}_1\mathfrak{p}_2$ in K since $5 \not\equiv 1 \pmod{8}$ and $5^2 \equiv 1 \pmod{8}$. Therefore, P ramifies as the case (2) in Lemma 3.4. Then, we have $\mathfrak{D}_{B/k} = \mathfrak{P}^2$, meanwhile $|d_K| = 2^8$. Consequently by the chain rule of differents, we have

$$\begin{aligned} |d_B| &= N_{B/\mathbb{Q}}(\mathfrak{D}_{B/\mathbb{Q}}) = N_{B/\mathbb{Q}}(\mathfrak{D}_{B/K} \cdot \mathfrak{D}_{K/\mathbb{Q}}) \\ &= N(\mathfrak{P}^2)|d_K|^3 = 5^4 \cdot 2^{24} \end{aligned}$$

and

$$|d_B|^{(1/12)} = 6.839903... .$$

But, this contradicts the fact that $|d_B|^{(1/12)}$ must be larger than 7.412879... □

Corollary 3.12. *There exists no elliptic curve E/k having everywhere good reduction except at P.*

3.3. The case $k = \mathbb{Q}(\sqrt{-3})$

Let $k = \mathbb{Q}(\sqrt{-3})$. Hereafter till the end of this section, let Q be a prime ideals of k which divides 2. Let $\mathfrak{Q}$ (resp. $\mathfrak{q}$, $\mathfrak{q}^{(i)}$) be a prime ideal of B (resp. K, $L^{(i)}$) which divides Q.

Lemma 3.13. *Let P be a prime ideal of k which divides 7 or 13 and let E/k be an elliptic curve having everywhere good reduction except at P and no rational 2-division point. Then,* $\mathrm{Gal}(B/k) \cong S_3$.

Proof. Assume that $\mathrm{Gal}(B/k) \cong A_3$. Then, B is a subfield of a class field correspondent to $S_{\mathfrak{m}}$ where $\mathfrak{m} = P^r Q^s (r, s \in \mathbb{N})$ and we have $[A_{\mathfrak{m}} : S_{\mathfrak{m}}] \not\equiv 0 \pmod 3$. This is absurd. □

Proposition 3.14. *Let P be a prime ideal of k which divides 7. Then, there exists no elliptic curve E/k of conductor P with no rational 2-division point.*

Proof. By the above lemma, we may assume that $\mathrm{Gal}(B/k) \cong S_3$. We will suppose that there exists such an elliptic curve E. By the assumption of conductor, P ramifies as the case (4) in Lemma 3.4. Meanwhile, Q must ramify in K/k by class field theory. Therefore, Q ramifies as the case (4). Then we have $\mathfrak{D}_{B/k} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3(\mathfrak{Q}_1\mathfrak{Q}_2\mathfrak{Q}_3)^2$ and $|d_B|^{1/12} = 5.634626...$ But, this is a contradiction. □

Proposition 3.15. *Notation as above. There exists no elliptic curve E/k of conductor P^2 with no rational 2-division point.*

Proof. We may assume that $\mathrm{Gal}(B/k) \cong S_3$. Suppose that there exists such an elliptic curve E. Let Δ be a discriminant of E. By the assumption of conductor, P ramifies as the case (2) or (3) in Lemma 3.4. Therefore, we have $K = \mathbb{Q}(\zeta_{12})$ (ζ is a primitive 12th root of unity.) since $K = \mathbb{Q}(\sqrt{\Delta})$ and P does not ramify in K/k. Meanwhile, Q ramifies as the case (4) since $K = \mathbb{Q}(\zeta_{12})$. Then, we have $|d_k| = 2^4 \cdot 3^2$ and $|d_B|^{(1/12)} = N(\mathfrak{D}_{B/K} \cdot \mathfrak{D}_{K/\mathbb{Q}})^{1/12} = 6.626588...$ But, this is absurd. □

Proposition 3.16. *Let P be a prime ideal of k which divides 13. Then, there exists no elliptic curve E/k of conductor P with no rational 2-division point.*

Proof. We may assume that $\mathrm{Gal}(B/k) \cong S_3$. Suppose that there exists such an elliptic curve E. By the assumption of conductor and class field theory, P ramifies as the case (4) in Lemma 3.4 and Q unramifies in B/k or ramifies as the case (2), (3) or (4). Then, we have

$$\mathfrak{D}_{B/k} = \begin{cases} \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3 \\ \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{Q}^2 \\ \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3(\mathfrak{Q}_1\mathfrak{Q}_2)^2 \\ \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3(\mathfrak{Q}_1\mathfrak{Q}_2\mathfrak{Q}_3)^2 \end{cases}$$

hence, we have

$$|d_B|^{(1/12)} = 3.288868..., \quad 5.220752... \text{ or } \quad 6.577736...$$

This is absurd. □

Remark 3.17. Notation as Lemma 3.16. Let consider the case conductor of E is P^2. In this case, P ramifies as the case (2) or (3) in Lemma 3.4. So, we have $K = \mathbb{Q}(\zeta_{12})$ since $K = \mathbb{Q}(\sqrt{\Delta})$ and P does not ramify in K/k. Meanwhile, Q ramifies as the case (4) since $K = \mathbb{Q}(\zeta_{12})$. Therefore, we have $|d_B|^{1/12} = 8.145262...$ So, it fails.

Remark 3.18. By using the above method, we can prove that there exists no elliptic curve E/k having everywhere good reduction and no rational 2-division point for $k = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7})$.

References

[1] J. Cassels and A. Fröhlich: Algebraic Number Theory, Academic Press, 1967.

[2] J.E. Cremona: *Hyperbolic Tessellations, Modular Symbols and Elliptic curves over complex quadratic fields*, Composition Math. **51** (1984), 275–323.

[3] Diaz y Diaz, F: *Tables minorant la racine n-ième du discriminant d'un corps de de degré n*, Publ. Math. d'Orsay. Orsay, Université d'Orsay, (1980).

[4] J.M. Fountain: *Il n'y a pas de variété abélienne sur* **Z**, Invent. Math. **81** (1985), 515–538.

[5] G. Fujisaki: Introduction to Algebraic Number Theory (in Japanese), Syoukabou, **1, 2** 1975.

[6] T. Hadano: *On the conductor of an elliptic curve with a rational point of order 2*, Nagoya Math. J. **53** (1974), 199–210.

[7] S. Iyanaga: Number Theory (in Japanese), Iwanamishoten, 1969.

[8] Y. Kawada: Number Theory (in Japanese), Iwanamishoten, 1972.

[9] S. Lang: Algebaic Number Theory, Graduate Texts in Mathematics, Springer-Verlag, 1986.

[10] I. Miyawaki: *Elliptic curves of prime power conductor with* **Q***-rational points of finite order*, Osaka Math. J. **10** (1973), 309–323.

[11] A. Ogg: *Elliptic curves and wild ramification*, Amer. J. Math. **89** (1967), 1–21.

[12] G. Poitou: *Minorations de discriminants*, Lecture Notes in Math, Springer-Verlag, **567** (1976), 136–153.

[13] G. Poitou: *Séminaire Delange-Pisot-Poitou*, Théorie des nombres, Université Pierre et Marie Curie Institut Henri Poincaré, (1977).

[14] J.P. Serre: *Corps locaux*, Hermann, (1962).

[15] J.P. Serre: Abelian l adic Representations and Elliptic Curves, Benjamin, 1968.

[16] C.B. Setzer: *Elliptic curves of prime power conductor*, J. London Math. Soc. **10 (2)** (1975), 367–378.

[17] C.B. Setzer: *Elliptic curves over complex quadratic fields*, Pacific J. Math. **74** (1978), 235–250.

[18] G. Shimura: Introduction to the Arithmetic Theory of Automorphic Functions, Priceton Univ. Press, 1971.

[19] J. Silverman: The Arithmetic of Elliptic curves, Graduate Texts in Mathematics, Springer-Verlag, 1986.

[20] J. Silverman: Advanced Topics in the Arithmetic of Elliptic curves, Graduate Texts in Mathematics, Springer-Verlag, 1994.

[21] T. Takagi: Algebraic Number Theory (in Japanese), Iwanamishoten, 1971.

[22] J. Tate: *The Arithmetic of ellitic curves*, Invent. Math. **23** (1974), 179–206.

[23] J. Tate: *Algorithm for determining the type of singular fibre in an elliptic pencil. Modular Functions of one variable IV*, Lecture Notes in Math., Springer-Verlag, **476** (1975), 33–52.

Department of Mathematical Sciences
University of Tokyo
3-8-1, Komaba Meguro-ku
Tokyo 153, Japan