Sato, A.
Osaka J. Math.
48 (2011), 809–826

ON THE CLASS NUMBERS OF CERTAIN NUMBER FIELDS OBTAINED FROM POINTS ON ELLIPTIC CURVES III

ATSUSHI SATO

(Received October 6, 2009, revised March 23, 2010)

Abstract

We study the ramifications in the extensions of number fields arising from an isogeny of elliptic curves. In particular, we start with an elliptic curve with a rational torsion point, and show that the extension is unramified if and "only if" the point which generates the extension is reduced into a nonsingular point (we need to assume certain conditions in order to prove the "only if" part). We also study a characterization of quadratic number fields with class numbers divisible by 5.

1. Introduction

The ideal class groups of number fields have been studied for a long time. One studies the ideal class groups by using certain Diophantine equations, especially the arithmetic theory of elliptic curves. For example, T. Honda [2] (see also [3]) used elliptic curves to construct infinitely many (real and imaginary) quadratic number fields with class numbers divisible by 3. He also studied a characterization of such number fields (cf. [5]). In [10] and [11] (see also [12]), the author gave a geometric interpretation for Honda's work, and introduced a way to construct, from an elliptic curve with a rational torsion point of order $l \in \{3, 5, 7\}$, infinitely many quadratic number fields with class numbers divisible by l.

Let k be a number field of finite degree, and let E be an elliptic curve defined over k which has a k-rational point T_0 of prime order l. Then there exist an elliptic curve E^* and an isogeny $\lambda\colon E \to E^*$, which are defined over k, such that $\mathrm{Ker}\,\lambda = \langle T_0 \rangle$. Here $\langle T_0 \rangle$ denotes the subgroup of $E(k)$ generated by T_0. Such a pair (E^*, λ) is unique up to k-isomorphism, and E^* is often denoted by $E/\langle T_0 \rangle$. Taking certain equation for E and using Vélu's formulas, the author studied, in [10] and [11], the ramification in the extension $k(\lambda^{-1}(Q))/k(Q)$ for a point Q on E^* with $X(Q) \in k$, and obtained a sufficient condition for the extension unramified at every finite place. Roughly speaking, the extension is unramified if Q is reduced into a nonsingular point (see Theorem 5.1). In its proof, the following fact (see Theorem 2.1) plays an important role:

Let $\mathfrak{p}$ be a prime ideal in k, and let $\tilde{E}$ (resp. $\tilde{E}^*$) be the curve, defined over the residue field $\mathcal{O}_k/\mathfrak{p}$, which is obtained from the equation for E (resp. E^*). Then, for

2000 Mathematics Subject Classification. Primary 11R29; Secondary 11G05, 11G07.

a point Q on E^* whose image on $\tilde{E}^*$ is nonsingular, at least one point in $\lambda^{-1}(Q)$ is reduced into a nonsingular point on $\tilde{E}$.

In the present paper, we study the converse of the scheme described above. In Sections 2 through 4, we prove that the image of Q on $\tilde{E}^*$ is nonsingular if at least one point in $\lambda^{-1}(Q)$ is reduced into a nonsingular point on $\tilde{E}$, assuming $l \neq 2$ for simplicity (Theorem 2.2). In Section 5, we apply it to show that the sufficient condition for the extension unramified is also a necessary condition, under certain assumptions (Theorem 5.2 and Corollary 5.3). Thus, roughly speaking, the extension $k(\lambda^{-1}(Q))/k(Q)$ is unramified if and "only if" Q is reduced into a nonsingular point.

Now, taking $k = \mathbb{Q}$ and $l \in \{3, 5, 7\}$, we can construct a lot of quadratic number fields with class numbers divisible by l (see Theorem 6.1 for the case of $l = 5$). In Section 6, we study a characterization of quadratic number fields with class numbers divisible by 5. The case where $l = 5$ is particular, since the quintic polynomial which appears in our theory is closely related to Brumer's quintic polynomial, which is a generic polynomial for the dihedral group of order 10.

2. Reduction of isogenies via Vélu's formulas

In order to state the main result, we shall briefly repeat the settings in [11, Section 4]. For details, see the original paper.

Let k be a perfect field with $\operatorname{char} k \neq 2$, and let v be a non-archimedean valuation on k. We denote the valuation ring, the valuation ideal and the residue field by $\mathcal{O}_v$, $\mathfrak{p}_v$ and by κ_v, respectively. For $a \in \mathcal{O}_v$, we sometimes denote its image in κ_v by $\tilde{a}$.

Let E be an elliptic curve defined over k *which has a k-rational point T_0 of prime order $l \neq 2$*. Then we can take a Weierstrass equation for E of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

with

$$a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_v.$$

Moreover, we can take an equation so that the condition

$$x(T_0), y(T_0) \in \mathcal{O}_v$$

is also satisfied. We denote the discriminant of Equation (2.1) by Δ. We fix such an equation and consider the reduction of E modulo $\mathfrak{p}_v$. That is, let $\tilde{E} = E \bmod \mathfrak{p}_v$ be the curve defined over κ_v which is given by

$$y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6, \tag{2.2}$$

and let

$$E(k) \ni P \mapsto \tilde{P} = P \bmod \mathfrak{p}_v \in \tilde{E}(\kappa_v)$$

be the reduction of E modulo $\mathfrak{p}_v$ *with respect to* Equation (2.1). Using the reduction map, we define two subsets of $E(k)$ as

$$\mathscr{E}_0(k;\mathfrak{p}_v)=\{P\in E(k);\ \tilde{P}\in\tilde{E}_{\mathrm{ns}}(\kappa_v)\},\quad \mathscr{E}_+(k;\mathfrak{p}_v)=\{P\in E(k);\ \tilde{P}=\tilde{O}\}.$$

Here $\tilde{E}_{\mathrm{ns}}(\kappa_v)$ denotes the set of nonsingular κ_v-rational points on $\tilde{E}$. Then $\mathscr{E}_0(k;\mathfrak{p}_v)$ is a subgroup of $E(k)$, and

$$\mathscr{E}_0(k;\mathfrak{p}_v)\ni P\mapsto\tilde{P}\in\tilde{E}_{\mathrm{ns}}(\kappa_v)$$

is a group homomorphism of kernel $\mathscr{E}_+(k;\mathfrak{p}_v)$. We call $P\in E(k)$ is *good* modulo $\mathfrak{p}_v$ with respect to (2.1) if it belongs to $\mathscr{E}_0(k;\mathfrak{p}_v)$ (we often omit the phrase "modulo $\mathfrak{p}_v$ with respect to ..."). Similarly, we call $P\in E(k)$ is *bad* if it does not belong to $\mathscr{E}_0(k;\mathfrak{p}_v)$.

Let Γ be the subgroup of $E(k)$ generated by T_0, and let

$$Y^2+A_1XY+A_3Y=X^3+A_2X^2+A_4X+A_6 \tag{2.3}$$

be the equation for the elliptic curve $E^*=E/\Gamma$ and $\lambda\colon E\to E^*$ the isogeny which are given by Vélu's formulas [13] (see also [11, Section 2] or [14, Section 12.3]). Then we have

$$A_1,\ A_2,\ A_3,\ A_4,\ A_6\in\mathcal{O}_v.$$

We denote the discriminant of Equation (2.3) by Δ^*. Let $\tilde{E}^*=E^* \bmod \mathfrak{p}_v$ be the curve defined over κ_v which is given by

$$y^2+\tilde{A}_1xy+\tilde{A}_3y=x^3+\tilde{A}_2x^2+\tilde{A}_4x+\tilde{A}_6, \tag{2.4}$$

and let

$$E^*(k)\ni Q\mapsto\tilde{Q}=Q \bmod \mathfrak{p}_v\in\tilde{E}^*(\kappa_v)$$

be the reduction of E^* modulo $\mathfrak{p}_v$ with respect to (2.3). We define $\mathscr{E}_0^*(k;\mathfrak{p}_v)$, $\mathscr{E}_+^*(k;\mathfrak{p}_v)\subseteq E^*(k)$ in the same manner as for E.

In [11], the author showed that the inverse image by λ of every good point contains a good point:

Theorem 2.1 ([11, Theorem 4.5]). *If $Q\in\mathscr{E}_0^*(k;\mathfrak{p}_v)$ satisfies $\lambda^{-1}(Q)\subseteq E(k)$, we have $\lambda^{-1}(Q)\cap\mathscr{E}_0(k;\mathfrak{p}_v)\neq\emptyset$.*

The main result of the present paper is that the converse of the above theorem holds. That is, we prove the following theorem:

Theorem 2.2. *If $Q \in E^*(k)$ satisfies $\lambda^{-1}(Q) \subseteq E(k)$ and $\lambda^{-1}(Q) \cap \mathscr{E}_0(k; \mathfrak{p}_v) \neq \emptyset$, we have $Q \in \mathscr{E}_0^*(k; \mathfrak{p}_v)$.*

REMARK 2.3. We have either $\Gamma \cap \mathscr{E}_0(k; \mathfrak{p}_v) = \{O\}$ or $\Gamma \cap \mathscr{E}_0(k; \mathfrak{p}_v) = \Gamma$. In the former case, the set $\lambda^{-1}(Q) \cap \mathscr{E}_0(k; \mathfrak{p}_v)$ consists of at most one point. In the latter case, $\lambda^{-1}(Q) \cap \mathscr{E}_0(k; \mathfrak{p}_v)$ coincides with $\lambda^{-1}(Q)$ or $\emptyset$. We also have $\Gamma \cap \mathscr{E}_+(k; \mathfrak{p}_v) = \{O\}$ in both cases.

REMARK 2.4. The assertion of Theorem 2.1 holds even if $\operatorname{char} k = 2$ or if $l = 2$ (in [11, Section 4], k is arbitrary perfect field, and l is arbitrary prime number). We can also show Theorem 2.2 in these cases. However, we shall assume $\operatorname{char} k \neq 2$ and $l \neq 2$, since the proof for these cases are complicated, and we will apply the theorem only in the case where $\operatorname{char} k = 0$ and $l \neq 2$.

Before giving a proof of Theorem 2.2, we show the following (cf. [11, Remark 4.6]):

Corollary 2.5. *The curve $\tilde{E}$ is nonsingular if and only if so is the curve $\tilde{E}^*$:*

$$\Delta \equiv 0 \pmod{\mathfrak{p}_v} \iff \Delta^* \equiv 0 \pmod{\mathfrak{p}_v}.$$

Proof. As we will see in the beginning of Section 3.2, the condition $\Gamma \cap \mathscr{E}_0(k; \mathfrak{p}_v) = \{O\}$ implies that both of the curves are singular. Thus it suffices to show the assertion in the case where $\Gamma \cap \mathscr{E}_0(k; \mathfrak{p}_v) = \Gamma$. We may also replace k with its finite extension.

First, suppose $\tilde{E}$ is singular. Then we can take a point $P \in E(k) - \mathscr{E}_0(k; \mathfrak{p}_v)$ (for sufficiently large k). Thus, putting $Q = \lambda(P)$, we have $\lambda^{-1}(Q) \cap \mathscr{E}_0(k; \mathfrak{p}_v) = \emptyset$ because of the assumption $\Gamma \cap \mathscr{E}_0(k; \mathfrak{p}_v) = \Gamma$ (see Remark 2.3). Therefore we obtain $Q \notin \mathscr{E}_0^*(k; \mathfrak{p}_v)$ by Theorem 2.1, and hence $\tilde{E}^*$ is also singular.

Conversely, suppose $\tilde{E}^*$ is singular. Then we can take a point $Q \in E^*(k) - \mathscr{E}_0^*(k; \mathfrak{p}_v)$ such that $\lambda^{-1}(Q) \subseteq E(k)$ (for sufficiently large k). Therefore we obtain $\lambda^{-1}(Q) \cap \mathscr{E}_0(k; \mathfrak{p}_v) = \emptyset$ by Theorem 2.2, and hence $\tilde{E}$ is also singular. □

3. Proof of Theorem 2.2 (Part I)

3.1. Relations among X, Y and x, y. In what follows, for a function f and a point P on E, we often denote the value $f(P)$ by f_P. We also denote $F(Q)$ by F_Q for a function F and a point Q on E^*. Now we recall that the isogeny $\lambda : E \to E^*$ is given by

$$X = \frac{I(x)}{J_0(x)^2}, \quad Y = \frac{I_0(x) + I_1(x)y}{J_0(x)^3} \tag{3.1}$$

with polynomials

$$I(x) = x^l - 2\left(\sum_{T\in\Gamma_0} x_T\right)x^{l-1} + \cdots, \quad I_0(x), \quad I_1(x)$$

and

$$J_0(x) = \prod_{T\in\Gamma_0}(x - x_T) = x^{(l-1)/2} - \left(\sum_{T\in\Gamma_0} x_T\right)x^{(l-3)/2} + \cdots$$

in x, where $\Gamma_0 \subseteq \Gamma$ is a perfect representatives for $(\Gamma - \{O\})/\pm 1$ (see [11, Section 3.2]). We note that all the coefficients of these polynomials are in $\mathcal{O}_v$, and that $I(x)$ and $J_0(x)$ do not have any common root. We define $g^x, g^y \in k(E)$ and $G^X, G^Y \in k(E^*)$ by

$$g^x = 3x^2 + 2a_2x + a_4 - a_1y, \quad g^y = -2y - a_1x - a_3$$

and by

$$G^X = 3X^2 + 2A_2X + A_4 - A_1Y, \quad G^Y = -2Y - A_1X - A_3,$$

respectively. In the proof which we will describe, the formula

$$X_Q + \sum_{T\in\Gamma-\{O\}} x_T = \sum_{P\in\lambda^{-1}(Q)} x_P \tag{3.2}$$

(see [11, Remark 2.1]) and the formulas

$$G^X_Q = m_P g^x_P + n_P (g^y_P)^2, \quad G^Y_Q = m_P g^y_P \tag{3.3}$$

for $P \in \lambda^{-1}(Q)$ (see [11, Section 3.1]) play important roles. Here we define $m, n \in k(E)$ by

$$m = 1 - \sum_{T\in\Gamma_0}\left(\frac{2g^x_T - a_1 g^y_T}{(x-x_T)^2} + \frac{2(g^y_T)^2}{(x-x_T)^3}\right), \quad n = \sum_{T\in\Gamma_0}\left(\frac{2g^x_T - a_1 g^y_T}{(x-x_T)^3} + \frac{3(g^y_T)^2}{(x-x_T)^4}\right).$$

3.2. The case $\Gamma \cap \mathscr{E}_0(k; \mathfrak{p}_v) = \{O\}$. We first consider the case $\Gamma \cap \mathscr{E}_0(k; \mathfrak{p}_v) = \{O\}$, i.e., the case where every $T \in \Gamma - \{O\}$ is bad. In this case, we have

$$A_1 = a_1, \quad A_2 = a_2, \quad A_3 = a_3, \quad A_4 \equiv a_4 \pmod{\mathfrak{p}_v}, \quad A_6 \equiv a_6 \pmod{\mathfrak{p}_v}$$

(see [11, Proof of Theorem 4.5]). Thus Equation (2.4) for $\tilde{E}^*$ coincides with Equation (2.2) for $\tilde{E}$. Consequently, we obtain

$$\Delta \equiv \Delta^* \equiv 0 \pmod{\mathfrak{p}_v}.$$

Since all $T \in \Gamma - \{O\}$ are bad points, writing α the x-coordinate of the (unique) singular point on $\tilde{E}$, we have $\tilde{x}_T = \alpha$ for all $T \in \Gamma - \{O\}$. We recall that the set $\lambda^{-1}(Q) \cap \mathscr{E}_0(k; \mathfrak{p}_v)$ consists of at most one point, as mentioned in Remark 2.3.

Proposition 3.1. *If $Q \in E^*(k)$ satisfies $\lambda^{-1}(Q) \subseteq E(k)$ and $\lambda^{-1}(Q) \cap \mathscr{E}_0(k; \mathfrak{p}_v) = \{P\}$, we have $Q \in \mathscr{E}_0^*(k; \mathfrak{p}_v)$.*

Proof. Assume $Q \neq O$ and $\lambda^{-1}(Q) \cap \mathscr{E}_0(k; \mathfrak{p}_v) = \{P\}$ (the assertion is clear if $Q = O$). Then every $P' \in \lambda^{-1}(Q) - \{P\}$ is bad, and hence satisfies $\tilde{x}_{P'} = \alpha$. Therefore

$$X_Q - x_P = \sum_{P' \in \lambda^{-1}(Q) - \{P\}} x_{P'} - \sum_{T \in \Gamma - \{O\}} x_T$$

(see (3.2)) belongs to $\mathfrak{p}_v$. Consequently, if $x_P \in \mathcal{O}_v$, we have $X_Q \in \mathcal{O}_v$ and $x_P \equiv X_Q \pmod{\mathfrak{p}_v}$, which imply $Q \in \mathscr{E}_0^*(k; \mathfrak{p}_v) - \mathscr{E}_+^*(k; \mathfrak{p}_v)$. If $x_P \notin \mathcal{O}_v$, we have $X_Q \notin \mathcal{O}_v$, and hence $Q \in \mathscr{E}_+^*(k; \mathfrak{p}_v)$. In both cases, we conclude $Q \in \mathscr{E}_0^*(k; \mathfrak{p}_v)$. □

3.3. The case $\Gamma \cap \mathscr{E}_0(k; \mathfrak{p}_v) = \Gamma$. We next consider the case $\Gamma \cap \mathscr{E}_0(k; \mathfrak{p}_v) = \Gamma$, i.e., the case where every $T \in \Gamma$ is good. In this case, the set $\lambda^{-1}(Q) \cap \mathscr{E}_0(k; \mathfrak{p}_v)$ coincides with $\lambda^{-1}(Q)$ or $\emptyset$, as mentioned in Remark 2.3.

Proposition 3.2. *If $Q \in E^*(k)$ satisfies $\lambda^{-1}(Q) \subseteq E(k)$ and $\lambda^{-1}(Q) \cap \mathscr{E}_0(k; \mathfrak{p}_v) = \lambda^{-1}(Q)$, we have $Q \in \mathscr{E}_0^*(k; \mathfrak{p}_v)$.*

In order to prove the above proposition, we need the following lemma, which we will show in the next section:

Lemma 3.3. *Assume $\Gamma \subseteq \mathscr{E}_0(k; \mathfrak{p}_v)$ and $\Delta^* \equiv 0 \pmod{\mathfrak{p}_v}$. If $P \in \mathscr{E}_0(k; \mathfrak{p}_v) - \mathscr{E}_+(k; \mathfrak{p}_v)$ satisfies $x_P \not\equiv x_T \pmod{\mathfrak{p}_v}$ for all $T \in \Gamma - \{O\}$, we have either $m_P \in \mathcal{O}_v^\times$ or $n_P g_P^y \in \mathcal{O}_v^\times$.*

REMARK 3.4. In the above lemma, it immediately follows from the assumptions that

$$x_P, y_P, g_P^x, g_P^y, m_P, n_P \in \mathcal{O}_v.$$

Hence we may write the assertion as "$m_P \not\equiv 0 \pmod{\mathfrak{p}_v}$ or $n_P g_P^y \not\equiv 0 \pmod{\mathfrak{p}_v}$."

Using Lemma 3.3, we can prove Proposition 3.2 as follows:

Proof of Proposition 3.2. Since the assertion is clear if $Q = O$ or if $\Delta^* \not\equiv 0 \pmod{\mathfrak{p}_v}$, we assume $\Gamma \subseteq \mathscr{E}_0(k; \mathfrak{p}_v)$, $Q \neq O$ and $\Delta^* \equiv 0 \pmod{\mathfrak{p}_v}$.

(i) Suppose $\tilde{P} = \tilde{T}$ holds for some $P \in \lambda^{-1}(Q)$ and $T \in \Gamma$. Then we have $\widetilde{P+T'} = \widetilde{T+T'}$ for each $T' \in \Gamma$, and hence

$$\{\tilde{P};\ P \in \lambda^{-1}(Q)\} = \{\tilde{T};\ T \in \Gamma\}.$$

In particular, we have $\tilde{P} = \tilde{O}$ for some $P \in \lambda^{-1}(Q)$, and such a point P is uniquely determined. Therefore

$$X_Q - x_P = \sum_{P' \in \lambda^{-1}(Q)-\{P\}} x_{P'} - \sum_{T \in \Gamma - \{O\}} x_T$$

(see (3.2)) belongs to $\mathfrak{p}_v$, and we obtain $X_Q \notin \mathcal{O}_v$, for $x_P \notin \mathcal{O}_v$. Thus we conclude $Q \in \mathscr{E}_+^*(k;\mathfrak{p}_v)$.

(ii) Suppose $\tilde{P} = \tilde{T}$ does not hold for any $P \in \lambda^{-1}(Q)$ and $T \in \Gamma$. Let P be a point in $\lambda^{-1}(Q)$. Then clearly $P \in \mathscr{E}_0(k;\mathfrak{p}_v) - \mathscr{E}_+(k;\mathfrak{p}_v)$, and it is easy to verify that $x_P \not\equiv x_T \pmod{\mathfrak{p}_v}$ hold for all $T \in \Gamma - \{O\}$. Hence we have $X_Q, Y_Q \in \mathcal{O}_v$ by (3.1). Now suppose $Q \notin \mathscr{E}_0^*(k;\mathfrak{p}_v)$, which means $G_Q^X \equiv G_Q^Y \equiv 0 \pmod{\mathfrak{p}_v}$. Then it follows from (3.3) that

$$m_P g_P^x + n_P (g_P^y)^2 \equiv m_P g_P^y \equiv 0 \pmod{\mathfrak{p}_v}.$$

However, by Lemma 3.3, we also have either $m_P \in \mathcal{O}_v^\times$ or $n_P g_P^y \in \mathcal{O}_v^\times$. Therefore we must have ($m_P \in \mathcal{O}_v^\times$ and) $g_P^x \equiv g_P^y \equiv 0 \pmod{\mathfrak{p}_v}$, which contradicts $P \in \mathscr{E}_0(k;\mathfrak{p}_v)$. Thus we conclude $Q \in \mathscr{E}_0^*(k;\mathfrak{p}_v) - \mathscr{E}_+^*(k;\mathfrak{p}_v)$. □

4. Proof of Theorem 2.2 (Part II)

In order to complete the proof of Theorem 2.2, we have to show Lemma 3.3. In the present section, we assume $\Gamma \subseteq \mathscr{E}_0(k;\mathfrak{p}_v)$ and $\Delta^* \equiv 0 \pmod{\mathfrak{p}_v}$, fix a point $P \in \mathscr{E}_0(k;\mathfrak{p}_v) - \mathscr{E}_+(k;\mathfrak{p}_v)$ which satisfies $x_P \not\equiv x_T \pmod{\mathfrak{p}_v}$ for all $T \in \Gamma - \{O\}$, and show that either $m_P \not\equiv 0 \pmod{\mathfrak{p}_v}$ or $n_P g_P^y \not\equiv 0 \pmod{\mathfrak{p}_v}$ holds ($x_P, y_P, g_P^x, g_P^y, m_P, n_P \in \mathcal{O}_v$ are immediate, as mentioned in Remark 3.4). Since we may replace k with its finite extension without loss of generality, we assume $E[2] \subseteq E(k)$. The group $E[2]$ consists of 4 points, and hence the order of its subgroup, such as $E[2] \cap \mathscr{E}_0(k;\mathfrak{p}_v)$ and $E[2] \cap \mathscr{E}_+(k;\mathfrak{p}_v)$, is 1, 2 or 4.

4.1. Relations among *m, n* and *x*.

Putting

$$M(x) = I'(x)J_0(x) - 2I(x)J_0'(x) = x^{(3l-3)/2} - 3\left(\sum_{T \in \Gamma_0} x_T\right) x^{(3l-5)/2} + \cdots,$$

$$N(x) = M'(x)J_0(x) - 3M(x)J_0'(x),$$

we can rewrite m, n as

$$m = \frac{M(x)}{J_0(x)^3}, \quad n = \frac{N(x)}{2J_0(x)^4}.$$

We note that all the coefficients of $M(x)$ and $N(x)$ are in $\mathcal{O}_v$, and that $M(x)$ and $J_0(x)$ do not have any common root. In the proof of Lemma 3.3 which we will describe, we shall compare the reduction of $M(x)$ and $J_0(x)$. We denote by $\tilde{M}(x)$ and $\tilde{J}_0(x)$ their reductions modulo $\mathfrak{p}_v$.

Now we recall that the points of order 2 on E and E^* are the zeros of g^y and G^Y, respectively:

$$E[2]-\{O\} = \{T \in E(k)-\{O\};\ g_T^y = 0\},$$
$$E^*[2]-\{O\} = \{U \in E^*(k)-\{O\};\ G_U^Y = 0\}.$$

Thus it follows from $\lambda^{-1}(E^*[2]) = E[2]+\Gamma$ that each $T \in (E[2]-\{O\})+(\Gamma-\{O\})$ satisfies $g_T^y \neq 0$ and $G_{\lambda(T)}^Y = 0$. Since such T also satisfies $J_0(x_T) \neq 0$, we have

$$0 = G_{\lambda(T)}^Y = m_T g_T^y = \frac{M(x_T)}{J_0(x_T)^3} g_T^y$$

(see (3.3)), and hence $M(x_T) = 0$. Consequently we obtain

$$M(x) = \prod_{T \in (E[2]-\{O\})+\Gamma_0} (x - x_T),$$

for the set $(E[2]-\{O\})+\Gamma_0$ consists of $(3l-3)/2$ points.

4.2. The case $\mathrm{char}\,\kappa_v \neq 2$. If the characteristic of κ_v is not 2, one easily verifies $E[2] \cap \mathscr{E}_+(k;\mathfrak{p}_v) = \{O\}$. Thus we consider according to the order of $E[2] \cap \mathscr{E}_0(k;\mathfrak{p}_v)$, and obtain:

Lemma 4.1. *Let the notation and the assumptions be the same as in* Lemma 3.3. *We also assume* $E[2] \subseteq E(k)$ *and* $\mathrm{char}\,\kappa_v \neq 2$. *Then*:
(i) *If* $E[2] \cap \mathscr{E}_0(k;\mathfrak{p}_v) = \{O\}$, *we have* $m_P \not\equiv 0 \pmod{\mathfrak{p}_v}$.
(ii) *If* $E[2] \cap \mathscr{E}_0(k;\mathfrak{p}_v) \neq \{O\}$ *and if* $m_P \equiv 0 \pmod{\mathfrak{p}_v}$, *we have* $n_P g_P^y \not\equiv 0 \pmod{\mathfrak{p}_v}$.

Proof. We first claim that the assumptions imply $(E[2]+\Gamma) \cap \mathscr{E}_+(k;\mathfrak{p}_v) = \{O\}$. Indeed, if $T \in E[2]$ and $T' \in \Gamma$ satisfy $T+T' \in \mathscr{E}_+(k;\mathfrak{p}_v)$, we have

$$T = [l]T = [l](T+T') \in \mathscr{E}_+(k;\mathfrak{p}_v),$$

and hence $T = T' = O$ because of $E[2] \cap \mathscr{E}_+(k;\mathfrak{p}_v) = \{O\}$ and $\Gamma \cap \mathscr{E}_+(k;\mathfrak{p}_v) = \{O\}$ (see Remark 2.3).

It follows from the claim that the reduction map

$$(E[2]+\Gamma) \cap \mathscr{E}_0(k;\mathfrak{p}_v) \ni T \mapsto \tilde{T} \in \tilde{E}_{\mathrm{ns}}(\kappa_v)$$

is an injective group homomorphism. Therefore, for good points T and T' in $(E[2]+\Gamma)-\{O\}$, we have

$$x_T \equiv x_{T'} \pmod{\mathfrak{p}_v} \iff T = \pm T'.$$

In what follows, we denote by α the x-coordinate of the singular point on $\tilde{E}$ if $\Delta \equiv 0 \pmod{\mathfrak{p}_v}$. Then clearly $\tilde{x}_P \neq \alpha$.

(i) Assume $E[2] \cap \mathscr{E}_0(k;\mathfrak{p}_v) = \{O\}$. Then each $T \in E[2]-\{O\}$ is bad, and $T+\Gamma$ consists only of bad points. Thus we have

$$\tilde{M}(x) = (x-\alpha)^{(3l-3)/2},$$

and hence

$$m_P = \frac{M(x_P)}{J_0(x_P)^3} \not\equiv 0 \pmod{\mathfrak{p}_v}.$$

(ii)$'$ Assume $E[2] \cap \mathscr{E}_0(k;\mathfrak{p}_v) = \{O, T_1\}$ $(T_1 \neq O)$ and $m_P \equiv 0 \pmod{\mathfrak{p}_v}$. Then we can show

$$\tilde{M}(x) = (x-\alpha)^{l-1} \prod_{T \in T_1+\Gamma_0} (x-\tilde{x}_T), \quad \tilde{x}_T \neq \alpha \quad \text{for} \quad T \in T_1+\Gamma_0$$

in the same manner as in (i). We also have $\tilde{x}_T \neq \tilde{x}_{T'}$ for distinct points T and T' in $(T_1+\Gamma_0)\cup\{T_1\}$. Since $m_P \equiv 0 \pmod{\mathfrak{p}_v}$, there exists (unique) $T \in T_1+\Gamma_0$ which satisfies $\tilde{x}_P = \tilde{x}_T$, and then $M'(x_P) \not\equiv 0 \pmod{\mathfrak{p}_v}$. Thus we have

$$N(x_P) = M'(x_P)J_0(x_P) - 3M(x_P)J_0'(x_P) \equiv M'(x_P)J_0(x_P) \not\equiv 0 \pmod{\mathfrak{p}_v},$$

and hence

$$n_P = \frac{N(x_P)}{2J_0(x_P)^4} \not\equiv 0 \pmod{\mathfrak{p}_v}.$$

Furthermore, it immediately follows from $\tilde{x}_T \neq \alpha$ and $\tilde{x}_T \neq \tilde{x}_{T_1}$ that $g_P^y \not\equiv 0 \pmod{\mathfrak{p}_v}$.

(ii)$''$ Assume $E[2] \cap \mathscr{E}_0(k;\mathfrak{p}_v) = E[2]$ and $m_P \equiv 0 \pmod{\mathfrak{p}_v}$. Then we have $E[2]+\Gamma \subseteq \mathscr{E}_0(k;\mathfrak{p}_v)$, and hence $\tilde{x}_T \neq \tilde{x}_{T'}$ for distinct points T and T' in $(E[2]+\Gamma_0)\cup(E[2]-\{O\})$. Thus we can show $n_P \not\equiv 0 \pmod{\mathfrak{p}_v}$ and $g_P^y \not\equiv 0 \pmod{\mathfrak{p}_v}$ in the same manner as in (ii)$'$. □

4.3. The case $\mathrm{char}\,\kappa_v = 2$. If the characteristic of κ_v is 2, it is not hard to verify

$$(a_1^2 g_T^x)^2 \equiv \Delta \pmod{\mathfrak{p}_v} \quad \text{for} \quad T \in E[2]-\mathscr{E}_+(k;\mathfrak{p}_v). \tag{4.1}$$

Indeed, since $T \in E[2]-\mathscr{E}_+(k;\mathfrak{p}_v)$ satisfies $g_T^y = 0$, we have

$$a_1 x_T \equiv a_3 \pmod{\mathfrak{p}_v}, \quad a_1^3 y_T^2 \equiv a_3^3 + a_1 a_2 a_3^2 + a_1^2 a_3 a_4 + a_1^3 a_6 \pmod{\mathfrak{p}_v},$$

and hence

$$\begin{aligned}\left(a_1^2 g_T^x\right)^2 &\equiv a_1^4(x_T^4 + a_4^2 + a_1^2 y_T^2) \equiv a_3^4 + a_1^4 a_4^2 + a_1^3(a_3^3 + a_1 a_2 a_3^2 + a_1^2 a_3 a_4 + a_1^3 a_6) \\ &\equiv \Delta \pmod{\mathfrak{p}_v}.\end{aligned}$$

We also have

$$(a_1^2 G_U^X)^2 \equiv \Delta^* \pmod{\mathfrak{p}_v} \quad \text{for} \quad U \in E^*[2] - \mathscr{E}_+^*(k; \mathfrak{p}_v), \tag{4.2}$$

for $A_1 = a_1$. We consider according as a_1 belongs to $\mathfrak{p}_v$ or not, and obtain:

Lemma 4.2. *Let the notation and the assumptions be the same as in* Lemma 3.3. *We also assume* $E[2] \subseteq E(k)$ *and* $\operatorname{char} \kappa_v = 2$. *Then we have* $m_P \not\equiv 0 \pmod{\mathfrak{p}_v}$.

Proof. (i) Assume $a_1 \equiv 0 \pmod{\mathfrak{p}_v}$. Then it follows from $\operatorname{char} \kappa_v = 2$ that

$$m_P = 1 - \sum_{T \in \Gamma_0} \left(\frac{2 g_T^x - a_1 g_T^y}{(x_P - x_T)^2} + \frac{2 (g_T^y)^2}{(x_P - x_T)^3} \right) \equiv 1 \pmod{\mathfrak{p}_v}.$$

(ii) Assume $a_1 \not\equiv 0 \pmod{\mathfrak{p}_v}$ and $\Delta \equiv 0 \pmod{\mathfrak{p}_v}$. Then, for each $T \in E[2] - \mathscr{E}_+(k; \mathfrak{p}_v)$, we have $g_T^x \equiv 0 \pmod{\mathfrak{p}_v}$ by (4.1). Since such T also satisfies $g_T^y = 0$, we have $T \notin \mathscr{E}_0(k; \mathfrak{p}_v)$, and conclude $E[2] \cap \mathscr{E}_0(k; \mathfrak{p}_v) = E[2] \cap \mathscr{E}_+(k; \mathfrak{p}_v)$. Hence, putting $e = \#(E[2] \cap \mathscr{E}_+(k; \mathfrak{p}_v))$, we obtain

$$\tilde{M}(x) = \tilde{J}_0(x)^{e-1} (x - \alpha)^{(4-e)(l-1)/2},$$

where α denotes the x-coordinate of the singular point on $\tilde{E}$. Thus we can show $m_P \not\equiv 0 \pmod{\mathfrak{p}_v}$ in the same manner as in the proof of Lemma 4.1.

(iii) Assume $a_1 \not\equiv 0 \pmod{\mathfrak{p}_v}$ and $\Delta \not\equiv 0 \pmod{\mathfrak{p}_v}$. Then the reduction map

$$E[2] + \Gamma \ni T \mapsto \tilde{T} \in \tilde{E}(\kappa_v)$$

is a group homomorphism of kernel $E[2] \cap \mathscr{E}_+(k; \mathfrak{p}_v)$. Now we claim $E[2] \subseteq \mathscr{E}_+(k; \mathfrak{p}_v)$. In fact, if this is not the case, taking a point $T_1 \in E[2] - \mathscr{E}_+(k; \mathfrak{p}_v)$, we can show

$$x_{T_1} \not\equiv x_T \pmod{\mathfrak{p}_v} \quad \text{for} \quad T \in \Gamma - \{O\},$$

and hence $\lambda(T_1) \in E^*[2] - \mathscr{E}_+^*(k; \mathfrak{p}_v)$. Thus it follows from (3.3), (4.1), (4.2) and $g_{T_1}^y = 0$ that

$$\Delta^* \equiv (a_1^2 G_{\lambda(T_1)}^X)^2 \equiv (a_1^2 m_{T_1} g_{T_1}^x)^2 \equiv m_{T_1}^2 (a_1^2 g_{T_1}^x)^2 \equiv m_{T_1}^2 \Delta \pmod{\mathfrak{p}_v}.$$

However, it is not hard to show $m_{T_1} = M(x_{T_1})/J_0(x_{T_1})^3 \not\equiv 0 \pmod{\mathfrak{p}_v}$. Therefore we have $\Delta^* \not\equiv 0 \pmod{\mathfrak{p}_v}$, which contradicts the assumptions. Consequently we obtain $E[2] \subseteq \mathscr{E}_+(k; \mathfrak{p}_v)$, which implies

$$\tilde{M}(x) = \tilde{J}_0(x)^3.$$

Hence we conclude $m_P \not\equiv 0 \pmod{\mathfrak{p}_v}$. □

5. Application to number theory

From now on, k denotes a number field of finite degree, and we denote its ring of integers by $\mathcal{O}_k$.

Let E be an elliptic curve defined over k *which has a* k*-rational point* T_0 *of prime order* $l \neq 2$. Then we can take a Weierstrass equation for E of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with

$$a_1, a_2, a_3, a_4, a_6, x_{T_0}, y_{T_0} \in \mathcal{O}_k.$$

Let

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6 \tag{5.1}$$

be the equation for the elliptic curve $E^* = E/\langle T_0 \rangle$ and $\lambda\colon E \to E^*$ the isogeny of kernel $\langle T_0 \rangle$ which are given by Vélu's formulas. Then we have

$$A_1, A_2, A_3, A_4, A_6 \in \mathcal{O}_k.$$

We also note that all the coefficients of the polynomials $I(x)$ and $J_0(x)$, defined in Section 3.1, are in $\mathcal{O}_k$. We define a cubic polynomial $F(X)$ and a polynomial $\Lambda_t(x)$ of degree l (with a parameter t) by

$$F(X) = 4X^3 + (A_1^2 + 4A_2)X^2 + 2(A_1A_3 + 2A_4)X + A_3^2 + 4A_6$$

and by

$$\Lambda_t(x) = I(x) - tJ_0(x)^2,$$

respectively.

Now we take $\xi \in k$ which satisfies the following two conditions:
(C0) $F(\xi) \neq 0$.
(C1) $\Lambda_\xi(x)$ is irreducible over k.

We also take a point Q on E^* with $X_Q = \xi$, and put

$$K = k(Q)\ (= k(\sqrt{F(\xi)})), \quad L = k(\lambda^{-1}(Q))\ (= K(\lambda^{-1}(Q))).$$

Then L/K is a cyclic extension of degree l, and L is the splitting field of $\Lambda_\xi(x)$ over K (see [11, Lemma 5.5]). Moreover we have

$$\Lambda_\xi(x) = \prod_{P \in \lambda^{-1}(Q)} (x - x_P). \tag{5.2}$$

With the notation and the assumptions described above, the author showed in [11] that the extension L/K is unramified if the point Q is good:

Theorem 5.1 (See [11, Theorem 5.1]). *Suppose that the point Q is good modulo $\mathfrak{P}$ with respect to* (5.1) *for a prime ideal $\mathfrak{P}$ in K. Then the extension L/K is unramified at $\mathfrak{P}$.*

Conversely, we can easily show the following theorem by using Theorem 2.2:

Theorem 5.2. *Suppose that the point Q is bad modulo $\mathfrak{P}$ with respect to* (5.1) *for a prime ideal $\mathfrak{P}$ in K. Then all the coefficients of the polynomial $\Lambda_\xi(x)$ are $\mathfrak{p}$-integral, and we have*

$$\Lambda_\xi(x) \equiv (x - a)^l \pmod{\mathfrak{p}}$$

for some $a \in \mathcal{O}_k$. Here $\mathfrak{p}$ denotes the prime ideal in k lying below $\mathfrak{P}$.

Proof. Suppose that Q is a bad point modulo $\mathfrak{P}$. Then $\xi = X_Q$ is a $\mathfrak{p}$-integer, and it follows from Theorem 2.2 that all the points in $\lambda^{-1}(Q)$ are bad (modulo each prime divisor of $\mathfrak{P}$ in L). Thus, writing α the x-coordinate of the (unique) singular point on $\tilde{E} = E \bmod \mathfrak{p}$, we have $\tilde{x}_P = \alpha$ for all $P \in \lambda^{-1}(Q)$, which implies $\tilde{\Lambda}_\xi(x) = (x - \alpha)^l$ (see (5.2)). Hence, taking $a \in \mathcal{O}_k$ such that $\tilde{a} = \alpha$, we have $\Lambda_\xi(x) \equiv (x - a)^l \pmod{\mathfrak{p}}$. □

Theorem 5.2 does not assert that the converse of Theorem 5.1 holds. In fact, the converse does not necessarily hold (see Example 6.7). However, under certain assumptions, we can show the converse of Theorem 5.1:

Corollary 5.3. *Let the notation and the assumptions be the same as in* Theorem 5.2. *We also assume $\xi \in \mathcal{O}_k$ and $[\mathcal{O}_{k(\theta)} : \mathcal{O}_k[\theta]] \not\equiv 0 \pmod{\mathfrak{p}}$. Here θ is a root of $\Lambda_\xi(x)$, and $\mathcal{O}_{k(\theta)}$ denotes the ring of integers of $k(\theta)$. Then the extension L/K is ramified at $\mathfrak{P}$.*

Proof. It follows from the assumptions and Theorem 5.2 that $\mathfrak{p}$ is decomposed into the form $\mathfrak{p} = (\mathfrak{p}, \theta - a)^l$ in $k(\theta)$ (see, e.g., [1, Proposition 2.3.9]). Hence we obtain the assertion because of $[L : K] = l$ and $[K : k] \leq 2$. □

We recall that the extension K/k is trivial, i.e., $K = k$, or quadratic according as $\sqrt{F(\xi)} \in k$ holds or not. In the latter case, we have the following:

Proposition 5.4. *Suppose that the extension K/k is quadratic. Then L/k is a dihedral extension of degree $2l$, and L is the splitting field of $\Lambda_\xi(x)$ over k.*

Proof. Let P be a point in $\lambda^{-1}(Q)$. Then we have $L = k(P)$, for $\langle T_0 \rangle \subseteq E(k)$. Moreover, for any $\sigma \in \mathrm{Gal}(\bar{k}/k)$, there exists $(i_\sigma, j_\sigma) \in (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/l\mathbb{Z})$ such that

$$Q^\sigma = [(-1)^{i_\sigma}]Q, \quad P^\sigma = [(-1)^{i_\sigma}]P + [j_\sigma]T_0.$$

The pair (i_σ, j_σ) is uniquely determined by σ, and the map $\sigma \mapsto (i_\sigma, j_\sigma)$ satisfies

$$i_{\sigma\tau} = i_\sigma + i_\tau, \quad j_{\sigma\tau} = j_\sigma + (-1)^{i_\sigma} j_\tau.$$

Thus we obtain the former assertion. The latter assertion immediately follows from the former one. □

It follows from the above proposition that the multiple $[i]Q$, where i is an integer not divisible by l, has the same properties as Q:

Corollary 5.5. *Let the notation and the assumptions be the same as in* Proposition 5.4. *We take an integer i not divisible by l, and put*

$$Q' = [i]Q, \quad \xi' = X_{Q'}.$$

Then we have $\xi' \in k$, $k(Q') = K$ and $k(\lambda^{-1}(Q')) = L$. Moreover, ξ' satisfies the two conditions (C0) *and* (C1), *replaced ξ with ξ'.*

Proof. The first assertion $\xi' \in k$ is obvious. We put $K' = k(Q')$ and $L' = k(\lambda^{-1}(Q'))$. Then we have $K' = k(\sqrt{F(\xi')}) \subseteq K$ and $L' \subseteq L$. Now the extension L'/K' is trivial or cyclic of degree l according as $Q' \in \lambda(E(K'))$ holds or not. However, taking the integers j, j' such that $ij + lj' = 1$, we obtain

$$Q = [ij]Q + [lj']Q \in [j]Q' + \lambda(E(K)),$$

since we have $[l]E^*(K) \subseteq \lambda(E(K))$. Thus, if L'/K' is trivial, we obtain

$$Q \in \lambda(E(K')) + \lambda(E(K)) = \lambda(E(K)),$$

which contradicts $[L : K] = l$. Hence L'/K' is cyclic of degree l, which implies $K' = K$ and $L' = L$, for L/K is dihedral of degree $2l$. The rest of the assertions are immediate. □

6. Quadratic number fields with class numbers divisible by 5

For nonzero integers a and b, the elliptic curve E defined by

$$y^2 + (a+b)xy + ab^2y = x^3 + abx^2$$

has a rational point $T_0 = (0, 0)$ of order 5. Then $\lambda : E \to E^* = E/\langle T_0 \rangle$ is given by

$$\begin{aligned} Y^2 + (a+b)XY + ab^2Y = X^3 + abX^2 + 5ab(a^2 - 2ab - b^2)X \\ + ab(a^4 - 10a^3b - 5a^2b^2 - 15ab^3 - b^4), \end{aligned}$$

which has $\Delta^* = -ab(a^2 + 11ab - b^2)^5$, with

$$\begin{aligned} I(x) &= x^5 + 2abx^4 - ab(a^2 - 3ab - b^2)x^3 + 3a^2b^3(a+b)x^2 + a^3b^4(a+3b)x + a^4b^6, \\ J_0(x) &= x^2 + abx. \end{aligned}$$

Consequently, putting

$$\begin{aligned} F(a, b; X) = 4X^3 + (a^2 + 6ab + b^2)X^2 + 2ab(10a^2 - 19ab - 9b^2)X \\ + ab(4a^4 - 40a^3b - 20a^2b^2 - 59ab^3 - 4b^4) \end{aligned}$$

and

$$\begin{aligned} &\Lambda(a, b, t; x) \\ &= x^5 + 2abx^4 - ab(a^2 - 3ab - b^2)x^3 + 3a^2b^3(a+b)x^2 + a^3b^4(a+3b)x + a^4b^6 \\ &\quad - t(x^4 + 2abx^3 + a^2b^2x^2), \end{aligned}$$

we have:

Theorem 6.1 (See [11, Theorem 5.1]). *Let ξ be a rational number which satisfies the following two conditions*:
(C1) *$\Lambda(a, b, \xi; x)$ is irreducible over $\mathbb{Q}$.*
(C2) *For any prime divisor p of $ab(a^2 + 11ab - b^2)$,*

$$\begin{cases} \min\{\operatorname{ord}_p F(a, b; \xi), \operatorname{ord}_p F'(a, b; \xi)\} \le 0 & (\text{if } p \ne 2), \\ \operatorname{ord}_2 \xi \le 0 & (\text{if } p = 2). \end{cases} \tag{6.1}$$

Then the field $\mathbb{Q}(\sqrt{F(a, b; \xi)})$ is quadratic with class number divisible by 5.

REMARK 6.2. (i) The condition (C1) implies $ab \neq 0$ and $F(a,b;\xi) \neq 0$. Indeed, we have $\Lambda(a, b, \xi; x) = x^4(x - \xi)$ if $ab = 0$, and the discriminant of $\Lambda(a, b, \xi; x)$ is equal to $a^{14}b^{14}F(a, b; \xi)^2$.
(ii) The condition (6.1) means that the point Q on E^* with $X_Q = \xi$ is good modulo p.

Using Theorem 6.1, we can easily construct a lot of quadratic number fields with class numbers divisible by 5 (cf. [9]). We close the present paper with studying the "converse" of the theorem:

QUESTION 6.3. For a quadratic number field with class number divisible by 5, can we express the field as $\mathbb{Q}(\sqrt{F(a, b; \xi)})$ with some integers a, b and some rational number ξ satisfying the conditions (C1) and (C2)?

A numerical experiment with PARI/GP [7] shows:

EXAMPLE 6.4. There are 687 quadratic number fields K which satisfy $|d_K| \leq 10000$ and $5 \mid h_K$. Here d_K and h_K denote the discriminant and the class number of K, respectively. We can express all of them with a, b and ξ satisfying the conditions (C1), (C2) and

$$|a| \leq 100, \quad |b| \leq 100, \quad |(\text{numerator of } \xi) \cdot (\text{denominator of } \xi)| \leq 10000,$$

except $K = \mathbb{Q}(\sqrt{-2290})$. We can also express $\mathbb{Q}(\sqrt{-2290})$ with much larger parameters, which are obtained with the help of Professor Yuichi Rikuna [8].

If we ignore the condition (C2), it is not hard to obtain a positive answer:

Theorem 6.5. *Let K be a quadratic number field with class number divisible by* 5. *Then there exist nonzero integers a, b and a rational number ξ, satisfying the condition* (C1), *such that $K = \mathbb{Q}(\sqrt{F(a, b; \xi)})$.*

In order to show the above theorem, we introduce Brumer's quintic polynomial

$$B(s, u; z) = z^5 + (s - 3)z^4 + (u - s + 3)z^3 + (s^2 - s - 2u - 1)z^2 + uz + s,$$

which has the following property:

Lemma 6.6 (See, e.g., [4, Theorem 2.3.5] or [6, Théorème 2.1]). *Let k be an arbitrary field, and let L/k be a dihedral extension of degree* 10. *Then L is the splitting field of $B(s, u; z)$ over k for some $s, u \in k$.*

With a similar calculation to the one in [6, Section 2], we can verify that $B(s,u;z)$ is connected with $\Lambda(a, b, t; x)$ via the following formula:

$$B(s, u; z) = \frac{z^5}{s^4}\Lambda\left(-s, 1, -2s-u; \frac{s}{z}\right).$$

Proof of Theorem 6.5. Let K be a quadratic number field with class number divisible by 5. Then it follows from the class field theory that there exists a unramified cyclic extension L/K of degree 5, and that $L/\mathbb{Q}$ is a dihedral extension of degree 10 (see, e.g., [2, Lemma 3]). Hence L is the splitting field of $B(s, u; z)$ over $\mathbb{Q}$ for some $s,u \in \mathbb{Q}$. Then clearly $s \neq 0$. Thus, taking (nonzero) integers a,b and a rational number ξ with

$$-s = \frac{a}{b}, \quad -2s-u = \frac{\xi}{b^2},$$

we have

$$B(s, u; z) = \frac{z^5}{a^4b^6}\Lambda\left(a, b, \xi; -\frac{ab}{z}\right).$$

Consequently, L is also the splitting field of $\Lambda(a,b,\xi;x)$ over $\mathbb{Q}$, and hence $\Lambda(a,b,\xi;x)$ cannot be reducible over $\mathbb{Q}$. Finally, we define elliptic curves E, E^* and an isogeny $\lambda : E \to E^*$ in the same manner as in the beginning of the present section. We also take a point Q on E^* with $X_Q = \xi$. Then we have $L = \mathbb{Q}(\lambda^{-1}(Q))$, and hence $K = \mathbb{Q}(Q) = \mathbb{Q}(\sqrt{F(a, b; \xi)})$. □

In view of Theorem 5.2 and Corollary 5.3, one might expect that the integers a, b and the rational number ξ in Theorem 6.5 also satisfy the condition (C2). The following example shows that the expectation does not necessarily hold, and that we still have a possibility of obtaining a positive answer to Question 6.3.

EXAMPLE 6.7. Taking $a = b = 1$ and $\xi = -106$, we have $\Delta^* = -11^5$ and

$$F(1, 1; X) = 4X^3 + 8X^2 - 36X - 119,$$
$$\Lambda(1, 1, -106; x) = x^5 + 108x^4 + 215x^3 + 112x^2 + 4x + 1.$$

It is not hard to verify that $\Lambda(1, 1, -106; x)$ is irreducible over $\mathbb{Q}$, and that the class number of $\mathbb{Q}(\sqrt{F(1, 1; -106)}) = \mathbb{Q}(\sqrt{-319})$ is equal to 10. On the other hand, these a, b and ξ do not satisfy the condition (C2):

$$F(1, 1; -106) = -11^5 \cdot 29, \quad F'(1, 1; -106) = 2^2 \cdot 5^2 \cdot 11^3.$$

In other words, any point Q on E^* with $X_Q = -106$ is bad modulo 11. Moreover, we have

$$\Lambda(1, 1, -106; x) \equiv (x-7)^5 \pmod{11}, \quad [\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]] = 11^4,$$

where θ is a root of $\Lambda(1, 1, -106; x)$ and $\mathcal{O}_{\mathbb{Q}(\theta)}$ denotes the ring of integers of $\mathbb{Q}(\theta)$. Nevertheless, taking $Q' = [2]Q$ instead of Q, we have $X_{Q'} = -785/29$ and

$$F\left(1, 1; -\frac{785}{29}\right) = -\frac{11 \cdot 12689^2}{29^3}, \quad F'\left(1, 1; -\frac{785}{29}\right) = \frac{2^3 \cdot 719 \cdot 1217}{29^2}.$$

Hence $\mathbb{Q}(\sqrt{-319})$ can be expressed with $a = b = 1$ and $\xi' = -785/29$, which satisfy the conditions (C1) and (C2), replaced ξ with ξ' (cf. Corollary 5.5). Thus $\mathbb{Q}(\lambda^{-1}(Q)) = \mathbb{Q}(\lambda^{-1}(Q'))$ is a cyclic extension of $\mathbb{Q}(Q) = \mathbb{Q}(Q') = \mathbb{Q}(\sqrt{-319})$ of degree 5, in which every finite place is unramified.

References

[1] H. Cohen: Advanced Topics in Computational Number Theory, Graduate Texts in Mathematics **193**, Springer, New York, 2000.

[2] T. Honda: *Isogenies, rational points and section points of group varieties*, Japan. J. Math. **30** (1960), 84–101.

[3] T. Honda: *On real quadratic fields whose class numbers are multiples of* 3, J. Reine Angew. Math. **233** (1968), 101–102.

[4] C.U. Jensen, A. Ledet and N. Yui: Generic Polynomials, Constructive Aspects of the Inverse Galois Problem, Mathematical Sciences Research Institute Publications **45**, Cambridge Univ. Press, Cambridge, 2002.

[5] Y. Kishi and K. Miyake: *Parametrization of the quadratic fields whose class numbers are divisible by three*, J. Number Theory **80** (2000), 209–217.

[6] O. Lecacheux: *Constructions de polynômes génériques à groupe de Galois résoluble*, Acta Arith. **86** (1998), 207–216.

[7] PARI/GP, version 2.3.4, Bordeaux, 2008, `http://pari.math.u-bordeaux.fr/`.

[8] Y. Rikuna: *Private communication*.

[9] M. Sase: *On a family of quadratic fields whose class numbers are divisible by five*, Proc. Japan Acad. Ser. A Math. Sci. **74** (1998), 120–123.

[10] A. Sato: *On the class numbers of certain number fields obtained from points on elliptic curves*, Osaka J. Math. **38** (2001), 811–825.

[11] A. Sato: *On the class numbers of certain number fields obtained from points on elliptic curves* II, Osaka J. Math. **45** (2008), 375–390.

[12] A. Sato: *Construction of number fields of odd degree with class numbers divisible by three, five or by seven*, Interdiscip. Inform. Sci., to appear.

[13] J. Vélu: *Isogénies entre courbes elliptiques*, C.R. Acad. Sci. Paris Sér. A-B **273** (1971), 238–241.

[14] L.C. Washington: Elliptic Curves, Number Theory and Cryptography, second edition, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2008.

Mathematical Institute
Tohoku University
Sendai 980-8578
Japan
e-mail: atsushi@math.tohoku.ac.jp