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

Atsushi SATO

Abstract

We construct a family of cyclic extensions of number fields, in which every finite place is unramified, from an elliptic curve with a rational torsion point. As an application, we obtain such polynomials $F(X)$ of rational coefficients that have the following property: For a rational number ξ chosen at random, the class number of the field generated by the square root of $F(\xi)$ is "often" divisible by $3, 5$ or by 7.

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 [3] (see also [2]) used elliptic curves to find infinitely many real quadratic fields whose class numbers are multiple of 3. The author [6] gave a geometric interpretation of Honda's work, and showed, e.g., that the cubic polynomial $4X^3 - 27$ has the following property: *For $\xi \in \mathbb{Q}$ chosen at random, the class number of the field $\mathbb{Q}\big(\sqrt{4\xi^3 - 27}\big)$ is divisible by* 3 *with "probability" greater than or equal to* $3/4$.

On the other hand, J.-F. Mestre [5] used elliptic curves to find infinitely many imaginary and real quadratic fields whose 5-ranks or 7-ranks are at least 2. Mestre's work is based on scheme-theoretic argument, and the minimal models play an important role in the proof.

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

In the present paper, we study a way to construct cyclic extensions of number fields, in which every finite place is unramified, from an elliptic curve with a rational torsion point. Our method is similar to Mestre's in a certain sense. However, we do not use scheme theory nor minimal models. Instead of those tools, we use Vélu's formulas [9] (see Section 2) and the notion of "good points" on an elliptic curve with respect to a Weierstrass equation (see Section 4).

Here we briefly state the main results. 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. We 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

$$a_1,\ a_2,\ a_3,\ a_4,\ a_6,\ x(T_0),\ y(T_0) \in \mathcal{O}_k$$

and we denote its discriminant by Δ. Here $\mathcal{O}_k$ denotes the ring of integers of k. Let

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6$$

be the equation for $E^* = E/\langle T_0 \rangle$ and $\lambda : E \to E^*$ the isogeny of kernel $\langle T_0 \rangle$ which are given by Vélu's formulas (E^* is known to be an elliptic curve defined over k). Here $\langle T_0 \rangle$ denotes the subgroup of $E(k)$ generated by T_0. With the notation and the assumptions described above, we can state the main results as follows:

We can construct a subset Ξ of k (for the definition, see Theorem 5.1*) which satisfies the following two properties*:

(i) (Theorem 5.1) *For any $Q \in E^* - \{O\}$ with $X(Q) \in \Xi$, the field $k\big(\lambda^{-1}(Q)\big)$ is a cyclic extension of $k(Q)$ of degree l in which every finite place is unramified.*

(ii) (Corollary 6.4) *The set Ξ has a positive density in k*:

$$\lim_{B\to\infty} \frac{\#\{\xi \in \Xi\ ;\ H_k(\xi) \le B\}}{\#\{\xi \in k\ ;\ H_k(\xi) \le B\}} = \prod_{i=1}^{r} \frac{N\mathfrak{p}_i}{N\mathfrak{p}_i + 1},$$

where $H_k(\xi)$ denotes the exponential height relative to k of ξ. Here $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ denote the distinct prime divisors of Δ in k, and $N\mathfrak{p}_i$ denotes the absolute norm of $\mathfrak{p}_i$.

From these results, we conclude that the cubic polynomial

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

has the following property:

Assume $l \neq 2$. Then the elements $\xi \in k$ for which the class number of $K_\xi = k\big(\sqrt{F(\xi)}\,\big)$ is divisible by l have a positive density in k:

$$\liminf_{B\to\infty} \frac{\#\left\{\xi \in k \ ; \ l \mid h_{K_\xi},\ H_k(\xi) \leq B\right\}}{\#\left\{\xi \in k \ ; \ H_k(\xi) \leq B\right\}} \geq \prod_{i=1}^{r} \frac{N\mathfrak{p}_i}{N\mathfrak{p}_i + 1}.$$

We close this section with an example (see Examples 2.4 and 6.7). Let E be the elliptic curve defined over $k = \mathbb{Q}$ given by

$$y^2 - 78xy + 6241y = x^3 - 79x^2,$$

whose discriminant is $-79^5 \cdot 7109$, which has a rational point $T_0 = (0, 0)$ of order $l = 5$. For this case, our results imply: *For $\xi \in \mathbb{Q}$ chosen at random, the class number of*

$$\mathbb{Q}\big(\sqrt{4\xi^3 + 5768\xi^2 + 8635964\xi + 10019781641}\,\big)$$

is divisible by 5 with "probability" greater than or equal to

$$\frac{79}{79+1} \cdot \frac{7109}{7109+1} = 0.9873\cdots.$$

2 Review of Vélu's formulas

In this section, we briefly review Vélu's formulas. For details, see Vélu's original paper [9] (cf. also [4]).

Let E be an elliptic curve defined over a perfect field k, and let Γ be a finite subgroup of E which is invariant under the action of $\mathrm{Gal}(\bar{k}/k)$. Here $\bar{k}$ denotes an algebraic closure of k and $\mathrm{Gal}(\,\cdot\,)$ the Galois group. Then there exist an elliptic curve E^* and a separable isogeny $\lambda : E \to E^*$, which are defined over k, such that $\mathrm{Ker}\,\lambda = \Gamma$. Such a pair (E^*, λ)

is unique up to k-isomorphism, and E^* is often denoted by E/Γ. Given Weierstrass equation for E and the coordinates for the points in Γ, computing an equation for E^* and an explicit form for $\lambda : E \to E^*$ of kernel Γ can be done by using *Vélu's formulas*.

Let

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in k) \tag{2.1}$$

be an equation for E. We define $g^x, g^y \in k(E)$ by

$$g^x = 3x^2 + 2a_2x + a_4 - a_1y, \qquad g^y = -2y - a_1x - a_3. \tag{2.2}$$

For $P \in E - \{O\}$, we shall write the values $x(P)$, $y(P)$, $g^x(P)$, $g^y(P)$ by x_P, y_P, g^x_P, g^y_P, respectively, and set

$$t_P = \begin{cases} g^x_P & \text{if } P \in E[2] \\ 2g^x_P - a_1g^y_P & \text{otherwise} \end{cases}, \qquad u_P = (g^y_P)^2.$$

Taking a set $\Gamma_0 \subseteq \Gamma$ of perfect representatives for $(\Gamma - \{O\})/\pm 1$, we put

$$t = \sum_{T \in \Gamma_0} t_T, \qquad w = \sum_{T \in \Gamma_0} (u_T + x_T t_T).$$

These two quantities are in k, and do not depend on the choice of Γ_0. Letting

$$A_1 = a_1, \quad A_2 = a_2, \quad A_3 = a_3, \quad A_4 = a_4 - 5t, \quad A_6 = a_6 - (a_1^2 + 4a_2)t - 7w,$$

we can state the formulas as follows:

The elliptic curve $E^* = E/\Gamma$ and the separable isogeny $\lambda : E \to E^*$ of kernel Γ are given by

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

and by

$$\begin{aligned} X &= x + \sum_{T \in \Gamma_0} \left(\frac{t_T}{x - x_T} + \frac{u_T}{(x - x_T)^2} \right), \\ Y &= y - \sum_{T \in \Gamma_0} \left(u_T \frac{2y + a_1x + a_3}{(x - x_T)^3} + t_T \frac{a_1(x - x_T) + y - y_T}{(x - x_T)^2} + \frac{a_1u_T - g^x_Tg^y_T}{(x - x_T)^2} \right), \end{aligned} \tag{2.4}$$

respectively.

REMARK 2.1 Expressions (2.4) are derived from

$$X = x + \sum_{T\in\Gamma-\{O\}} (x\circ\tau_T - x_T), \qquad Y = y + \sum_{T\in\Gamma-\{O\}} (y\circ\tau_T - y_T),$$

or equivalently,

$$X + \sum_{T\in\Gamma-\{O\}} x_T = \sum_{T\in\Gamma} x\circ\tau_T, \qquad Y + \sum_{T\in\Gamma-\{O\}} y_T = \sum_{T\in\Gamma} y\circ\tau_T$$

by using the addition formulas. Here τ_T denotes the translation-by-T-map on E. Note that we regard $k(E^*)$ as a subfield of $k(E)$:

$$k(E^*) = \{\phi\in k(E)\ ;\ \phi\circ\tau_T = \phi \text{ for all } T\in\Gamma\}\,.$$

Thus we have

$$(2.5)\quad X_Q + \sum_{T\in\Gamma-\{O\}} x_T = \sum_{P\in\lambda^{-1}(Q)} x_P,\ \ Y_Q + \sum_{T\in\Gamma-\{O\}} y_T = \sum_{P\in\lambda^{-1}(Q)} y_P \quad \text{for } Q\in E^*-\{O\},$$

where X_Q and Y_Q denote $X(Q)$ and $Y(Q)$, respectively.

REMARK 2.2 One verifies that the invariant differential

$$\omega(x,y) = \frac{dx}{-g^y} = \frac{dy}{g^x}$$

on E associated with (2.1) is equal to the one

$$\omega(X,Y) = \frac{dX}{-G^Y} = \frac{dY}{G^X}$$

on E^* associated with (2.3). Here we define $G^X, G^Y\in k(E^*)$ by

$$(2.6)\qquad G^X = 3X^2 + 2A_2X + A_4 - A_1Y, \qquad G^Y = -2Y - A_1X - A_3.$$

EXAMPLE 2.3 (The case of $\Gamma\cong\mathbb{Z}/3\mathbb{Z}$) If E has a k-rational point T_0 of order 3, then E has an equation of the form

$$y^2 + axy + by = x^3 \qquad \big(a,b\in k,\ b(a^3-27b)\neq 0\big)$$

with $T_0 = (0,0)$, and $E^* = E/\langle T_0\rangle$ is given by

$$Y^2 + aXY + bY = X^3 - 5abX - a^3b - 7b^2.$$

EXAMPLE 2.4 (The case of $\Gamma \cong \mathbb{Z}/5\mathbb{Z}$) If E has a k-rational point T_0 of order 5, then E has an equation of the form

$$y^2 + (a+b)xy + ab^2y = x^3 + abx^2 \qquad \big(a, b \in k,\ ab(a^2 + 11ab - b^2) \neq 0\big)$$

with $T_0 = (0,0)$, and $E^* = E/\langle T_0 \rangle$ is given by

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

EXAMPLE 2.5 (The case of $\Gamma \cong \mathbb{Z}/7\mathbb{Z}$) If E has a k-rational point T_0 of order 7, then E has an equation of the form

$$\begin{gathered} y^2 + (a^2 + ab - b^2)xy + a^3b^2(a-b)y = x^3 + ab^2(a-b)x^2 \\ \big(a, b \in k,\ ab(a-b)(a^3 + 5a^2b - 8ab^2 + b^3) \neq 0\big) \end{gathered}$$

with $T_0 = (0,0)$, and $E^* = E/\langle T_0 \rangle$ is given by

$$\begin{aligned} &Y^2 + (a^2 + ab - b^2)XY + a^3b^2(a-b)Y \\ &\quad = X^3 + ab^2(a-b)X^2 \\ &\qquad + 5ab(a-b)(a^2 - ab + b^2)(a^3 - 5a^2b + 2ab^2 + b^3)X \\ &\qquad + ab(a-b)(a^9 - 18a^8b + 76a^7b^2 - 182a^6b^3 + 211a^5b^4 \\ &\qquad\qquad - 132a^4b^5 + 70a^3b^6 - 37a^2b^7 + 9ab^8 + b^9). \end{aligned}$$

3 Consequences of the formulas

In this section, we study about the form of the isogeny $\lambda : E \to E^*$ which is given by Vélu's formulas. Notation and assumptions are the same as in the previous section.

3.1 Relations among G^X, G^Y and g^x, g^y The functions $G^X, G^Y \in k(E^*)$, defined by (2.6), can be written by using $g^x, g^y \in k(E)$, defined by (2.2), as

$$G^X = m\, g^x + n(g^y)^2, \qquad G^Y = m\, g^y.$$

Here we define $m, n \in k(E)$ by

$$m = 1 - \sum_{T \in \Gamma_0} \left(\frac{t_T}{(x - x_T)^2} + \frac{2u_T}{(x - x_T)^3} \right), \qquad n = \sum_{T \in \Gamma_0} \left(\frac{t_T}{(x - x_T)^3} + \frac{3u_T}{(x - x_T)^4} \right).$$

Thus we have

$$(3.1)\quad G_Q^X = m_P\, g_P^x + n_P (g_P^y)^2, \qquad G_Q^Y = m_P\, g_P^y \qquad \text{for } Q \in E^* - \{O\} \text{ and } P \in \lambda^{-1}(Q),$$

where G_Q^X, G_Q^Y, m_P, n_P denote $G^X(Q)$, $G^Y(Q)$, $m(P)$, $n(P)$, respectively (note that m and n are regular on $E - \Gamma$). These relations can be deduced from

$$\frac{dx}{-g^y} = \frac{dy}{g^x} = \frac{dX}{-G^Y} = \frac{dY}{G^X}$$

(see Remark 2.2) combined with

$$dX = m\, dx, \qquad dY = -ng^y\, dx + m\, dy.$$

3.2 Relation between X and x We can rewrite the former expression of (2.4) into

$$X = \frac{I(x)}{J(x)}$$

with

$$I(x) = x^l - \Big(\sum_{T \in \Gamma - \{O\}} x_T\Big) x^{l-1} + \cdots,$$

$$J(x) = \prod_{T \in \Gamma - \{O\}} (x - x_T) = x^{l-1} - \Big(\sum_{T \in \Gamma - \{O\}} x_T\Big) x^{l-2} + \cdots,$$

where $l = \#\Gamma$ $(= \deg \lambda)$. It is easy to verify that all the coefficients of $I(x)$ and $J(x)$ are in k. Moreover, since $[k(x) : k(X)]$ is equal to $[k(E) : k(E^*)] = l$, these polynomials do not have any common root.

Let Q be a point on E^* with $[2]Q \neq O$. Then, for each $P \in \lambda^{-1}(Q)$, we have $P \neq O$, $J(x_P) \neq 0$ and $I(x_P) - X_Q J(x_P) = 0$. Therefore we conclude

$$(3.2)\qquad I(x) - X_Q J(x) = \prod_{P \in \lambda^{-1}(Q)} (x - x_P),$$

since the assumption $[2]Q \neq O$ implies

$$\#\left\{x_P \;;\; P \in \lambda^{-1}(Q)\right\} = \#\lambda^{-1}(Q) = l.$$

3.3 The field extensions arising from $\boldsymbol{\lambda}$ Let Q be a point on E^* with $[2]Q \neq O$. We denote the fields

$$k(Q) = k(X_Q, Y_Q), \qquad k\big(\lambda^{-1}(Q)\big) = k\big(x_P,\, y_P\ ;\ P \in \lambda^{-1}(Q)\big)$$

by K, K', respectively. Since the isogeny λ is defined over k, we have $K \subseteq K'$.

Now, we assume that the the field k is not of characteristic 2. Then we have

$$K = k(X_Q, G_Q^Y), \qquad K' = k\big(x_P,\, g_P^y\ ;\ P \in \lambda^{-1}(Q)\big).$$

Here, it follows from (3.1) and the assumption $[2]Q \neq O$ (i.e. $G_Q^Y \neq 0$) that $m_P \neq 0$ and $g_P^y = m_P^{-1} G_Q^Y \in k(x_P, G_Q^Y)$. Therefore we conclude

$$K' = K\big(x_P\ ;\ P \in \lambda^{-1}(Q)\big). \tag{3.3}$$

Thus K' is the splitting field of the polynomial $I(x) - X_Q J(x)$ over K (see (3.2)).

4 Relation with reduction maps

In this section, we shall apply Vélu's formulas to elliptic curves of certain type, and study about the relation among the isogeny and the reduction maps with respect to a non-archimedean valuation on the ground field.

Let k be a perfect field, 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 the element $a \bmod \mathfrak{p}_v$ of κ_v by $\widetilde{a}$.

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4.1}$$

with

$$a_1,\ a_2,\ a_3,\ a_4,\ a_6,\ x_{T_0},\ y_{T_0} \in \mathcal{O}_v. \tag{4.2}$$

We fix such an equation and consider the reduction of E modulo $\mathfrak{p}_v$. That is, let $\widetilde{E} = E \bmod \mathfrak{p}_v$ be the curve defined over κ_v which is given by

$$y^2 + \widetilde{a}_1xy + \widetilde{a}_3y = x^3 + \widetilde{a}_2x^2 + \widetilde{a}_4x + \widetilde{a}_6, \tag{4.3}$$

and let

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

be the reduction of E modulo $\mathfrak{p}_v$ *with respect to* Equation (4.1). Using the reduction map, we define two subsets of $E(k)$ as

$$\mathcal{E}_0(k;\mathfrak{p}_v) = \left\{ P \in E(k) \ ; \ \widetilde{P} \in \widetilde{E}_{\mathrm{ns}}(\kappa_v) \right\}, \qquad \mathcal{E}_+(k;\mathfrak{p}_v) = \left\{ P \in E(k) \ ; \ \widetilde{P} = \widetilde{O} \right\}.$$

We call $P \in E(k)$ is *good* modulo $\mathfrak{p}_v$ with respect to (4.1) if it belongs to $\mathcal{E}_0(k;\mathfrak{p}_v)$ (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 $\mathcal{E}_0(k;\mathfrak{p}_v)$. Then clearly $\{O\} \subseteq \mathcal{E}_+(k;\mathfrak{p}_v) \subseteq \mathcal{E}_0(k;\mathfrak{p}_v)$. Moreover, it is easy to observe:

Proposition 4.1 (i) *For $P \in E(k) - \{O\}$, we have*

$$P \in \mathcal{E}_+(k;\mathfrak{p}_v) \quad \Longleftrightarrow \quad x_P \notin \mathcal{O}_v \quad \Longleftrightarrow \quad y_P \notin \mathcal{O}_v.$$

(ii) *For $P \in E(k) - \mathcal{E}_+(k;\mathfrak{p}_v)$, we have*

$$P \notin \mathcal{E}_0(k;\mathfrak{p}_v) \quad \Longleftrightarrow \quad g_P^x \equiv g_P^y \equiv 0 \pmod{\mathfrak{p}_v}.$$

Remark 4.2 Whether a point $P \in E(k)$ is good or bad is determined only by a congruent condition for its x-coordinate modulo $\mathfrak{p}_v$. More precisely, putting Δ the discriminant of (4.1), we have:

(i) If $\Delta \not\equiv 0 \pmod{\mathfrak{p}_v}$, then every $P \in E(k)$ is good.

(ii) If $\Delta \equiv 0 \pmod{\mathfrak{p}_v}$, then $P \in E(k)$ is bad if and only if $x_P \in \mathcal{O}_v$ and

$$\begin{cases} f(x_P) \equiv f'(x_P) \equiv 0 \pmod{\mathfrak{p}_v} & \text{if } 2 \not\equiv 0 \pmod{\mathfrak{p}_v} \\ x_P^2 \equiv a_4 \pmod{\mathfrak{p}_v} & \text{if } 2 \equiv a_1 \equiv 0 \pmod{\mathfrak{p}_v} \\ x_P \equiv a_3/a_1 \pmod{\mathfrak{p}_v} & \text{if } 2 \equiv 0,\ a_1 \not\equiv 0 \pmod{\mathfrak{p}_v} \end{cases}$$

hold. Here we define a cubic polynomial $f(x)$ by

$$f(x) = 4x^3 + (a_1^2 + 4a_2)x^2 + 2(a_1a_3 + 2a_4)x + a_3^2 + 4a_6.$$

Note the sets $\mathcal{E}_0(k;\mathfrak{p}_v)$ and $\mathcal{E}_+(k;\mathfrak{p}_v)$ defined above are not uniquely determined by k, v and by E. However, one can verify the following (cf., e.g., [8, Chapter VII, Proposition 2.1]):

Proposition 4.3 *The set $\mathcal{E}_0(k;\mathfrak{p}_v)$ is a subgroup of $E(k)$, and the map*

$$\mathcal{E}_0(k;\mathfrak{p}_v) \ni P \longmapsto \widetilde{P} \in \widetilde{E}_{\rm ns}(\kappa_v)$$

is a group homomorphism of kernel $\mathcal{E}_+(k;\mathfrak{p}_v)$.

Let Γ be the subgroup of $E(k)$ generated by T_0. Then Γ is of prime order l, and its subgroups $\Gamma \cap \mathcal{E}_0(k;\mathfrak{p}_v)$ and $\Gamma \cap \mathcal{E}_+(k;\mathfrak{p}_v)$ must coincide with $\{O\}$ or Γ. On the other hand, the assumption $x_{T_0}, y_{T_0} \in \mathcal{O}_v$ implies $T_0 \notin \mathcal{E}_+(k;\mathfrak{p}_v)$. Thus we have:

Corollary 4.4 (i) $\Gamma \cap \mathcal{E}_0(k;\mathfrak{p}_v)$ *coincides with* $\{O\}$ *or* Γ.
(ii) $\Gamma \cap \mathcal{E}_+(k;\mathfrak{p}_v) = \{O\}$.

We note that the corollary above implies

$$x_T,\ y_T,\ g_T^x,\ g_T^y,\ t_T,\ u_T \in \mathcal{O}_v \qquad \text{for all } T \in \Gamma - \{O\}. \tag{4.4}$$

Now, let

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6 \tag{4.5}$$

be the equation for the elliptic curve $E^* = E/\Gamma$ and $\lambda : E \to E^*$ the isogeny which are given by Vélu's formulas. Then the assumption (4.2) together with (4.4) imply

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

Moreover, one easily observes that all the coefficients of the polynomials $I(x)$ and $J(x)$, defined in Section 3.2, are in $\mathcal{O}_v$. Let $\widetilde{E}^* = E^* \bmod \mathfrak{p}_v$ be the curve defined over κ_v which is given by

$$y^2 + \widetilde{A}_1xy + \widetilde{A}_3y = x^3 + \widetilde{A}_2x^2 + \widetilde{A}_4x + \widetilde{A}_6, \tag{4.6}$$

and let

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

be the reduction of E^* modulo $\mathfrak{p}_v$ with respect to (4.5). Using the reduction map, we define $\mathcal{E}_0^*(k;\mathfrak{p}_v)$, $\mathcal{E}_+^*(k;\mathfrak{p}_v) \subseteq E^*(k)$ in the same manner as for E. Then we can obtain the same ones for E^* as Proposition 4.1, Remark 4.2 and Proposition 4.3.

With the notation and the assumptions described above, we have the following theorem, which asserts that the inverse image by λ of every good point contains a good point:

Theorem 4.5 *Let Q be a point in $\mathcal{E}_0^*(k;\mathfrak{p}_v)$ such that $\lambda^{-1}(Q) \subseteq E(k)$. Then at least one point in $\lambda^{-1}(Q)$ is contained in $\mathcal{E}_0(k;\mathfrak{p}_v)$:*

$$\lambda^{-1}(Q) \cap \mathcal{E}_0(k;\mathfrak{p}_v) \neq \emptyset.$$

Proof. Since the assertion is clear if $Q = O$, we assume $Q \neq O$. As mentioned in Corollary 4.4, the set $\Gamma \cap \mathcal{E}_0(k;\mathfrak{p}_v)$ coincides with $\{O\}$ or Γ.

(i) We first consider the case $\Gamma \cap \mathcal{E}_0(k;\mathfrak{p}_v) = \{O\}$, i.e. the case where every $T \in \Gamma - \{O\}$ is bad. In that case, it follows from Proposition 4.1 that each $T \in \Gamma - \{O\}$ satisfies $g_T^x \equiv g_T^y \equiv 0 \pmod{\mathfrak{p}_v}$, and hence $t_T \equiv u_T \equiv 0 \pmod{\mathfrak{p}_v}$. Therefore we have $t \equiv w \equiv 0 \pmod{\mathfrak{p}_v}$ and

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

Thus Equation (4.6) for $\widetilde{E}^*$ coincides with Equation (4.3) for $\widetilde{E}$. We also note that all $T \in \Gamma - \{O\}$ are reduced into the same point. That is, writing α the x-coordinate of the (unique) singular point on $\widetilde{E}$, we have $\widetilde{x}_T = \alpha$ for all $T \in \Gamma - \{O\}$.

Now, suppose $\lambda^{-1}(Q) \cap \mathcal{E}_0(k;\mathfrak{p}_v) = \emptyset$. Then every $P \in \lambda^{-1}(Q)$ is bad, and hence satisfies $\widetilde{x}_P = \alpha$. Consequently, it follows from (2.5) that $X_Q \in \mathcal{O}_v$ and $\widetilde{X}_Q = \alpha$. Therefore we conclude $Q \notin \mathcal{E}_0^*(k;\mathfrak{p}_v)$, which contradicts the assumption.

(ii) We next consider the case $\Gamma \cap \mathcal{E}_0(k;\mathfrak{p}_v) = \Gamma$, i.e. the case where every $T \in \Gamma$ is good. In that case, we have $\lambda^{-1}(Q) \subseteq \mathcal{E}_0(k;\mathfrak{p}_v)$. Indeed, if $\lambda^{-1}(Q)$ has a bad point P, then we have $x_P, y_P \in \mathcal{O}_v$ and $g_P^x \equiv g_P^y \equiv 0 \pmod{\mathfrak{p}_v}$. Moreover, the assumption $\Gamma \subseteq \mathcal{E}_0(k;\mathfrak{p}_v)$ implies $x_P \not\equiv x_T \pmod{\mathfrak{p}_v}$ for all $T \in \Gamma - \{O\}$, and hence we obtain $X_Q, Y_Q \in \mathcal{O}_v$ by (2.4). On the other hand, it follows from (3.1) that $G_Q^X \equiv G_Q^Y \equiv 0 \pmod{\mathfrak{p}_v}$. Thus we conclude $Q \notin \mathcal{E}_0^*(k;\mathfrak{p}_v)$, which contradicts the assumption. □

Remark 4.6 From the argument in the above proof, one observes that the condition $\Delta \equiv 0 \pmod{\mathfrak{p}_v}$ implies $\Delta^* \equiv 0 \pmod{\mathfrak{p}_v}$. Here Δ^* denotes the discriminant of (4.5).

5 Construction of unramified extensions

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. Then we can take a Weierstrass equation for E of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5.1}$$

with

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

Let Γ be the subgroup of $E(k)$ generated by T_0. Then it follows from the local argument in Section 4 that

$$x_T,\ y_T,\ g_T^x,\ g_T^y,\ t_T,\ u_T \in \mathcal{O}_k \qquad \text{for all } T \in \Gamma - \{O\}. \tag{5.2}$$

Thus, letting

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6 \tag{5.3}$$

be the equation for the elliptic curve $E^* = E/\Gamma$ and $\lambda : E \to E^*$ the isogeny of kernel Γ which are given by Vélu's formulas, 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 $J(x)$, defined in Section 3.2, are in $\mathcal{O}_k$.

Now, we define a cubic polynomial $F(X)$ 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 put $K_\xi = k\big(\sqrt{F(\xi)}\,\big)$ for $\xi \in k$. For $Q \in E^* - \{O\}$ with $X_Q = \xi \in k$, it is easy to verify that the field K_ξ coincides with $k(Q)$. We also define a polynomial $\Lambda_\xi(x)$ of degree l by

$$\Lambda_\xi(x) = I(x) - \xi J(x)$$

for each $\xi \in k$. Let Δ and Δ^* denote the discriminants of (5.1) and (5.3), respectively. For each prime divisor $\mathfrak{p}$ of Δ in k (it is also a prime divisor of Δ^* by Remark 4.6), let $\mathcal{X}_{\mathrm{bad}}(k;\mathfrak{p})$ be the set of such $\xi \in \mathcal{O}_{k,\mathfrak{p}}$ that satisfy the condition

$$\begin{cases} F(\xi) \equiv F'(\xi) \equiv 0 \pmod{\mathfrak{p}} & \text{if } 2 \not\equiv 0 \pmod{\mathfrak{p}} \\ \xi^2 \equiv A_4 \pmod{\mathfrak{p}} & \text{if } 2 \equiv A_1 \equiv 0 \pmod{\mathfrak{p}} \\ \xi \equiv A_3/A_1 \pmod{\mathfrak{p}} & \text{if } 2 \equiv 0,\ A_1 \not\equiv 0 \pmod{\mathfrak{p}} \end{cases}$$

(cf. Remark 4.2). Here $\mathcal{O}_{k,\mathfrak{p}}$ denotes the localization of $\mathcal{O}_k$ at $\mathfrak{p}$. One might call $\mathcal{X}_{\mathrm{bad}}(k;\mathfrak{p})$ the set of *bad X-coordinates* on E^* modulo $\mathfrak{p}$ with respect to (5.3).

With the notation and the assumptions described above, we have:

Theorem 5.1 *Let Ξ be the set of such $\xi \in k$ that satisfy the following three conditions*:

(C0) $F(\xi) \neq 0$.

(C1) $\Lambda_\xi(x)$ *is irreducible over k.*

(C2) $\xi \notin \mathcal{X}_{\mathrm{bad}}(k;\mathfrak{p})$ *for all prime divisors $\mathfrak{p}$ of Δ in k.*

Then, for any $Q \in E^* - \{O\}$ with $X_Q \in \Xi$, the field $k\big(\lambda^{-1}(Q)\big)$ is a cyclic extension of $k(Q)$ of degree l in which every finite place is unramified.

Since a Galois extension of odd degree is unramified at every infinite place, by using the class field theory, we obtain the following:

Corollary 5.2 *Suppose $l \neq 2$. Then, for any $\xi \in \Xi$, the class number of the field K_ξ is divisible by l.*

Remark 5.3 Setting $a = 0$ in Example 2.3 (the case of $l = 3$), we have $F(X) = 4X^3 - 27b^2$, which the author studied in [6].

Remark 5.4 In the case where the field k is totally imaginary, one has the same result as the corollary above even if $l = 2$.

Now, we give a proof of Theorem 5.1. Roughly speaking, our method to prove the theorem is similar to the proof of the Weak Mordell-Weil Theorem (see, e.g., [8, Chapter VIII, Section 1]). We shall use Theorem 4.5 in place of the direct calculation in [6].

At first, we fix a point $Q \in E^* - \{O\}$ with $X_Q = \xi \in \Xi$, and put

$$K = k(Q)\ (= K_\xi), \qquad K' = k\big(\lambda^{-1}(Q)\big).$$

Then:

Lemma 5.5 (i) *K' is a cyclic extension of K of degree l.*

(ii) *For any $P \in \lambda^{-1}(Q)$, we have $K' = K(P)$.*

(iii) *The map*

$$\iota : \mathrm{Gal}(K'/K) \ni \sigma \longmapsto P^\sigma - P \in \Gamma$$

(P is a point in $\lambda^{-1}(Q)$) is a group isomorphism.

Proof. It is immediate from $\Gamma \subseteq E(k) \subseteq E(K)$ and $Q \in E^*(K)$ that K'/K is a Galois extension, $K' = K(P)$ holds for any $P \in \lambda^{-1}(Q)$ and that ι is an injective group homomorphism. Thus we have only to show that ι is surjective.

Since the group Γ is of prime order l, its subgroup $\mathrm{Im}\,\iota$ must coincide with $\{O\}$ or Γ. Moreover, the assumption (C0) implies that K' is the splitting field of $\Lambda_\xi(x)$ over K (see (3.3)). Hence we conclude $\mathrm{Im}\,\iota = \Gamma$ by the assumption (C1). □

Next, we fix a prime ideal $\mathfrak{P}$ in K and show that K'/K is unramified at $\mathfrak{P}$. Since $[K' : K] = l$ is prime, we may assume that $\mathfrak{P}$ is not decomposed in K'. Let $\mathfrak{P}'$ denote the unique prime divisor of $\mathfrak{P}$ in K' and κ' its residue field. Let

$$E(K') \ni P \longmapsto P \bmod \mathfrak{P}' \in (E \bmod \mathfrak{P}')(\kappa')$$

be the reduction of E modulo $\mathfrak{P}'$ with respect to (5.1). Using the reduction map, we define $\mathcal{E}_0(K';\mathfrak{P}')$, $\mathcal{E}_+(K';\mathfrak{P}') \subseteq E(K')$ in the same manner as in Section 4. These subsets are $\mathrm{Gal}(K'/K)$-invariant subgroups of $E(K')$, for we have assumed that $\mathfrak{P}$ is not decomposed in K'. Therefore, putting $I_{\mathfrak{P}'/\mathfrak{P}}$ the inertia group for $\mathfrak{P}'/\mathfrak{P}$, we have $P^\sigma - P \in \mathcal{E}_+(K';\mathfrak{P}')$ for any $P \in \mathcal{E}_0(K';\mathfrak{P}')$ and any $\sigma \in I_{\mathfrak{P}'/\mathfrak{P}}$. In particular, taking P from $\lambda^{-1}(Q) \cap \mathcal{E}_0(K';\mathfrak{P}')$, which is a nonempty set by the assumption (C2) and Theorem 4.5, we obtain

$$P^\sigma - P \in \Gamma \cap \mathcal{E}_+(K';\mathfrak{P}')$$

for all $\sigma \in I_{\mathfrak{P}'/\mathfrak{P}}$. However, it follows from (5.2) that $\Gamma \cap \mathcal{E}_+(K';\mathfrak{P}') = \{O\}$, and hence the point P is invariant under the action of $\sigma \in I_{\mathfrak{P}'/\mathfrak{P}}$. On the other hand, we also have $K' = K(P)$. Thus we conclude $I_{\mathfrak{P}'/\mathfrak{P}} = \{1\}$. That is, K'/K is unramified at $\mathfrak{P}$, which completes the proof of Theorem 5.1.

6 The density of Ξ

In this section, we show that the set Ξ defined in the previous section has a positive density in k with respect to a height function. For a k-rational point $P \in \mathbb{P}^{d-1}(k)$ on $(d-1)$-dimensional projective space, we denote its exponential height relative to k by $H_k(P)$ (for the definition and the basic properties of heights, see, e.g., [1, Part B]). Then, as was shown by Schanuel [7], one has

$$\# \left\{ P \in \mathbb{P}^{d-1}(k) \ ; \ H_k(P) \le B \right\} \sim C_{d,k}\, B^d \tag{6.1}$$

as $B \to \infty$. Here $C_{d,k}$ is a positive constant depending only on d and k which can be written in an explicit form. We regard $\mathbb{P}^1(k)$ as $k \cup \{\infty\}$, and study the asymptotic behavior of the counting function $\# \{\xi \in \Xi \ ; \ H_k(\xi) \le B\}$.

Recall that the set Ξ is defined by using three conditions (C0)–(C2). Among them, the condition (C0) holds for all but finitely many $\xi \in k$ (there are at most three exceptions). Thus we may omit the condition (C0). On the other hand, we can estimate the number of such $\xi \in k$ that do not satisfy the condition (C1) as follows:

Lemma 6.1 *We have*

$$\# \{\xi \in k \ ; \ \Lambda_\xi(x) \text{ is reducible over } k, \ H_k(\xi) \le B\} \asymp B^{2/l}$$

as $B \to \infty$.

Proof. We first show that, for $\xi \in k$ with $F(\xi) \neq 0$, the following conditions are equivalent:

(a) $\Lambda_\xi(x)$ is reducible over k.

(b) $\Lambda_\xi(x)$ has a root in k.

(b)′ $\xi = I(\zeta)/J(\zeta)$ holds for some $\zeta \in k$ satisfying $J(\zeta) \neq 0$.

Clearly, (b) implies (a). It is also immediate to see the equivalence between (b) and (b)′. Thus we have only to show that (a) implies (b). The assertion is obvious in the case where $l = 2$, and we shall assume $l \neq 2$ for the time being. Then, for $\xi \in k$ with $F(\xi) \neq 0$, one can show that the following conditions are equivalent in a similar fashion to the proof of Lemma 5.5:

(A) $\Lambda_\xi(x)$ is reducible over K_ξ.

(B) $\Lambda_\xi(x)$ is decomposed into linear factors over K_ξ.

Here, clearly (a) implies (A). Moreover, since l is assumed to be odd, it follows from $[K_\xi : k] \leq 2$ that (B) implies (b). Consequently, for $\xi \in k$ with $F(\xi) \neq 0$, the five conditions described above are equivalent (under the assumption $l \neq 2$).

By the equivalence between (a) and (b)′, we obtain

$$\#\left\{\xi \in k \ ; \ \Lambda_\xi(x) \text{ is reducible over } k, \ H_k(\xi) \leq B\right\} \asymp \#\left\{\zeta \in k \ ; \ H_k\big(I(\zeta)/J(\zeta)\big) \leq B\right\}.$$

On the other hand, since $I(x)/J(x)$ is a rational function of degree l, we observe

$$H_k\big(I(\,\cdot\,)/J(\,\cdot\,)\big) \asymp H_k(\,\cdot\,)^l$$

on k. Hence we conclude the assertion by the asymptotic formula (6.1). □

Now, we study about the condition (C2). Recall that the sets $\mathcal{X}_{\mathrm{bad}}(k;\mathfrak{p})$ are defined for prime divisors $\mathfrak{p}$ of Δ in k. It follows from the definition that, for each $\mathfrak{p}$, there exists a point $\xi_\mathfrak{p} \in \mathbb{P}^1(\mathcal{O}_k/\mathfrak{p}) - \{\infty\}$ such that

$$\mathcal{X}_{\mathrm{bad}}(k;\mathfrak{p}) = \left\{\xi \in \mathbb{P}^1(k) \ ; \ \xi \bmod \mathfrak{p} = \xi_\mathfrak{p}\right\}.$$

The distribution of rational points on a projective space with such conditions on reductions as above can be estimated as follows:

Lemma 6.2 *Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be distinct prime ideals in a number field k of finite degree. Then, for every $(P_1, \dots, P_r) \in \prod_{i=1}^r \mathbb{P}^{d-1}(\mathcal{O}_k/\mathfrak{p}_i)$, we have*

$$\#\left\{P \in \mathbb{P}^{d-1}(k) \ ; \ P \bmod \mathfrak{p}_i = P_i \ \textit{for all } i, \ H_k(P) \leq B\right\} \sim \left(\prod_{i=1}^r \frac{N\mathfrak{p}_i - 1}{N\mathfrak{p}_i^d - 1}\right) C_{d,k}\, B^d$$

as $B \to \infty$. Here $N\mathfrak{p}_i$ denotes the absolute norm of $\mathfrak{p}_i$.

The lemma above can be shown in a similar (but more complicated) way to Schanuel's original proof (see also Watanabe [10, Example 1], which treats a modified height function).

Summing up the asymptotic formulas described above, we obtain:

Theorem 6.3 *We have*

$$\#\left\{\xi \in \Xi \ ;\ H_k(\xi) \leq B\right\} \sim \left(\prod_{i=1}^{r} \frac{N\mathfrak{p}_i}{N\mathfrak{p}_i + 1}\right) C_{2,k}\, B^2$$

as $B \to \infty$. *Here* $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ *denote the distinct prime divisors of* Δ *in* k.

Corollary 6.4 *The set* Ξ *has a positive density in* k *in the following sense*:

$$\lim_{B\to\infty} \frac{\#\left\{\xi \in \Xi \ ;\ H_k(\xi) \leq B\right\}}{\#\left\{\xi \in k \ ;\ H_k(\xi) \leq B\right\}} = \prod_{i=1}^{r} \frac{N\mathfrak{p}_i}{N\mathfrak{p}_i + 1}.$$

Remark 6.5 For an extension K of k, one can show that

$$\#\left\{\xi \in \Xi \ ;\ K_\xi = K,\ H_k(\xi) \leq B\right\} \asymp (\log B)^{r/2}$$

holds for some $r \in \mathbb{Z}_{\geq 0}$. Thus the family $\{K_\xi\}_{\xi\in\Xi}$ of (at most quadratic) extensions of k, parametrized by Ξ, consists of infinitely many fields.

Now, we assume $l \neq 2$. Then it follows from Corollaries 5.2 and 6.4 that the elements $\xi \in k$ for which the class number of $K_\xi = k\big(\sqrt{F(\xi)}\,\big)$ is divisible by l have a positive density in k:

$$\liminf_{B\to\infty} \frac{\#\left\{\xi \in k \ ;\ l \mid h_{K_\xi},\ H_k(\xi) \leq B\right\}}{\#\left\{\xi \in k \ ;\ H_k(\xi) \leq B\right\}} \geq \prod_{i=1}^{r} \frac{N\mathfrak{p}_i}{N\mathfrak{p}_i + 1}.$$

Thus one might say: *For* $\xi \in k$ *chosen at random, the class number of the field* K_ξ *is divisible by* l *with "probability" greater than or equal to* $\prod_i N\mathfrak{p}_i/(N\mathfrak{p}_i + 1)$.

Example 6.6 Putting $k = \mathbb{Q},\ a = 98$ and $b = -1$ in Example 2.3, we obtain

$$F(X) = 4X^3 + 9604X^2 + 1764X + 3764741, \qquad \Delta = -101 \cdot 9319.$$

Thus, for $\xi \in \mathbb{Q}$, the class number of $\mathbb{Q}\big(\sqrt{F(\xi)}\,\big)$ is divisible by 3 with "probability" greater than or equal to

$$\frac{101}{101+1} \cdot \frac{9319}{9319+1} = 0.9900\cdots.$$

EXAMPLE 6.7 Putting $k = \mathbb{Q}$, $a = 1$ and $b = -79$ in Example 2.4, we obtain

$$F(X) = 4X^3 + 5768X^2 + 8635964X + 10019781641, \qquad \Delta = -79^5 \cdot 7109.$$

Thus, for $\xi \in \mathbb{Q}$, the class number of $\mathbb{Q}\big(\sqrt{F(\xi)}\,\big)$ is divisible by 5 with "probability" greater than or equal to

$$\frac{79}{79+1} \cdot \frac{7109}{7109+1} = 0.9873\cdots .$$

EXAMPLE 6.8 Putting $k = \mathbb{Q}$, $a = 4$ and $b = -97$ in Example 2.5, we obtain

$$F(X) = 4X^3 + 110872905X^2 + 6379117545341648X + 66809139857632818992656,$$
$$\Delta = -2^{14} \cdot 97^7 \cdot 101^7 \cdot 1221457.$$

Thus, for $\xi \in \mathbb{Q}$, the class number of $\mathbb{Q}\big(\sqrt{F(\xi)}\,\big)$ is divisible by 7 with "probability" greater than or equal to

$$\frac{2}{2+1} \cdot \frac{97}{97+1} \cdot \frac{101}{101+1} \cdot \frac{1221457}{1221457+1} = 0.6533\cdots .$$

References

[1] M. Hindry and J.H. Silverman: Diophantine Geometry: An Introduction, Graduate Texts in Mathematics **201**, 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] R. Lercier and F. Morain: *Algorithms for computing isogenies between elliptic curves*; in Computational Perspectives on Number Theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math. **7**, Amer. Math. Soc., Providence, RI, 1998, 77–96.

[5] J.-F. Mestre: *Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques*, J. Reine Angew. Math. **343** (1983), 23–35.

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

[7] S.H. Schanuel: *Heights in number fields*, Bull. Soc. Math. France **107** (1979), 433–449.

[8] J.H. Silverman: The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics **106**, Springer, New York, 1985.

[9] J. Vélu: *Isogénies entre courbes elliptiques*, C.R. Acad. Sc. Paris **273** (1971), 238–241.

[10] T. Watanabe: *The Hardy-Littlewood property of flag varieties*, Nagoya Math. J. **170** (2003), 185–211.

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