Sato, A.
Osaka J. Math.
38 (2001), 811–825

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

ATSUSHI SATO

(Received February 24, 1999)

1. Introduction

Let k be a number field of finite degree and $\overline{k}$ an algebraic closure of k, and let E/k be an elliptic curve which is given by the Weierstrass equation of the form $y^2 = f(x)$, where $f(x) \in k[x]$ is a cubic polynomial. For a subset Ξ of $\mathbb{P}^1(k)$ (regarded as $k \cup \{\infty\}$), we denote the set $\{P \in E(\overline{k})\ ;\ x(P) \in \Xi\}$ by $x^{-1}(\Xi)$. That is,

$$x^{-1}(\Xi) = \{(x, y) = (\xi, \pm\sqrt{f(\xi)})\ ;\ \xi \in \Xi\},$$

if $\infty \notin \Xi$. Let $H_{\mathbb{P}^1} : \mathbb{P}^1(\overline{k}) \to \mathbb{R}$ be the standard absolute (exponential) height, and let $H_x = H_{\mathbb{P}^1} \circ x : E(\overline{k}) \to \mathbb{R}$ be the height relative to x. Then we have

$$(\ddagger) \qquad \sharp\{P \in x^{-1}(\mathbb{P}^1(k))\ ;\ H_x(P) \le T\} \asymp T^{2[k:\mathbb{Q}]} \quad \text{as } T \to \infty$$

(see e.g., [4, pp. 70–75]).

The class numbers 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. We quote a classical result due to T. Honda [2], in which he treats the case $k = \mathbb{Q}$ (see Section 3 for details).

Proposition 1.1 (Honda). *Let $f(x) = 4x^3 - 27n^2$ (n is a nonzero integer), and let ξ be an integer satisfying the following three conditions*:
(C0) $\sqrt{f(\xi)} \notin \mathbb{Q}$.
(C1) $F_\xi(z) = z^3 - \xi z + n \in \mathbb{Z}[z]$ *is irreducible over* $\mathbb{Q}$.
(C2) $(\xi, 3n) = 1$.
Then, the class number of the quadratic field $\mathbb{Q}(\sqrt{f(\xi)})$ *is divisible by* 3.

We note that all but finitely many $\xi \in \mathbb{Z}$ satisfy the conditions (C0) and (C1):

$$\sharp\{\xi \in \mathbb{Z}\ ;\ \sqrt{f(\xi)} \in \mathbb{Q}\} = \sharp\{(\xi, \eta) \in \mathbb{Z}^2\ ;\ \eta^2 = f(\xi),\ \eta \ge 0\} < \infty,$$
$$\sharp\{\xi \in \mathbb{Z}\ ;\ F_\xi(z) \text{ is reducible over } \mathbb{Q}\} = \sharp(\{\zeta^2 + n\zeta^{-1}\ ;\ \zeta \in \mathbb{Z}, \neq 0\} \cap \mathbb{Z}) < \infty.$$

Hence, putting Ξ the set of such $\xi \in \mathbb{Z}$ that satisfy the above three conditions (C0)–

(C2), we have $3|h_{\mathbb{Q}(P)}$ for any $P \in x^{-1}(\Xi)$ and

$$\sharp\{P \in x^{-1}(\Xi)\ ;\ H_x(P) \le T\} \sim 2\sharp\{\xi \in \mathbb{Z}\ ;\ (\xi, 3n) = 1,\ |\xi| \le T\} \asymp T \quad \text{as } T \to \infty.$$

Consequently, in view of the asymptotic formula (‡), we might say: *For quite a few points $P \in x^{-1}(\mathbb{P}^1(\mathbb{Q}))$, the class number of $\mathbb{Q}(P)$ is divisible by* 3.

We generalize these results into the following form:

Theorem 1.2. *Let $f(x) = 4x^3 - 27n^2$ (n is a nonzero integer in k), and let Ξ^* be the set of such $\xi \in k$ that satisfy the following two conditions*:
(C1)* $F_\xi(z) = z^3 - \xi z + n \in k[z]$ *is irreducible over k.*
(C2)* $\mathrm{ord}_{\mathfrak{p}}(\xi) \le 0$ *for all prime divisors $\mathfrak{p}$ in k of $3n$.*
Then:
(i) *For any $P \in x^{-1}(\Xi^*)$, the class number of the field $k(P)$ is divisible by* 3.
(ii) *When $k = \mathbb{Q}$, we have*

$$\sharp\{P \in x^{-1}(\Xi^*)\ ;\ H_x(P) \le T\} = \frac{24}{\pi^2}\left(\prod_{\substack{p\ \text{prime}\\ p|3n}} \frac{p}{p+1}\right) T^2 + O(T\log T) \quad \text{as } T \to \infty.$$

We will show the theorem in Sections 4 and 5. Roughly speaking, our method to prove the former assertion of the theorem is closely related to the proof of the Weak Mordell-Weil Theorem and is considered as a geometric counterpart of Honda's.

The above theorem together with

$$\sharp\{P \in x^{-1}(\mathbb{P}^1(\mathbb{Q}))\ ;\ H_x(P) \le T\} = \frac{24}{\pi^2} T^2 + O(T\log T) \quad \text{as } T \to \infty$$

(the precise form of (‡) in the case where $k = \mathbb{Q}$) imply:

Corollary 1.3. *When $k = \mathbb{Q}$, the points $P \in x^{-1}(\mathbb{P}^1(\mathbb{Q}))$ for which the class number of $\mathbb{Q}(P)$ is divisible by* 3 *have a positive density in the whole set $x^{-1}(\mathbb{P}^1(\mathbb{Q}))$:*

$$\liminf_{T\to\infty} \frac{\sharp\{P \in x^{-1}(\mathbb{P}^1(\mathbb{Q}))\ ;\ 3|h_{\mathbb{Q}(P)},\ H_x(P) \le T\}}{\sharp\{P \in x^{-1}(\mathbb{P}^1(\mathbb{Q}))\ ;\ H_x(P) \le T\}} \ge \prod_{\substack{p\ \text{prime}\\ p|3n}} \frac{p}{p+1}.$$

ACKNOWLEDGEMENT. The author would like to express his thanks to Professor Shigeki Akiyama for improving the latter assertion of the theorem.

2. Some basic facts

In this section, we recall some facts on the quadratic twists and the field extensions arising from an isogeny, which will play an important role in our theorem and

its proof. We do not attempt at complete generality and concentrate on what we need later. See e.g., [5] for details.

2.1. The quadratic twists Let k be a number field of finite degree and E/k an elliptic curve. For $d \in k^\times/k^{\times 2}$, let $\chi_d : \mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(E)$ be the homomorphism defined by

$$\chi_d(\sigma) = \begin{cases} 1 \text{ if } \sqrt{d}^{\,\sigma} = \sqrt{d} \\ -1 \text{ if } \sqrt{d}^{\,\sigma} = -\sqrt{d} \end{cases}.$$

Here, $\mathrm{Gal}(\cdot)$ denotes the Galois group. Then, there exist an elliptic curve E_d/k and an isomorphism $\theta_d : E_d \to E$ defined over $k(\sqrt{d})$ such that

$$\chi_d(\sigma) = \theta_d^\sigma \circ \theta_d^{-1} \quad \text{for all } \sigma \in \mathrm{Gal}(\overline{k}/k).$$

The elliptic curve E_d and the isomorphism θ_d are uniquely determined by d up to isomorphism over k, and E_d is called the quadratic twist of E with respect to $k(\sqrt{d})/k$, if $d \not\equiv 1 (\mathrm{mod}\ k^{\times 2})$ (E_d is isomorphic to E over k, if $d \equiv 1 (\mathrm{mod}\ k^{\times 2})$). Furthermore, the image of $E_d(k)$ by θ_d is characterized in $E(k(\sqrt{d}))$ as

$$\theta_d(E_d(k)) = \{P \in E(k(\sqrt{d})) \ ; \ P^\sigma = \chi_d(\sigma)P \text{ for all } \sigma \in \mathrm{Gal}(\overline{k}/k)\}.$$

If E is given by the Weierstrass equation of the form $y^2 = f(x)$ with a cubic polynomial $f(x) \in k[x]$, we can choose the equation for E_d of the form $dy_d^2 = f(x_d)$. Then the isomorphism $\theta_d : E_d \to E$ is given by $x = x_d$, $y = \sqrt{d}\, y_d$. Thus,

$$\theta_d(E_d(k)) = \left\{(x, y) = \left(\xi, \pm\sqrt{f(\xi)}\right) \ ; \ \xi \in k, \ f(\xi) \equiv d \ (\mathrm{mod}\ k^{\times 2})\right\} \cup E[2](k).$$

Hence we have

$$x^{-1}(\mathbb{P}^1(k)) = \bigcup_{d \in k^\times/k^{\times 2}} \theta_d(E_d(k)).$$

We note that the above union is almost disjoint in the following sense:

$$\theta_d(E_d(k)) \cap \theta_{d'}(E_{d'}(k)) = E[2](k) \qquad \text{if } d \not\equiv d' \pmod{k^{\times 2}}.$$

2.2. The field extensions arising from an isogeny Let k be a number field of finite degree, E/k (resp. E'/k) an elliptic curve which is given by the Weierstrass equation of the form $y^2 = f(x)$ (resp. $v^2 = g(u)$) with a cubic polynomial $f(x) \in k[x]$ (resp. $g(u) \in k[u]$), and let $\lambda : E' \to E$ be an isogeny defined over k. We assume that $\mathrm{Ker}\,\lambda$ is contained in $E'(k)$ and that $l = \deg \lambda$ is an odd prime number. Then there exist rational functions $\lambda_x(u)$, $\lambda_x^*(u)$, $\lambda_y(u)$, $\lambda_y^*(u) \in k(u)$ for which the isogeny λ is given

by

$$x = \lambda_x(u) + \lambda_x^*(u)v, \qquad y = \lambda_y^*(u) + \lambda_y(u)v.$$

Since $\lambda(u, -v) = (x, -y)$, we have $\lambda_x^*(u) = \lambda_y^*(u) = 0$. For $Q \in E'(\overline{k})$, let ord_Q denote the normalized valuation on $k(E')$ attached to Q. Then we have

$$\mathrm{ord}_Q(\lambda_x(u)) < 0 \iff \mathrm{ord}_Q(\lambda_y(u)v) < 0 \iff Q \in \mathrm{Ker}\,\lambda.$$

For each $Q \in \mathrm{Ker}\,\lambda$, the equality $(\lambda_y(u)v)^2 = f(\lambda_x(u))$ implies

$$2\,\mathrm{ord}_Q(\lambda_y(u)) + 2\,\mathrm{ord}_Q(v) = 3\,\mathrm{ord}_Q(\lambda_x(u)) < 0.$$

In the case of $Q \neq O$, we have $\mathrm{ord}_Q(v) = 0$, because l is odd, and hence

$$2\,\mathrm{ord}_Q(\lambda_y(u)) = 3\,\mathrm{ord}_Q(\lambda_x(u)) < 0.$$

Therefore, we can write $\lambda_x(u)$ and $\lambda_y(u)$ as

$$\lambda_x(u) = \frac{\lambda_x^{(1)}(u)}{\lambda^{(2)}(u)^2}, \qquad \lambda_y(u) = \frac{\lambda_y^{(1)}(u)}{\lambda^{(2)}(u)^3}$$

with polynomials $\lambda_x^{(1)}(u),\ \lambda_y^{(1)}(u),\ \lambda^{(2)}(u) \in k[u]$ satisfying

$$(\lambda_x^{(1)}(u),\ \lambda^{(2)}(u)) = (\lambda_y^{(1)}(u),\ \lambda^{(2)}(u)) = 1.$$

Here, it follows from

$$\mathrm{ord}_O(\lambda_x(u)) = \left(\deg \lambda_x^{(1)}(u) - 2\deg \lambda^{(2)}(u)\right) \mathrm{ord}_O(u) < 0$$

and

$$l = [k(u) : k(x)] = \max\{\deg \lambda_x^{(1)}(u),\ 2\deg \lambda^{(2)}(u)\}$$

that

$$\deg \lambda_x^{(1)}(u) = l, \qquad \deg \lambda^{(2)}(u) < \frac{l}{2}.$$

Moreover, it is easy to verify

$$\deg \lambda_y^{(1)}(u) = \frac{3(l-1)}{2}.$$

For $\xi \in k$, we put

$$\Lambda_\xi(u) = \lambda_x^{(1)}(u) - \xi\lambda^{(2)}(u)^2 \in k[u].$$

Then, for $P \in x^{-1}(\mathbb{P}^1(k)) - E[2](k)$ given by $(x, y) = (\xi, \eta)$, we have

$$\lambda^{-1}(P) = \left\{ (u, v) = \left(\zeta\,,\ \frac{\eta}{\lambda_y(\zeta)} \right)\ ;\ \zeta \in \overline{k},\ \ \Lambda_\xi(\zeta) = 0 \right\}$$

(note that $\Lambda_\xi(\zeta) = 0$ implies $\lambda_y^{(1)}(\zeta) \neq 0$ and $\lambda^{(2)}(\zeta) \neq 0$), and hence

$$\sharp\{\zeta \in \overline{k}\ ;\ \Lambda_\xi(\zeta) = 0\} = \sharp\lambda^{-1}(P) = l = \deg \Lambda_\xi(u).$$

Thus $\Lambda_\xi(u)$ does not have multiplicative roots, and $k(\lambda^{-1}(P))$ is the splitting field of $\Lambda_\xi(u)$ over $k(P) = k(\eta)$.

For $P \in E(\overline{k})$, the map

$$\mathrm{Gal}(k(\lambda^{-1}(P))/k(P)) \longrightarrow \mathrm{Ker}\,\lambda, \qquad \sigma \longmapsto Q^\sigma - Q,$$

Q is a point in $\lambda^{-1}(P)$, is an injective homomorphism. Since l is prime, $k(\lambda^{-1}(P))/k(P)$ is a cyclic extension of degree 1 or l according as $P \in \lambda(E'(k(P)))$ or not, and we have $k(\lambda^{-1}(P)) = k(P, Q)$ for any $Q \in \lambda^{-1}(P)$. Furthermore, one easily observes:

Lemma 2.1. *Let the notation and the assumptions be as above. Then, for* $P \in x^{-1}(\mathbb{P}^1(k)) - E[2](k)$ *whose* x*-coordinate is* ξ*, the following conditions are equivalent*:
(a) $\xi = \lambda_x(\zeta)$ *for some* $\zeta \in k$ *satisfying* $\lambda^{(2)}(\zeta) \neq 0$.
(b) $\Lambda_\xi(u)$ *is reducible over* k.
(c) $k(\lambda^{-1}(P)) = k(P)$.

3. Honda's result

In this section, we briefly review the proof of Proposition 1.1 due to Honda. As is seen in [2], his method is concerned with certain isogenies of elliptic curves. Namely, let $E/\mathbb{Q}$ (resp. $E'/\mathbb{Q}$) be the elliptic curve which is given by the Weierstrass equation $y^2 = 4x^3 - 27n^2$ (resp. $v^2 = 4nu^3 + 1$), and let $\lambda : E' \to E$ be the isogeny defined over $\mathbb{Q}$ which is given by

$$x = \frac{1 + nu^3}{u^2}, \qquad y = \frac{2 - nu^3}{u^3}\, v.$$

Then, $\deg \lambda = 3$ and $\mathrm{Ker}\,\lambda = \{(u, v) = (0, 1),\ (0, -1)\} \cup \{O\}$ is contained in $E'(\mathbb{Q})$. Thus we can apply the whole argument in Section 2.2. We may take $1 + nu^3$ and u as $\lambda_x^{(1)}(u)$ and $\lambda^{(2)}(u)$, respectively, and then we have

$$\Lambda_\xi(u) = nu^3 - \xi u^2 + 1.$$

For $P \in x^{-1}(\mathbb{Q})$ whose x-coordinate is ξ, it is clear that the condition (C0) is equivalent to the condition $[\mathbb{Q}(P) : \mathbb{Q}] = 2$. Moreover, under the assumption $f(\xi) \neq 0$,

the condition (C1) is equivalent to the condition $[\mathbb{Q}(\lambda^{-1}(P)) : \mathbb{Q}(P)] = 3$ because of Lemma 2.1 and

$$F_\xi(z) = z^3 \Lambda_\xi\left(\frac{1}{z}\right).$$

We also note that E has good reduction at every prime which does not divide $3n$.

Proof of Proposition 1.1 (cf. also, [3]). Let ξ be an integer which satisfies the three conditions (C0)–(C2), and let P be a point in $x^{-1}(\{\xi\})$. Putting $K = \mathbb{Q}(P) = \mathbb{Q}(\sqrt{f(\xi)})$ and $K' = \mathbb{Q}(\lambda^{-1}(P))$, we have $[K : \mathbb{Q}] = 2$ and $[K' : K] = 3$ because of the assumptions (C0) and (C1). Since the discriminant of the cubic polynomial $F_\xi(z)$ equals $f(\xi)$, K' is the splitting field of $F_\xi(z)$ over $\mathbb{Q}$, and hence $K'/\mathbb{Q}$ is a dihedral extension of degree 6. We shall prove that K'/K is unramified. Let K'' be a cubic subfield of K'. If a prime divisor in K of a prime number p were ramified in K', p must have been fully ramified in K''. Therefore we should have a congruence

$$F_\xi(z) \equiv (z - \alpha)^3 \pmod{p}$$

with some $\alpha \in \mathbb{Z}$. Comparing the both sides of the congruence, we should have either $p|(\xi, n)$ or $3|\xi$, which would contradict the assumption (C2). □

REMARK 3.1. Honda's original result [2, Proposition 10] showed not only Proposition 1.1 but also its inverse. Thus, he also proved: *If the class number of a quadratic field K is divisible by 3, K is of the form $\mathbb{Q}(\sqrt{f(\xi)})$ for some n and some $\xi \in \mathbb{Z}$ which satisfies the conditions* (C0)–(C2) (note that the polynomial $f(x)$ and the three conditions depend on the choice of n).

4. Proof of the theorem (part 1)

In this section, we give a proof of Theorem 1.2, (i). Our method is concerned with certain isogenies of elliptic curves as well as Honda's, and we use the elliptic curve and the isogeny which are defined by the same manner as in Section 3. Namely, let E'/k be the elliptic curve which is given by the Weierstrass equation $v^2 = 4nu^3 + 1$, and let $\lambda : E' \to E$ be the isogeny defined over k which is given by

$$x = \frac{1 + nu^3}{u^2}, \qquad y = \frac{2 - nu^3}{u^3}\, v.$$

Then, $\deg \lambda = 3$, $\operatorname{Ker} \lambda \subseteq E'(k)$, and we can apply the whole argument in Section 2.2. We have

$$\Lambda_\xi(u) = nu^3 - \xi u^2 + 1$$

as well as in Section 3. For $P \in x^{-1}(\mathbb{P}^1(k)) - E[2](k)$ whose x-coordinate is ξ, the condition (C1)* is equivalent to the condition $[k(\lambda^{-1}(P)) : k(P)] = 3$ because of

Lemma 2.1. Putting

$$U = nu, \qquad V = \frac{n(v+1)}{2},$$

we have another Weierstrass equation for E'/k

$$(*) \qquad V^2 - nV = U^3,$$

whose discriminant is $-27n^4$, and then,

$$\operatorname{Ker}\lambda = \{(U, V) = (0, 0),\ (0, n)\} \cup \{O\}.$$

Now, we fix a point P in $x^{-1}(\Xi^*)$ given by $(x, y) = (\xi, \eta)$ and put

$$K = k(P) = k(\eta), \qquad K' = k(\lambda^{-1}(P)), \qquad G = \operatorname{Gal}(K'/K).$$

Then we have $[K : k] \leq 2$ and $[K' : K] = 3$, for $P \notin E[2](k)$ follows from the assumption (C2)*. Moreover, for any $Q \in \lambda^{-1}(P)$, we have $K' = K(Q)$ and

$$Q^\sigma - Q \in \operatorname{Ker}\lambda \quad \text{for all } \sigma \in G.$$

Theorem 1.2, (i) is an immediate consequence of the following proposition and the class field theory (note that a Galois extension of odd degree is unramified at every infinite place):

Proposition 4.1. *Let the notation and the assumptions be as above. Then, the extension K'/K is unramified at every finite place.*

For the time being, we use the following notation:

$\mathfrak{P}$	a prime ideal in K.
$\mathfrak{P}'$	a prime divisor in K' of $\mathfrak{P}$.
κ'	the residue field of $\mathfrak{P}'$.
D	the decomposition group for $\mathfrak{P}'/\mathfrak{P}$.
I	the inertia group for $\mathfrak{P}'/\mathfrak{P}$.

As the first step to show Proposition 4.1, we shall consider the reduction of E' modulo $\mathfrak{P}'$. Namely, let

$$E'(K') \longrightarrow (E' \bmod \mathfrak{P}')(\kappa'), \qquad Q \longmapsto Q \bmod \mathfrak{P}'$$

be the reduction map modulo $\mathfrak{P}'$ with respect to the Weierstrass equation $(*)$. We define two subsets of $E'(K')$ as

$$E'_0(K'; \mathfrak{P}') = \{Q \in E'(K')\ ;\ Q \bmod \mathfrak{P}' \in (E' \bmod \mathfrak{P}')_{\mathrm{ns}}(\kappa')\},$$
$$E'_1(K'; \mathfrak{P}') = \{Q \in E'(K')\ ;\ Q \bmod \mathfrak{P}' = O \bmod \mathfrak{P}'\}.$$

Note that the equation $(*)$ is not necessarily minimal. Thus the two subsets defined above are not uniquely determined by E', K' and by $\mathfrak{P}'$, in general. However, we can verify that $E'_0(K';\mathfrak{P}')$ is a subgroup of $E'(K')$, and that the map $E'_0(K';\mathfrak{P}') \to (E' \bmod \mathfrak{P}')_{\mathrm{ns}}(\kappa')$ is a homomorphism with its kernel $E'_1(K';\mathfrak{P}')$. We can characterize $E'_0(K';\mathfrak{P}')$ and $E'_1(K';\mathfrak{P}')$ in $E'(K')$ in terms of $\mathfrak{P}'$-adic valuations of U-coordinates as follows:

Lemma 4.2. *Being the notation as above, we have*

$$E'_0(K';\mathfrak{P}') = \begin{cases} \{(U,V) = (\zeta,\omega)\ ;\ \mathrm{ord}_{\mathfrak{P}'}(\zeta^3 + n^2) \le 0\} \cup \{O\} & \text{if } \mathfrak{P}|3n, \\ E'(K') & \text{otherwise} \end{cases}$$

and

$$E'_1(K';\mathfrak{P}') = \{(U,V) = (\zeta,\omega)\ ;\ \mathrm{ord}_{\mathfrak{P}'}(\zeta) < 0\} \cup \{O\}.$$

Proof. The latter equality is clear. We show the former one.

In the case of $\mathfrak{P} \nmid 3n$, the elliptic curve E' has good reduction at $\mathfrak{P}'$, and hence we have $E'_0(K';\mathfrak{P}') = E'(K')$.

Suppose that $\mathfrak{P}|3n$. Then, for $Q \in E'(K') - \{O\}$ given by $(U,V) = (\zeta,\omega)$, the condition $Q \notin E'_0(K';\mathfrak{P}')$ is equivalent to

$$\mathrm{ord}_{\mathfrak{P}'}(\zeta) \ge 0, \qquad \mathrm{ord}_{\mathfrak{P}'}(3\zeta^2) > 0 \quad \text{and} \quad \mathrm{ord}_{\mathfrak{P}'}(2\omega - n) > 0.$$

Here, we may replace the condition $\mathrm{ord}_{\mathfrak{P}'}(2\omega - n) > 0$ by $\mathrm{ord}_{\mathfrak{P}'}(\zeta^3 + n^2) > 0$, for

$$(2\omega - n)^2 = 4\zeta^3 + n^2 = 3\zeta^3 + (\zeta^3 + n^2).$$

Furthermore, the condition $\mathrm{ord}_{\mathfrak{P}'}(\zeta^3 + n^2) > 0$ implies $\mathrm{ord}_{\mathfrak{P}'}(\zeta) \ge 0$ and $\mathrm{ord}_{\mathfrak{P}'}(3\zeta^2) > 0$. Thus $Q \notin E'_0(K';\mathfrak{P}')$ holds if and only if $\mathrm{ord}_{\mathfrak{P}'}(\zeta^3 + n^2) > 0$, and hence we obtain the desired equality. □

As the second step, we show $\lambda^{-1}(P) \cap E'_0(K';\mathfrak{P}') \neq \emptyset$.

Lemma 4.3. *Let the notation and the assumptions be as above. Then, at least one point in $\lambda^{-1}(P)$ is contained in $E'_0(K';\mathfrak{P}')$.*

Proof. In the case where $\mathfrak{P} \nmid 3n$, the assertion is clear.

Suppose that $\mathfrak{P}|3n$. Let $\lambda^{-1}(P) = \{Q_1, Q_2, Q_3\}$, and let ζ_i denote the U-coordinate of Q_i. Then, the cubic polynomial

$$n^2 \Lambda_\xi\left(\frac{U}{n}\right) = U^3 - \xi U^2 + n^2 \in k[U]$$

is decomposed as

$$U^3 - \xi U^2 + n^2 = (U - \zeta_1)(U - \zeta_2)(U - \zeta_3).$$

Comparing the both sides of the equality, we have

$$\zeta_1 + \zeta_2 + \zeta_3 = \xi.$$

Hence $\mathrm{ord}_{\mathfrak{P}'}(\zeta_{i_0}) \leq 0$ holds for some $i_0 \in \{1, 2, 3\}$ because of the assumption (C2)*, and then,

$$\mathrm{ord}_{\mathfrak{P}'}(\zeta_{i_0}^3 + n^2) = \mathrm{ord}_{\mathfrak{P}'}(\xi\zeta_{i_0}^2) = \mathrm{ord}_{\mathfrak{P}'}(\xi) + 2\,\mathrm{ord}_{\mathfrak{P}'}(\zeta_{i_0}) \leq 0.$$

Thus, $Q_{i_0} \in E_0'(K'; \mathfrak{P}')$. □

REMARK 4.4. In fact, we have $\lambda^{-1}(P) \subseteq E_0'(K'; \mathfrak{P}')$ if $\mathfrak{P} \nmid n$.

As the third step, we show that $\mathfrak{P}$ is unramified in K' (i.e., $I = \{1\}$) assuming that $\mathfrak{P}$ is not decomposed in K' (i.e., $D = G$).

Lemma 4.5. *With the notation and the assumptions as above, we also assume that $\mathfrak{P}$ is not decomposed in K'. Then, $\mathfrak{P}$ is unramified in K'.*

Proof. Under the assumption $D = G$, the prime ideal $\mathfrak{P}'$ is the unique prime divisor in K' of $\mathfrak{P}$, and the subsets $E_0'(K'; \mathfrak{P}')$ and $E_1'(K'; \mathfrak{P}')$ of $E'(K')$ are G-stable. Hence, for any $Q \in E_0'(K'; \mathfrak{P}')$, we have

$$Q^\sigma - Q \in E_1'(K'; \mathfrak{P}') \quad \text{for all } \sigma \in I.$$

Let Q be a point in $\lambda^{-1}(P) \cap E_0'(K'; \mathfrak{P}')$, which is a nonempty set by Lemma 4.3. Since $\mathrm{Ker}\,\lambda \cap E_1'(K'; \mathfrak{P}') = \{O\}$, we have

$$Q^\sigma = Q \quad \text{for all } \sigma \in I.$$

On the other hand, we have $K' = K(Q)$. Thus, $I = \{1\}$. □

Since $D \neq G$ implies $D = \{1\}$ and $I = \{1\}$, we obtain Proposition 4.1.

REMARK 4.6. In the case where $\mathfrak{P}|n$, we can show $D = \{1\}$ without using the reduction map.

Finally, we shall mention the condition (C2)*. Putting

$$X = x, \qquad Y = \frac{y + n}{2},$$

we have another Weierstrass equation for E/k

$$Y^2 - nY = X^3 - 7n^2.$$

Let K be a finite extension of k. For a prime ideal $\mathfrak{P}$ in K, let

$$E(K) \longrightarrow (E \bmod \mathfrak{P})(\kappa), \qquad P \longmapsto P \bmod \mathfrak{P}$$

be the reduction map modulo $\mathfrak{P}$ with respect to the above equation, where κ denotes the residue field of $\mathfrak{P}$. We define a subset $E_0(K;\mathfrak{P})$ of $E(K)$ in the same manner as before:

$$E_0(K;\mathfrak{P}) = \{P \in E(K)\ ;\ P \bmod \mathfrak{P} \in (E \bmod \mathfrak{P})_{\mathrm{ns}}(\kappa)\}.$$

Then, it is easy to verify

$$E_0(K;\mathfrak{P}) = \begin{cases} \{(X,Y) = (\xi,\eta)\ ;\ \mathrm{ord}_{\mathfrak{P}}(\xi) \le 0\} \cup \{O\} & \text{if } \mathfrak{P}|3n, \\ E(K) & \text{otherwise.} \end{cases}$$

Thus, a point P in $E(K) \cap x^{-1}(k)$ is contained in $\bigcap_{\mathfrak{P}} E_0(K;\mathfrak{P})$ if and only if its X-coordinate ($= x$-coordinate) ξ satisfies the condition (C2)*.

5. Proof of the theorem (part 2)

In this section, we give a proof of Theorem 1.2, (ii).

First, we prove asymptotic formulas, due to S. Akiyama [1], for the partial sums of two arithmetical functions.

Proposition 5.1. *Let N be a positive integer. We define two arithmetical functions φ_N and ψ_N by*

$$\varphi_N(m) = \sharp\{i \in \mathbb{Z}\ ;\ 0 < i \le m,\ (Ni, m) = 1\},$$
$$\psi_N(m) = \sharp\{i \in \mathbb{Z}\ ;\ 0 < i \le m,\ (i, Nm) = 1\}.$$

Then,

$$\sum_{m \le T} \varphi_N(m) = c_N T^2 + O(T \log T), \qquad \sum_{m \le T} \psi_N(m) = c_N T^2 + O(T \log T) \quad \text{as } T \to \infty,$$

where

$$c_N = \frac{3}{\pi^2} \prod_{\substack{p \text{ prime} \\ p|N}} \frac{p}{p+1}.$$

REMARK 5.2. (i) When $N = 1$, we have $\varphi_1 = \psi_1 = \varphi$, where φ is the Euler totient function. In this case, the asymptotic formulas are well-known (we regard c_1 as $3/\pi^2$).
(ii) The functions φ_N, ψ_N and the constant c_N depend only on the prime divisors of N.
(iii) One easily observes

$$\varphi_N(m) = \sharp\{\xi \in \mathbb{Q} \ ; \ \xi \geq 1, \ \mathrm{ord}_p(\xi) \leq 0 \text{ for all } p \in S, \ H_{\mathbb{P}^1}(\xi) = m\},$$
$$\psi_N(m) = \sharp\{\xi \in \mathbb{Q} \ ; \ 0 < \xi \leq 1, \ \mathrm{ord}_p(\xi) \leq 0 \text{ for all } p \in S, \ H_{\mathbb{P}^1}(\xi) = m\}.$$

Here, S denotes the set of prime divisors of N.

Corollary 5.3. *For any finite set S of prime numbers, we have*

$$\sharp\{\xi \in \mathbb{Q} \ ; \ \mathrm{ord}_p(\xi) \leq 0 \text{ for all } p \in S, \ H_{\mathbb{P}^1}(\xi) \leq T\} = c_S T^2 + O(T \log T) \quad \text{as } T \to \infty,$$

where

$$c_S = \frac{12}{\pi^2} \prod_{p \in S} \frac{p}{p+1}.$$

We will give a proof of Proposition 5.1 after showing two lemmas. For a positive integer j, we shall denote the integer $j/(j, N)$ by j^*. Then we can rewrite φ_N and ψ_N with the Möbius function as follows:

Lemma 5.4. *We have*

$$\varphi_N(m) = \sum_{j|m} \mu(j) \frac{m}{j^*}, \qquad \psi_N(m) = \sum_{j|Nm} \mu(j) \left[\frac{m}{j}\right].$$

Here, μ is the Möbius function.

Proof. We start with the relations

$$\varphi_N(m) = \sum_{i=1}^{m} \sum_{j|(Ni,m)} \mu(j), \qquad \psi_N(m) = \sum_{i=1}^{m} \sum_{j|(i,Nm)} \mu(j),$$

and obtain

$$\varphi_N(m) = \sum_{j|m} \mu(j) \sum_{\substack{i \leq m \\ j^*|i}} 1 = \sum_{j|m} \mu(j) \frac{m}{j^*}, \qquad \psi_N(m) = \sum_{j|Nm} \mu(j) \sum_{\substack{i \leq m \\ j|i}} 1 = \sum_{j|Nm} \mu(j) \left[\frac{m}{j}\right].$$

□

The constant c_N in Proposition 5.1 is related to Möbius function in the following manner:

Lemma 5.5. *We have*

$$\sum_{j=1}^{\infty} \frac{\mu(j)}{jj^*} = 2c_N.$$

Proof. One easily observes that the function $\mu(\cdot)(\cdot, N)$ is multiplicative:

$$\mu(jj')(jj', N) = \mu(j)(j, N) \cdot \mu(j')(j', N) \quad \text{whenever } (j, j') = 1.$$

Hence the series

$$\sum_{j=1}^{\infty} \frac{\mu(j)}{jj^*} = \sum_{j=1}^{\infty} \frac{\mu(j)(j, N)}{j^2},$$

which is dominated by $N \sum_{j=1}^{\infty} j^{-2}$, has the Euler product and coincides with

$$\prod_p \left(\sum_{e=0}^{\infty} \frac{\mu(p^e)(p^e, N)}{p^{2e}} \right) = \prod_p \left(1 - \frac{(p, N)}{p^2} \right) = \prod_{p|N} \left(1 - \frac{1}{p} \right) \cdot \prod_{p \nmid N} \left(1 - \frac{1}{p^2} \right) = 2c_N.$$

□

Proof of Proposition 5.1. It follows from Lemma 5.4 that

$$\sum_{m \le T} \varphi_N(m) = \sum_{m \le T} m \sum_{j|m} \frac{\mu(j)}{j^*} = \sum_{j \le T} \frac{\mu(j)}{j^*} \sum_{\substack{m \le T \\ j|m}} m$$

and that

$$\sum_{m \le T} \psi_N(m) = \sum_{m \le T} m \sum_{j|Nm} \frac{\mu(j)}{j} + O\left(\sum_{m \le T} \sigma_0(m) \right) = \sum_{j \le NT} \frac{\mu(j)}{j} \sum_{\substack{m \le T \\ j^* | m}} m + O(T \log T).$$

Here, $\sigma_0(m)$ denotes the number of divisors of m, and we have used

$$\left| \sum_{j|Nm} \mu(j) \right| \le \sigma_0(Nm) \le \sigma_0(N)\sigma_0(m)$$

to obtain the latter equality. Hence we have

$$\sum_{m \le T} \varphi_N(m) = \frac{1}{2} \sum_{j \le T} \frac{\mu(j)}{jj^*} T^2 + O(T \log T),$$

$$\sum_{m \le T} \psi_N(m) = \frac{1}{2} \sum_{j \le NT} \frac{\mu(j)}{jj^*} T^2 + O(T \log T)$$

by

$$\sum_{\substack{m\le T\\ j\mid m}} m = \sum_{m\le T/j} jm = \frac{j}{2}\left[\frac{T}{j}\right]\left(\left[\frac{T}{j}\right]+1\right) = \frac{T^2}{2j}+O(T),$$
$$\sum_{\substack{m\le T\\ j^*\mid m}} m = \sum_{m\le T/j^*} j^*m = \frac{j^*}{2}\left[\frac{T}{j^*}\right]\left(\left[\frac{T}{j^*}\right]+1\right) = \frac{T^2}{2j^*}+O(T)$$

and by

$$\left|\sum_{j\le T}\frac{\mu(j)}{j^*}\right| \le N\sum_{j\le T}\frac{1}{j} \sim N\log T, \qquad \left|\sum_{j\le NT}\frac{\mu(j)}{j}\right| \le \sum_{j\le NT}\frac{1}{j} \sim \log T.$$

On the other hand, one easily observes

$$\sum_{j\le T}\frac{\mu(j)}{jj^*} = \sum_{j=1}^{\infty}\frac{\mu(j)}{jj^*}+O\left(\frac{1}{T}\right), \qquad \sum_{j\le NT}\frac{\mu(j)}{jj^*} = \sum_{j=1}^{\infty}\frac{\mu(j)}{jj^*}+O\left(\frac{1}{T}\right).$$

Thus the desired formulas follow from Lemma 5.5. □

Next, we show the following asymptotic formula:

Proposition 5.6. *Let the notation and the assumptions be as in* Section 2.2. *Then,*

$$\sharp\{\xi\in k\ ;\ \Lambda_\xi(u) \text{ is reducible over } k,\ H_{\mathbb{P}^1}(\xi)\le T\} \asymp T^{2[k:\mathbb{Q}]/l} \quad \text{as } T\to\infty.$$

Corollary 5.7. *Let the notation and the assumptions be as in* Theorem 1.2. *Then,*

$$\sharp\{\xi\in k\ ;\ F_\xi(z) \text{ is reducible over } k,\ H_{\mathbb{P}^1}(\xi)\le T\} \asymp T^{2[k:\mathbb{Q}]/3} \quad \text{as } T\to\infty.$$

Theorem 1.2, (ii) immediately follows from Corollaries 5.3 and 5.7.

Proof of Proposition 5.6. It follows from Lemma 2.1 that

$$\sharp\{\xi\in k\ ;\ \Lambda_\xi(u) \text{ is reducible over } k,\ H_{\mathbb{P}^1}(\xi)\le T\} \asymp \sharp\{\zeta\in k\ ;\ (H_{\mathbb{P}^1}\circ\lambda_x)(\zeta)\le T\}.$$

On the other hand, since $\lambda_x(u)$ is a rational function of degree l, we have

$$H_{\mathbb{P}^1}\circ\lambda_x \asymp H_{\mathbb{P}^1}^l \quad \text{on } \mathbb{P}^1(\bar{k}).$$

Hence we obtain the assertion by the asymptotic formula (‡) in Section 1. □

REMARK 5.8. If we could show

$$\sharp\{\xi \in k \ ; \ \mathrm{ord}_{\mathfrak{p}}(\xi) \leq 0 \text{ for all } \mathfrak{p} \in S, \ H_{\mathbb{P}^1}(\xi) \leq T\} \asymp T^{2[k:\mathbb{Q}]} \quad \text{as } T \to \infty$$

for any finite set S of prime ideals in a number field k, we would obtain

$$\sharp\{P \in x^{-1}(\Xi^*) \ ; \ H_x(P) \leq T\} \asymp T^{2[k:\mathbb{Q}]} \quad \text{as } T \to \infty$$

and

$$\liminf_{T\to\infty} \frac{\sharp\{P \in x^{-1}(\mathbb{P}^1(k)) \ ; \ 3|h_{k(P)}, \ H_x(P) \leq T\}}{\sharp\{P \in x^{-1}(\mathbb{P}^1(k)) \ ; \ H_x(P) \leq T\}} > 0.$$

6. Some remarks

Let k be a number field of finite degree and E/k an elliptic curve which is given by the Weierstrass equation of the form $y^2 = f(x)$ with a cubic polynomial $f(x) \in k[x]$. For $d \in k^\times/k^{\times 2}$, let E_d and θ_d be as in Section 2.1, and we denote the Mordell-Weil rank of E_d over k by r_d. For given $d \in k^\times/k^{\times 2}$, it seems very difficult to determine whether r_d is positive without calculating the Mordell-Weil group $E_d(k)$. Therefore, we cannot characterize such $d \in k^\times/k^{\times 2}$ that satisfy $r_d > 0$ in terms of some arithmetic invariants, such as the class numbers, of the fields $k(\sqrt{d})$ at present. However, we have

$$\sharp\{P \in \theta_d(E_d(k)) \ ; \ H_x(P) \leq T\} \asymp (\log T)^{r_d/2} \quad \text{as } T \to \infty$$

for each $d \in k^\times/k^{\times 2}$ (see e.g., [4, pp. 124–127]), and hence infinitely many $d \in k^\times/k^{\times 2}$ satisfy $r_d > 0$. (One obtains much more precise results by specializing some sections of an elliptic surface. See e.g., [6] and some other papers referred in it.) Moreover, since $\bigcup_{d\in k^\times/k^{\times 2}} \theta_d(E_d(k)_{\mathrm{tor}})$ is known to be a finite set, we have $\theta_d(E_d(k)_{\mathrm{tor}}) = E[2](k)$ for all but finitely many $d \in k^\times/k^{\times 2}$. Thus the condition $r_d > 0$ is equivalent to the condition $\theta_d(E_d(k)) \neq E[2](k)$ with finitely many exceptions. In other words, putting

$$\mathcal{K} = \{k(P) \ ; \ P \in x^{-1}(\mathbb{P}^1(k))\}, \qquad \mathcal{K}_+ = \{k(\sqrt{d}) \ ; \ d \in k^\times/k^{\times 2}, \ r_d > 0\},$$

we have

$$\mathcal{K}_+ \subseteq \mathcal{K}, \qquad \sharp\mathcal{K}_+ = \infty, \qquad \sharp(\mathcal{K} - \mathcal{K}_+) < \infty.$$

Now, let the notation and the assumptions be the same as in Theorem 1.2, and we define two subsets of $\mathcal{K}$ as

$$\mathcal{K}_3 = \{k(P) \ ; \ P \in x^{-1}(\mathbb{P}^1(k)), \ 3|h_{k(P)}\}, \qquad \mathcal{K}(\Xi^*) = \{k(P) \ ; \ P \in x^{-1}(\Xi^*)\}.$$

Then, our results seem to suggest that the set $\mathcal{K}_3 \cap \mathcal{K}_+$ has a positive "density" (in a suitable sense) in the whole set $\mathcal{K}_+$. Indeed, the former assertion of Theorem 1.2 means $\mathcal{K}(\Xi^*) \subseteq \mathcal{K}_3$, while the latter one implies

$$\sharp\mathcal{K}(\Xi^*) = \infty, \qquad \sharp(\mathcal{K}(\Xi^*) - \mathcal{K}_+) < \infty$$

and shows that $x^{-1}(\Xi^*)$ is sufficiently large in $x^{-1}(\mathbb{P}^1(\mathbb{Q}))$. However, that does not help us to estimate the largeness of $\mathcal{K}(\Xi^*)$ in $\mathcal{K}$.

References

[1] S. Akiyama: private communication.

[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] S. Lang: Fundamentals of Diophantine Geometry, Springer, New York, 1983.

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

[6] C.L. Stewart and J. Top: *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943–973.

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