J. Math. Soc. Japan
Vol. 68, No. 2 (2016) pp. 899–915
doi: 10.2969/jmsj/06820899

On the class number divisibility of pairs of quadratic fields obtained from points on elliptic curves

By Yoshichika Iizuka, Yutaka Konomi and Shin Nakano

(Received Aug. 30, 2013)
(Revised July 31, 2014)

Abstract. Let l be the prime $3, 5$ or 7 and let m be a nonzero integer. We give a method for constructing an infinite family of pairs of quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{mD})$ with both class numbers divisible by l. Such quadratic fields are parametrized by rational points on a specified elliptic curve.

Introduction.

Let l be a prime and let K be a number field of finite degree. In his paper [**10**], Sato used an elliptic curve over K with torsion points of order l to construct quadratic extensions K'/K each having a cyclic extension L of degree l unramified at all finite places. Such extensions K' and L are explicitly described by using Vélu's formulas for isogenies of elliptic curves (cf. [**14**]). In particular, for the case $K = \mathbb{Q}$, he gave a family of explicit cubic polynomials $F(X) \in \mathbb{Q}[X]$ such that, for many rational numbers ξ, the class number of $\mathbb{Q}\big(\sqrt{F(\xi)}\big)$ is divisible by $3, 5$ or by 7. This is close to Mestre's earlier work [**7**] that provides a method for constructing quadratic fields whose ideal class groups have l-rank at least 2, in the cases that $l = 5$ and 7. (For $l = 3$, there had been a stronger result due to Craig [**3**] before.)

In the present paper, we follow Sato's arguments to investigate the class number divisibility of pairs of quadratic fields. Our goal is to prove the following result.

Theorem 1. *Let l be any of the primes $3, 5$ or 7. For any given nonzero integer m, there exist infinitely many quadratic fields $\mathbb{Q}\big(\sqrt{D}\big)$ such that the class numbers of $\mathbb{Q}\big(\sqrt{D}\big)$ and $\mathbb{Q}\big(\sqrt{mD}\big)$ are both divisible by l.*

For the 3-divisibility, this has already been proved by Komatsu [**5**]. His proof is based on the rather ingenious and complicated solution of some diophantine equation concerned with the 3-divisibility of the class numbers of quadratic fields. Although, even in this paper, a diophantine equation defined by Sato's explicit cubic polynomials is used, we treat it as an elliptic curve. This enables us to utilize the powerful tools of the arithmetic of elliptic curves.

1. Sato's construction.

We begin with the theorem due to Sato on the class number divisibility of quadratic

2010 *Mathematics Subject Classification.* Primary 11R29, 11R11; Secondary 11G05.
Key Words and Phrases. class number, quadratic field, elliptic curve.

fields. To state the theorem, we require some polynomials that are obtained via Vélu's isogeny formulas and explicitly appeared in [**11**]. For each $l \in \{3, 5, 7\}$, let $F(a, b, X)$ be the cubic polynomial with two parameters a, b as follows:

- For $l = 3$,

$$F(a, b, X) = 4X^3 + a^2X^2 - 18a^3bX - a^4b(4a + 27b).$$

- For $l = 5$,

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

- For $l = 7$,

$$\begin{aligned} F(a, b, X) = 4X^3 &+ (a^4 + 2a^3b + 3a^2b^2 - 6ab^3 + b^4)X^2 \\ &+ 2ab(a - b)(10a^5 - 59a^4b + 81a^3b^2 - 61a^2b^3 + 10ab^4 + 10b^5)X \\ &+ ab(a - b)(4a^9 - 72a^8b + 304a^7b^2 - 727a^6b^3 + 843a^5b^4 \\ &\qquad - 528a^4b^5 + 280a^3b^6 - 148a^2b^7 + 36ab^8 + 4b^9). \end{aligned}$$

The discriminant of $F(a, b, X)$ is given by $16\delta(a, b)$, where

$$\delta(a, b) = \begin{cases} a^8b(a - 27b)^3 & (l = 3), \\ -ab(a^2 + 11ab - b^2)^5 & (l = 5), \\ -ab(a - b)(a^3 + 5a^2b - 8ab^2 + b^3)^7 & (l = 7). \end{cases}$$

We also prepare the polynomial

$$\Lambda(a, b, \xi, X) = I(a, b, X) - \xi J(a, b, X)$$

of degree l with an additional parameter ξ, where $I(a, b, X), J(a, b, X)$ are given as follows:

- For $l = 3$,

$$\begin{aligned} I(a, b, X) &= X^3 + a^3bX + a^4b^2, \\ J(a, b, X) &= X^2. \end{aligned}$$

- For $l = 5$,

$$\begin{aligned} I(a, b, X) &= X^5 + 2abX^4 - ab(a^2 - 3ab - b^2)X^3 \\ &\qquad + 3a^2b^3(a + b)X^2 + a^3b^4(a + 3b)X + a^4b^6, \\ J(a, b, X) &= X^2(X + ab)^2. \end{aligned}$$

- For $l = 7$,

$$\begin{aligned} I(a,b,X) &= X^7 + 2ab(a-b)(a+b)X^6 \\ &\quad - ab(a-b)(a^5 - 7a^4b + 5a^3b^2 - 3a^2b^3 + 2ab^4 + b^5)X^5 \\ &\quad + a^3b^3(a-b)^2(a^4 + 13a^3b - 12a^2b^2 + 9ab^3 - 6b^4)X^4 \\ &\quad + a^4b^4(a-b)^3(a^5 + 7a^4b + 8a^3b^2 - 4a^2b^3 - ab^4 - b^5)X^3 \\ &\quad + a^7b^6(a-b)^4(a+b)(3a^2 + 5ab - 3b^2)X^2 \\ &\quad + a^9b^8(a-b)^5(3a^2 + 3ab - b^2)X + a^{12}b^{10}(a-b)^6, \\ J(a,b,X) &= X^2(X + ab^2(a-b))^2(X + a^2b(a-b))^2. \end{aligned}$$

The discriminant of $\Lambda(a,b,\xi,X)$ is computed as

$$a^4b^2F(a,b,\xi), \quad a^{14}b^{14}F(a,b,\xi)^2, \quad a^{44}b^{44}(a-b)^{44}F(a,b,\xi)^3,$$

according to $l = 3, 5$ or 7. For a prime p, we denote by v_p the normalized p-adic valuation.

With these notations, Sato proved the following theorem.

THEOREM 2 ([**10**, Theorem 5.1]). *Suppose that $a, b \in \mathbb{Z}$ and $\xi \in \mathbb{Q}$ satisfy the following conditions*:

(C1) *$\Lambda(a,b,\xi,X)$ is irreducible over $\mathbb{Q}$.*
(C2) *$v_p(\xi) < 0$ for all prime factors p of $\delta(a,b)$.*

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

REMARK 1. From the condition (C1), the splitting field of $\Lambda(a,b,\xi,X)$ over $\mathbb{Q}$ is a cyclic extension of $\mathbb{Q}\big(\sqrt{F(a,b,\xi)}\big)$ of degree l, and furthermore (C2) guarantees this extension to be unramified. Although the condition (C2) can be more precisely given, we refer to it as a simple form here. See [**10**, Section 5], [**12**, Theorem 6.1] and also [**11**] for details.

Now the rest of this section summarizes how our main theorem is deduced from Theorem 2.

Let m be a nonzero integer. In order to generate pairs of quadratic fields stated as in Theorem 1, we combine two cubic polynomials, and consider a cubic curve defined by

$$C : F(a,b,X) = m^3F(c,d,Y)$$

where $a, b, c, d \in \mathbb{Z}$ are suitably chosen later. If there is a rational point $(\xi, \eta) \in C(\mathbb{Q})$ that satisfies the conditions (C1) and (C2) of Theorem 2 not only for (a,b,ξ) but for (c,d,η), then we may obtain a pair of quadratic fields

$$\mathbb{Q}\big(\sqrt{F(a,b,\xi)}\big) \quad \text{and} \quad \mathbb{Q}\big(\sqrt{F(c,d,\eta)}\big) = \mathbb{Q}\big(\sqrt{mF(a,b,\xi)}\big)$$

which both have class number divisible by l. Now since the cubic curve C has a rational point

$$O = [m : 1 : 0]$$

on the line at infinity, one can treat C as an elliptic curve over $\mathbb{Q}$ with O in many cases. If so, the various tools of elliptic curves may become available. This is a reason why we adopt m^3 instead of m in the definition of C.

We now state the following theorem which plays an important role in the present paper.

THEOREM 3. *Let a, b, c, d and m be integers with $\delta(a,b)\delta(c,d)m \neq 0$ such that C is an elliptic curve over $\mathbb{Q}$ with base point $O = [m : 1 : 0]$. Then the Mordell-Weil group $C(\mathbb{Q})$ has a subgroup H of finite index such that, for any rational point $(\xi, \eta) \in H \setminus \{O\}$, the class numbers of $\mathbb{Q}\big(\sqrt{F(a,b,\xi)}\big)$ and $\mathbb{Q}\big(\sqrt{F(c,d,\eta)}\big)$ are both divisible by l.*

Note that the theorem says nothing when $C(\mathbb{Q})$ is finite, because $\{O\}$ can be taken as H. Thus, for our purpose, the parameters should be chosen so that the Mordell-Weil rank of $C(\mathbb{Q})$ is at least 1. In many cases, this may be confirmed, but we will illustrate it later only for specified values of a, b, c and d.

The following proposition consists of two assertions corresponding to the conditions (C1) and (C2) of Theorem 2, respectively.

PROPOSITION 1. *Let a, b, c, d and m be integers as in Theorem 3.*

(A1) *Both $\Lambda(a,b,\xi,X)$ and $\Lambda(c,d,\eta,X)$ are irreducible over $\mathbb{Q}$ for all but finitely many rational points $(\xi,\eta) \in C(\mathbb{Q}) \setminus \{O\}$.*

(A2) *There exists a subgroup H of finite index in $C(\mathbb{Q})$ such that if $(\xi,\eta) \in H \setminus \{O\}$ then $v_p(\xi) < 0$ and $v_p(\eta) < 0$ for any prime factor p of $\delta(a,b)\delta(c,d)$.*

Theorem 3 is a simple consequence of this proposition as follows. Take a subgroup H as in (A2) and a natural number n to be sufficiently large. It then follows from (A1) that, for any $(\xi,\eta) \in nH \setminus \{O\}$, both $\Lambda(a,b,\xi,X)$ and $\Lambda(c,d,\eta,X)$ are irreducible over $\mathbb{Q}$. Thus we can apply Theorem 2 to conclude Theorem 3, replacing H by nH.

We will prove Proposition 1 in the next two sections.

2. Irreducibility.

To verify the assertion (A1) of Proposition 1, we first notice the fact that, for $a, b, \xi \in \mathbb{Q}$ with $F(a,b,\xi) \neq 0$, the polynomial $\Lambda(a,b,\xi,X)$ is reducible over $\mathbb{Q}$ if and only if it has a rational root, as shown in the proof of [**10**, Lemma 6.1]. For integers a, b, c, d and m, let Γ be the set of the points $(\xi,\eta) \in C(\mathbb{Q})$ with

$$F(a,b,\xi) = F(c,d,\eta) = 0.$$

Suppose that $(\xi,\eta) \in C(\mathbb{Q}) \setminus \Gamma$ is a rational point such that $\Lambda(a,b,\xi,X)$ is reducible over $\mathbb{Q}$. Then, from above, there is a rational point (ξ,η,ζ) on the space curve $\mathcal{X}$ over $\mathbb{Q}$

defined by

$$\mathcal{X} : F(a,b,X) = m^3 F(c,d,Y) \quad \text{and} \quad \Lambda(a,b,X,Z) = 0.$$

Similarly, letting $\mathcal{Y}$ be the curve over $\mathbb{Q}$ defined by

$$\mathcal{Y} : F(a,b,X) = m^3 F(c,d,Y) \quad \text{and} \quad \Lambda(c,d,Y,Z) = 0,$$

we see that a rational point $(\xi,\eta) \in C(\mathbb{Q}) \setminus \Gamma$ such that $\Lambda(c,d,\eta,X)$ is reducible over $\mathbb{Q}$ comes from a rational point (ξ,η,ζ) on $\mathcal{Y}$. Therefore, as Γ is finite, the assertion (A1) follows from the finiteness of $\mathcal{X}(\mathbb{Q})$ and $\mathcal{Y}(\mathbb{Q})$.

We now put

$$\kappa(Z) = \frac{I(a,b,Z)}{J(a,b,Z)}$$

and define the polynomial in Z, Y with parameters a, b, c, d and m

$$G(Z,Y) = J(a,b,Z)^3 \left(F(a,b,\kappa(Z)) - m^3 F(c,d,Y)\right)$$

that is obtained by eliminating X from the definition of $\mathcal{X}$.

LEMMA 1. *If a, b, c, d and m are integers as in Theorem 3, then the polynomial $G(Z,Y)$ is absolutely irreducible.*

PROOF. First we note that no non-constant polynomial in $\bar{\mathbb{Q}}[Z]$ can be a factor of $G(Z,Y)$. In fact, if such a polynomial exists, then, taking its root $z_0 \in \bar{\mathbb{Q}}$, one easily has $J(a,b,z_0) = 0$ and thus

$$G(z_0,Y) = 4I(a,b,z_0)^3 = 0.$$

But this is impossible by $\delta(a,b) \neq 0$ and the calculations as follows: when $l = 3$,

$$I(a,b,0) = a^4 b^2 \neq 0,$$

when $l = 5$,

$$I(a,b,0) = a^4 b^6 \neq 0, \quad I(a,b,-ab) = a^6 b^4 \neq 0,$$

and when $l = 7$,

$$\begin{aligned} I(a,b,0) &= a^{12} b^{10} (a-b)^6 \neq 0, \\ I(a,b,-ab^2(a-b)) &= a^6 b^{12} (a-b)^{10} \neq 0, \\ I(a,b,-a^2 b(a-b)) &= a^{10} b^6 (a-b)^{12} \neq 0. \end{aligned}$$

Now suppose that $G(Z,Y)$ is reducible over $\bar{\mathbb{Q}}$. Since it is reducible as a cubic polynomial in Y over $\bar{\mathbb{Q}}(Z)$ from above, we can find a rational function $\lambda(Z) \in \bar{\mathbb{Q}}(Z)$ such that $G(Z,\lambda(Z))$ is identically 0, and a non-constant rational map

$$\mathbb{P}^1 \longrightarrow C, \quad Z \mapsto (\kappa(Z), \lambda(Z)).$$

This contradicts our assumption that C is an elliptic curve. □

From this lemma, for a, b, c, d and m as in Theorem 3, we can define the irreducible plane curve

$$\mathcal{X}_0 : G(Z,Y) = 0.$$

It is clear that the finiteness of $\mathcal{X}(\mathbb{Q})$ is equivalent to that of $\mathcal{X}_0(\mathbb{Q})$. Consider the rational map

$$\phi : \mathcal{X}_0 \longrightarrow C, \quad (Z,Y) \mapsto (\kappa(Z), Y).$$

The degree of ϕ is equal to l, since the relation $\kappa(Z) = X$ is equivalent to $\Lambda(a,b,X,Z) = 0$. Let $R = (x_0, y_0)$ be a point of $C(\bar{\mathbb{Q}})$ satisfying

$$F(a,b,x_0) = F(c,d,y_0) = 0.$$

Recall that the discriminant of $\Lambda(a,b,X,Z)$ with respect to Z is divisible by $F(a,b,X)$. This shows $\#\phi^{-1}(R) < l$ which means that ϕ is ramified at some point in $\phi^{-1}(R)$. We remark that such a point (z_0, y_0) on $\mathcal{X}_0$ is nonsingular. In fact, we have

$$\frac{\partial G}{\partial Y}(z_0, y_0) = -m^3 J(a,b,z_0)^3 F'(c,d,y_0) \neq 0,$$

because $J(a,b,z_0) \neq 0$ which was shown in the proof of Lemma 1, and further $F'(c,d,y_0) \neq 0$ since $F(c,d,Y)$ has no multiple roots by $\delta(c,d) \neq 0$. So, we can apply the Riemann-Hurwitz formula for ϕ to see that the genus of $\mathcal{X}_0$ is greater than 1. This implies the finiteness of $\mathcal{X}_0(\mathbb{Q})$ and also $\mathcal{X}(\mathbb{Q})$ from Faltings' theorem. The finiteness of $\mathcal{Y}(\mathbb{Q})$ can be shown in a similar manner. The assertion (A1) is confirmed by their finiteness.

3. Local properties.

Let p be a prime. Before proving (A2), we recall some local properties concerning elliptic curves over the p-adic field $\mathbb{Q}_p$. Let $E/\mathbb{Q}_p$ be an elliptic curve given by a Weierstrass equation

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

with coefficients $a_i \in \mathbb{Z}_p$. For $n \geq 1$, we define subsets of $E(\mathbb{Q}_p)$ by

$$E_n(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \,|\, v_p(x(P)) \le -2n\} \cup \{O\}.$$

It is well known that all of them are subgroups of $E(\mathbb{Q}_p)$. Further, if the Weierstrass equation is minimal then the group $E(\mathbb{Q}_p)/E_n(\mathbb{Q}_p)$ is finite for any $n \ge 1$ (see [**13**, Chapter VII]). When the equation may not be minimal, there is a coordinate change

$$x = u^2x' + r, \qquad y = u^3y' + u^2sx' + t$$

with $u, r, s, t \in \mathbb{Z}_p$ giving a minimal equation with the coordinates (x', y'). Then, for $P \in E(\mathbb{Q}_p)$ and $n \ge 1$,

$$v_p(x(P)) \le -2n \quad \text{if and only if} \quad v_p(x'(P)) \le -2(n + v_p(u)).$$

From this, one can deduce the finiteness of $E(\mathbb{Q}_p)/E_n(\mathbb{Q}_p)$, whether the equation is minimal or not.

LEMMA 2. *Let E be an elliptic curve over $\mathbb{Q}$ given by a Weierstrass equation with coordinates (x, y) having coefficients in $\mathbb{Z}$. Let S be a finite set of primes. Then, for $n \ge 1$, there exists a subgroup H of finite index in $E(\mathbb{Q})$ such that $v_p(x(P)) \le -2n$ and $v_p(y(P)) \le -3n$ for any $P \in H \setminus \{O\}$ and any $p \in S$.*

PROOF. Let p be a prime. We have, via the embedding $E(\mathbb{Q}) \to E(\mathbb{Q}_p)$, the natural homomorphism

$$E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}_p)/E_n(\mathbb{Q}_p).$$

Denote by H_p its kernel, in other words,

$$H_p = \{P \in E(\mathbb{Q}) \,|\, v_p(x(P)) \le -2n\} \cup \{O\}$$

that has finite index in $E(\mathbb{Q})$ by the above argument. It is easy to see that the subgroup

$$H = \bigcap_{p \in S} H_p$$

of $E(\mathbb{Q})$ has the desired property. □

Returning now to our curve C, we consider a, b, c, d and m as indeterminates and try to transform the equation

$$F(a, b, X) = m^3F(c, d, Y)$$

to a Weierstrass equation

$$y^2 = x^3 + Ax + B \qquad \text{with} \quad A, B \in \mathbb{Z}[a, b, c, d, m]$$

such that the points at infinity, $[m : 1 : 0]$ on the former and $[0 : 1 : 0]$ on the latter, correspond with each other. Although this may be done completely, in principle, after Nagell's method [**8**] (see also Cassels [**2**, Section 8]), we make use of the command *Weierstrassform* on the computer algebra system Maple [**6**] for convenience. Indeed, we obtain not only the coefficients A and B but also the rational maps for coordinate changes

$$\Phi(x, y) = (X, Y) \quad \text{and} \quad \Psi(X, Y) = (x, y).$$

However, their expressions are too large for exhibiting here. We need to merely observe that the map $\Phi(x, y) = (X, Y)$ is given by the formulas

$$X = \frac{s_0 + s_1 x + s_2 x^2 + s_3 y + sxy}{r_0 + r_1 x + r x^2}, \qquad Y = \frac{t_0 + t_1 x + t_2 x^2 + t_3 y + sxy}{m(r_0 + r_1 x + r x^2)}$$

with $r_i, s_i, t_i \in \mathbb{Z}[a, b, c, d, m]$ and $r, s \in \mathbb{Z} \smallsetminus \{0\}$. These computations are checked by Magma [**1**] and also PARI/GP [**9**].

We are now ready to show the assertion (A2). Let a, b, c, d and m be integers as in Theorem 3. Take a natural number n to be sufficiently large. The curve C is also defined by the Weierstrass equation as above. So, in the rest of this section, suppose that rational points on C are represented using the two systems of coordinates, (X, Y) for the original equation and (x, y) for the Weierstrass equation. Then, by Lemma 2, there is a subgroup H of $C(\mathbb{Q})$ of finite index such that $v_p(x(P)) \le -2n$ and $v_p(y(P)) \le -3n$ for any $P \in H \smallsetminus \{O\}$ and any prime factor p of $\delta(a, b)\delta(c, d)$. Fix such a rational point P and a prime factor p. Write

$$x = x(P), \quad y = y(P), \quad \xi = X(P), \quad \eta = Y(P)$$

which are connected by $\Phi(x, y) = (\xi, \eta)$. Since $v_p(x) \le -2n < 0$, it is seen that

$$v_p(x) = -2v \quad \text{and} \quad v_p(y) = -3v$$

for some integer $v \ge n$. So, from the above formulas for Φ, we compute

$$v_p(\text{the numerator of } \xi) = v_p(sxy) = v_p(s) - 5v,$$
$$v_p(\text{the denominator of } \xi) = v_p(rx^2) = v_p(r) - 4v,$$

and further

$$v_p(\xi) = v_p(s) - v_p(r) - v \le v_p(s) - v_p(r) - n < 0,$$

since n is sufficiently large. Similarly, the inequality $v_p(\eta) < 0$ is also verified. This completes the proof of (A2). As a result, we obtain Proposition 1 and also Theorem 3.

Remark 2. Assume that $C(\mathbb{Q})$ has infinitely many rational points. In this case, H is also infinite. Let (x, y) and (ξ, η) be the coordinates for $P \in H$ as above. Since H

is dense in the connected component of the real curve $C(\mathbb{R})$ containing O, $x = x(P)$ can be arbitrarily large. We then observe that

$$\left|\frac{y}{x}\right| \to \infty \quad \text{and} \quad \xi \sim \frac{sy}{rx} \quad \text{as} \quad P \to O.$$

Since $-P$ corresponds to $(x, -y)$, there can be a rational point $P \in H$ such that ξ has a sufficiently large absolute value with an arbitrary sign, and so does $F(a, b, \xi)$.

4. Number of quadratic fields.

In order to apply Theorem 3, we have to choose the parameters a, b, c, d and m such that $C/\mathbb{Q}$ is an elliptic curve having infinitely many rational points. However, even if it is possible, the theorem does not ensure the infiniteness of the collection of quadratic fields we want. To deal with this problem, for integers a, b, c, d and m satisfying $\delta(a, b)\delta(c, d)m \neq 0$, we consider the space curve $\mathcal{Z}$ defined by the equations

$$\mathcal{Z} : F(a, b, X) = m^3 F(c, d, Y) = Z^2$$

which has the curve C as the projection into the XY-plane. The other plane projections are given by

$$C' : Z^2 = F(a, b, X), \qquad C'' : Z^2 = m^3 F(c, d, Y).$$

These are, indeed, elliptic curves over $\mathbb{Q}$ since the discriminants of $F(a, b, X)$ and $F(c, d, Y)$ are both nonzero by $\delta(a, b)\delta(c, d) \neq 0$.

The next proposition tells us how to choose the parameters to generate infinitely many quadratic fields in Theorem 3, assuming that $C(\mathbb{Q})$ is infinite.

PROPOSITION 2. *Let a, b, c, d and m be integers as in Theorem 3. Suppose that not all of C, C' and C'' are isogenous over $\bar{\mathbb{Q}}$. Then, for any quadratic field K, there are only finitely many rational points $(\xi, \eta) \in C(\mathbb{Q})$ satisfying $K = \mathbb{Q}\big(\sqrt{F(a, b, \xi)}\big)$.*

PROOF. Assume that there is a quadratic field K with $K = \mathbb{Q}\big(\sqrt{F(a, b, \xi)}\big)$ for infinitely many rational points $(\xi, \eta) \in C(\mathbb{Q})$. In this case, we have infinitely many K-rational points $\big(\xi, \eta, \sqrt{F(a, b, \xi)}\big)$ on $\mathcal{Z}$. This contradicts Faltings' theorem, since any irreducible component of $\mathcal{Z}$ has genus greater than 1, which we prove below. Let $\mathcal{W}$ be an irreducible component of $\mathcal{Z}$. Let

$$\sigma : \mathcal{W} \longrightarrow C, \qquad \tau : \mathcal{W} \longrightarrow C', \qquad \rho : \mathcal{W} \longrightarrow C''$$

be the maps defined by the projections on the XY, XZ and YZ-planes respectively. Clearly, the maps σ, τ and ρ are all non-constant. It follows that the genus of $\mathcal{W}$ is greater than 0. Suppose that $\mathcal{W}$ has genus 1. Then a point $O_1 \in \mathcal{W}(\bar{\mathbb{Q}})$ satisfying $\sigma(O_1) = O$ determines an elliptic curve $\mathcal{W}_1 = (\mathcal{W}, O_1)$ over $\bar{\mathbb{Q}}$, and thus σ is an isogeny from $\mathcal{W}_1$ to C over $\bar{\mathbb{Q}}$. Similarly, we can take points $O_2, O_3 \in \mathcal{W}(\bar{\mathbb{Q}})$ and make $\mathcal{W}$ to

be elliptic curves $\mathcal{W}_2 = (\mathcal{W}, O_2)$ and $\mathcal{W}_3 = (\mathcal{W}, O_3)$ over $\bar{\mathbb{Q}}$ being isogenous to C' and C'' respectively. Since the three elliptic curves $\mathcal{W}_i$ $(i = 1, 2, 3)$ are isomorphic over $\bar{\mathbb{Q}}$ to each other, we conclude that C, C' and C'' must be all isogenous. This contradicts the assumption. Hence $\mathcal{W}$ has genus at least 2. □

REMARK 3. In this proposition, the curve C'' can be replaced by

$$C''' : Z^2 = F(c, d, Y)$$

that is a quadratic twist of C''. It is more advantageous to use C''' rather than C'', because of the independence from m.

REMARK 4. Let E_1, E_2 be two elliptic curves over $\mathbb{Q}$. Assume that there is a prime p at which E_1 has good reduction while E_2 has multiplicative reduction. Then, by the semistable reduction theorem, E_1 and E_2 have different reduction types at a prime lying above p over any finite extension of $\mathbb{Q}$. Hence they are not isogenous over $\bar{\mathbb{Q}}$. For details, see [**13**, Chapter VII].

5. Proof of the main theorem.

Let m be a nonzero integer. We will apply Theorem 3 and Proposition 2 (with Remark 3) to establish Theorem 1. In fact, we will choose integers a, b, c and d with $\delta(a, b)\delta(c, d) \neq 0$ that make the curves

$$C : F(a, b, X) = m^3 F(c, d, Y), \quad C' : Z^2 = F(a, b, X), \quad C''' : Z^2 = F(c, d, Y)$$

have the following properties:

- C' and C''' are not isogenous over $\bar{\mathbb{Q}}$.
- C is an elliptic curve over $\mathbb{Q}$.
- C has a rational point of infinite order.

It is easy to check the first property by Remark 4 in most cases. Regarding m to be a variable, we can forcibly transform C to a Weierstrass equation

$$y^2 = x^3 + Ax + B \qquad (A, B \in \mathbb{Z}[m]),$$

by the Maple command. So the second property follows from the nonvanishing of the discriminant $\Delta = -16(4A^3 + 27B^2)$ which is not difficult to check. Next, to find a rational point of infinite order on C, we notice that the point $O = [m : 1 : 0]$ at infinity on C is not inflection point in general. Thus the tangent line at O may intersect C at another point. We may confirm that such a new point on C is not torsion, using, for example, the theorem of Lutz and Nagell ([**13**, Chaoter Viii]).

In the following arguments, we will illustrate how to verify the above properties with specified integers a, b, c, d for each prime $l = 3, 5$ or 7.

Case $l = 3$: Choose $(a, b, c, d) = (1, 1, 2, 1)$ satisfying

$$\delta(1,1) = -2^3 \cdot 13^3, \quad \delta(2,1) = -2^8 \cdot 5^6.$$

The two elliptic curves

$$C' : Z^2 = F(1,1,X) = 4X^3 + X^2 - 18X - 31,$$
$$C''' : Z^2 = F(2,1,Y) = 4Y^3 + 4Y^2 - 144Y - 560$$

are isomorphic to the curves named 26a1 and 20a3 in Cremona's Elliptic Curve Data [**4**], respectively. Comparing the conductors, we know that C' has good reduction at 5 while C''' has multiplicative reduction. Thus, by Remark 4, they are not isogenous over $\bar{\mathbb{Q}}$.

Now we have the curve $C : F(1,1,X) = m^3 F(2,1,Y)$, namely,

$$C : 4X^3 + X^2 - 18X - 31 = m^3(4Y^3 + 4Y^2 - 144Y - 560)$$

that is transformed to the Weierstrass equation $y^2 = x^3 + Ax + B$ where

$$A = -638631m^2 = -3^3 \cdot 7 \cdot 31 \cdot 109m^2,$$
$$B = -2916000000m^6 + 594146718m^3 - 12812904.$$

If the discriminant $\Delta = -16(4A^3 + 27B^2)$ vanishes, then, for $p = 7, 31$ or 109,

$$3v_p(A) = v_p(4A^3) = v_p(27B^2) = 2v_p(B) \equiv 0 \pmod 2$$

which is a contradiction. This ensures that C is an elliptic curve over $\mathbb{Q}$ for arbitrary $m \neq 0$. The coordinate change $(X, Y) \to (x, y)$ is given by

$$\begin{aligned} x &= 108(X^2 + mXY + m^2Y^2) \\ &\quad + 18(2m+1)X + 9m(8m+1)Y - 3(432m^2 - m + 54), \\ y &= -1944X(X^2 + mXY + m^2Y^2) \\ &\quad - 162((4m+3)X^2 + 2m(4m+1)XY + m^2Y^2) \\ &\quad + 27(864m^2 - 4m + 431/2)X - 108m(218m^2 + m - 27)Y \\ &\quad - 243(544m^3 - 8m^2 - 4m - 63/2), \end{aligned}$$

while the inverse $(x, y) \to (X, Y)$ is given by

$$X = \frac{s_0 + s_1x + s_2x^2 + s_3y + sxy}{r_0 + r_1x + rx^2}, \qquad Y = \frac{t_0 + t_1x + t_2x^2 + t_3y + sxy}{m(r_0 + r_1x + rx^2)},$$

where $r = 144,\ s = -8$ and

$$\begin{cases} r_0 = 81(3041536m^4 - 378448m^2 + 47089), \\ r_1 = -108(1744m^2 + 217), \end{cases}$$

$$\begin{cases} s_0 = -27(760384m^4 - 5996144m^3 - 94612m^2 + 357399), \\ s_1 = -36(27632m^3 - 436m^2 - 1647), \\ s_2 = -12, \\ s_3 = 6(3488m^2 - 217), \end{cases}$$

$$\begin{cases} t_0 = -27m(51231744m^4 - 378448m^2 - 2777756m + 47089), \\ t_1 = 9(117504m^3 + 868m - 6371), \\ t_2 = -48m, \\ t_3 = -12(872m^2 - 217). \end{cases}$$

Next, to find a rational point of infinite order on C, we apply the "tangent method" for $O = [m : 1 : 0]$. In fact, a new rational point, say M, is obtained as

$$X(M) = -\frac{221056m^3 + 5232m^2 - 13393}{36(1744m^2 - 217)},$$

$$Y(M) = -\frac{120992m^3 - 1302m - 6371}{18m(1744m^2 - 217)}.$$

This has the corresponding coordinates for the Weierstrass equation

$$x(M) = \frac{f(m)}{4(1744m^2 - 217)^2}, \quad y(M) = \frac{g(m)}{8(1744m^2 - 217)^3},$$

where

$$\begin{aligned} f(m) &= 32952438784m^6 + 1980039936m^4 - 5633391104m^3 \\ &\quad + 246369648m^2 + 131703625, \\ g(m) &= (110528m^3 - 6371)(49991561216m^6 + 5940119808m^4 \\ &\quad - 11266782208m^3 + 739108944m^2 + 232752311). \end{aligned}$$

We notice that $x(M)$ never be an integer, because the denominator is even and the numerator is odd. This shows that M has infinite order, by the theorem of Lutz and Nagell ([**13**, Chapter VIII]). Hence we obtain Theorem 1 for the case $l = 3$.

Case $l = 5$: The proof is done by the same way as $l = 3$. We choose $(a, b, c, d) = (3, 1, 2, 2)$ satisfying

$$\delta(3, 1) = -3 \cdot 41^5, \quad \delta(2, 2) = -2^{12} \cdot 11^5.$$

The two elliptic curves

$$C' : Z^2 = F(3,1,X) = 4X^3 + 28X^2 + 144X - 3351,$$
$$C''' : Z^2 = F(2,2,Y) = 4Y^3 + 32Y^2 - 576Y - 7616$$

are isomorphic to the curves 123a2 and 11a1 respectively. Checking the reduction, for instance, at 11, we see that they are not isogenous over $\bar{\mathbb{Q}}$.

We now have

$$C : 4X^3 + 28X^2 + 144X - 3351 = m^3(4Y^3 + 32Y^2 - 576Y - 7616)$$

and its Weierstrass equation $y^2 = x^3 + Ax + B$ with

$$A = 12642048m^2 = 2^8 \cdot 3^3 \cdot 31 \cdot 59m^2,$$
$$B = -480895709184m^6 + 836729758080m^3 - 253377511587.$$

It follows from $v_{31}(A) \equiv 1 \pmod 2$ that C is always an elliptic curve. The coordinate change $(X,Y) \to (x,y)$ is given by

$$\begin{aligned} x &= 108(X^2 + mXY + m^2Y^2) \\ &\quad + 72(4m+7)X + 36m(16m+7)Y - 48(108m^2 - 14m - 27), \\ y &= -1944X(X^2 + mXY + m^2Y^2) \\ &\quad - 648((8m+21)X^2 + 2m(8m+7)XY + 7m^2Y^2) \\ &\quad + 216(432m^2 - 112m - 265)X - 864m(124m^2 + 28m + 27)Y \\ &\quad - 243(7104m^3 - 896m^2 + 256m - 3239). \end{aligned}$$

On the other hand, the inverse $(x,y) \to (X,Y)$ is given by the same form as in the case $l = 3$ with coefficients $r = 18,\ s = -1$ and

$$\begin{cases} r_0 = 2592(246016m^4 + 29264m^2 + 3481), \\ r_1 = -216(496m^2 - 59), \end{cases}$$

$$\begin{cases} s_0 = -108(13776896m^4 + 9443776m^3 + 1638784m^2 - 5516559), \\ s_1 = -9(160064m^3 - 27776m^2 - 93501), \\ s_2 = -42, \\ s_3 = 12(992m^2 + 59), \end{cases}$$

$$\begin{cases} t_0 = -1728m(5946048m^4 + 117056m^2 - 3000955m + 13924), \\ t_1 = 9(191808m^3 - 3776m - 96805), \\ t_2 = -48m, \\ t_3 = -24(248m^2 + 59). \end{cases}$$

With the "tangent method", we find the point M on C given by

$$X(M) = -\frac{160064m^3 + 41664m^2 - 91849}{36(496m^2 + 59)},$$
$$Y(M) = -\frac{207680m^3 + 5664m - 96805}{36m(496m^2 + 59)}.$$

The coordinates for the Weierstrass equation are

$$x(M) = \frac{f(m)}{4(496m^2 + 59)^2}, \quad y(M) = \frac{g(m)}{8(496m^2 + 59)^3},$$

where

$$\begin{aligned} f(m) &= 19763335168m^6 - 696717312m^4 - 30989991040m^3 \\ &\quad + 82875648m^2 + 9381066217, \\ g(m) &= (160064m^3 - 96805)(16834760704m^6 - 1045075968m^4 \\ &\qquad - 30989991040m^3 + 124313472m^2 + 9385995313). \end{aligned}$$

Obviously, $x(M) \notin \mathbb{Z}$ which implies that M has infinite order. This completes the proof for the case $l = 5$.

Case $l = 7$: We adopt the parameters $(a, b, c, d) = (2, 3, 1, 2)$ with

$$\delta(2, 3) = -2 \cdot 3 \cdot 7^{14}, \quad \delta(1, 2) = -2 \cdot 13^7,$$

and the elliptic curves

$$C' : Z^2 = F(2, 3, X) = 4X^3 - 71X^2 - 9384X - 373656,$$
$$C''' : Z^2 = F(1, 2, Y) = 4Y^3 - 15Y^2 - 832Y - 4184.$$

They are isomorphic to 294b1 and 26b2 respectively, and not isogenous over $\bar{\mathbb{Q}}$ by considering the reduction at 13.

By a similar way as above, it is verified that

$$C : 4X^3 - 71X^2 - 9384X - 373656 = m^3(4Y^3 - 15Y^2 - 832Y - 4184)$$

is an elliptic curve which has the Weierstrass equation $y^2 = x^3 + Ax + B$ with

$$A = -400359547m^2 = -7^6 \cdot 41 \cdot 83m^2,$$
$$B = -8031810176m^6 + 7801622136406m^3 - 260437659974016,$$

by the coordinate change given by

$$\begin{aligned}
x &= 48(X^2 + mXY + m^2Y^2) \\
&\quad - 4(15m + 142)X - 4m(30m + 71)Y - (3328m^2 - 355m + 37536), \\
y &= -576X(X^2 + mXY + m^2Y^2) \\
&\quad + 48((15m + 213)X^2 + 2m(15m + 71)XY + 71m^2Y^2) \\
&\quad + 4(9984m^2 - 2130m + 220175)X - 12m(3403m^2 + 710m - 37536)Y \\
&\quad - 16(20388m^3 + 14768m^2 + 35190m - 1598169).
\end{aligned}$$

For the inverse $(x, y) \to (X, Y)$, the coefficients r, s and so on of the formulas are given by $r = 36,\ s = -3$ and

$$\begin{cases} r_0 = 4(104223681m^4 - 1201078641m^2 + 13841287201), \\ r_1 = -12(10209m^2 + 117649), \end{cases}$$

$$\begin{cases} s_0 = 2466627117m^4 + 44383438197m^3 - 28425527837m^2 - 3321908928240, \\ s_1 = -3(377253m^3 + 241613m^2 - 28235760), \\ s_2 = 213, \\ s_3 = 20418m^2 - 117649, \end{cases}$$

$$\begin{cases} t_0 = -m(3330257472m^4 + 6005393205m^2 - 316684401677m - 69206436005), \\ t_1 = 978624m^3 - 1764735m - 93060359, \\ t_2 = 45m, \\ t_3 = -(10209m^2 - 235298). \end{cases}$$

There can be found the point M on C, by the "tangent method", with

$$X(M) = -\frac{2263518m^3 - 2174517m^2 - 161061481}{36(10209m^2 - 117649)},$$

$$Y(M) = -\frac{1804113m^3 + 5294205m - 186120718}{36m(10209m^2 - 117649)}$$

and the Weierstrass coordinates

$$x(M) = \frac{f(m)}{9(10209m^2 - 117649)^2}, \quad y(M) = \frac{g(m)}{27(10209m^2 - 117649)^3},$$

where

$$\begin{aligned}
f(m) = 7(&275922151191m^6 + 5255062219701m^4 - 120367884390264m^3 \\
&+ 60559586157861m^2 + 4250811553586311),
\end{aligned}$$

$$g(m) = (1131759m^3 - 93060359) \times (670851438687m^6 + 110356306613721m^4 - 1685150381463696m^3 + 1271751309315081m^2 + 54626120956477007).$$

The coefficients of $f(m)$ are all divisible by 3 except the constant term, exactly, $f(m) \equiv 1 \pmod 3$. So, $x(M)$ is not an integer, and M has infinite order. From this, we obtain Theorem 1 for the case $l = 7$.

Remark 5. From Remark 2, we see that there are infinitely many both real and imaginary quadratic fields $\mathbb{Q}(\sqrt{D})$ having the property in Theorem 1.

Remark 6. Letting m be the square of any integer, we may deduce the result of Mestre [**7**] mentioned in the introduction.

Acknowledgements. The authors would like to thank Atsushi Sato and Kazuo Matsuno for valuable information and useful suggestions on the arithmetic of algebraic curves. They also thank Masanari Kida and Nobuhiro Terai for stimulating discussions, and Shoichi Nakajima for his helpful advice.

References

[1] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system, I, The user language, J. Symbolic Comput., **24** (1997), 235–265, Computational algebra and number theory, London, 1993.
[2] J. W. S. Cassels, Lectures on Elliptic Curves, Cambridge Univ. Press, 1991.
[3] M. Craig, A construction for irregular discriminants, Osaka J. Math., **14** (1977), 365–402.
[4] J. E. Cremona, Algorithms for Modular Elliptic Curves, 2nd ed., Cambridge Univ. Press, 1997.
[5] T. Komatsu, An infinite family of pairs of quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{mD})$ whose class numbers are both divisible by 3, Acta Arith., **104** (2002), 129–136.
[6] Maplesoft, Maple 16, 2012, http://www.maplesoft.com/products/maple/
[7] J.-F. Mestre, Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques, J. Reine Angew. Math., **343** (1983), 23–35
[8] T. Nagell, Sur les propriétés arithmétiques des cubiques planes du premier genre, Acta Math., **52** (1929), 93–126.
[9] The PARI Group, PARI/GP, version 2.3.4, 2008, http://pari.math.u-bordeaux.fr/
[10] A. Sato, On the class numbers of certain number fields obtained from points on elliptic curves II, Osaka J. Math., **45** (2008), 375–390.
[11] A. Sato, Construction of number fields of odd degree with class numbers divisible by three, five or by seven, Interdiscip. Inform. Sci., **16** (2010), 39–43.
[12] A. Sato, On the class numbers of certain number fields obtained from points on elliptic curves III, Osaka J. Math., **48** (2011), 809–826.
[13] J. H. Silverman, The Arithmetic of Elliptic Curves, 2nd ed., GTM 106, Springer-Verlag, 2009.
[14] J. Vélu, Isogénies entre courbes elliptiques, C. R. Acad. Sci. Paris Sér. A-B, **273** (1971), 238–241.

Yoshichika Iizuka

Department of Mathematics
Gakushuin University
Mejiro, Toshima-ku
Tokyo 171-8588, Japan
E-mail: iizuka@math.gakushuin.ac.jp

Yutaka Konomi

Department of Mathematics
Gakushuin University
Mejiro, Toshima-ku
Tokyo 171-8588, Japan
E-mail: konomi@math.gakushuin.ac.jp

Shin Nakano

Department of Mathematics
Gakushuin University
Mejiro, Toshima-ku
Tokyo 171-8588, Japan
E-mail: shin@math.gakushuin.ac.jp