人間情報学研究，第26巻
2021年，11～18頁

On Unramified Abelian Extensions of Number Fields Arising from Multiplication of Elliptic Curves

Atsushi SATO*

Abstract

We introduce a way to construct number fields with class numbers divisible by a power of a prime number. In particular, we start with an elliptic curve E defined over a number field k such that $E[l^n] \subset E(k)$, where l is an odd prime number, and show a way to construct infinitely many quadratic extensions of k with class numbers divisible by l^{2n}.

Keywords: Divisibility of Class Numbers, Isogeny of Elliptic Curves

1 Introduction

Let k be an algebraic number field of finite degree, $m \geq 2$ an integer, and let E be an elliptic curve defined over k such that $E[m] \subset E(k)$. Let P be a point on E, and let $K = k(P)$ (resp. $L = k([m]^{-1}P)$) be the field generated over k by the coordinates of P (resp. the points in $[m]^{-1}P$). Here, $[m]$ denotes the multiplication-by-m map on E, and $E[m]$ its kernel (that is, the m-torsion subgroup of E). Then, as is well known (see, *e.g.*, [4, Chapter VIII]), we have:

(i) L/K is an abelian extension of exponent m.

(ii) L/K is unramified at a finite place $\mathfrak{p}$ if E has good reduction at $\mathfrak{p}$ and if $\mathfrak{p} \nmid m$.

We also note that L/K is a Kummer extension, since the assumption $E[m] \subset E(k)$ implies $\mu_m \subset k$, where μ_m denotes the group of m-th roots of unity. Furthermore, we have $[L : K] = m^2$ for "generic" P.

In the present paper, we show the following theorem:

Theorem 1.1 *Let k be an algebraic number*

*Associate Professor at Faculty of Liberal Arts, Tohoku Gakuin University

field of finite degree, l^n a power of an add prime number, and let E be an elliptic curve defined over k such that $E[l^n] \subset E(k)$. Let

$$y^2 = x^3 + ax + b \quad (a, b \in \mathcal{O}_k,\ 4a^3 + 27b^2 \neq 0)$$

be a Weierstrass equation for E with

$$x(T),\, y(T) \in \mathcal{O}_k \quad (T \in E[l] - \{O\}).$$

Let P be a point on E with $x(P) \in k$, and let $K = k(P),\ L = k([l^n]^{-1}P)$. Moreover, assume that $c = x(P)$ satisfies the following condition: For any finite place $\mathfrak{p}$ of k such that E has bad reduction at $\mathfrak{p}$ or $\mathfrak{p} \mid l$,

$$\min\bigl\{\mathrm{ord}_{\mathfrak{p}}(c^3 + ac + b),\, \mathrm{ord}_{\mathfrak{p}}(3c^2 + a)\bigr\} \leq 0.$$

Here, we replace the inequality above by

$$\mathrm{ord}_{\mathfrak{p}}(c^2 + a) \leq 0$$

if $\mathfrak{p} \mid 2$, and by

$$\mathrm{ord}_{\mathfrak{p}}(l^{2n} c) \leq 0$$

if $\mathfrak{p} \mid l$. Then L/K is unramified at all finite places. Here, $\mathcal{O}_k$ denotes the ring of integers of k, while $\mathrm{ord}_{\mathfrak{p}}$ the normalized additive valuation of k associated with $\mathfrak{p}$.

The field $K = k\bigl(\sqrt{c^3 + ac + b}\bigr)$ in the theorem above is a quadratic extension of k for generic c. Thus, using the theorem and varying c in k, we can construct infinitely many quadratic extensions of k with class numbers divisible by l^{2n}, for L/K is also unramified at all infinite places. We will give a proof of the theorem in Sections 3 and 4, after studying about the explicit form of dual isogenies in Section 2.

2 Dual isogeny via Vélu's formulas

Let k be a field of characteristic 0,

$$E:\ y^2 = x^3 + ax + b \quad (a, b \in k,\ 4a^3 + 27b^2 \neq 0)$$

an elliptic curve defined over k, and let Γ be a finite subgroup of E of order $l \geq 2$ which is stable under the action of $\mathrm{Gal}(\bar{k}/k)$. Here, $\bar{k}$ is an algebraic closure of k, and Gal stands for Galois group. Let

$$\begin{aligned} &E^*:\ Y^2 = X^3 + AX + B, \\ &\lambda:\ X = \xi(x),\quad Y = \eta(x)\, y \end{aligned} \tag{2.1}$$

be the equations for $\lambda : E \to E^* = E/\Gamma$ that are given by Vélu's formulas [5] (for the formulas, see also [3, Section 2] or [6, Section 12.3]). Then $\Gamma^* = \lambda(E[l])$ is a subgroup of E^* of order l which is stable under the action of $\mathrm{Gal}(\bar{k}/k)$. Let

$$\begin{aligned} &E':\ (y')^2 = (x')^3 + a'x' + b', \\ &\lambda^*:\ x' = \xi^*(X),\quad y' = \eta^*(X)\, Y \end{aligned} \tag{2.2}$$

be the equations for $\lambda^* : E^* \to E' = E^*/\Gamma^*$ that are given by Vélu's formulas. Note that E' is naturally identified with $E/E[l]$. We can also apply Vélu's formulas to $E[l]$, and then obtain the same equations as for $\lambda^* \circ \lambda : E \to E'$.

On the other hand, $E/E[l]$ is isomorphic to E via the multiplication-by-l map. Thus there exists an isomorphism $\phi : E \to E'$ such that $\lambda^* \circ \lambda = \phi \circ [l]$. In fact:

Proposition 2.1 *We have*

$$a' = l^4\, a, \quad b' = l^6\, b.$$

Moreover, the isomorphism $\phi : E \to E'$ is given by

$$x' = l^2\, x, \quad y' = l^3\, y.$$

Proof Since E' is isomorphic to E, we have

$$x' = u^2\, x \circ [l], \quad y' = u^3\, y \circ [l]$$

for some $u \in k - \{0\}$. Here we regard x', y', $x \circ [l]$, $y \circ [l]$ as ($E[l]$-invariant) functions on E. It follows from Vélu's formulas that

$$x' = \frac{x^{l^2} + \text{lower degree terms}}{x^{l^2-1} + \text{lower degree terms}},$$
$$y' = \frac{x^m + \text{lower degree terms}}{x^m + \text{lower degree terms}}\, y,$$

where

$$m = \begin{cases} \frac{3}{2}(l^2-1) & \text{if } l \text{ odd}, \\ \frac{3}{2}\, l^2 & \text{if } l \text{ even}. \end{cases}$$

We also have

$$x \circ [l] = \frac{x^{l^2} + \text{lower degree terms}}{l^2 x^{l^2-1} + \text{lower degree terms}},$$
$$y \circ [l] = \frac{x^m + \text{lower degree terms}}{l^3 x^m + \text{lower degree terms}}\, y$$

by the formulas on division polynomials (see, *e.g.*, [6, Section 3.2]), and hence conclude $u = l$. Namely we have

$$x' = l^2\, x \circ [l], \quad y' = l^3\, y \circ [l],$$

which immediately imply the assertions of the proposition. □

Corollary 2.2 *The dual isogeny $\hat{\lambda} : E^* \to E$ is given by*

$$x = \frac{1}{l^2}\, \xi^*(X), \quad y = \frac{1}{l^3}\, \eta^*(X)\, Y.$$

Example 2.3 (i) If E is given by $y^2 = x^3 + ax$ ($a \neq 0$), then $E[2]$ consists of

$$O,\ (0,0),\ (\pm\sqrt{-a}, 0),$$

and hence $\Gamma = \{O, (0,0)\}$ is a subgroup of order 2. In this case, $\lambda : E \to E^*$ and $\lambda^* : E^* \to E'$ are given by

$$E^* :\ Y^2 = X^3 - 4aX,$$
$$\lambda :\ X = \frac{x^2 + a}{x}, \quad Y = \frac{x^2 - a}{x^2}\, y,$$

thus $\Gamma^* = \{O, (0,0)\}$, and by

$$E' :\ (y')^2 = (x')^3 + 16ax',$$
$$\lambda^* :\ x' = \frac{X^2 - 4a}{X}, \quad y' = \frac{X^2 + 4a}{X^2}\, Y,$$

respectively. Hence $\hat{\lambda} : E^* \to E$ is given by

$$x = \frac{X^2 - 4a}{4X}, \quad y = \frac{X^2 + 4a}{8X^2}\, Y.$$

(ii) If E is given by $y^2 = x^3 + b$ ($b \neq 0$), then $E[3]$ consists of

$$O,\ (0, \pm\sqrt{b}\,),\ (-\sqrt[3]{4b}, \pm\sqrt{-3b}\,),$$
$$(-\omega\sqrt[3]{4b}, \pm\sqrt{-3b}\,),\ (-\omega^2\sqrt[3]{4b}, \pm\sqrt{-3b}\,),$$

where $\omega = (-1 + \sqrt{-3}\,)/2$, and hence $\Gamma = \{O, (0, \pm\sqrt{b}\,)\}$ is a subgroup of order 3. In this case, $\lambda : E \to E^*$ and $\lambda^* : E^* \to E'$ are given by

$$E^* :\ Y^2 = X^3 - 27b,$$
$$\lambda :\ X = \frac{x^3 + 4b}{x^2}, \quad Y = \frac{x^3 - 8b}{x^3}\, y,$$

thus $\Gamma^* = \{O, (0, \pm 3\sqrt{-3b}\,)\}$, and by

$$E' :\ (y')^2 = (x')^3 + 729b,$$
$$\lambda^* :\ x' = \frac{X^3 - 108b}{X^2}, \quad y' = \frac{X^3 + 216b}{X^3}\, Y,$$

respectively. Hence $\hat{\lambda} : E^* \to E$ is given by

$$x = \frac{X^3 - 108b}{9X^2}, \quad y = \frac{X^3 + 216b}{27X^3}\, Y.$$

3 A chain of isogenies

Let the notation and the assumptions be the same as in the previous section. We define isogenies

$$\lambda_i : E_i \to E_i^*, \quad \lambda_i^* : E_i^* \to E_{i+1}$$

$(i = 0, 1, 2, \ldots)$ by

$$(3.1) \qquad \begin{aligned} E_i &: \ y_i^2 = x_i^3 + l^{4i} a\, x_i + l^{6i} b, \\ E_i^* &: \ Y_i^2 = X_i^3 + l^{4i} A\, X_i + l^{6i} B, \end{aligned}$$

and by

$$\lambda_i : \ X_i = l^{2i}\, \xi\Big(\frac{x_i}{l^{2i}}\Big), \quad Y_i = \eta\Big(\frac{x_i}{l^{2i}}\Big)\, y_i,$$

$$\lambda_i^* : \ x_{i+1} = l^{2i}\, \xi^*\Big(\frac{X_i}{l^{2i}}\Big), \quad y_{i+1} = \eta^*\Big(\frac{X_i}{l^{2i}}\Big)\, Y_i.$$

We note that E_{i+1} is nothing but E_i' with the notation in the previous section. We also define isomorphisms

$$\phi_i : E \to E_i, \quad \phi_i^* : E^* \to E_i^*$$

by

$$\phi_i : \ x_i = l^{2i}\, x, \quad y_i = l^{3i}\, y,$$
$$\phi_i^* : \ X_i = l^{2i}\, X, \quad Y_i = l^{3i}\, Y.$$

Then:

Proposition 3.1 *We have*

$$\lambda_i \circ \phi_i = \phi_i^* \circ \lambda, \quad \lambda_i^* \circ \phi_i^* = \phi_{i+1} \circ \hat{\lambda}.$$

Proof Immediate from Proposition 2.1 and Corollary 2.2. □

Corollary 3.2 *The equations for $\lambda_i : E_i \to E_i^*$ and $\lambda_i^* : E_i^* \to E_{i+1}$ described above are the ones that are given by Vélu's formulas applied to $\phi_i(\Gamma)$ and $\phi_i^*(\Gamma^*)$, respectively.*

Proof We first note that the equations (2.1) for $\lambda : E \to E^*$ are derived from

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

Here τ_T denotes the translation-by-T map on E. Hence, regarding

$$\begin{array}{ccc} k(E) & \supset & k(E^*) \\ \cup & & \cup \\ k(E_i) & \supset & k(E_i^*) \end{array}$$

by the commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\lambda} & E^* \\ {\scriptstyle \phi_i}\big\downarrow & & \big\downarrow{\scriptstyle \phi_i^*} \\ E_i & \xrightarrow{\lambda_i} & E_i^* \end{array}$$

(see Proposition 3.1), we have

$$\begin{aligned} X_i &= l^{2i}\, X \\ &= l^{2i}\Big(x + \sum_{T \in \Gamma - \{O\}} \big(x \circ \tau_T - x(T)\big)\Big) \\ &= x_i + \sum_{T \in \Gamma - \{O\}} \big(x_i \circ \tau_{\phi_i T} - x_i(\phi_i T)\big), \end{aligned}$$

that is

$$X_i = x_i + \sum_{T_i \in \phi_i(\Gamma) - \{O\}} \big(x_i \circ \tau_{T_i} - x_i(T_i)\big).$$

We also have

$$Y_i = y_i + \sum_{T_i \in \phi_i(\Gamma) - \{O\}} \big(y_i \circ \tau_{T_i} - y_i(T_i)\big)$$

in the same manner. Thus we have shown the assertion for $\lambda_i : E_i \to E_i^*$. Since the equations (2.2) for $\lambda^* : E^* \to E'$ are derived from

$$x' = X + \sum_{U \in \Gamma^* - \{O\}} \big(X \circ \tau_U - X(U)\big),$$
$$y' = Y + \sum_{U \in \Gamma^* - \{O\}} \big(Y \circ \tau_U - Y(U)\big),$$

we can show the assertion for $\lambda_i^* : E_i^* \to E_{i+1}$ in a similar fashion. □

4 Field extensions

Let k be an algebraic number field of finite degree, l an odd prime number, n a positive integer, and let

$$E:\ y^2 = x^3+ax+b\ \ (a,b \in \mathcal{O}_k,\ 4a^3+27b^2 \neq 0)$$

be an elliptic curve defined over k such that $E[l^n] \subset E(k)$. We assume that the Weierstrass equation above is taken so that the condition

$$x(T),\ y(T) \in \mathcal{O}_k \quad (T \in E[l] - \{O\})$$

is satisfied. Taking a subgroup Γ of E of order l, we define $\lambda : E \to E^*,\ \lambda^* : E^* \to E'$, etc. in the same manner as in Sections 2 and 3. Then $A, B \in \mathcal{O}_k$ and

$$X(U),\ Y(U) \in \mathcal{O}_k \quad (U \in \Gamma^* - \{O\}).$$

Consequently, we have

$$(4.1)\ \ x_i(T_i),\ y_i(T_i) \in \mathcal{O}_k \quad (T_i \in \phi_i(\Gamma) - \{O\})$$

and

$$(4.2)\ \ X_i(U_i), Y_i(U_i) \in \mathcal{O}_k\ (U_i \in \phi_i^*(\Gamma^*) - \{O\}).$$

Let P be a point on E with $x(P) \in k$, and let $K = k(P),\ L = k([l^n]^{-1}P)$. It follows from the assumption $E[l^n] \subset E(k)$ that L/K is an abelian extension of exponent l^n. Putting $P_n = \phi_n P$, which is a point on E_n, we define intermediate fields K_j $(0 \leq j \leq n)$ and K_j^* $(1 \leq j \leq n)$ of L/K by

$$K_j = k((\lambda_{n-1}^* \circ \lambda_{n-1} \circ \cdots \circ \lambda_{n-j}^* \circ \lambda_{n-j})^{-1} P_n)$$

and by

$$K_j^* = k((\lambda_{n-1}^* \circ \lambda_{n-1} \circ \cdots \circ \lambda_{n-j+1} \circ \lambda_{n-j}^*)^{-1} P_n),$$

respectively. Then we have

$$K_n \supset K_n^* \supset \cdots \supset K_2 \supset K_2^* \supset K_1 \supset K_1^* \supset K_0$$

and $K_j = k([l^j]^{-1}P)$. In particular, $K_0 = K,\ K_n = L$. We also have:

Proposition 4.1 *Let i be an integer such that $1 \leq i \leq n-1$, and let $j = n - i$. Then*:

(i) *For any point P_i on E_i with*

$$(\lambda_{n-1}^* \circ \lambda_{n-1} \circ \cdots \circ \lambda_i^* \circ \lambda_i) P_i = P_n,$$

we have $K_j = k(P_i)$ and an injective homomorphism

$$\mathrm{Gal}(K_j/K_j^*) \ni \sigma \longmapsto P_i^\sigma - P_i \in \phi_i(\Gamma).$$

(ii) *For any point P_i^* on E_i^* with*

$$(\lambda_{n-1}^* \circ \lambda_{n-1} \circ \cdots \circ \lambda_{i+1} \circ \lambda_i^*) P_i^* = P_n,$$

we have $K_j^* = k(P_i^*)$ and an injective homomorphism

$$\mathrm{Gal}(K_j^*/K_{j-1}) \ni \sigma \longmapsto (P_i^*)^\sigma - P_i^* \in \phi_i^*(\Gamma^*).$$

Proof Immediate from

$$\begin{aligned}&\mathrm{Ker}(\lambda_{n-1}^* \circ \lambda_{n-1} \circ \cdots \circ \lambda_i^* \circ \lambda_i)\\ &= (\lambda_{i-1}^* \circ \lambda_{i-1} \circ \cdots \circ \lambda_0^* \circ \lambda_0) E_0[l^n],\end{aligned}$$

which is a subgroup of $E_i(k)$, and

$$\begin{aligned}&\mathrm{Ker}(\lambda_{n-1}^* \circ \lambda_{n-1} \circ \cdots \circ \lambda_{i+1} \circ \lambda_i^*)\\ &= (\lambda_i \circ \lambda_{i-1}^* \circ \cdots \circ \lambda_0^* \circ \lambda_0) E_0[l^n],\end{aligned}$$

which is a subgroup of $E_i^*(k)$. □

Now, we assume that $c = x(P)$ satisfies the condition

$$\min\bigl\{\mathrm{ord}_{\mathfrak{p}}(c^3+ac+b),\ \mathrm{ord}_{\mathfrak{p}}(3c^2+a)\bigr\} \le 0 \tag{4.3}$$

for any finite place $\mathfrak{p}$ of k such that E has bad reduction at $\mathfrak{p}$ or $\mathfrak{p} \mid l$. Here, we replace the inequality above by

$$\mathrm{ord}_{\mathfrak{p}}(c^2 + a) \le 0 \tag{4.3$'$}$$

if $\mathfrak{p} \mid 2$, and by

$$\mathrm{ord}_{\mathfrak{p}}(l^{2n}c) \le 0 \tag{4.3$''$}$$

if $\mathfrak{p} \mid l$. Then we have:

Proposition 4.2 *The extensions K_j/K_j^* and K_j^*/K_{j-1} are unramified at all finite places.*

Proof We fix a finite place $\mathfrak{P}$ of L such that E has bad reduction at $\mathfrak{P}$ or $\mathfrak{P} \mid l$, for L/K is unramified at other finite places, and put

$$\mathcal{E}_i(L;\mathfrak{P}) = \{Q \in E_i(L)\ ;\ \widetilde{Q} \in (\widetilde{E}_i)_{\mathrm{ns}}(\kappa)\},$$
$$\mathcal{E}_i^*(L;\mathfrak{P}) = \{Q^* \in E_i^*(L)\ ;\ \widetilde{Q}^* \in (\widetilde{E}_i^*)_{\mathrm{ns}}(\kappa)\}.$$

Here,

$$E_i(L) \ni Q \longmapsto \widetilde{Q} \in \widetilde{E}_i(\kappa),$$
$$E_i^*(L) \ni Q^* \longmapsto \widetilde{Q}^* \in \widetilde{E}_i^*(\kappa)$$

(κ denotes the residue field of $\mathfrak{P}$) are the reduction modulo $\mathfrak{P}$ maps *with respect to the equations* (3.1), and the symbol "ns" means non-singular points. Then the assumption (4.3) (or (4.3)$'$ or (4.3)$''$) implies $P_n \in \mathcal{E}_n(L;\mathfrak{P})$. Therefore, by Corollary 3.2, (4.1), (4.2) and by [3, Theorem 4.5], there exist $P_i \in \mathcal{E}_i(L;\mathfrak{P})$ $(0 \le i \le n-1)$ and $P_i^* \in \mathcal{E}_i^*(L;\mathfrak{P})$ $(0 \le i \le n-1)$ such that

$$P_0 \overset{\lambda_0}{\longmapsto} P_0^* \overset{\lambda_0^*}{\longmapsto} \cdots \overset{\lambda_{n-3}^*}{\longmapsto} P_{n-2} \overset{\lambda_{n-2}}{\longmapsto} P_{n-2}^* \overset{\lambda_{n-2}^*}{\longmapsto} P_{n-1} \overset{\lambda_{n-1}}{\longmapsto} P_{n-1}^* \overset{\lambda_{n-1}^*}{\longmapsto} P_n.$$

These points might depend on the place $\mathfrak{P}$. However, the fields

$$k(P_i) = K_{n-i},\ k(P_i^*) = K_{n-i}^* \quad (0 \le i \le n-1)$$

do not depend on the choice of such points (see Proposition 4.1). Hence we can show that K_j/K_j^* and K_j^*/K_{j-1} are unramified at $\mathfrak{P}$ in a similar fashion to the argument in [3, Section 5], in which we use Proposition 4.1 again (note that an extension of degree 1 is unramified). □

Proposition 4.2 immediately implies that L/K is unramified at all finite places, which is the assertion of Theorem 1.1.

5 Some examples

We close the present paper with giving some examples of biquadratic number fields, which contain $\sqrt{-3}$, with class numbers divisible by 9. Let $k = \mathbb{Q}(\sqrt{-3})$, $l = 3$, $n = 1$, and let

$$E:\ y^2 = x^3 + 16.$$

Then, by using Magma [1], we have

$$x \circ [3] = \frac{x^9 - 1536x^6 + 12288x^3 + 262144}{9x^2(x^3+64)^2},$$
$$\mathrm{rank}\, E(\mathbb{Q}) = \mathrm{rank}\, E_{k/\mathbb{Q}}(\mathbb{Q}) = 0,$$

where

$$E_{k/\mathbb{Q}}:\ -3y^2 = x^3 + 16$$

is the quadratic twist of E with respect to $k/\mathbb{Q}$, and $E(k)_{\mathrm{tors}} = E[3]$ consists of

$$O,\ (0,\pm 4),\ (-4,\pm 4\sqrt{-3}\,),$$
$$(2+2\sqrt{-3}\,,\pm 4\sqrt{-3}\,),\ (2-2\sqrt{-3}\,,\pm 4\sqrt{-3}\,).$$

Therefore $E(k) = E[3]$. It is not hard to observe that E is isomorphic to

$$(y')^2 + y' = (x')^3,$$

which has discriminant -27. Thus E has good reduction at every finite place except $\mathfrak{p} = (\sqrt{-3}\,)$. In this case, the condition on $c = x(P)$ in Theorem 1.1 becomes

$$\mathrm{ord}_{\mathfrak{p}}(9c) \le 0.$$

Moreover $L = k([3]^{-1}P)$ coincides with the splitting field of

$$f_c(x) = x^9 - 1536x^6 + 12288x^3 + 262144 - 9cx^2(x^3+64)^2$$

over $K = k(P) = k(\sqrt{c^3+16}\,)$, since $y(P) \neq 0$. Consequently, if $\mathrm{ord}_{\mathfrak{p}}(9c) \le 0$ and if $f_c(x)$ is irreducible over K, then L/K is an unramified abelian extension of degree 9, and hence the class number of K is divisible by 9. We note that these conditions imply $[K : k] = 2$, for the class number of k is 1.

In what follows, we shall consider the case where $c \in \mathbb{Q}$. Then $K = \mathbb{Q}(\sqrt{-3}\,, \sqrt{c^3+16}\,)$ is a biquadratic field (that is, $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the Klein 4-group) unless $c = 0$ or $c = -4$. Hence, if $f_c(x)$ is irreducible over $\mathbb{Q}$, so is over K. Thus Theorem 1.1 implies:

Corollary 5.1 *Let c be a rational number satisfying the following two conditions*:

(a) $\mathrm{ord}_3(9c) \le 0$.

(b) $f_c(x)$ *is irreducible over* $\mathbb{Q}$.

Then the class number of $\mathbb{Q}(\sqrt{-3}\,, \sqrt{c^3+16}\,)$ *is divisible by* 9.

Example 5.2 Using PARI/GP [2], we have the following table. Here h_K denotes the class number of $K = \mathbb{Q}(\sqrt{-3}\,, \sqrt{c^3+16}\,)$. We have $9 \mid h_K$, except for $c = \pm 3/9, \pm 6/9, \pm 9/9$ or $c = -4/9$. The values $c = \pm 3/9, \pm 6/9$ and $c = \pm 9/9$ do not satisfy the condition (a), while the values $c = 9/9$ and $c = -4/9$ do not satisfy the condition (b).

c	h_K	c	h_K
1/9	540	−1/9	1296
2/9	108	−2/9	432
3/9	96	−3/9	21
4/9	54	−4/9	3
5/9	189	−5/9	432
6/9	24	−6/9	6
7/9	270	−7/9	315
8/9	9	−8/9	36
9/9	1	−9/9	2
10/9	72	−10/9	144

References

[1] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput. **24** (1997), 235–265.

[2] The PARI Group, PARI/GP version `2.5.2`, Univ. Bordeaux, 2012, `http://pari.math.u-bordeaux.fr/`.

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

[4] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106**, Springer-Verlag, New York, 1986.

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

[6] L.C. Washington, *Elliptic Curves*: *Number Theory and Cryptography*, 2nd ed., Discrete Mathematics and Its Applications, Chapman & Hall/CRC, Boca Raton, FL, 2008.