Construction of Number Fields of Odd Degree with Class Numbers Divisible by Three, Five or by Seven

Atsushi SATO

Mathematical Institute, Tohoku University, Sendai 980-8578, Japan

E-mail: atsushi@math.tohoku.ac.jp

Abstract

We introduce a simple way to construct a family of number fields of given degree with class numbers divisible by a given integer, by using the arithmetic theory of elliptic curves. In particular, we start with an elliptic curve defined over the rational number field with a rational torsion point of order $l \in \{3, 5, 7\}$, and show a way to construct infinitely many number fields of given odd degree $d \geq 3$ with class numbers divisible by l.

KEYWORDS: divisibility of class numbers, isogeny of elliptic curves

1 Introduction

The divisibility of class numbers, not only for quadratic number fields but also for arbitrary number fields, has been studied for a long time. For example, Azuhata and Ichimura (1984) proved that, for any integers $d \geq 2$ and $l \geq 2$, there exist infinitely many number fields of degree d with class numbers divisible by l. In fact, they proved a much deeper theorem. Combining with a work of Nakano (1985), we can rewrite the theorem into the following form: *There exist infinitely many number fields with prescribed number of real and imaginary places with class numbers divisible by a given integer.* The proof of this theorem, due to Azuhata-Ichimura and Nakano, also describes a way to construct such number fields. However, in order to construct them in practice, we have to check a number of conditions.

In the present paper, we introduce a simple way to construct, from an elliptic curve with a rational torsion point of prime order $l \neq 2$ (hence $l \in \{3, 5, 7\}$, because of Mazur's theorem), infinitely many number fields of given odd degree $d \geq 3$ with class numbers divisible by l. Our result states nothing new about the existence of number fields. However, our way is so simple that we can construct such number fields very easily.

We close the present section with giving an example (see Example 5.1). Let a be a positive integer, and let E be an elliptic curve given by

$$y^2 + ay = x^3,$$

which has a rational point $(0, 0)$ of order three. For this case, our results imply: *Let c be a positive integer satisfying* $\gcd(c, 3a) = 1$*, and suppose that the polynomial*

$$4(x^3 + a^2)^d - 27a^2(x^3 + a^2)^{d-3}\, x^6 - c^2\, x^{2d}$$

is irreducible over the rational number field ($d \geq 3$ is an odd integer, as mentioned above). Then, for any root ξ of $4X^d - 27a^2X^{d-3} - c^2$, the number field obtained by adjoining ξ to the rational number field is of degree d with class number divisible by three.

2 The Field Extensions Arising from an Isogeny

Before describing the main results, we shall briefly review some properties about an isogeny of elliptic curves, which plays an important role in our theory, in the general setting. We also observe how to obtain number fields with class numbers divisible by l from an isogeny of degree l.

Let k be a number field of finite degree, and let E be an elliptic curve defined over k which has a k-rational point T_0 of prime order l. Then we can take a Weierstrass equation for E of the form

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

with

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

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 a defining 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 (for the formulas, see Vélu (1971), Section 12.3 of Washington (2008) or Section 2 of Sato (2008)). Here $\langle T_0 \rangle$ denotes the subgroup of $E(k)$ generated by T_0.

Let Q be a point on E^*. We denote the fields $k(Q) = k(X(Q), Y(Q))$ and $k(\lambda^{-1}(Q)) = k(x(P), y(P)\ ;\ P \in \lambda^{-1}(Q))$ by K and L, respectively. Then, L/K is a Galois extension, $L = K(P)$ holds for any $P \in \lambda^{-1}(Q)$, and the map

$$\mathrm{Gal}(L/K) \ni \sigma \longmapsto P^\sigma - P \in \langle T_0 \rangle$$

(P is a point in $\lambda^{-1}(Q)$) is an injective group homomorphism. Since $\#\langle T_0 \rangle = l$ is prime, the extension L/K is cyclic of degree l if the following condition is satisfied (otherwise we have $L = K$):

(C1) $$Q \notin \lambda(E(K)).$$

In Sato (2008), the author studied about the ramification in L/K, and obtained a sufficient condition for which the extension is unramified at every finite place. The main results in that paper (Theorems 4.5 and 5.1) can be rephrased as follows: *Let $\mathfrak{p}$ be a prime ideal in k, and let $\widetilde{E}^* = E^* \bmod \mathfrak{p}$ be the curve, defined over the residue field $\mathcal{O}_k/\mathfrak{p}$, which is given by*

$$y^2 + \widetilde{A}_1 xy + \widetilde{A}_3 y = x^3 + \widetilde{A}_2 x^2 + \widetilde{A}_4 x + \widetilde{A}_6,$$

where $\widetilde{A}_i$ denotes the image of A_i in $\mathcal{O}_k/\mathfrak{p}$ (we have $A_1, A_2, A_3, A_4, A_6 \in \mathcal{O}_k$). Let $\mathfrak{P}$ be a prime divisor of $\mathfrak{p}$ in K. Then L/K is unramified at $\mathfrak{P}$ if the image of Q on $\widetilde{E}^*$ is nonsingular.

Using the facts described above, we can construct number fields with class numbers divisible by l. In fact, the extension L/K is unramified at every finite place if we can choose Q so that the following condition is satisfied:

(C2) The image of Q on $E^* \bmod \mathfrak{p}$ is nonsingular for every $\mathfrak{p}$.

If $l \neq 2$ (or if K is totally imaginary), the extension is also unramified at every infinite place. Therefore, the two conditions (C1) and (C2) imply that the class number of K is

divisible by l, for the Hilbert class field of K contains L. Moreover, if Q satisfies $Z(Q) \in k$ for some function $Z \in k(E^*)$ of degree d, we may expect

(C3) $$[K : k] = d.$$

In the case where $Z = X$ (hence $d = 2$) and $[2]Q \neq O$, we can write down the two conditions (C1) and (C2), in terms of the X-coordinate of Q, in an explicit form (see Theorem 5.1 of Sato (2008)). We can also estimate the density of such X-coordinates in k that satisfy the two conditions (see Corollary 6.4 of Sato (2008)). In that case, we have either $[K : k] = 2$ or $K = k$. Thus, putting $k = \mathbb{Q}$ (hence $l \in \{3, 5, 7\}$), we can obtain quadratic number fields with class numbers divisible by l. Indeed, if the class number of K is divisible by l, we cannot have $K = \mathbb{Q}$.

In what follows, we shall apply the above scheme to construct number fields of given odd degree $d \geq 3$ with class numbers divisible by l. That is, putting $k = \mathbb{Q}$ and $Z = X^{(d-3)/2}(2Y + A_1X + A_3)$, we study the three conditions (C1), (C2) and (C3) for such points Q that satisfy $Z(Q) \in \mathbb{Q}$. We can also construct number fields of even degree $d \geq 2$ with the same property by putting $Z = X^{d/2}$. However we shall not treat the even case in the present paper.

3 Main Results

Let $d \geq 3$ be an odd integer, and let E be an elliptic curve defined over $\mathbb{Q}$ which has a rational point T_0 of prime order $l \neq 2$ (thus $l \in \{3, 5, 7\}$). 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

$$a_1,\ a_2,\ a_3,\ a_4,\ a_6,\ x(T_0),\ y(T_0) \in \mathbb{Z}.$$

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. Then, we have $A_1, A_2, A_3, A_4, A_6 \in \mathbb{Z}$, and λ is given by

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

(we shall omit the expression for Y) with monic polynomials $I(x),\ J(x) \in \mathbb{Z}[x]$ satisfying $\deg I(x) = l,\ \deg J(x) = l - 1$. Furthermore, we denote the discriminant of Equation $(*)$ by Δ^*, and define polynomials $F(X)$ and $H(Z\,;x)$ 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 by

$$\begin{aligned} H(Z\,;x) = {} & 4I(x)^d + (A_1^2 + 4A_2)I(x)^{d-1}J(x) \\ & + 2(A_1A_3 + 2A_4)I(x)^{d-2}J(x)^2 + (A_3^2 + 4A_6)I(x)^{d-3}J(x)^3 - Z^2J(x)^d, \end{aligned}$$

respectively. With the notation and the assumptions described above, we can state the main theorem, which we will show in the next section:

Theorem 3.1 *Let the notation and the assumptions be as above, and let c be a nonzero rational number which satisfies the following two conditions*:

(a) $\mathrm{ord}_p\, c \leq 0$ *for any prime divisor p of Δ^*.*

(b) $H(c\,;x)$ *is irreducible over $\mathbb{Q}$.*

Here ord_p *denotes the normalized additive valuation for p. Then, for any root ξ of the polynomial $X^{d-3}\,F(X) - c^2$, the number field $\mathbb{Q}(\xi)$ is of degree d with class number divisible by l.*

For a nonzero integer c, the condition (a) in the above theorem is equivalent to $\gcd(c, \Delta^*) = 1$. Hence it follows from a variant of Hilbert's irreducibility theorem (see, e.g., Chapter 9 of Lang (1983)) that there exist infinitely many integers c such that the two conditions in the theorem are satisfied. Indeed, as we will see in the next section, the polynomial $H(Z\,;x)$ is irreducible over the rational function field $\mathbb{Q}(Z)$. Moreover, by using Siegel's theorem on the finiteness of integral points on a curve of genus one (see, e.g., Chapter IX of Silverman (1986)) we can show the following:

Corollary 3.2 *By varying positive integers c in the above theorem, we can obtain infinitely many number fields of degree d with class number divisible by l.*

4 Proof of Theorem 3.1

Let the notation and the assumptions be the same as in the previous section. First, we study about the polynomials $F(X)$ and $H(Z\,;x)$, especially their origins. We denote the function fields $\mathbb{Q}(E) = \mathbb{Q}(x, y)$ and $\mathbb{Q}(E^*) = \mathbb{Q}(X, Y)$ by $\mathfrak{L}$ and $\mathfrak{K}$, respectively. We can regard $\mathfrak{L}$ as a cyclic extension of $\mathfrak{K}$ of degree l, and then $\mathfrak{L} = \mathfrak{K}(x)$. Now we note that Equation $(*)$ for E^* can be rewritten as

$$(2Y + A_1X + A_3)^2 = F(X).$$

Putting $Z = X^{(d-3)/2}\,(2Y + A_1X + A_3) \in \mathfrak{K}$, which is of degree d, we can also rewrite the equation as

$$Z^2 = X^{d-3}\,F(X).$$

Here we shall regard the function Z as a morphism from E^* to the projective line $\mathbb{P}^1$, and we denote the function field $\mathbb{Q}(\mathbb{P}^1) = \mathbb{Q}(Z)$ by $\mathfrak{F}$. We can regard $\mathfrak{K}$ as an extension of $\mathfrak{F}$ of degree d, and then $\mathfrak{K} = \mathfrak{F}(X)$. Thus we obtain the following tower of function fields:

$$\begin{array}{ll} \mathfrak{L} = \mathfrak{K}(x) & \\ \Big| \; l & I(x) - XJ(x) = 0 \\ \mathfrak{K} = \mathfrak{F}(X) & \\ \Big| \; d & X^{d-3}\,F(X) - Z^2 = 0 \\ \mathfrak{F} = \mathbb{Q}(Z) & \end{array}$$

Hence we have $\mathfrak{L} = \mathfrak{F}(x)$. Since the polynomial $H(Z\,;x)$, which is of degree $d\,l$ with respect to x, is defined so that

$$\frac{H(Z\,;x)}{J(x)^d} = \left(\frac{I(x)}{J(x)}\right)^{d-3} F\left(\frac{I(x)}{J(x)}\right) - Z^2$$

holds, we conclude that $H(Z\,;x)$ is irreducible over $\mathfrak{F}$ (if we regard x as an indeterminate).

Next, we specialize the argument described above, and study the meaning of the assumption (b) in the theorem. Let c and ξ be as in the statement of the theorem. Then there exists a (unique) point Q on E^* which satisfies $X(Q) = \xi$ and $Z(Q) = c$. Since $c \neq 0$, we have $F(\xi) \neq 0$, and hence $[2]Q \neq O$. We put $K = \mathbb{Q}(Q)$ and $L = \mathbb{Q}\big(\lambda^{-1}(Q)\big)$, which are the specializations of $\mathfrak{K}$ and $\mathfrak{L}$, respectively. Then, as discussed in Section 2, L/K is a cyclic extension. In the present case, we have $K = \mathbb{Q}(\xi)$ and $[K : \mathbb{Q}] \leq d$.

Moreover, we can obtain $L = K(\omega)$ and $[L : K] \leq l$, where ω is a root of the polynomial $I(x) - \xi J(x)$ (we also have $J(\omega) \neq 0$). In fact, L is the splitting field of $I(x) - \xi J(x)$ over K (see Section 3.3 of Sato (2008)). Thus we obtain the following tower of number fields:

$$\begin{array}{ll} & L = K(\omega) \\ l \geq & \Big| \qquad\qquad\qquad I(\omega) - \xi J(\omega) = 0,\ J(\omega) \neq 0 \\ & K = \mathbb{Q}(\xi) \\ d \geq & \Big| \qquad\qquad\qquad \xi^{d-3} F(\xi) - c^2 = 0 \\ & \mathbb{Q} \end{array}$$

Hence we have $L = \mathbb{Q}(\omega)$ and $H(c\,;\omega) = 0$. Therefore the assumption (b) in the theorem implies $[K : \mathbb{Q}] = d$ and $[L : K] = l$, for $H(c\,;x)$ is of degree $d\,l$. The former equality is nothing but the condition (C3) in Section 2, and the latter one is equivalent to the condition (C1).

Finally, we show that the assumption (a) in the theorem implies the condition (C2). Let p be a prime number, and let $\widetilde{E}^* = E^* \bmod p$ be the curve, defined over $\mathbb{Z}/p\mathbb{Z}$, which is given by

$$y^2 + \widetilde{A}_1 xy + \widetilde{A}_3 y = x^3 + \widetilde{A}_2 x^2 + \widetilde{A}_4 x + \widetilde{A}_6,$$

where $\widetilde{A}_i$ denotes the image of A_i in $\mathbb{Z}/p\mathbb{Z}$. Let $\mathfrak{P}$ be a prime divisor of p in K. Our goal is to show that the image of Q on $\widetilde{E}^*$ is nonsingular. Clearly we may assume that p divides Δ^*. Then the assumption (a) implies

$$\frac{d-3}{2} \operatorname{ord}_{\mathfrak{P}} X(Q) + \operatorname{ord}_{\mathfrak{P}}\big(2Y(Q) + A_1 X(Q) + A_3\big) \leq 0.$$

Here $\operatorname{ord}_{\mathfrak{P}}$ denotes the normalized additive valuation for $\mathfrak{P}$. If $\operatorname{ord}_{\mathfrak{P}} X(Q) < 0$, we have $\operatorname{ord}_{\mathfrak{P}} Y(Q) < 0$, and hence Q is reduced into the point at infinity, which is a nonsingular point on $\widetilde{E}^*$. If $\operatorname{ord}_{\mathfrak{P}} X(Q) \geq 0$, we have $\operatorname{ord}_{\mathfrak{P}} Y(Q) \geq 0$, and hence it follows from the above inequality that

$$\operatorname{ord}_{\mathfrak{P}}\big(2Y(Q) + A_1 X(Q) + A_3\big) = 0,$$

which implies that the image of Q on $\widetilde{E}^*$ is nonsingular.

5 Examples

In order to construct the number fields $\mathbb{Q}(\xi)$ described in Theorem 3.1 in practice, we need to prepare four data $\Delta^*, I(x), J(x)$ and $F(X)$. We close the present paper with

giving some examples.

Example 5.1 (The case of $l = 3$) If E has a rational point T_0 of order three, E has an equation of the form

$$y^2 + axy + a^2by = x^3 \qquad (a, b \in \mathbb{Z},\ ab(a - 27b) \neq 0)$$

or

$$y^2 + ay = x^3 \qquad (a \in \mathbb{Z},\ a \neq 0)$$

with $T_0 = (0, 0)$.

(i) In the former case, E^* is given by

$$Y^2 + aXY + a^2bY = X^3 - 5a^3bX - a^4b(a + 7b),$$

which has $\Delta^* = a^8b(a - 27b)^3$, with

$$I(x) = x^3 + a^3bx + a^4b^2, \qquad J(x) = x^2.$$

Consequently we have

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

(ii) In the latter case, E^* is given by

$$Y^2 + aY = X^3 - 7a^2,$$

which has $\Delta^* = -3^9\, a^4$, with

$$I(x) = x^3 + a^2, \qquad J(x) = x^2.$$

Consequently we have

$$F(X) = 4X^3 - 27a^2.$$

Example 5.2 (The case of $l = 5$) If E has a rational point T_0 of order five, E has an equation of the form

$$y^2 + (a + b)xy + ab^2y = x^3 + abx^2 \qquad (a, b \in \mathbb{Z},\ ab \neq 0)$$

with $T_0 = (0, 0)$. Then E^* is given by

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

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

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

Consequently we have

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

Example 5.3 (The case of $l = 7$) If E has a rational point T_0 of order seven, E has an equation of the form

$$y^2 + (a^2 + ab - b^2)xy + a^3b^2(a-b)y = x^3 + ab^2(a-b)x^2 \qquad (a, b \in \mathbb{Z},\ ab(a-b) \neq 0)$$

with $T_0 = (0, 0)$. Then E^* is given by

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

which has $\Delta^* = -ab(a-b)(a^3 + 5a^2b - 8ab^2 + b^3)^7$, with

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

Consequently we have

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

References

[1] Azuhata, T. and Ichimura, H., On the divisibility problem of the class numbers of algebraic number fields, *J. Fac. Sci. Univ. Tokyo*, **30**: 579–585 (1984).

[2] Lang, S., Fundamentals of Diophantine Geometry, Springer, New York (1983).

[3] Nakano, S., On ideal class groups of algebraic number fields, *J. Reine Angew. Math.*, **358**: 61–75 (1985).

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

[5] Silverman, J. H., The Arithmetic of Elliptic Curves, Graduate Texts in Math. 106, Springer, New York (1986).

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

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