

Title	Leading coefficients of isogenies of degree $p$ over $\mathbb{Q}_p$
Author(s)	Kawachi, Mayumi
Citation	Osaka Journal of Mathematics. 48(3) P.691-P.708
Issue Date	2011-09
Text Version	publisher
URL	<a href="https://doi.org/10.18910/8290">https://doi.org/10.18910/8290</a>
DOI	10.18910/8290
rights	
Note	

*Osaka University Knowledge Archive : OUKA*

<https://ir.library.osaka-u.ac.jp/>

Osaka University

## LEADING COEFFICIENTS OF ISOGENIES OF DEGREE $p$ OVER $\mathbb{Q}_p$

MAYUMI KAWACHI

(Received November 26, 2008, revised March 1, 2010)

### Abstract

Let  $E$  be an elliptic curve over  $\mathbb{Q}_p$  which has potentially supersingular good reduction. Let  $L/\mathbb{Q}_p$  be a totally ramified extension such that  $E$  has good reduction over  $L$  and  $\tilde{E}$  be the reduction of  $E \bmod \pi$ , where  $\pi$  is a prime element of the ring of integers  $\mathcal{O}_L$  of  $L$ . Let  $\hat{E}$  be the formal group over  $\mathcal{O}_L$  associated to  $E/\mathcal{O}_L$ . The multiplication by  $p$  map  $[p]: \hat{E} \rightarrow \hat{E}$  is written by power series  $[p](x) = px + c_2x^2 + \cdots + c_px^p + \cdots + c_{p^2}x^{p^2} + \cdots \in \mathcal{O}_L[[x]]$ . By using the liftings over  $\mathcal{O}_L$  of the Dieudonné module of  $p$ -divisible group  $\tilde{E}(p)$  over  $\mathbb{F}_p$ , we determine the values of  $v_L(c_p)$ .

### 1. Introduction

Let  $p \geq 5$  be a prime number and  $E$  be an elliptic curve over the  $p$ -adic number field  $\mathbb{Q}_p$ . We assume  $v_p(j) \geq 0$ , where  $v_p$  is the normalized additive  $p$ -adic valuation and  $j$  is the  $j$ -invariant of  $E$ . Then  $E$  has potentially good reduction over  $\mathbb{Q}_p$ . Let  $E/\mathbb{Z}_p$  be the minimal Weierstrass equation for  $E$  over the  $p$ -adic integer ring  $\mathbb{Z}_p$ . Put  $e = 12/\gcd(v_p(\Delta), 12)$ , where  $\Delta$  is the discriminant of  $E/\mathbb{Z}_p$ . Let  $\pi$  be an element of the algebraic closure  $\tilde{\mathbb{Q}}_p$  of  $\mathbb{Q}_p$  such that  $\pi^e + p = 0$ . Then  $L = \mathbb{Q}_p(\pi)$  is the unique totally ramified extension of degree  $e$  over  $\mathbb{Q}_p$ . Then  $E$  has good reduction over  $L$ . Let  $E/\mathcal{O}_L$  be the minimal Weierstrass equation for  $E$  over the ring of integers  $\mathcal{O}_L$  of  $L$ . Let  $\tilde{E}/\mathbb{F}_p$  be the reduction of  $E/\mathcal{O}_L \bmod \pi$ . Let  $\hat{E}$  be the formal group over  $\mathcal{O}_L$  associated to  $E/\mathcal{O}_L$  [7, IV, §1]. The multiplication by  $p$  map  $[p]: \hat{E} \rightarrow \hat{E}$  is written by a power series  $[p](x) = px + c_2x^2 + \cdots + c_px^p + \cdots + c_{p^2}x^{p^2} + \cdots \in \mathcal{O}_L[[x]]$ . The purpose of this paper is to determine the valuation of a coefficient  $c_p$  of  $x^p$ , when  $\tilde{E}/\mathbb{F}_p$  is supersingular.

**Theorem.** *Assume that  $j$  is integral and  $\tilde{E}/\mathbb{F}_p$  is supersingular. If  $c_p = 0$  or  $v_L(c_p) < e$ , we have the followings.*

- 1) For  $e = 1$ ,  $c_p = 0$ .
- 2) For  $e = 2$ ,  $c_p = 0$ .

- 3) For  $e = 3$ ,  $c_p = 0$  if and only if  $j = 0$ . If  $j \neq 0$ , then  $v_L(c_p) = 1$  or  $2$ . More precisely, if  $v_p(\Delta) = 4$  then  $v_L(c_p) = 2$ , and if  $v_p(\Delta) = 8$  then  $v_L(c_p) = 1$ .
- 4) For  $e = 4$ ,  $c_p = 0$  if and only if  $j = 1728$ . If  $j \neq 1728$ , then  $v_L(c_p) = 2$ .
- 5) For  $e = 6$ ,  $c_p = 0$  if and only if  $j = 0$ . If  $j \neq 0$ , then  $v_L(c_p) = 2$  or  $4$ . More precisely, if  $v_p(\Delta) = 2$  then  $v_L(c_p) = 2$ , and if  $v_p(\Delta) = 10$  then  $v_L(c_p) = 4$ .

Under the condition of Theorem, it follows that  $v_p(\Delta) = 4$  or  $8$  for  $e = 3$  and that  $v_p(\Delta) = 2$  or  $10$  for  $e = 6$ .

If we assume that there exists an elliptic curve  $E'$  over  $\mathbb{Q}_p$  and an isogeny  $\nu: E \rightarrow E'$  of degree  $p$  over  $\mathbb{Q}_p$ , then  $v_L(c_p) < e$  by Lemma 4.1.1. Moreover since  $E$  and  $E'$  are isogenous,  $E'$  has good reduction over  $L$ . Let  $\hat{E}'$  be a formal group over  $\mathcal{O}_L$  associated to  $E'/\mathcal{O}_L$ . Then we can construct an isogeny  $\hat{\nu}_L: \hat{E} \rightarrow \hat{E}'$  of height 1 over  $\mathcal{O}_L$ . Let  $\hat{\nu}_L(x) = a_1x + a_2x^2 + \dots$ . We are interested in the valuation of the leading coefficient  $a_1$ . Put  $t = v_L(a_1)$ . By Lemma 4.1.1,  $t = e - v_L(c_p)$  if  $e < p$ . So we can determine the value of  $t$  by Theorem.

In [6], we determine the image of a local Kummer map  $\delta: E'(K)/\nu_K E(K) \rightarrow H^1(K, \ker \nu_K)$ , where  $K$  is a finite extension of  $\mathbb{Q}_p$  and  $\nu_K: E \rightarrow E'$  is a  $p$ -isogeny over  $K$ . The image  $\text{Im} \delta$  is the local image of the connecting homomorphism at a prime over  $p$  of the Selmer group of an isogeny of degree  $p$  over a number field. And the image is described using the filtration on the unit group of  $K$  and the valuation of the leading coefficient of the formal power series of  $\nu_K$ . It is important to know the value of  $t$  in order to calculate the Selmer groups of isogenies of degree  $p$  over  $\mathbb{Q}$ .

**Corollary.** 1) For  $e = 1$ ,  $E$  does not have isogenies of degree  $p$  over  $\mathbb{Q}_p$ .

2) For  $e = 2$ ,  $E$  does not have isogenies of degree  $p$  over  $\mathbb{Q}_p$ .

3) For  $e = 3$ , if  $j = 0$ , then  $E$  does not have isogenies of degree  $p$  over  $\mathbb{Q}_p$ . If  $j \neq 0$ , then  $t = 1$  or  $2$ . More precisely if  $v_p(\Delta) = 4$  then  $t = 1$ , and if  $v_p(\Delta) = 8$  then  $t = 2$ .

4) For  $e = 4$ , if  $j = 1728$ , then  $E$  does not have isogenies of degree  $p$  over  $\mathbb{Q}_p$ . If  $j \neq 1728$ , then  $t = 2$ .

5) For  $e = 6$ , if  $j = 0$ , then  $E$  does not have isogenies of degree  $p$  over  $\mathbb{Q}_p$ . If  $j \neq 0$ , then  $t = 2$  or  $4$ . More precisely if  $v_p(\Delta) = 2$  then  $t = 4$ , and if  $v_p(\Delta) = 10$  then  $t = 2$ .

In order to prove Theorem, we must know the formal logarithm  $\log_{\hat{E}}$  of  $\hat{E}$ , since  $[p](x) = \log_{\hat{E}}^{-1} \circ p \circ \log_{\hat{E}}$ . In §2, we obtained the power series expansion of  $\log_{\hat{E}}$  in Proposition 2.2.1. If  $e = 1$ ,  $\log_{\hat{E}}$  is uniquely determined by the theory of Honda formal groups. When  $e > 1$ , we prove that  $\log_{\hat{E}}$  corresponds to a generator of the lifting of the Deudonné module of the  $p$ -divisible group of  $\tilde{E}$  over  $\mathbb{F}_p$  and describe the power series of  $\log_{\hat{E}}$  by using the parameter  $\beta \in \mathcal{O}_L$  which appears in the lifting. In §3, we determine the value of  $v_L(c_p)$  by using the proposition of Volkov [10] under the conditions that  $E$  is defined over  $\mathbb{Q}_p$  and  $\tilde{E}$  is supersingular. In §4, we consider isogenies

of degree  $p$  over  $\mathbb{Q}_p$  and prove Corollary. We give examples of elliptic curves whose values of  $t$  can be determined by Corollary.

**2. Honda formal groups and Dieudonné modules**

Let notations and assumptions be as in §1.

**2.1. The case  $e = 1$ .** For a commutative ring  $R$ , we write  $R[[x]]_0 = \{f \in R[[x]] \mid f \equiv 0 \pmod{x}\}$ . Let  $\Gamma$  be a formal group over  $\mathbb{Z}_p$  and  $\log_\Gamma(x) \in \mathbb{Q}_p[[x]]_0$  the formal logarithm of  $\Gamma/\mathbb{Z}_p$  [7, IV, §5]. It satisfies  $\log_\Gamma(x) = x + \dots$  and  $\log_\Gamma(x) + \log_\Gamma(y) = \log_\Gamma(\Gamma(x, y))$ . For  $\sum a_i x^i \in \mathbb{Q}_p[[x]]$ , define the Frobenius endomorphism  $\varphi$  by

$$(2.1) \quad \varphi\left(\sum a_i x^i\right) = \sum a_i x^{pi}.$$

Assume that  $\log_\Gamma(x)$  is of type  $T^2 + p$ , that is  $(\varphi^2 + p)\log_\Gamma(x) \equiv 0 \pmod{p\mathbb{Z}_p[[x]]_0}$  [5, §2].

**Lemma 2.1.1** (cf. [3, 2.4, Lemma]). *We have*

$$\log_\Gamma(x) = \sum_{k=1, p^2 \nmid k}^\infty \sum_{m=0}^\infty \left\{ (-1)^m \frac{1}{p^m} b_k + \sum_{i=1}^m \frac{1}{p^{m-i}} a_i^{(k)} \right\} x^{kp^{2m}},$$

where  $b_1 = 1$ ,  $b_k \in \mathbb{Z}_p$  and  $a_i^{(k)} \in \mathbb{Z}_p$ . Therefore let  $\log_\Gamma(x) = x + b_2x^2 + \dots + b_px^p + \dots + b_{p^2}x^{p^2} + \dots$ , then

$$\begin{cases} b_i \in \mathbb{Z}_p & \text{for } p^2 \nmid i, \\ v_p(b_{p^{2m}}) = -m & \text{for } m = 1, 2, \dots, \\ v_p(b_{kp^{2m}}) \geq -m & \text{for } m = 1, 2, \dots \text{ and } p^2 \nmid k. \end{cases}$$

*Epecially we can choose  $\Gamma$  over  $\mathbb{Z}_p$  in the strong isomorphism class such that*

$$\log_\Gamma(x) = x - \frac{1}{p}x^{p^2} + \frac{1}{p^2}x^{p^4} + \dots + (-1)^m \frac{1}{p^m}x^{p^{2m}} + \dots.$$

**Proof.** Let  $\log_\Gamma(x) = x + b_2x^2 + \dots + b_px^p + \dots + b_{p^2}x^{p^2} + \dots$ . Then

$$\begin{aligned} & (\varphi^2 + p)\log_\Gamma(x) \\ &= x^{p^2} + b_2x^{2p^2} + \dots + b_px^{p^3} + \dots + b_{p^2}x^{p^4} + \dots \\ & \quad + px + pb_2x^2 + \dots + pb_px^p + \dots + pb_{p^2}x^{p^2} + \dots + pb_{p^4}x^{p^4} + \dots \\ & \equiv 0 \pmod{p\mathbb{Z}_p[[x]]_0}. \end{aligned}$$

Let  $p^2 \nmid k$ , then  $pb_k \equiv 0 \pmod{p\mathbb{Z}_p}$ . So  $b_k \in \mathbb{Z}_p$ . Since  $b_k + pb_{kp^2} \equiv 0 \pmod{p\mathbb{Z}_p}$ ,

$$b_{kp^2} = -\frac{1}{p}b_k + a_1^{(k)}, \quad a_1^{(k)} \in \mathbb{Z}_p.$$

Since  $b_{kp^{2(m-1)}} + pb_{kp^{2m}} \equiv 0 \pmod{p\mathbb{Z}_p}$ ,

$$b_{kp^{2m}} = (-1)^m \frac{1}{p^m}b_k + \sum_{i=1}^m \frac{1}{p^{m-i}}a_i^{(k)}, \quad \text{where } a_i^{(k)} \in \mathbb{Z}_p, \text{ for } m = 2, 3, \dots$$

We choose the  $\Gamma$  over  $\mathbb{Z}_p$  in the strong isomorphism class such that  $(\varphi^2 + p)\log_\Gamma(x) = px$ . Then  $\log_\Gamma(x) = x - (1/p)x^{p^2} + (1/p^2)x^{p^4} + \dots + (-1)^m(1/p^m)x^{p^{2m}} + \dots$ .  $\square$

If  $e = 1$ ,  $E$  has good reduction over  $\mathbb{Q}_p$ . Assume that the reduction  $\tilde{E}/\mathbb{F}_p$  of  $E/\mathbb{Z}_p$  is supersingular. Let  $\hat{E}$  be the formal group over  $\mathbb{Z}_p$  associated to  $E/\mathbb{Z}_p$  and  $\log_{\hat{E}}(x)$  be the formal logarithm of  $\hat{E}/\mathbb{Z}_p$ .

**Proposition 2.1.1.** *For  $e = 1$ , if  $c_p = 0$  or  $v_p(c_p) < 1$ , then  $c_p = 0$ .*

*Proof.* If  $e = 1$ ,  $\log_{\hat{E}}(x)$  is of type  $T^2 + p$  ([4, Theorem 5], [5, Theorem 9]). So let  $\log_{\hat{E}}(x) = x + b_2x^2 + \dots + b_px^p + \dots$ , then  $b_2, \dots, b_p \in \mathbb{Z}_p$ . Hence  $\log_{\hat{E}}^{-1}(x) = x + d_2x^2 + \dots + d_px^p + \dots$ , where  $d_2, \dots, d_p \in \mathbb{Z}_p$  and

$$\begin{aligned} [p](x) &= \log_{\hat{E}}^{-1} \circ p \circ \log_{\hat{E}}(x) \\ &= px + \dots + pb_px^p + \dots \\ &\quad + d_2(px + \dots + pb_px^p + \dots)^2 + \dots \\ &\quad + d_p(px + \dots + pb_px^p + \dots)^p + \dots \\ &= px + \dots + (pb_p + p^2s_2 + \dots + p^{p-1}s_{p-1} + p^pd_p)x^p + \dots, \end{aligned}$$

where  $s_2, \dots, s_{p-1} \in \mathbb{Z}_p$ . So  $v_p(c_p) \geq v_p(p) = 1$ , we have  $c_p = 0$ .  $\square$

Let  $\tilde{E}(p)$  be the  $p$ -divisible group of  $\tilde{E}$  over  $\mathbb{F}_p$  [8, §2] and  $M = \mathbb{M}(\tilde{E}(p)) = \text{Hom}_{\mathbb{D}_{\mathbb{F}_p}}(\tilde{E}(p), \widehat{CW}_{\mathbb{F}_p})$  the Dieudonné module of  $\tilde{E}(p)$  over  $\mathbb{F}_p$  [2, p. 126], where  $\mathbb{D}_{\mathbb{F}_p} = \mathbb{Z}_p[F, V]$ . For a commutative ring  $R$ , let  $\Lambda(R) = R[[x]]$  and  $\Lambda_0(R) = R[[x]]_0$ . By Yoneda's lemma  $M = \text{Hom}_{\mathbb{D}_{\mathbb{F}_p}}(\tilde{E}(p), \widehat{CW}_{\mathbb{F}_p})$  is a  $\mathbb{D}_{\mathbb{F}_p}$ -submodule of  $\widehat{CW}_{\mathbb{F}_p}(\Lambda_0(\mathbb{F}_p))$ , where  $CW$  is the group of Witt covectors [2, p. 74] and  $\widehat{CW}_{\mathbb{F}_p}(A) = CW(A)$  for a

profinite  $\mathbb{F}_p$ -ring  $A$  [2, p. 90, p. 93]. For  $(\dots, a_{-n}, \dots, a_{-1}, a_0) \in \widehat{CW}_{\mathbb{F}_p}(\Lambda_0(\mathbb{F}_p))$ , let

$$F(\dots, a_{-n}, \dots, a_{-1}, a_0) = (\dots, a_{-n}^p, \dots, a_{-1}^p, a_0^p)$$

and

$$V(\dots, a_{-n}, \dots, a_{-1}, a_0) = (\dots, a_{-n-1}, \dots, a_{-2}, a_{-1}).$$

By [2, III, Proposition 6.1] the functor  $\mathbb{M}$  induces an anti-equivalence between the categories of  $p$ -divisible groups over  $\mathbb{F}_p$  and free  $\mathbb{Z}_p$ -modules of finite rank. Let  $\phi: \tilde{E}(p) \rightarrow \tilde{E}(p)$  be the  $p$ -th power Frobenius endomorphism, then  $F = \mathbb{M}(\phi)$ . If  $\tilde{E}$  is supersingular, then  $M$  is a free  $\mathbb{Z}_p$ -module of rank 2 and  $F$  satisfies  $F^2 + p = 0$ . Let  $e_1$  be a generator of the  $\mathbb{Z}_p[F]$ -module  $M$ . Then  $(e_1, e_2)$  is a  $\mathbb{Z}_p$ -base of  $M$  and  $e_2 = Fe_1$  [10, p. 86].

Let  $P(\Lambda_0(\mathbb{Z}_p)) = \{f \in \mathbb{Q}_p[[x]] \mid df/dx \in \mathbb{Z}_p[[x]]\} \cap \mathbb{Q}_p[[x]]_0$ . Define

$$w: \widehat{CW}_{\mathbb{F}_p}(\Lambda_0(\mathbb{F}_p)) \rightarrow P(\Lambda_0(\mathbb{Z}_p))/p\Lambda_0(\mathbb{Z}_p),$$

by

$$(\dots, a_{-n}, \dots, a_{-1}, a_0) \mapsto \sum p^{-n} \hat{a}_{-n}^{p^n}.$$

For  $a = \sum b_i x^i \in \mathbb{F}_p[[x]]$ , let  $\hat{a} = \sum [b_i] x^i$ , where  $[ ]: \mathbb{F}_p \rightarrow \mathbb{Z}_p$  is the multiplicative system of representatives of  $\mathbb{Z}_p = W(\mathbb{F}_p)$ . Then  $\varphi = w \circ F$ . By abuse of language, we denote  $\varphi$  by  $F$ . So  $P(\Lambda_0(\mathbb{Z}_p))$  is  $\mathbb{Z}_p[[F]]$ -module and  $w$  is an isomorphism of  $\mathbb{Z}_p[[F]]$ -modules [2, p. 240]. Let

$$\mathcal{MH}_{\mathbb{Z}_p}(\Gamma) = \{f \in P(\Lambda_0(\mathbb{Z}_p)) \mid f(x) + f(y) - f(\Gamma(x, y)) \in p\mathbb{Z}_p[[x, y]]_0\}$$

and

$$MH_{\mathbb{Z}_p}(\Gamma) = \mathcal{MH}_{\mathbb{Z}_p}(\Gamma)/p\mathbb{Z}_p[[x]]_0.$$

By [2, III, Proposition 6.5],  $w: M \simeq MH_{\mathbb{Z}_p}(\Gamma)$  is an isomorphism of  $\mathbb{Z}_p[[F]]$ -modules. Let

$$\mathcal{LH}_{\mathbb{Z}_p}(\Gamma) = \{f \in P(\Lambda_0(\mathbb{Z}_p)) \mid f(x) + f(y) - f(\Gamma(x, y)) = 0\}$$

and

$$\rho: \mathcal{LH}_{\mathbb{Z}_p}(\Gamma) \xrightarrow{\text{inclusion}} \mathcal{MH}_{\mathbb{Z}_p}(\Gamma) \xrightarrow{\text{mod } p\mathbb{Z}_p[[x]]_0} MH_{\mathbb{Z}_p}(\Gamma) \simeq M.$$

Then  $\mathcal{LH}_{\mathbb{Z}_p}(\Gamma)/p\mathcal{LH}_{\mathbb{Z}_p}(\Gamma) \simeq M/FM$  as  $\mathbb{F}_p$ -vector space by [2, IV, Proposition 1.1]. And  $\mathcal{LH}_{\mathbb{Z}_p}(\Gamma)$  is a free  $\mathbb{Z}_p$ -module of rank 1 generated by  $\log_{\Gamma}(x)$ .

**Lemma 2.1.2.** *For a generator  $e_1$  of  $\mathbb{Z}_p[F]$ -module  $M$ , there exists  $\log_\Gamma(x)$  of type  $T^2 + p$  such that  $w(e_1) = u' \log_\Gamma(x)$ , where  $u' \in \mathbb{Z}_p^\times$ .*

*Proof.* Let  $M = \mathbb{Z}_p e_1 + \mathbb{Z}_p e_2 = \langle e_1, e_2 \rangle$  and  $e_2 = Fe_1$ . Then  $Fe_2 = F^2 e_1 = -pe_1$ . Since  $\mathcal{LH}_{\mathbb{Z}_p}(\Gamma)/p\mathcal{LH}_{\mathbb{Z}_p}(\Gamma) \simeq M/FM$ ,

$$\begin{aligned} \langle \log_\Gamma(x) \rangle / p \langle \log_\Gamma(x) \rangle &\simeq \langle e_1, e_2 \rangle / \langle Fe_1, Fe_2 \rangle \\ &= \langle e_1, e_2 \rangle / \langle e_2, -pe_1 \rangle \\ &\simeq \langle e_1 \rangle / p \langle e_1 \rangle. \end{aligned}$$

Therefore there exist  $u_1 \in \mathbb{Z}_p^\times$  and  $a' \in \mathbb{Z}_p$  such that

$$\begin{aligned} w(e_1) &= u_1 \log_\Gamma(x) + pa' \log_\Gamma(x) \\ &= (u_1 + pa') \log_\Gamma(x). \end{aligned}$$

Putting  $u = u_1 + pa'$ , then  $w(e_1) = u' \log_\Gamma(x)$ , where  $u' \in \mathbb{Z}_p^\times$ . □

**2.2. The case  $e > 1$ .** By [10, 4.1.3], if  $e < p - 1$ , we consider liftings over  $\mathcal{O}_L$  of  $M$ , that is  $\mathcal{O}_L$ -submodules  $\mathcal{L}$  of rank 1 of  $\mathcal{M} = \mathcal{O}_L \otimes_{\mathbb{Z}_p} M + p^{-1}\pi \mathcal{O}_L \otimes_{\mathbb{Z}_p} FM$  such that

$$\mathcal{L}/\pi\mathcal{L} \simeq \mathcal{M}/p^{-1}\pi \otimes_{\mathbb{Z}_p} FM.$$

Because  $M = \mathbb{Z}_p e_1 + \mathbb{Z}_p e_2$ ,  $Fe_1 = e_2$  and  $Fe_2 = -pe_1$ ,  $\mathcal{O}_L$ -module  $\mathcal{M}$  is written by

$$\mathcal{M} = \langle 1 \otimes e_1, 1 \otimes e_2, p^{-1}\pi \otimes e_2, \pi \otimes e_1 \rangle = \langle 1 \otimes e_1, p^{-1}\pi \otimes e_2 \rangle.$$

By [10, 4.2], liftings over  $\mathcal{O}_L$  of  $M$  correspond bijectively to

$$\mathcal{L}(\beta) = (1 \otimes e_1 + \beta p^{-1}\pi \otimes e_2)\mathcal{O}_L, \quad \beta \in \mathcal{O}_L.$$

Indeed, we define  $\psi: \mathcal{L} \rightarrow \mathcal{M}/p^{-1}\pi \otimes FM$  by

$$1 \otimes e_1 + \beta p^{-1}\pi \otimes e_2 \mapsto 1 \otimes e_1 + \beta p^{-1}\pi \otimes e_2 \pmod{p^{-1}\pi \otimes FM}.$$

Then  $\psi$  is surjective because

$$\begin{aligned} &\langle 1 \otimes e_1 + \beta p^{-1}\pi \otimes e_2 \rangle + p^{-1}\pi \otimes FM \\ &= \langle 1 \otimes e_1 + \beta p^{-1}\pi \otimes e_2, p^{-1}\pi \otimes e_2, \pi \otimes e_1 \rangle \\ &= \langle 1 \otimes e_1, p^{-1}\pi \otimes e_2 \rangle \\ &= \mathcal{M}. \end{aligned}$$

Let  $\alpha \in \mathcal{O}_L$  such that  $\alpha(1 \otimes e_1 + \beta p^{-1}\pi \otimes e_2) \in \langle p^{-1}\pi \otimes e_2, \pi \otimes e_1 \rangle$ , then  $\alpha \in \pi \mathcal{O}_L$ . So  $\mathcal{L}/\pi \mathcal{L} \simeq \mathcal{M}/p^{-1}\pi \otimes_{\mathbb{Z}_p} FM$ .

For  $\mathcal{O}_L$  and  $\mathbb{D}_{\mathbb{F}_p}$ -module  $\mathfrak{M}$ , we define  $\mathfrak{M}_{\mathcal{O}_L}$  as in [2, p.190]. For  $j \in \mathbb{Z}$ ,  $\mathfrak{M}^{(j)}$  is a  $\mathbb{D}_{\mathbb{F}_p}$ -submodule of  $\mathfrak{M}$  defined in [2, p.188] and  $v: \mathfrak{M}^{(j)} \rightarrow \mathfrak{M}^{(j+1)}$  (resp.  $f: \mathfrak{M}^{(j)} \rightarrow \mathfrak{M}^{(j-1)}$ ) is defined by  $v(a) = Va$  (resp.  $f(a) = Fa$ ). If  $f$  is injective  $f^j: \mathfrak{M}^{(j)} \simeq F^j \mathfrak{M}$ . If  $1 < e \leq p - 1$ ,  $\mathfrak{M}_{\mathcal{O}_L}$  is defined by the inductive limit of the following diagram,

$$\begin{array}{ccc} \pi \mathcal{O}_L \otimes \mathfrak{M} & \xrightarrow{v_0} & p^{-1}\pi \mathcal{O}_L \otimes \mathfrak{M}^{(1)} \\ \varphi_0 \downarrow & & \uparrow \varphi'_0 \\ \mathcal{O}_L \otimes \mathfrak{M} & \xleftarrow{f_0} & \mathcal{O}_L \otimes \mathfrak{M}^{(1)} \end{array}$$

where  $\varphi_0(\lambda \otimes a) = \lambda \otimes a$ ,  $f_0(\lambda \otimes a) = \lambda \otimes f(a)$ ,  $\varphi'_0(\lambda \otimes a) = \lambda \otimes a$ ,  $v_0(\lambda \otimes a) = p^{-1}\lambda \otimes v(a)$ . Then  $\mathfrak{M}_{\mathcal{O}_L}$  is written by

$$\mathcal{O}_L \otimes \mathfrak{M} \oplus p^{-1}\pi \mathcal{O}_L \otimes \mathfrak{M}^{(1)} / \langle \text{Im } \varphi_0, \text{Im } f_0, \text{Im } \varphi'_0, \text{Im } v_0 \rangle,$$

where  $\text{Im } \varphi_0 = \pi \mathcal{O}_L \otimes \mathfrak{M}$ ,  $\text{Im } f_0 = \mathcal{O}_L \otimes f(\mathfrak{M}^{(1)}) = \mathcal{O}_L \otimes F\mathfrak{M}$ ,  $\text{Im } \varphi'_0 = \mathcal{O}_L \otimes \mathfrak{M}^{(1)}$  and  $\text{Im } v_0 = p^{-1}\pi \mathcal{O}_L \otimes v(\mathfrak{M})$ . If  $f$  is injective,  $f: \text{Im } \varphi'_0 = \mathcal{O}_L \otimes \mathfrak{M}^{(1)} \simeq \mathcal{O}_L \otimes F\mathfrak{M}$  and  $f: \text{Im } v_0 = p^{-1}\pi \mathcal{O}_L \otimes v(\mathfrak{M}) \simeq p^{-1}\pi \mathcal{O}_L \otimes FV\mathfrak{M} = p^{-1}\pi \mathcal{O}_L \otimes p\mathfrak{M} = \pi \mathcal{O}_L \otimes \mathfrak{M}$ . Therefore if  $f$  is injective,

$$\mathfrak{M}_{\mathcal{O}_L} \simeq \mathcal{O}_L \otimes \mathfrak{M} \oplus p^{-1}\pi \mathcal{O}_L \otimes F\mathfrak{M} / \langle \pi \mathcal{O}_L \otimes \mathfrak{M}, \mathcal{O}_L \otimes F\mathfrak{M} \rangle.$$

Denote the above isomorphism by  $f'$ .

Let  $N = CW(\mathbb{F}_p[[x]])$ . When  $\mathfrak{M} = N$ ,  $f$  is injective and  $v$  is surjective [2, p.199, p.202].

**Lemma 2.2.1.**  $f': N_{\mathcal{O}_L} \simeq \mathcal{O}_L \otimes N + p^{-1}\pi \mathcal{O}_L \otimes FN$ .

*Proof.* We must show  $\mathcal{O}_L \otimes N \cap p^{-1}\pi \mathcal{O}_L \otimes FN = \langle \pi \mathcal{O}_L \otimes N, \mathcal{O}_L \otimes FN \rangle$ . Since  $VN = N$ ,  $p^{-1}\pi \mathcal{O}_L \otimes FN = \pi \mathcal{O}_L \otimes p^{-1}FN = \pi \mathcal{O}_L \otimes V^{-1}N = \pi \mathcal{O}_L \otimes N$ . So  $\mathcal{O}_L \otimes N \cap p^{-1}\pi \mathcal{O}_L \otimes FN = \pi \mathcal{O}_L \otimes N \subset \langle \pi \mathcal{O}_L \otimes N, \mathcal{O}_L \otimes FN \rangle$ . Since  $F$  is injective,  $\mathcal{O}_L \otimes FN \subset \mathcal{O}_L \otimes N$ . So  $\langle \pi \mathcal{O}_L \otimes N, \mathcal{O}_L \otimes FN \rangle \subset \mathcal{O}_L \otimes N \cap p^{-1}\pi \mathcal{O}_L \otimes FN$ .  $\square$

Let  $P(\Lambda_0(\mathcal{O}_L)) = \{f \in L[[x]] \mid df/dx \in \mathcal{O}_L[[x]]\} \cap L[[x]]_0$ . Since  $VN = N$ ,  $w'': N_{\mathcal{O}_L} \rightarrow P(\Lambda_0(\mathcal{O}_L))/\pi \mathcal{O}_L[[x]]_0$  is defined and an  $\mathcal{O}_L$ -isomorphism by [2, IV, Proposition 3.2]. Define  $\varphi_1: p^{-1}\pi \mathcal{O}_L \otimes N \rightarrow \mathcal{O}_L \otimes N$  by  $p^{-1}\lambda \otimes a \mapsto \lambda \otimes c$ , where  $c \in N \text{ mod } \ker V$  such that  $v(c) = a$ . So  $\varphi: p^{-1}\pi \mathcal{O}_L \otimes FN \rightarrow \mathcal{O}_L \otimes N$  is defined by  $p^{-1}\lambda \otimes f(a) \mapsto \lambda \otimes c$ , where  $pc = f \circ v(c) = f(a)$ . Let  $w' = w'' \circ (f')^{-1}$ . Then  $w': \mathcal{O}_L \otimes N + p^{-1}\pi \mathcal{O}_L \otimes FN \rightarrow P(\Lambda_0(\mathcal{O}_L))/\pi \mathcal{O}_L[[x]]_0$  is written by  $w' = 1 \otimes w + (1 \otimes w) \circ \varphi$  [2, p.199].



**Lemma 2.2.2.** For  $1 \otimes e_1 + \beta p^{-1}\pi \otimes e_2 \in \mathcal{O}_L \otimes N + p^{-1}\pi\mathcal{O}_L \otimes FN$ ,

$$w'(1 \otimes e_1 + \beta p^{-1}\pi \otimes e_2) = 1 \otimes w(e_1) + \beta\pi \otimes p^{-1}Fw(e_1).$$

Proof. For  $e_1 \in N$ , there exists  $c \in N \bmod \ker V$  such that  $v(c) = e_1$ , so  $pc = f(e_1)$ . Since  $w$  is an isomorphism of  $\mathbb{Z}_p[F, V]$ -modules,  $pw(c) = f \circ v \circ w(c) = f \circ w(e_1)$ . So  $w(c) = p^{-1}f \circ w(e_1)$ . Hence

$$\begin{aligned} &w'(1 \otimes e_1 + \beta p^{-1}\pi \otimes Fe_1) \\ &= (1 \otimes w)(1 \otimes e_1) + (1 \otimes w) \circ \varphi(p^{-1}\beta\pi \otimes Fe_1) \\ &= (1 \otimes w)(1 \otimes e_1) + (1 \otimes w)(\beta\pi \otimes c) \\ &= 1 \otimes w(e_1) + \beta\pi \otimes w(c) \\ &= 1 \otimes w(e_1) + \beta\pi \otimes p^{-1}Fw(e_1). \end{aligned} \quad \square$$

When  $\mathfrak{M} = M$ ,  $f$  is injective. We put  $M_0 = \mathcal{O}_L \otimes M$ ,  $M'_0 = \pi\mathcal{O}_L \otimes M$ ,  $M''_1 = \mathcal{O}_L \otimes FM$  and  $M_1 = p^{-1}\pi\mathcal{O}_L \otimes FM$ . Then  $f': M_{\mathcal{O}_L} \simeq M_0 \oplus M_1 / \langle M'_0, M''_1 \rangle$ .

**Lemma 2.2.3.**  $M_{\mathcal{O}_L} \simeq \mathcal{M}$ .

Proof. Since  $M_0 \oplus M_1 / M_0 \cap M_1 = M_0 + M_1 = \mathcal{M}$ , we must show  $M_0 \cap M_1 = \langle M'_0, M''_1 \rangle$ . Because

$$\begin{aligned} M_0 \cap M_1 &= \mathcal{O}_L \otimes M \cap p^{-1}\pi\mathcal{O}_L \otimes FM \\ &= \langle 1 \otimes e_1, 1 \otimes e_2 \rangle \cap \langle p^{-1}\pi \otimes e_2, \pi \otimes e_1 \rangle \\ &= \langle \pi \otimes e_1, 1 \otimes e_2 \rangle \end{aligned}$$

and

$$\begin{aligned} \langle M'_0, M''_1 \rangle &= \langle \pi\mathcal{O}_L \otimes M, \mathcal{O}_L \otimes FM \rangle \\ &= \langle \pi \otimes e_1, \pi \otimes e_2, 1 \otimes e_2, p \otimes e_1 \rangle \\ &= \langle \pi \otimes e_1, 1 \otimes e_2 \rangle, \end{aligned}$$

$$M_0 \cap M_1 = \langle M'_0, M''_1 \rangle. \quad \square$$

For the formal group  $\hat{E}$  over  $\mathcal{O}_L$ , we define

$$\mathcal{MH}_{\mathcal{O}_L}(\hat{E}) = \{f \in P(\Lambda_0(\mathcal{O}_L)) \mid f(x) + f(y) - f(\hat{E}(x, y)) \in \pi\mathcal{O}_L[[x, y]]_0\}$$

and

$$MH_{\mathcal{O}_L}(\hat{E}) = \mathcal{MH}_{\mathcal{O}_L}(\hat{E})/\pi\mathcal{O}_L[[x]]_0.$$

By [2, IV, Proposition 4.1], the  $\mathcal{O}_L$ -isomorphism  $w'' : N_{\mathcal{O}_L} \rightarrow P(\Lambda_0(\mathcal{O}_L)/\pi\mathcal{O}_L[[x]])_0$  induces the  $\mathcal{O}_L$ -isomorphism  $w'' : M_{\mathcal{O}_L} \simeq MH_{\mathcal{O}_L}(\hat{E})$ . We define

$$\mathcal{LH}_{\mathcal{O}_L}(\hat{E}) = \{f \in P(\Lambda_0(\mathcal{O}_L)) \mid f(x) + f(y) - f(\hat{E}(x, y)) = 0\}$$

and

$$\rho' : \mathcal{LH}_{\mathcal{O}_L}(\hat{E}) \xrightarrow{\text{inclusion}} \mathcal{MH}_{\mathcal{O}_L}(\hat{E}) \xrightarrow{\text{mod } \pi\mathcal{O}_L[[x]]_0} MH_{\mathcal{O}_L}(\hat{E}) \simeq M_{\mathcal{O}_L} \simeq \mathcal{M}.$$

Then  $\mathcal{LH}_{\mathcal{O}_L}(\hat{E})/\pi\mathcal{LH}_{\mathcal{O}_L}(\hat{E}) \simeq M_{\mathcal{O}_L}/p^{-1}\pi \otimes FM$  as  $\mathbb{F}_p$ -vector space by [2, IV, Proposition 4.2].

**Lemma 2.2.4.** *Let  $\mathcal{L} = \rho'(\mathcal{LH}_{\mathcal{O}_L}(\hat{E}))$  and  $l = 1 \otimes e_1 + \beta p^{-1}\pi \otimes e_2$  be a generator of  $\mathcal{L} = \mathcal{L}(\beta)$ , then  $\log_{\hat{E}}(x) = uw'(l)$ , where  $u \in \mathcal{O}_L^\times$ .*

Proof.  $\mathcal{LH}_{\mathcal{O}_L}(\hat{E})/\pi\mathcal{LH}_{\mathcal{O}_L}(\hat{E}) \simeq \mathcal{M}/p^{-1}\pi \otimes FM \simeq \mathcal{L}/\pi\mathcal{L}$  as  $\mathbb{F}_p$ -vector space. So  $\log_{\hat{E}}(x) = u_2w'(l) + \pi a''w'(l)$ , where  $u_2 \in \mathcal{O}_L^\times$  and  $a'' \in \mathcal{O}_L$ . Put  $u = u_2 + \pi a''$ ,  $\log_{\hat{E}}(x) = uw'(l)$ . □

**Lemma 2.2.5.** *If  $v_L(c_p) < e$ , then the value of  $v_L(c_p)$  does not depend on the choice of a minimal model  $E/\mathcal{O}_L$ .*

Proof. Put  $R = \mathcal{O}_L/(\pi^e)$ . Then we have an isogeny  $\overline{[p]}(x) = [p](x) \text{ mod } (\pi^e) = \bar{p}x + \dots + \bar{c}_p x^p + \dots$  over  $R$ . Since  $R$  is a ring of characteristic  $p$ , there exists an integer  $h$  such that  $\overline{[p]}(x)$  is a power series of  $x^{p^h}$  [6, Lemma 2.1.1, Lemma 2.1.2]. If  $v_L(c_p) < e$ , then  $h$  must be 1. So  $\overline{[p]}(x) = \bar{c}_p x^p + \dots$ . Hence we have  $v_L(c_j) > v_L(c_p)$  for  $j = 2, \dots, p-1$ . Let  $E_1/\mathcal{O}_L$  be the other minimal model of  $E$  over  $\mathcal{O}_L$  and  $\hat{E}_1$  be a formal group over  $\mathcal{O}_L$  associated to  $E_1/\mathcal{O}_L$ . Then there exists an isomorphism  $\psi : \hat{E} \rightarrow \hat{E}_1$  written by  $\psi(x) = x(b_0 + b_1x + \dots)$ , where  $b_0 \in \mathcal{O}_L^\times$  and  $b_1, b_2, \dots \in \mathcal{O}_L$ . Put  $x' = \psi(x)$  then  $\psi^{-1}$  is written by  $\psi^{-1}(x') = x'(b'_0 + b'_1x' + \dots)$ , where  $b'_0 \in \mathcal{O}_L^\times$  and  $b'_1, b'_2, \dots \in \mathcal{O}_L$ . Hence the coefficient of  $x'^p$  of  $[p](x') = \psi([p](\psi^{-1}(x')))$  is  $c_p b_0'^p b_0 + \text{higher valuation terms}$ . So its valuation is equal to  $v_L(c_p)$ . □

**Proposition 2.2.1.** *We have*

$$\log_{\hat{E}}(x) = x + b_2x^2 + \dots + b_{p-1}x^{p-1} + \left(b_p + \frac{\beta\pi}{p}\right)x^p + \dots$$

and

$$[p](x) = px + \dots + (\beta\pi + pa)x^p + \dots, \quad a \in \mathcal{O}_L.$$

Therefore the value  $v_L(c_p)$  does not depend on the choice of a generator  $e_1$  of  $\mathbb{Z}_p[F]$ -module  $M$  and  $v_L(c_p) = v_L(\beta\pi)$ .

**Proof.** By Lemma 2.2.4,  $\log_{\hat{E}}(x) = uw'(1 \otimes e_1 + \beta p^{-1}\pi \otimes e_2)$ . Let  $\log_{\Gamma}(x) = x + \sum_{i=2}^{\infty} b_i x^i$ . Then by Lemma 2.2.2 and Lemma 2.1.2,

$$\begin{aligned} \log_{\hat{E}}(x) &= uw'(1 \otimes e_1 + \beta p^{-1}\pi \otimes e_2) \\ &= u\{1 \otimes w(e_1) + \beta\pi \otimes p^{-1}Fw(e_1)\} \\ &= u\{1 \otimes u' \log_{\Gamma}(x) + \beta\pi \otimes p^{-1}Fu' \log_{\Gamma}(x)\} \\ &= uu' \left\{ 1 \otimes \left( x + \sum_{i=2}^{\infty} b_i x^i \right) + \beta\pi \otimes p^{-1} \left( x^p + \sum_{i=2}^{\infty} b_i x^{pi} \right) \right\}. \end{aligned}$$

By the definition of  $\log_{\hat{E}}(x)$ ,  $uu' = 1$ . So

$$\log_{\hat{E}}(x) = x + \cdots + b_{p-1}x^{p-1} + \left( b_p + \frac{\beta\pi}{p} \right) x^p + \cdots.$$

Let  $\log_{\hat{E}}^{-1}(x) = x + d_2x^2 + \cdots + d_{p-1}x^{p-1} + d_px^p + \cdots$ . Then  $x = \log_{\hat{E}}^{-1} \circ \log_{\hat{E}}(x) = x + (b_2 + d_2)x^2 + \cdots + (b_p + \beta\pi/p + \cdots + d_p)x^p + \cdots$ . Since  $b_k \in \mathbb{Z}_p$  for  $p^2 \nmid k$ ,  $d_2, \dots, d_{p-1} \in \mathbb{Z}_p$  and  $d_p = -\beta\pi/p + d_p'$ , where  $d_p' \in \mathbb{Z}_p$ . Hence

$$\begin{aligned} [p](x) &= \log_{\hat{E}}^{-1} \circ p \circ \log_{\hat{E}}(x) \\ &= px + \cdots + pb_{p-1}x^{p-1} + (pb_p + \beta\pi)x^p + \cdots \\ &\quad + d_2\{px + \cdots + pb_{p-1}x^{p-1} + (pb_p + \beta\pi)x^p + \cdots\}^2 + \cdots \\ &\quad + d_p\{px + \cdots + pb_{p-1}x^{p-1} + (pb_p + \beta\pi)x^p + \cdots\}^p + \cdots \\ &= px + \cdots \\ &\quad + \left\{ (pb_p + \beta\pi) + p^2s_2 + \cdots + p^{p-1}s_{p-1} + p^p \left( -\frac{\beta\pi}{p} + d_p' \right) \right\} x^p + \cdots, \end{aligned}$$

where  $s_2, \dots, s_{p-1} \in \mathbb{Z}_p$ . So  $c_p = \beta\pi + pa$ , where  $a \in \mathcal{O}_L$ . Since  $v_L(c_p) < e$ , we have  $v_L(c_p) = v_L(\beta\pi)$ .  $\square$

### 3. Proof of Theorem

Let notations and assumptions be as in §1 and §2.

Let  $K_e$  be the Galois closure of  $L$  in  $\bar{\mathbb{Q}}_p$ . Since the order of  $(\mathbb{Z}/e\mathbb{Z})^\times$  is 1 or 2,  $p \equiv 1 \pmod{e}$  or  $p \equiv -1 \pmod{e}$ . Let  $\zeta_e$  be a primitive  $e$ -th root of 1. So the cases of  $K_e$  are as follows. If  $e = 1$ ,  $K_1 = \mathbb{Q}_p$ . If  $e = 2$ ,  $K_2 = \mathbb{Q}_p(\pi)$  and  $\text{Gal}(K_2/\mathbb{Q}_p) = \langle \tau \rangle$  ( $\tau\pi = -\pi$ ). If  $e = 3, 4, 6$  and  $e \mid p-1$ ,  $K_e = \mathbb{Q}_p(\pi)$  and  $\text{Gal}(K_e/\mathbb{Q}_p) = \langle \tau \rangle$  ( $\tau\pi = \zeta_e\pi$ ). If  $e = 3, 4, 6$  and  $e \mid p+1$ ,  $K_e = \mathbb{Q}_{p^2}(\pi) = \mathbb{Q}_{p^2}(\pi, \zeta_e)$  and  $\text{Gal}(K_e/\mathbb{Q}_p) = \langle \tau \rangle \rtimes \langle \omega \rangle$  ( $\tau\pi = \zeta_e\pi$ ,  $\tau\zeta_e = \zeta_e$ ,  $\omega\pi = \pi$ ,  $\omega\zeta_e = \zeta_e^{-1}$ ) [10, p. 74].

Let  $e \in \{3, 4, 6\}$  and  $e \mid p+1$ . For  $[\zeta_e] \in \text{Aut}_{\mathbb{F}_{p^2}}(\bar{E})$ , put  $\xi_e = \mathbb{M}_{\mathbb{F}_{p^2}}([\zeta_e](p))$ . Then we can take the basis  $(e_1, e_2)$  of  $M \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}$  such that  $\xi_e e_1 = \zeta_e^e e_1$  and  $\xi_e e_2 = \zeta_e^{-e} e_2$ ,

( $\varepsilon \in \{\pm 1\}$ ) [10, p. 87]. Moreover using the condition  $E$  is defined over  $\mathbb{Q}_p$ ,  $\tau$  acts on  $M \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}$  rising from  $\langle \tau \rangle \hookrightarrow \text{Aut}_{\mathbb{F}_{p^2}}(\tilde{E})$  and the action is preserved on  $\mathcal{L}(\beta) \otimes_{\mathcal{O}_L} \mathcal{O}_{K_e}$ . Then  $\tau e_1 = \xi_e e_1 = \zeta_e^\varepsilon e_1$  and  $\tau e_2 = \xi_e e_2 = \zeta_e^{-\varepsilon} e_2$ , ( $\varepsilon \in \{\pm 1\}$ ) [10, p. 94].

**Proposition 3.1.1** ([10, Proof of Proposition 4.8]). *Let  $\beta$  be as in Lemma 2.2.4 and  $e \in \{3, 4, 6\}$  such that  $e \mid p + 1$  and  $e < p - 1$ . Assume that  $\tilde{E}$  is supersingular. Let  $j$ -invariant of  $\tilde{E}$  be 0 (for  $e = 3, 6$ ) and 1728 (for  $e = 4$ ). We choose a generator  $e_1$  of  $\mathbb{Z}_p[F]$ -module  $M$  and  $e_2 = F(e_1)$  such that  $\xi_e e_1 = \zeta_e^\varepsilon e_1$  and  $\xi_e e_2 = \zeta_e^{-\varepsilon} e_2$ , where  $\varepsilon \in \{\pm 1\}$ . Then*

- 1) *The  $j$ -invariant of  $E$  is 0 if and only if  $\beta = 0$  for  $e = 3, 6$ . The  $j$ -invariant of  $E$  is 1728 if and only if  $\beta = 0$  for  $e = 4$ .*
- 2)  *$E$  is defined over  $\mathbb{Q}_p$  if and only if*

$$\begin{cases} \beta \in \pi \mathbb{Z}_p & \text{for } \varepsilon = 1, \\ \beta \in \pi^{e-3} \mathbb{Z}_p & \text{for } \varepsilon = -1. \end{cases}$$

By the Tate algorithm [9], if  $e = 3$  or  $6$  then  $j(\tilde{E}) = 0$  and if  $e = 4$  then  $j(\tilde{E}) = 1728$ .

**Lemma 3.1.1.** *If  $\tilde{E}$  is supersingular,  $e \mid p + 1$ .*

Proof. By [7, III, Theorem 10.1], if  $e = 3, 6$  (resp.  $e = 4$ ),  $\text{Aut } \tilde{E} \simeq \mu_6$  (resp.  $\text{Aut } \tilde{E} \simeq \mu_4$ ). So  $\text{Aut } \tilde{E} \ni \zeta_e$ . In order to prove  $e \mid p + 1$ , we must show that  $\text{Aut } \tilde{E}$  is not defined over  $\mathbb{F}_p$  but over  $\mathbb{F}_{p^2}$  if  $\tilde{E}$  is supersingular.

We write  $\tilde{E}$  by the equation  $y^2 = x^3 + Ax + B$ ,  $A, B \in \mathbb{F}_p$  and the automorphism by the form  $(x', y') \mapsto (u^2 x', u^3 y') = (x, y)$ , where  $u \in \bar{\mathbb{F}}_p$ .

- 1) The case  $j = 0$

In this case,  $\tilde{E}: y^2 = x^3 + B$  and  $u^6 \in \mathbb{F}_p^\times$ . By [7, V, Example 4.4],

$$\begin{aligned} E_1 \text{ is supersingular} \\ \iff \text{the coefficient of } x^{p-1} \text{ in } (x^3 + B)^{(p-1)/2} \text{ is } 0 \\ \iff p \equiv 2 \pmod{3}. \end{aligned}$$

If  $p \equiv 2 \pmod{3}$ , then  $(\mathbb{F}_p^\times)^3 = \mathbb{F}_p^\times$ . So  $u^2 \in \mathbb{F}_p^\times$ . Hence  $u \in \mathbb{F}_{p^2}$ . Since  $6 \nmid p - 1$ ,  $u$  is not contained in  $\mathbb{F}_p$ .

- 2) The case  $j = 1728$

In this case,  $\tilde{E}: y^2 = x^3 + Ax$  and  $u^4 \in \mathbb{F}_p$ . By [7, V, Example 4.5],

$$\begin{aligned} \tilde{E} \text{ is supersingular} \\ \iff \text{the coefficient of } x^{p-1} \text{ in } (x^3 + Ax)^{(p-1)/2} \text{ is } 0 \\ \iff p \equiv 3 \pmod{4}. \end{aligned}$$

Since  $\#(\mathbb{F}_{p^2}^\times) = p^2 - 1 = (p-1)(p+1)$ ,  $u^4 = c^{p+1}$ , where  $c \in \mathbb{F}_{p^2}$ . So  $u = c^{(p+1)/4} \in \mathbb{F}_{p^2}$ . Since  $4 \nmid p-1$ ,  $u$  is not contained in  $\mathbb{F}_p$ . □

**Lemma 3.1.2.** *If  $e = 3$  and  $v_p(\Delta) = 4$ , then  $\tau(e_1) = \zeta_e e_1$ .*

*If  $e = 3$  and  $v_p(\Delta) = 8$ , then  $\tau(e_1) = \zeta_e^{-1} e_1$ .*

*If  $e = 4$  and  $v_p(\Delta) = 3$ , then  $\tau(e_1) = \zeta_e e_1$ .*

*If  $e = 4$  and  $v_p(\Delta) = 9$ , then  $\tau(e_1) = \zeta_e^{-1} e_1$ .*

*If  $e = 6$  and  $v_p(\Delta) = 2$ , then  $\tau(e_1) = \zeta_e e_1$ .*

*If  $e = 6$  and  $v_p(\Delta) = 10$ , then  $\tau(e_1) = \zeta_e^{-1} e_1$ .*

Proof. For a generator  $e_1$  of  $\mathbb{Z}_p[F]$ -module  $M$ , put  $e_2 = F(e_1)$ . Then there exists  $\log_\Gamma(x)$  of type  $T^2 + p$  such that  $w(e_1) = u' \log_\Gamma(x)$ , where  $u' \in \mathbb{Z}_p^\times$  by Lemma 2.1.2. By Lemma 2.1.1, we can choose  $\Gamma$  such that

$$\log_\Gamma(x) = x - \frac{1}{p}x^{p^2} + \frac{1}{p^2}x^{p^4} + \dots$$

We regard  $(e_1, e_2)$  as the basis of  $M \otimes \mathbb{Z}_{p^2} = \mathbb{M}_{\mathbb{F}_{p^2}}(\tilde{E}(p)) = \text{Hom}_{\mathbb{D}_{\mathbb{F}_{p^2}}}(\tilde{E}(p), \widehat{C\tilde{W}}_{\mathbb{F}_{p^2}})$ , where  $\mathbb{D}_{\mathbb{F}_{p^2}} = \mathbb{Z}_{p^2}[F, V]$ . And as in §2, let

$$w: \widehat{C\tilde{W}}_{\mathbb{F}_{p^2}}(\Lambda_0(\mathbb{F}_{p^2})) \rightarrow P(\Lambda_0(\mathbb{Z}_{p^2}))/p\Lambda_0(\mathbb{Z}_{p^2}).$$

Then  $w$  is  $\mathbb{Z}_{p^2}[F]$ -isomorphism. Moreover we regard  $e_1$  as the element of  $\mathcal{L}(\beta) \otimes \mathcal{O}_{K_e}$ . For the parameter  $x$ , let  $(w \circ \xi_\varepsilon)(x) = \zeta_e^\varepsilon x$ , ( $\varepsilon \in \{\pm 1\}$ ). Then

$$\begin{aligned} w(\xi_\varepsilon(e_1)) &= u' \left( \zeta_e^\varepsilon x - \frac{1}{p}(\zeta_e^\varepsilon x)^{p^2} + \frac{1}{p^2}(\zeta_e^\varepsilon x)^{p^4} + \dots \right) \\ &= u' \left( \zeta_e^\varepsilon x - \frac{1}{p}\zeta_e^\varepsilon x^{p^2} + \frac{1}{p^2}\zeta_e^\varepsilon x^{p^4} + \dots \right) \end{aligned}$$

which by  $(\zeta_e^\varepsilon)^{p^2} = \zeta_e^\varepsilon$ , since  $\zeta_e^{p+1} = 1$

$$= \zeta_e^\varepsilon e_1.$$

Since  $F(x) = x^p$ ,

$$\begin{aligned} w(\xi_\varepsilon(e_2)) &= w(\xi_\varepsilon(F(e_1))) \\ &= u' \left( (\zeta_e^\varepsilon x)^p - \frac{1}{p}(\zeta_e^\varepsilon x)^{p^3} + \frac{1}{p^2}(\zeta_e^\varepsilon x)^{p^5} + \dots \right) \\ &= u' \left( \zeta_e^{-\varepsilon} x^p - \frac{1}{p}\zeta_e^{-\varepsilon} x^{p^3} + \frac{1}{p^2}\zeta_e^{-\varepsilon} x^{p^5} + \dots \right) \end{aligned}$$

which by  $(\zeta_e^\varepsilon)^p = \zeta_e^{-\varepsilon}$ , since  $\zeta_e^{p+1} = 1$

$$= \zeta_e^{-\varepsilon} e_2.$$

Hence  $e_1$  satisfies the condition of Proposition 3.1.1.

Let  $\hat{E}/\mathbb{Z}_p$  be a formal group over  $\mathbb{Z}_p$  associated to  $E/\mathbb{Z}_p$ . Let  $z$  be a parameter of  $\hat{E}/\mathbb{Z}_p$  such that  $x = uz$ , where  $u \in \mathcal{O}_L$ . If  $e = 3$  and  $v_p(\Delta) = 4$ , then we can take  $u = \pi$ . So

$$w(e_1) = u' \left( \pi z - \frac{1}{p}(\pi z)^{p^2} + \frac{1}{p^2}(\pi z)^{p^4} + \dots \right).$$

Then

$$\begin{aligned} \tau(w(e_1)) &= u' \left( \tau(\pi z) - \frac{1}{p}\tau((\pi z)^{p^2}) + \frac{1}{p^2}\tau((\pi z)^{p^4}) + \dots \right) \\ &= u' \left( \zeta_e \pi z - \frac{1}{p}(\zeta_e \pi z)^{p^2} + \frac{1}{p^2}(\zeta_e \pi z)^{p^4} + \dots \right) \\ &= u' \left( \zeta_e \pi z - \frac{1}{p}\zeta_e(\pi z)^{p^2} + \frac{1}{p^2}\zeta_e(\pi z)^{p^4} + \dots \right) \\ &= \zeta_e w(e_1). \end{aligned}$$

If  $e = 3$  and  $v_p(\Delta) = 8$ , then we can take  $u = \pi^2$ . So  $\tau(w(e_1)) = \zeta_e^{-1}w(e_1)$ .

If  $e = 4$  and  $v_p(\Delta) = 3$ , then we can take  $u = \pi$ . So  $\tau(w(e_1)) = \zeta_e w(e_1)$ .

If  $e = 4$  and  $v_p(\Delta) = 9$ , then we can take  $u = \pi^3$ . So  $\tau(w(e_1)) = \zeta_e^{-1}w(e_1)$ .

If  $e = 6$  and  $v_p(\Delta) = 2$ , then we can take  $u = \pi$ . So  $\tau(w(e_1)) = \zeta_e w(e_1)$ .

If  $e = 6$  and  $v_p(\Delta) = 10$ , then we can take  $u = \pi^5$ . So  $\tau(w(e_1)) = \zeta_e^{-1}w(e_1)$ .  $\square$

**Proof of Theorem.** The case  $e \in \{3, 4, 6\}$ . Except for the case  $e = 6, p = 5$ , the condition  $e < p - 1$  is hold. Assume  $v_p(j) \geq 0$  and  $\tilde{E}$  is supersingular. The assumptions about  $j$ -invariant are hold and  $e \mid p + 1$  is hold by Lemma 3.1.1. By Proof of Proposition 2.2.1,  $c_p = pb_p + \beta\pi + p^2s_2 + \dots + p^{p-1}s_{p-1} + p^p(-\beta\pi/p + d_p')$ , where  $b_p, s_2, \dots, s_{p-1}, d_p' \in \mathbb{Z}_p$ . If  $\beta = 0$ , then  $c_p \in p\mathbb{Z}_p$ . Since  $v_L(c_p) < e$ , it must be  $c_p = 0$ . Conversely if  $c_p = 0$ , then  $(1 - p^{p-1})\beta\pi \in p\mathbb{Z}_p$ . So  $\beta\pi/p \in \mathbb{Z}_p$ . Then  $\log_{\hat{E}}(x) \in \mathbb{Q}_p[[x]]$  by Proof of Proposition 2.2.1. Since  $\tilde{E}$  is supersingular,  $\hat{E}$  is strongly isomorphic to  $\Gamma$ . Therefore  $\beta = 0$ . Hence for  $e = 3, 6, c_p = 0$  if and only if  $j = 0$  and for  $e = 4, c_p = 0$  if and only if  $j = 1728$  by Proposition 3.1.1, 1). Since  $E$  is defined over  $\mathbb{Q}_p$ , by Proposition 3.1.1, 2),  $v_L(\beta) \equiv 1 \pmod e$  for  $\varepsilon = 1$  and  $v_L(\beta) \equiv e - 3 \pmod e$  for  $\varepsilon = -1$ . For  $e = 3$ , if  $j \neq 0$  and  $v_p(\Delta) = 4$ , then  $\varepsilon = 1$  by Lemma 3.1.2 so  $v_L(c_p) = v_L(\beta\pi) = 2$  since  $v_L(c_p) < e$ . For  $e = 3$ , if  $v_p(\Delta) = 8$ ,  $v_L(c_p) = 3 - 3 + 1 = 1$ . For  $e = 4$ , if  $v_p(\Delta) = 3$ ,  $v_L(c_p) = 1 + 1 = 2$  and if  $v_L(\Delta) = 9$ ,  $v_L(c_p) = 4 - 3 + 1 = 2$ . For  $e = 6$ , if  $v_p(\Delta) = 2$ ,  $v_L(c_p) = 1 + 1 = 2$  and if  $v_L(\Delta) = 10$ ,  $v_L(c_p) = 6 - 3 + 1 = 4$ .

If  $e = 6$  and  $p = 5$ , there exists a quadratic twist  $E_D$  which is isomorphic to  $E$  over the quadratic extension  $\mathbb{Q}_5(\sqrt{D})$ , that is  $E \ni (x_1, y_1) \rightarrow (x_1, \sqrt{D}y_1) \in E_D$ . Let  $\pi_m \in \tilde{\mathbb{Q}}_p$  such that  $\pi_m^m + p = 0$ , then  $\sqrt{D} = \pi_2u$ , where  $u$  is a unit of the ring of

integers of  $\mathbb{Q}_5(\sqrt{D})$ . Let  $\Delta_D$  be the discriminant of  $E_D$ . Then  $v_5(\Delta_D) = v_5(\Delta) + 6 \equiv 4$  or  $8 \pmod{12}$  for  $e = 6$ . Hence  $e_D = 12/\gcd(v_5(\Delta_D), 12) = 3$ . So  $E_D$  has good reduction over  $L' = \mathbb{Q}_p(\pi_3)$  which is a totally ramified extension of degree 3 over  $\mathbb{Q}_p$ . Let  $\hat{E}_D/\mathcal{O}_{L'}$  be the formal group over  $\mathcal{O}_{L'}$  associated to  $E_D/\mathcal{O}_{L'}$  and let  $x'$  be a parameter of  $\hat{E}_D/\mathcal{O}_{L'}$ . Let  $[p](x') = px' + \dots + c_p'x'^p + \dots$ . So if  $v_5(\Delta_D) = 4$ ,  $v_L(c_p') = 2$  and if  $v_5(\Delta_D) = 8$ ,  $v_L(c_p') = 1$ . For the parameter  $z = -x_1/y_1$  of  $\hat{E}/\mathbb{Z}_p$ , we take the parameter  $z' = -x_1/(\pi_2 y_1)$  of  $\hat{E}_D/\mathbb{Z}_p$ . We choose the minimal model  $E_D/\mathcal{O}_L$  such that  $x' = (\pi_3^2/\pi_2)z = \pi_6 z$ , so  $x = \pi_6 z = x'$ . Hence we can take  $c_p' = c_p$ . Therefore if  $v_5(\Delta) = 2$ ,  $v_L(c_p) = 2$  and if  $v_5(\Delta_D) = 10$ ,  $v_L(c_p) = 4$ .

The case  $e = 2$ . For  $\tau \in \text{Gal}(K_e/\mathbb{Q}_p)$ ,  $\tau e_1 = -e_1$ ,  $\tau e_2 = -e_2$  and  $\tau\pi = -\pi$  [10, p. 78]. By the similar argument of the proof of [10, Proposition 4.8],  $\tau$  acts to  $\mathcal{L}(\beta)$ . So

$$\tau(l) = (-1) \otimes e_1 + \tau(\beta) \frac{-\pi}{p} (-1) \otimes e_2.$$

Since  $\mathcal{L}(\beta)$  is  $\mathcal{O}_L$ -module of rank 1,

$$\tau(l) = (-1) \left( 1 \otimes e_1 + \beta \frac{\pi}{p} \otimes e_2 \right).$$

Hence  $\tau(\beta) = -\beta$ . So  $\tau(\beta\pi) = \beta\pi$ , that is  $\beta\pi \in \mathbb{Z}_p$ . If  $\beta \neq 0$ ,  $v_L(c_p) = 0$  by Proposition 2.2.1. Since  $\tilde{E}$  is supersingular,  $\text{ht}([p]) = 2$ . This is a contradiction. Hence  $\beta = 0$ . Therefore  $c_p = 0$  since  $v_L(c_p) < 2$ . □

#### 4. The isogenies of degree $p$ over $\mathbb{Q}_p$

Let notations and assumptions be as in previous sections.

**4.1. Leading coefficients of isogenies of degree  $p$ .** Assume that there exist an elliptic curve  $E'$  over  $\mathbb{Q}_p$  and an isogeny  $\nu: E \rightarrow E'$  of degree  $p$  over  $\mathbb{Q}_p$ . Since  $E$  and  $E'$  are isogenous,  $E'$  has good reduction over  $L$ . Let  $\hat{E}'$  be a formal group over  $\mathcal{O}_L$  associated to  $E'/\mathcal{O}_L$ . Then we can construct an isogeny  $\hat{\nu}_L: \hat{E} \rightarrow \hat{E}'$  of height 1 over  $\mathcal{O}_L$ . Let  $\hat{\nu}_L(z) = a_1 z + a_2 z^2 + \dots$  and put  $t = v_L(a_1)$ .

**Lemma 4.1.1.** *If there exists an isogeny  $\hat{\nu}_L: \hat{E} \rightarrow \hat{E}'$  of height 1 over  $\mathcal{O}_L$  and if  $e < p$ , then  $v_L(c_p) = e - t < e$ .*

*Proof.* Let  $\hat{\nu}_L: \hat{E}/\mathcal{O}_L \rightarrow \hat{E}'/\mathcal{O}_L$  be an isogeny of height 1 over  $\mathcal{O}_L$ . Then there exists  $\check{\nu}_L: \hat{E}'/\mathcal{O}_L \rightarrow \hat{E}/\mathcal{O}_L$  such that  $\check{\nu}_L \circ \hat{\nu}_L = [p]$ . Let  $\hat{\nu}_L(x) = a_1 x + a_2 x^2 + \dots + a_p x^p + \dots$  and  $\check{\nu}_L(x) = a'_1 x + a'_2 x^2 + \dots + a'_p x^p + \dots$ . Then  $v_L(a_i) > 0$  for  $i = 1, \dots, p-1$ ,  $v_L(a_p) = 0$  and  $a_1 \mid a_j$  for  $j = 2, \dots, p-1$  [6, Lemma 2.1.2]. Similarly  $v_L(a'_i) > 0$

for  $i = 1, \dots, p - 1$ ,  $v_L(a'_p) = 0$  and  $a'_1 \mid a'_j$  for  $j = 2, \dots, p - 1$  [6, Lemma 2.1.2].

$$\begin{aligned}
 [p](x) &= \check{v}_L \circ \hat{v}_L \\
 &= a'_1(a_1x + \dots + a_px^p + \dots) + a'_2(a_1x + \dots)^2 + \dots + a'_p(a_1x + \dots)^p + \dots \\
 &= a'_1a_1x + (a'_1a_2 + a'_2a_1^2)x^2 + \dots + \left( \sum_{k=1, \dots, p} a'_k \sum_{i_1 + \dots + i_k = p} a_{i_1}a_{i_2} \dots a_{i_k} \right) x^p + \dots
 \end{aligned}$$

Put  $v_L(a_1) = t$ . Since  $v_L(a'_1a_1) = v_L(p) = e$ ,  $v_L(a'_1) = e - t$ . Since  $a'_1 \mid a'_j$  for  $j = 2, \dots, p - 1$ ,  $v_L(c_p) = \min\{v_L(a'_1a_p), v_L(a'_pa_1^p)\}$  if  $v_L(a'_1a_p) \neq v_L(a'_pa_1^p)$ . If  $e < p$ ,  $v_L(a'_1a_p) = v_L(a'_1) < e < p \leq pv_L(a_1) = v_L(a'_pa_1^p)$ . Hence  $v_L(c_p) = e - t < e$ .  $\square$

**Proof of Corollary.** By Lemma 4.1.1, if  $c_p = 0$ ,  $\hat{E}$  does not have an isogeny of degree  $p$  over  $\mathcal{O}_L$  and if  $c_p \neq 0$ ,  $v_L(c_p) < e$ . Therefore we can substitute the value of  $v_L(c_p)$  in Theorem for  $t = e - v_L(c_p)$ .  $\square$

**4.2. Examples.** We consider an elliptic curve  $E$  defined over  $\mathbb{Q}$  satisfying the following conditions:

- (i) There exist an elliptic curve  $E'$  and an isogeny  $\nu: E \rightarrow E'$  of degree  $p$  defined over  $\mathbb{Q}$ .
- (ii) The curves  $E$  and  $E'$  have potentially supersingular reduction at  $p$ .

We can find the following examples of such elliptic curves in the table of [1]. We regard  $\nu$  as an isogeny over  $\mathbb{Q}_p$  by the inclusion  $\mathbb{Q}$  to  $\mathbb{Q}_p$ . By Corollary, we can determine the value of  $t$  for each  $\nu$  and the dual isogeny  $\check{\nu}$  of  $\nu$ .

We use the next notation in examples. Let  $N$  be the conductor of  $E$ , then  $E'$  has the same conductor [7, VII, 7.2]. The notation ‘CM’ implies that  $E$  has complex multiplication and ‘non-CM’ implies that  $E$  does not have complex multiplication. For  $E'$ , denote the discriminant by  $\Delta'$  and  $e' = 12/\gcd(v_p(\Delta'), 12)$ . We define  $t'$  for  $\check{\nu}$  by the same method as  $t$  for  $\nu$ .

EXAMPLE 4.2.1. For  $p = 5$  and  $N = 50 = 2 \cdot 5^2$ ,

$$E: y^2 + xy + y = x^3 - x - 2$$

satisfies the conditions (i), (ii) and we have  $v_p(\Delta) = 4$ ,  $e = 3$  and non-CM. Then

$$E': y^2 + xy + y = x^3 - 76x + 298$$

and we have  $v_p(\Delta') = 8$ ,  $e' = 3$  and non-CM. There exists 5-isogeny  $\nu: E \rightarrow E'$  over  $\mathbb{Q}$ . By Corollary, we have  $t = 1$ . The dual isogeny  $\check{\nu}: E' \rightarrow E$  is 5-isogeny over  $\mathbb{Q}$ . By Corollary, we have  $t' = 2$ .



EXAMPLE 4.2.2. For  $p = 7$  and  $N = 49 = 7^2$ ,

$$E: y^2 + xy = x^3 - x^2 - 2x - 1$$

satisfies the conditions (i), (ii) and we have  $v_p(\Delta) = 3$ ,  $e = 4$  and CM. Then

$$E': y^2 + xy = x^3 - x^2 - 107x + 552$$

and we have  $v_p(\Delta') = 9$ ,  $e' = 4$  and CM. There exists 7-isogeny  $v: E \rightarrow E'$  over  $\mathbb{Q}$ . By Corollary, we have  $t = 2$ . The dual isogeny  $\check{v}: E' \rightarrow E$  is 7-isogeny over  $\mathbb{Q}$ . By Corollary, we have  $t' = 2$ .

EXAMPLE 4.2.3. For  $p = 11$  and  $N = 121 = 11^2$ ,

$$E: y^2 + xy = x^3 + x^2 - 2x - 7$$

satisfies the conditions (i), (ii) and we have  $v_p(\Delta) = 4$ ,  $e = 3$  and non-CM. Then

$$E': y^2 + xy = x^3 + x^2 - 3632x + 82757$$

and we have  $v_p(\Delta') = 8$ ,  $e' = 3$  and non-CM. There exists 11-isogeny  $v: E \rightarrow E'$  over  $\mathbb{Q}$ . By Corollary, we have  $t = 1$ . The dual isogeny  $\check{v}: E' \rightarrow E$  is 11-isogeny over  $\mathbb{Q}$ . By Corollary, we have  $t' = 2$ .

EXAMPLE 4.2.4. For  $p = 11$  and  $N = 121 = 11^2$ ,

$$E: y^2 + y = x^3 - x^2 - 7x - 10$$

satisfies the conditions (i), (ii) and we have  $v_p(\Delta) = 3$ ,  $e = 4$  and CM. Then

$$E': y^2 + y = x^3 - x^2 - 7x - 10143$$

and we have  $v_p(\Delta') = 9$ ,  $e' = 4$  and non-CM. There exists 11-isogeny  $v: E \rightarrow E'$  over  $\mathbb{Q}$ . By Corollary, we have  $t = 2$ . The dual isogeny  $\check{v}: E' \rightarrow E$  is 11-isogeny over  $\mathbb{Q}$ . By Corollary, we have  $t' = 2$ .

EXAMPLE 4.2.5. For  $p = 17$  and  $N = 14450 = 2 \cdot 5^2 \cdot 17^2$ ,

$$E: y^2 + xy + y = x^3 - 3041x + 64278$$

satisfies the conditions (i), (ii) and we have  $v_p(\Delta) = 4$ ,  $e = 3$  and non-CM. Then

$$E': y^2 + xy + y = x^3 - 190891x - 36002922$$

and we have  $v_p(\Delta') = 8$ ,  $e' = 3$  and non-CM. There exists 17-isogeny  $v: E \rightarrow E'$  over  $\mathbb{Q}$ . By Corollary, we have  $t = 1$ . The dual isogeny  $\check{v}: E' \rightarrow E$  is 17-isogeny over  $\mathbb{Q}$ . By Corollary, we have  $t' = 2$ .

EXAMPLE 4.2.6. For  $p = 19$  and  $N = 361 = 19^2$ ,

$$E: y^2 + y = x^3 - 38x + 90$$

satisfies the conditions (i), (ii) and we have  $v_p(\Delta) = 3$ ,  $e = 4$  and CM. Then

$$E': y^2 + y = x^3 - 13718x - 619025$$

and we have  $v_p(\Delta') = 9$ ,  $e' = 4$  and CM. There exists 19-isogeny  $v: E \rightarrow E'$  over  $\mathbb{Q}$ . By Corollary, we have  $t = 2$ . The dual isogeny  $\check{v}: E' \rightarrow E$  is 19-isogeny over  $\mathbb{Q}$ . By Corollary, we have  $t' = 2$ .

Remark that Example 4.2.1 has been already known in [6, Example 5.2.1] by calculating the generator of  $\ker v$ . And if  $E$  has complex multiplication,  $t = e/2$ . So Example 4.2.2, 4.2.4, 4.2.6 have already known. We can determine the value of  $t$  in Example 4.2.3 and 4.2.5 for the first time by using our Corollary.

---

### References

- [1] J.E. Cremona: *Algorithms for Modular Elliptic Curves*, second edition, Cambridge Univ. Press, Cambridge, 1997.
- [2] J.-M. Fontaine: *Groupes  $p$ -Divisibles sur les Corps Locaux*, Astérisque **47–48**, Soc. Math. France, Paris, 1977.
- [3] M. Hazewinkel: *On norm maps for one dimensional formal groups*, III, *Duke Math. J.* **44** (1977), 305–314.
- [4] T. Honda: *Formal groups and zeta-functions*, *Osaka J. Math.* **5** (1968), 199–213.
- [5] T. Honda: *On the theory of commutative formal groups*, *J. Math. Soc. Japan* **22** (1970), 213–246.
- [6] M. Kawachi: *Isogenies of degree  $p$  of elliptic curves over local fields and Kummer theory*, *Tokyo J. Math.* **25** (2002), 247–259.
- [7] J.H. Silverman: *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1985.
- [8] J. Tate:  *$p$ -divisible groups*; in *Proc. Conf. Local Fields (Driebergen, 1966)*, Springer, Berlin, 158–183.
- [9] J. Tate: *Algorithm for determining the type of a singular fiber in an elliptic pencil*; in *Modular Functions of One Variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Math. **476**, Springer, Berlin, 33–52, 1975.
- [10] M. Volkov: *Les représentations  $l$ -adiques associées aux courbes elliptiques sur  $\mathbb{Q}_p$* , *J. Reine Angew. Math.* **535** (2001), 65–101.

Department of Mathematics and Information Sciences  
Tokyo Metropolitan University  
Mimami-Ohsawa, Hachioji-shi  
Tokyo, 192-0397  
Japan  
e-mail: kawachi@tmu.ac.jp