

# Zero-Cycles on Products of Elliptic Curves over $\mathbb{Q}_p$ -Adic Fields

Takemoto, Takashi  
Graduate School of Mathematics, Kyushu University

<https://hdl.handle.net/2324/4287>

---

出版情報 : Kyushu University Preprint Series in Mathematics, 2007-05-08. 九州大学大学院数理学研究院  
バージョン :  
権利関係 :



# Zero-Cycles on Products of Elliptic Curves over $p$ -Adic Fields

Takashi Takemoto

May 8, 2007

## Abstract

The structure of  $\mathrm{CH}_0(X)/p^n$  is determined when  $X$  is a product of two elliptic curves over a  $p$ -adic field which have ordinary good reduction or split multiplicative reduction.

## 1 Introduction

Let  $X$  be a smooth projective variety over a finite extension field  $K$  of  $\mathbb{Q}_p$ . We will consider the structure of the Chow group  $\mathrm{CH}_0(X)$  of 0-cycles on  $X$ . Let  $T(X)$  denote the kernel of the Albanese map on  $X$ . Then the structure of the quotient group  $\mathrm{CH}_0(X)/T(X)$  is understood very well. Indeed, the degree map  $\mathrm{CH}_0(X) \rightarrow \mathbb{Z}$  and the Albanese map  $\mathrm{Ker}[\mathrm{CH}_0(X) \rightarrow \mathbb{Z}] \rightarrow \mathrm{Alb}_X(K)$  have finite cokernels, and the structure of  $\mathrm{Alb}_X(K)$  is understood by Mattuck [Mat55, Theorem 7] since the Albanese variety of  $X$  is an abelian variety.

However, few results are known on  $T(X)$  when  $X$  has dimension greater than 1. Colliot-Thélène [CT95, 1.4(d), (e), (f)] conjectured that the group  $T(X)$  is the direct sum of a finite group and the maximal divisible subgroup of  $T(X)$ . This conjecture is known to be true for certain types of varieties. For example, Raskind-Spiess [RS00, Theorem 1.1] proved this conjecture when  $X$  is a product of curves whose Jacobians have a mixture of ordinary good and split multiplicative reduction.

In this paper, we will consider (not only the finiteness but also) the structure of  $T(X)/p^n$  in detail when  $X$  is a product of two elliptic curves which have ordinary good or split multiplicative reduction. Our main result is as follows.

**Theorem 1.1.** *Let  $E_1, E_2$  be elliptic curves defined over  $K$ . Assume that their  $p^n$ -torsion points are  $K$ -rational. We put  $X = E_1 \times E_2$  and let  $T(X)$  be the kernel of the Albanese map on  $X$ . Then the structure of  $T(X)/p^n$  is as follows.*

(1) *If both  $E_1$  and  $E_2$  have ordinary good or split multiplicative reduction over  $K$ , then*

$$T(X)/p^n \simeq \mathbb{Z}/p^n.$$

(2) *If one of the  $E_1, E_2$  has split multiplicative reduction over  $K$  and the other has ordinary good reduction over  $K$ , then*

$$T(X)/p^n \simeq (\mathbb{Z}/p^n)^{\oplus 2}.$$

**Remark 1.2.** In (1), the split multiplicative reduction case was proved by Yamazaki [Yam05, Theorem 5.1].

As mentioned above, the structure of the quotient group  $\mathrm{CH}_0(X)/T(X)$  is understood very well. Taking it into consideration, we see the structure of  $\mathrm{CH}_0(X)/p^n$  as follows.

**Corollary 1.3.** *Let the assumption and notation be as in Theorem 1.1. Let  $d$  be the extension degree of  $K/\mathbb{Q}_p$ . Then the structure of  $\mathrm{CH}_0(X)/p^n$  is as follows.*

(1) *If both  $E_1$  and  $E_2$  have ordinary good or split multiplicative reduction over  $K$ , then*

$$\mathrm{CH}_0(X)/p^n \simeq (\mathbb{Z}/p^n)^{\oplus(2d+6)}.$$

(2) *If one of the  $E_1, E_2$  has split multiplicative reduction over  $K$  and the other has ordinary good reduction over  $K$ , then*

$$\mathrm{CH}_0(X)/p^n \simeq (\mathbb{Z}/p^n)^{\oplus(2d+7)}.$$

Let the assumption and notation be as in Theorem 1.1. To show main result we will consider the cycle map

$$cl : T(X)/p^n \rightarrow H_{\text{ét}}^4(X, \mu_{p^n}^{\otimes 2}), \quad (1.1)$$

where  $\mu_{p^n}$  is the étale sheaf of all  $p^n$ -th roots of unity. In the case where  $E_1$  and  $E_2$  have the same reduction type as in Theorem 1.1(1), (2), Raskind-Spiess [RS00, Remark 4.5.8 (b)] proved the cycle map is injective under the assumption that the  $p^n$ -torsion points of  $E_1$  and  $E_2$  are  $K$ -rational. (The cycle map is not always injective. It is known the cycle map is not injective for certain types of varieties [PS95, Chap 8]). They explained how to calculate the image of (1.1) by analyzing the proof of their main result [RS00, Theorem 4.5]. (For any integer  $m$  prime to  $p$ , they also considered the structure of  $T(X)/m$  [RS00, Theorem 3.5]).

They also introduced another approach to calculating the image, which can be applied in the case where  $E_1$  and  $E_2$  have any reduction type. They showed the image is isomorphic to that of the composition of the connecting homomorphism, the cup product and the norm map:

$$\begin{aligned} \bigoplus_{K'/K} E_1(K') \otimes E_2(K') &\rightarrow \bigoplus_{K'/K} H^1(K', E_1[p^n]) \otimes H^1(K', E_2[p^n]) \\ &\rightarrow \bigoplus_{K'/K} H^2(K', E_1[p^n] \otimes E_2[p^n]) \rightarrow H^2(K, E_1[p^n] \otimes E_2[p^n]), \end{aligned} \quad (1.2)$$

where  $K'$  runs through all finite extensions of  $K$ . Following this approach, Yamazaki [Yam05, Theorem 5.1] obtained the result mentioned in Remark 1.2.

In the same way as above we will show Theorem 1.1. In section 2, to calculate the cup product of (1.2) we consider the Hilbert symbol  $K^\times/p^n \times K^\times/p^n \rightarrow \mu_{p^n}$ , which can be seen as the following cup product  $H^1(K, \mu_{p^n}) \otimes H^1(K, \mu_{p^n}) \rightarrow H^2(K, \mu_{p^n})$ . In section 3, to calculate the first arrow in (1.2) we consider the image of the connecting homomorphism  $\delta : E(K) \rightarrow H^1(K, E[p^n])$  for an elliptic curve  $E$  over  $K$ . In section 4, we calculate the image of the composition of (1.2) and complete the proof of our main result.

When either  $E_1$  or  $E_2$  has supersingular good reduction, the injectivity of the cycle map  $cl$  is not known. However, in the same way as above the image of the cycle map (1.1) can be calculated. We have the following result when  $n = 1$ .

**Theorem 1.4.** *Let  $E_1, E_2$  be elliptic curves defined over  $K$  and assume that their  $p$ -torsion points are  $K$ -rational. We put  $X = E_1 \times E_2$ . Then*

- (1) *If one of the  $E_1, E_2$  has split multiplicative reduction over  $K$  and the other has supersingular good reduction over  $K$ , then the image of  $T(X)/p$  by the cycle map is isomorphic to  $(\mathbb{Z}/p)^{\oplus 2}$ .*
- (2) *If one of the  $E_1, E_2$  has ordinary good reduction over  $K$  and the other has supersingular good reduction over  $K$ , then the image of  $T(X)/p$  by the cycle map is isomorphic to  $(\mathbb{Z}/p)^{\oplus 2}$ .*
- (3) *If both  $E_1$  and  $E_2$  have supersingular good reduction over  $K$ , then the image of  $T(X)/p$  by*

the cycle map is isomorphic to the following.

$$\begin{cases} (\mathbb{Z}/p)^{\oplus 2} & \text{if } t_1 \neq t_2 \text{ and } t_1 + t_2 \neq \frac{e}{p-1}, \\ \mathbb{Z}/p & \text{if } t_1 = t_2 \neq \frac{e}{2(p-1)} \text{ or } "t_1 \neq t_2 \text{ and } t_1 + t_2 = \frac{e}{p-1} ", \\ 0 & \text{if } t_1 = t_2 = \frac{e}{2(p-1)}, \end{cases}$$

where  $e$  is the ramification index of  $K/\mathbb{Q}_p$ , and  $t_1$  and  $t_2$  are respectively the invariants of  $E_1$  and  $E_2$  defined in (3.4).

This result is obtained by using Kawachi's result [Kaw02, Theorem 1.1(2)] of the image on  $\delta : E(K) \rightarrow H^1(K, E[p^n])$  for  $n = 1$ . Theorem 1.4 generalizes to the case of  $n \geq 1$  once the image of  $\delta$  has been calculated for that  $n$ .

## Notation

Throughout this paper, let  $K$  be a finite extension of  $\mathbb{Q}_p$ . Let  $\mathcal{O}_K$  be the ring of integers of  $K$ ,  $U_K$  the unit group of  $\mathcal{O}_K$ , and  $\mathcal{M}_K$  the maximal ideal of  $\mathcal{O}_K$ . Let  $U_K^{(0)} = U_K$  and  $U_K^{(s)} = 1 + \mathcal{M}_K^s$  for  $s \geq 1$ . This gives a filtration  $K^\times \supset U_K^{(0)} \supset U_K^{(1)} \supset U_K^{(2)} \supset \dots$  on the unit group of  $K$ . It also induces a filtration  $K^\times/p^n \supset U_{K,n}^{(0)} \supset U_{K,n}^{(1)} \supset U_{K,n}^{(2)} \supset \dots$ , where  $U_{K,n}^{(s)} = U_K^{(s)} / ((K^\times)^{p^n} \cap U_K^{(s)})$  for  $s \geq 0$ . Similar notation applies to any complete discrete valuation fields. For each positive integer  $k$ , let  $\zeta_{p^k}$  be a primitive  $p^k$ -th root of unity and  $\mu_{p^k}$  the group of all  $p^k$ -th roots of unity. Given an abelian group  $A$  and a nonzero integer  $m$ , let  $A[m]$  (resp.  $A/m$ ) be the kernel (resp. cokernel) of multiplication by  $m$  on  $A$ .

## 2 The Hilbert symbol and a filtration on the unit group

We fix a positive integer  $n$ , and assume that  $\mu_{p^n} \subset K$  throughout this section. Then the Hilbert symbol over the local field  $K$  is defined by

$$(\ , \ )_{p^n} : K^\times/p^n \times K^\times/p^n \rightarrow \mu_{p^n} ; (a, b) \mapsto \frac{\rho_K(a)(\sqrt[p^n]{b})}{\sqrt[p^n]{b}}, \quad (2.1)$$

where  $\rho_K : K^\times \rightarrow \text{Gal}(K^{\text{ab}}/K)$  is the reciprocity map of  $K$ .

**Lemma 2.1.** *Let  $a, b \in K^\times$ . Then the Hilbert symbol has the following properties.*

- (1) *The Hilbert symbol is a nondegenerate bilinear pairing.*
- (2)  *$(1 - a, a)_n = (a, 1 - a)_n = 1$  for  $a \neq 1$ .*
- (3)  *$(a, b)_n = (b, a)_n^{-1}$ .*
- (4)  *$(a, b)_{p^n}^{p^k} = (a, b)_{p^{n-k}}$  for each  $1 \leq k \leq n$ .*

*Proof.* See [FV02, Chap 4, (5.1)]. □

We shall calculate the order of the image  $(U_{K,n}^{(s)}, U_{K,n}^{(t)})_{p^n}$  of the subgroup  $U_{K,n}^{(s)} \times U_{K,n}^{(t)}$  by the Hilbert symbol. To calculate them we shall investigate the ramification for extensions  $K(\sqrt[p^n]{b})/K$ , where  $b \in K^\times$ . Let  $L = K(\sqrt[p^n]{b})$  and  $\rho_{L/K} : K^\times \rightarrow \text{Gal}(L/K)$  be the reciprocity map of  $L/K$ . By [Iwa86, Theorem 7.12],

$$\rho_{L/K}(U_K^{(s)}) = \text{Gal}(L/K)^s \quad (2.2)$$

for all  $s \geq 0$ , where  $\text{Gal}(L/K)^s$  is the  $s$ -th ramification subgroup in the upper numbering for  $L/K$ . We will calculate the Hasse-Herbrand function of  $L/K$ , which is used to define  $\text{Gal}(L/K)^s$  (cf. [FV02, Chap 3, §3]). This function is the inverse function of

$$\phi_{L/K}(s) = \int_0^s \frac{1}{(\text{Gal}(L/K)_0 : \text{Gal}(L/K)_r)} dr, \quad (2.3)$$

where  $\text{Gal}(L/K)_s$  is the  $s$ -th ramification subgroup in the lower numbering for  $L/K$ . Note that the function  $\phi_{L/K}$  is continuous and piecewise linear on  $s \geq 0$ .

**Lemma 2.2.** *Let  $L = K(\sqrt[p^n]{b})$  and let  $\psi_{L/K}$  be the Hasse-Herbrand function of  $L/K$ . For each  $1 \leq k \leq n$ , we put  $c_k = \frac{e}{p-1} + ke$ , where  $e$  is the ramification index of  $K/\mathbb{Q}_p$ . Then*

(1) *If  $b$  is a prime element of  $K$ , then*

$$\psi_{L/K}(r) = \begin{cases} r & (0 \leq r \leq c_1) \\ p^k r - kp^k e & (c_k \leq r \leq c_{k+1}) \\ p^n r - np^n e & (r \geq c_n). \end{cases} \quad (k = 1, 2, \dots, n-1)$$

*In particular, the breaks of  $\text{Gal}(L/K)^s$  occur at  $c_k$  for each  $1 \leq k \leq n$ .*

(2) *If  $b \in U_{K,1}^{(t)} \setminus U_{K,1}^{(t+1)}$ ,  $1 \leq t < c_1$  and  $p \nmid t$ , then*

$$\psi_{L/K}(r) = \begin{cases} r & (0 \leq r \leq c_1 - t) \\ p^k r - kp^k e + (p^k - 1)t & (c_k - t \leq r \leq c_{k+1} - t) \\ p^n r - np^n e + (p^n - 1)t & (r \geq c_n - t). \end{cases} \quad (k = 1, 2, \dots, n-1)$$

*In particular, the breaks of  $\text{Gal}(L/K)^s$  occur at  $c_k - t$  for each  $1 \leq k \leq n$ .*

*Proof.* Since the proofs are similar in both (1) and (2), we shall prove here only (2). Let  $v_L$  be the normalized valuation on  $L$ . Since  $\zeta_{p^n} \in K$  and  $b \notin (K^\times)^p$ , we see  $L/K$  is a cyclic extension of degree  $p^n$ . Let  $\sigma$  be the generator of  $\text{Gal}(L/K)$  such that  $\sigma(\sqrt[p^n]{b}) = \zeta_{p^n} \sqrt[p^n]{b}$ . Then

$$\begin{aligned} p^n v_L(\sqrt[p^n]{b} - 1) &= \sum_{j=1}^{p^n} v_L(\sigma^j(\sqrt[p^n]{b} - 1)) = \sum_{j=1}^{p^n} v_L(\zeta_{p^n}^j \sqrt[p^n]{b} - 1) = v_L\left(\prod_{j=1}^{p^n} (\zeta_{p^n}^j \sqrt[p^n]{b} - 1)\right) \\ &= v_L(b - 1) = e(L/K)t, \end{aligned}$$

where  $e(L/K)$  is the ramification index of  $L/K$ . Since  $p \nmid t$ , the field extension  $L/K$  is totally ramified and  $v_L(\sqrt[p^n]{b} - 1) = t$ . Therefore the ring of integers of  $L$  is generated by a prime element of  $L$ . We can choose integers  $g, h$  such that  $g > 0$  and  $gt + hp^n = 1$ . Then  $\pi' = (\sqrt[p^n]{b} - 1)^g \pi^h$  is a prime element of  $L$ , where  $\pi$  is a prime element of  $K$ . Therefore

$$\begin{aligned} \sigma^j(\pi') - \pi' &= \pi' \left\{ \left( \frac{\zeta_{p^n}^j \sqrt[p^n]{b} - 1}{\sqrt[p^n]{b} - 1} \right)^g - 1 \right\} = \pi' \left\{ \left( 1 + \frac{\zeta_{p^n}^j - 1}{\sqrt[p^n]{b} - 1} \sqrt[p^n]{b} \right)^g - 1 \right\} \\ &= \pi' \left\{ \sum_{l=1}^g \binom{g}{l} \left( \frac{\zeta_{p^n}^j - 1}{\sqrt[p^n]{b} - 1} \right)^l (\sqrt[p^n]{b})^l \right\}. \end{aligned}$$

If  $p^k$  divides  $j$  exactly, then  $v_L((\zeta_{p^n}^j - 1)/(\sqrt[p^n]{b} - 1)) = p^{k+1}e/(p-1) - t > 0$ . Thus the valuation of the terms in the above sum assumes the minimum for  $l = 1$ , and we have  $v_L(\sigma^j(\pi') - \pi') =$

$d_{k+1} + 1 - t$ , where we put  $d_k = p^k e / (p - 1)$ . Hence the order  $g_r$  of  $\text{Gal}(L/K)_r$  is

$$g_r = \begin{cases} p^n & (0 \leq r \leq d_1 - t) \\ p^{n-k} & (d_k - t < r \leq d_{k+1} - t) \quad (k = 1, 2, \dots, n-1) \\ 1 & (r > d_n - t). \end{cases}$$

By definition (2.3), we see (2) is proved.  $\square$

**Corollary 2.3.** *Let  $s \geq 0$ . For each  $1 \leq k \leq n$ , the following are equivalent.*

- (1)  $s > c_k$ .
- (2)  $(U_{K,k}^{(s)}, K^\times / p^k)_{p^k} = 1$ .
- (3)  $U_K^{(s)} \subset (K^\times)^{p^k}$ .

*Proof.* Since the Hilbert symbol is a nondegenerate pairing, (2) is equivalent to (3). By [FV02, Chap 1, (5.8)], if  $s > c_k$ , we have  $U_K^{(s)} \subset (K^\times)^{p^k}$ . Assume that  $s \leq c_k$ . Let  $L = K(\sqrt[p^k]{\pi})$ , where  $\pi$  is a prime element of  $K$ . By Lemma 2.2 (1),  $\psi_{L/K}(s) \leq \psi_{L/K}(c_k) = p^k e / (p - 1)$ . Therefore we see  $\text{Gal}(L/K)^s \neq 1$ . Hence we have  $(U_{K,k}^{(s)}, K^\times / p^k)_{p^k} \neq 1$  by (2.1) and (2.2).  $\square$

**Lemma 2.4 (cf. [Kat79] Lemma 2 in §2).** *For each  $s, t \geq 1$  and for each  $1 \leq k \leq n$ , we have  $(U_{K,k}^{(s)}, U_{K,k}^{(t)})_{p^k} \subseteq (U_{K,k}^{(s+t)}, K^\times / p^k)_{p^k}$ .*

*Proof.* Let  $1 + x \in U_K^{(s)}$  and  $1 + y \in U_K^{(t)}$ . Note that  $(1 - a, a)_{p^k} = 1$  for  $a \neq 1$  (Lemma 2.1(3)). Then

$$\begin{aligned} & (1 + x, 1 + y)_{p^k} \\ &= (1 + x, 1 + y)_{p^k} \left( \frac{1 + x + xy}{1 + x}, 1 + y \right)_{p^k} \left( \frac{1 + x + xy}{1 + x}, 1 + y \right)_{p^k}^{-1} \\ &= (1 + x + xy, 1 + y)_{p^k} \left( \frac{1 + x + xy}{1 + x}, 1 + y \right)_{p^k}^{-1} \\ &= (1 + x + xy, 1 + y)_{p^k} (1 + x + xy, -x(1 + y))_{p^k}^{-1} \left( \frac{1 + x + xy}{1 + x}, 1 + y \right)_{p^k}^{-1} \\ &= (1 + x + xy, -x)_{p^k}^{-1} \left( \frac{1 + x + xy}{1 + x}, 1 + y \right)_{p^k}^{-1} \\ &= (1 + x + xy, -x)_{p^k}^{-1} (1 + x, -x)_{p^k} \left( \frac{1 + x + xy}{1 + x}, 1 + y \right)_{p^k}^{-1} \\ &= \left( \frac{1 + x + xy}{1 + x}, -x \right)_{p^k}^{-1} \left( \frac{1 + x + xy}{1 + x}, 1 + y \right)_{p^k}^{-1}. \end{aligned} \tag{2.4}$$

Since  $(1 + x + xy)/(1 + x) \in U_K^{(s+t)}$ , we have  $(U_{K,k}^{(s)}, U_{K,k}^{(t)})_{p^k} \subseteq (U_{K,k}^{(s+t)}, K^\times / p^k)_{p^k}$ .  $\square$

**Proposition 2.5.** *Let  $s, t \geq 0$  and  $c_k = \frac{e}{p-1} + ke$  for each  $1 \leq k \leq n$ . Then*

(1)

$$\#(U_{K,n}^{(s)}, K^\times / p^n)_{p^n} = \begin{cases} p^n & (s \leq c_1) \\ p^{n-k} & (c_k < s \leq c_{k+1}) \quad (k = 1, 2, \dots, n-1) \\ 1 & (s > c_n). \end{cases}$$

(2) If  $p \nmid s$  or  $p \nmid t$ , then

$$\#(U_{K,n}^{(s)}, U_{K,n}^{(t)})_{p^n} = \begin{cases} p^n & (s+t \leq c_1) \\ p^{n-k} & (c_k < s+t \leq c_{k+1}) \quad (k=1, 2, \dots, n-1) \\ 1 & (s+t > c_n). \end{cases}$$

(3) If  $p \mid s$  and  $p \mid t$ , then

$$\#(U_{K,n}^{(s)}, U_{K,n}^{(t)})_{p^n} = \begin{cases} p^n & (s+t < c_1) \\ p^{n-k} & (c_k \leq s+t < c_{k+1}) \quad (k=1, 2, \dots, n-1) \\ 1 & (s+t \geq c_n). \end{cases}$$

*Proof.* (1) By Lemma 2.1(4) and Corollary 2.3, for each  $1 \leq k \leq n$ , we have  $(U_{K,n}^{(s)}, K^\times/p^n)_{p^n} \subseteq \mu_{p^{n-k}}$  if and only if  $s > c_k$ . Hence (1) follows by decreasing induction on  $k$ .

(2) By an argument similar to (1), it is sufficient to show that for each  $1 \leq k \leq n$ ,  $(U_{K,k}^{(s)}, U_{K,k}^{(t)})_{p^k} = 1$  if and only if  $s+t > c_k$ . If  $s+t > c_k$ , then by Lemma 2.4 and (1)  $(U_{K,k}^{(s)}, U_{K,k}^{(t)})_{p^k} \subseteq (U_{K,k}^{(s+t)}, K^\times/p^k)_{p^k} = 1$ . We shall prove the converse by induction on  $k$ . We may suppose that  $s+t = c_k$  and  $s \geq t$ . Then we have  $p \nmid t$  by  $p \mid c_k$ . When  $k=1$  or  $2$ , we have  $t < c_1$ . By Lemma 2.2 (2), we see  $\text{Gal}(K(\sqrt[p^k]{b})/K)^s \neq 1$  ( $b \in U_K^{(t)} \setminus U_K^{(t+1)}$ ). Hence we have  $(U_{K,k}^{(s)}, U_{K,k}^{(t)})_{p^k} \neq 1$  by (2.1) and (2.2). When  $k \geq 3$ , by induction on  $k$ , there exist  $a \in U_{K,k-1}^{(s-e)}$  and  $b \in U_{K,k-1}^{(t)}$  such that  $(a, b)_{p^{k-1}} = \zeta_p$ . Thus  $(a^p, b)_{p^k} = (a, b)_{p^k}^p = (a, b)_{p^{k-1}} = \zeta_p \neq 1$ . Since  $k \geq 3$ , we have  $s > c_1$ . Hence we have  $a^p \in U_{K,k}^{(s)}$  and  $(U_{K,k}^{(s)}, U_{K,k}^{(t)})_{p^k} \neq 1$ .

(3) By an argument similar to (1), for each  $1 \leq k \leq n$ , it is sufficient to show that  $(U_{K,k}^{(s)}, U_{K,k}^{(t)})_{p^k} = 1$  if and only if  $s+t \geq c_k$ . If  $s+t < c_k$ , then by (2),  $(U_{K,k}^{(s)}, U_{K,k}^{(t)})_{p^k} \supseteq (U_{K,k}^{(s+1)}, U_{K,k}^{(t)})_{p^k} \neq 1$ . Suppose that  $s+t \geq c_k$ . Since  $U_{K,k}^{(0)} = U_{K,k}^{(1)}$ , we may assume  $s, t \geq 1$ . Let  $1+x \in U_K^{(s)}$  and  $1+y \in U_K^{(t)}$ . Write  $x = u\pi^{ps'}$ , where  $\pi$  is a prime element of  $K$ ,  $u \in U_K$  and  $s' = s/p$ . By (2.4) in the proof of Lemma 2.4,

$$\begin{aligned} (1+x, 1+y)_{p^k} &= \left( \frac{1+x+xy}{1+x}, -x \right)_{p^k}^{-1} \left( \frac{1+x+xy}{1+x}, 1+y \right)_{p^k}^{-1} \\ &= \left( \frac{1+x+xy}{1+x}, \pi^{s'} \right)_{p^k}^{-p} \left( \frac{1+x+xy}{1+x}, -u \right)_{p^k}^{-1} \left( \frac{1+x+xy}{1+x}, 1+y \right)_{p^k}^{-1}. \end{aligned} \quad (2.5)$$

We see from  $s+t \geq c_k$  that  $(1+x+xy)/(1+x) \in U_K^{(c_k)}$ . Therefore each term in (2.5) vanishes by (1) and (2). Hence we have  $(U_{K,k}^{(s)}, U_{K,k}^{(t)})_{p^k} = 1$ .  $\square$

### 3 Elliptic curves over $K$

Let  $E$  be an elliptic curve defined over  $K$ . We fix a positive integer  $n$  and assume that the  $p^n$ -torsion points of  $E$  are  $K$ -rational. Then we see  $\mu_{p^n} \subset K$  by using Weil pairing.

The exact sequence

$$0 \longrightarrow E[p^n] \longrightarrow E \xrightarrow{[p^n]} E \longrightarrow 0$$

induces a long exact sequence

$$0 \longrightarrow E[p^n] \longrightarrow E(K) \xrightarrow{[p^n]} E(K) \xrightarrow{\delta_1^n} H^1(K, E[p^n]) \longrightarrow H^1(K, E) \longrightarrow \dots, \quad (3.1)$$

where  $\delta_1^n$  is the connecting homomorphism. If we choose an isomorphism

$$E[p^n] \simeq \mu_{p^n} \oplus \mu_{p^n}, \quad (3.2)$$

then we have an isomorphism

$$\kappa : H^1(K, E[p^n]) \xrightarrow{\sim} H^1(K, \mu_{p^n} \oplus \mu_{p^n}).$$

By Kummer theory, there exists an isomorphism

$$\delta_2^n : K^\times/p^n \oplus K^\times/p^n \xrightarrow{\sim} H^1(K, \mu_{p^n} \oplus \mu_{p^n}).$$

Let

$$\delta^n : E(K) \rightarrow K^\times/p^n \oplus K^\times/p^n$$

be the composite map  $(\delta_2^n)^{-1} \circ \kappa \circ \delta_1^n$ . We will investigate the image of  $\delta^n$ . To investigate the image of  $\delta^n$ , we choose the isomorphism (3.2) more carefully. Let  $E[p^n]^0$  be the subgroup of  $E[p^n]$  consisting of the  $\bar{K}$ -valued points of the maximal connected finite flat  $p^n$ -torsion subgroup scheme of the Néron model of  $E$  over  $\text{Spec } \mathcal{O}_K$ . Then choose an isomorphism  $E[p^n] \simeq \mu_{p^n} \oplus \mu_{p^n}$  which maps  $E[p^n]^0$  onto the first factor  $\mu_{p^n}$ .

In the case where  $E$  has split multiplicative reduction over  $K$ , Yamazaki [Yam05, Lemma 4.5] showed

$$\text{Im } \delta^n = K^\times/p^n \oplus 1. \quad (3.3)$$

We consider the case where  $E$  has ordinary good reduction over  $K$ .

**Proposition 3.1.** *If  $E$  has ordinary good reduction over  $K$  and we take the isomorphism (3.2) as above, then*

$$\text{Im } \delta^n = U_{K,n}^{(0)} \oplus A,$$

where  $A$  is the annihilator of  $U_{K,n}^{(0)}$  in the pairing (2.1), and is cyclic of order  $p^n$ .

*Proof.* Let  $v$  be the map  $(K^\times/p^n)^{\oplus 2} \rightarrow (\mathbb{Z}/p^n)^{\oplus 2}$  induced by the normalized valuation on  $K$ . We will show the composition of  $v$  and  $\delta^n$  is the zero map. To show this we may replace  $K$  by the completion of the maximal unramified extension of  $K$ , which is denoted by  $L$ . Since  $E$  has ordinary good reduction over  $K$ , we have the following exact sequence

$$\hat{E}(\mathcal{M}_L)/p^n \xrightarrow{s} E(L)/p^n \longrightarrow \tilde{E}(\bar{F})/p^n \longrightarrow 0,$$

where  $\hat{E}$  is the formal group attached to  $E$ ,  $\tilde{E}$  is the reduction of  $E$ , and  $\bar{F}$  is the residue field of  $L$ . Since the field  $\bar{F}$  is algebraically closed, we have  $\tilde{E}(\bar{F})/p^n = 0$ . Therefore it is sufficient to show that  $v \circ \delta^n \circ s = 0$ . Since  $E$  has ordinary good reduction, by Mazur [Maz72, Lemma 4.27]  $\hat{E}$  is isomorphic to the multiplicative group  $\hat{\mathbb{G}}_m$  over  $\mathcal{O}_L$ . We fix isomorphisms  $\hat{E}(\mathcal{M}_L) \simeq \hat{\mathbb{G}}_m(\mathcal{M}_L)$  and  $\hat{E}[p^n] \simeq \hat{\mathbb{G}}_m[p^n] = \mu_{p^n}$  such that the following diagram is commutative:

$$\begin{array}{ccccc} \hat{\mathbb{G}}_m(\mathcal{M}_L) & \longleftarrow & \hat{\mathbb{G}}_m[p^n] & \xrightarrow{i_1} & \mu_{p^n}^{\oplus 2} \\ \downarrow \simeq & & \downarrow \simeq & & \downarrow \simeq \\ \hat{E}(\mathcal{M}_L) & \longleftarrow & \hat{E}[p^n] & \longrightarrow & E[p^n], \end{array}$$



where the map  $i_1$  is defined by  $\zeta \mapsto (\zeta, 1)$  and the vertical isomorphism on the right is the one of (3.2). This is possible because of our choice of the isomorphism (3.2). Then we have the following commutative diagram:

$$\begin{array}{ccccccc}
\hat{\mathbb{G}}_m(\mathcal{M}_L)/p^n & \longrightarrow & H^1(L, \hat{\mathbb{G}}_m[p^n]) & \xrightarrow{\sim} & L^\times/p^n & \longrightarrow & \mathbb{Z}/p^n \\
\downarrow \simeq & & \downarrow \simeq & & \parallel & & \parallel \\
\hat{E}(\mathcal{M}_L)/p^n & \longrightarrow & H^1(L, \hat{E}[p^n]) & \xrightarrow{\sim} & L^\times/p^n & \longrightarrow & \mathbb{Z}/p^n \\
\downarrow s & & \downarrow & & \downarrow i_2 & & \downarrow i_3 \\
E(L)/p^n & \xrightarrow{\delta_1^n} & H^1(L, E[p^n]) & \xrightarrow{\sim} & (L^\times/p^n)^{\oplus 2} & \xrightarrow{v} & (\mathbb{Z}/p^n)^{\oplus 2},
\end{array}$$

where the maps  $i_2$  and  $i_3$  are defined by  $a \mapsto (a, 1)$  and  $N \mapsto (N, 0)$ , respectively. Since  $\hat{\mathbb{G}}_m(\mathcal{M}_L)/p^n = U_{L,n}^{(1)} = U_{L,n}^{(0)}$ , we have  $v \circ \delta^n \circ s = 0$  by the above diagram. It follows from  $\text{Ker}[K^\times/p^n \rightarrow \mathbb{Z}/p^n] = U_{K,n}^{(0)}$  that we have  $\text{Im } \delta^n \subseteq U_{K,n}^{(0)} \oplus A$ , where  $A = \text{Ker}[K^\times/p^n \rightarrow L^\times/p^n]$ . Since

$$A \simeq \text{Ker}[H^1(K, \mu_{p^n}) \rightarrow H^1(L, \mu_{p^n})] \simeq H^1(L/K, \mu_{p^n}) \simeq \mathbb{Z}/p^n,$$

the group  $A$  is cyclic of order  $p^n$  and the annihilator of  $U_{K,n}^{(0)}$  in the pairing (2.1). Furthermore, by Mattuck [Mat55, Theorem 7],

$$E(K) \simeq \mathbb{Z}_p^{\oplus d} \oplus (\text{torsion}),$$

where  $d$  is the extension degree of  $K/\mathbb{Q}_p$ . Since all  $p^n$ -torsion points of  $E$  are  $K$ -rational, the order of  $E(K)/p^n$  is  $(p^n)^{d+2}$ . On the other hand, the order of  $U_{K,n}^{(0)} \oplus A$  equals that of  $K^\times/p^n \simeq (\mathbb{Z}/p^n)^{\oplus(d+2)}$ . Since  $\delta^n : E(K)/p^n \rightarrow (K^\times/p^n)^{\oplus 2}$  is injective, we have  $\text{Im } \delta^n = U_{K,n}^{(0)} \oplus A$ .  $\square$

**Remark 3.2.** When  $n = 1$ , the image of  $\delta^n$  has already been calculated by Kawachi [Kaw02, Theorem 1.1] including the case of other types of reduction. Her results are as follows.

Let  $E$  be an elliptic curve over  $K$ . Assume that the  $p$ -torsion points are  $K$ -rational. Then

(1) If  $E$  has split multiplicative reduction over  $K$ , then

$$\text{Im } \delta^1 = K^\times/p \oplus 1.$$

(2) If  $E$  has ordinary good reduction over  $K$ , then

$$\text{Im } \delta^1 = U_{K,1}^{(0)} \oplus U_{K,1}^{(c_1)}.$$

(3) If  $E$  has supersingular good reduction over  $K$ , then

$$\text{Im } \delta^1 = U_{K,1}^{(1-pt+c_1)} \oplus U_{K,1}^{(1+pt)},$$

where  $t$  is an invariant depending on  $E$ , which is defined as follows. For  $i \geq 1$ , let  $E^i = \hat{E}(\mathcal{M}_K^i) \subset E(\mathcal{M}_K)$ . We define

$$t = \max\{i \geq 1 \mid Q \in E^i \text{ for all } Q \in \hat{E}[p]\}. \quad (3.4)$$

This invariant  $t$  satisfies  $1 \leq t < e/(p-1)$  (See [Kaw02] Lemma 2.3). Note that Proposition 3.1 is a generalization of (2) for arbitrary  $n \geq 1$ . The group  $U_{K,1}^{(c_1)}$  is cyclic of order  $p$ , and is the annihilator of  $U_{K,1}^{(0)}$  in the pairing (2.1) by Proposition 2.5 (3).

## 4 The structure of $\mathrm{CH}_0(E_1 \times E_2)/p^n$

Let  $E_1, E_2$  be elliptic curves defined over  $K$  and assume that their  $p^n$ -torsion points are  $K$ -rational. We put  $X = E_1 \times E_2$ . We consider the structure of  $\mathrm{CH}_0(X)/p^n$ . Let  $A_0(X)$  be the subgroup of  $\mathrm{CH}_0(X)$  generated by 0-cycles of degree 0 and  $T(X)$  the kernel of the Albanese map  $A_0(X) \rightarrow X(K)$  (Since the variety  $X$  is abelian, the Albanese variety of  $X$  is identified with  $X$ ). For any abelian variety  $X$ , since the degree map  $\mathrm{CH}_0(X) \rightarrow \mathbb{Z}$  and the Albanese map  $A_0(X) \rightarrow X(K)$  are surjective, we have

$$\mathrm{CH}_0(X)/T(X) \simeq \mathbb{Z} \oplus X(K).$$

By Mattuck [Mat55, Theorem 7],

$$X(K) \simeq \mathbb{Z}_p^{\oplus 2[K:\mathbb{Q}_p]} \oplus (\text{torsion}).$$

Since  $X(K)$  contains the  $p^n$ -torsion points of both  $E_1$  and  $E_2$ , we have

$$\mathrm{CH}_0(X)/p^n \simeq (\mathbb{Z}/p^n)^{\oplus (2d+5)} \oplus T(X)/p^n,$$

where  $d$  is the degree of  $K/\mathbb{Q}_p$ . Therefore we see that Theorem 1.1 and Corollary 1.3 are equivalent.

We will study the structure of  $T(X)/p^n$ . For that, we consider the cycle map

$$cl : T(X)/p^n \rightarrow H_{\text{ét}}^4(X, \mu_{p^n}^{\otimes 2}). \quad (4.1)$$

When  $E_1$  and  $E_2$  have the same reduction type as in Theorem 1.1(1), (2), Raskind-Spiess [RS00, Remark 4.5.8 (b)] showed that the cycle map is injective under the assumption that the  $p^n$ -torsion points of  $E_1$  and  $E_2$  are  $K$ -rational. Furthermore by the argument similar to the proof of [Yam05, Theorem 4.3], the image of  $T(X)/p^n$  by the cycle map is isomorphic to the image of the composition of the following maps:

$$\begin{aligned} \bigoplus_{K'/K} E_1(K') \otimes E_2(K') &\xrightarrow{\delta_1^n} \bigoplus_{K'/K} H^1(K', E_1[p^n]) \otimes H^1(K', E_2[p^n]) \\ &\xrightarrow{\text{cup}} \bigoplus_{K'/K} H^2(K', E_1[p^n] \otimes E_2[p^n]) \xrightarrow{N} H^2(K, E_1[p^n] \otimes E_2[p^n]), \end{aligned} \quad (4.2)$$

where  $K'$  runs through all finite extensions of  $K$ ,  $\delta_1^n$  is the connecting homomorphism, and  $N$  is the norm map. For each finite extension  $K'/K$ , by [Ser79, Chap XIV, Proposition 5] and  $\mu_{p^n} \subset K'$  we have the following commutative diagram:

$$\begin{array}{ccc} H^1(K', E_1[p^n]) \otimes H^1(K', E_2[p^n]) & \xrightarrow{\text{cup}} & H^2(K', E_1[p^n] \otimes E_2[p^n]) \\ \downarrow \simeq & & \downarrow \simeq \\ ((K')^\times/p^n)^{\oplus 2} \otimes ((K')^\times/p^n)^{\oplus 2} & \xrightarrow{(\cdot, \cdot)_{p^n}^{\oplus 4}} & \mu_{p^n}^{\oplus 4}, \end{array}$$

where the lower horizontal map is the direct sum of four Hilbert symbols. Thus the study of  $T(X)/p^n$  boils down to the calculation of the image of the composition of

$$E_1(K') \otimes E_2(K') \xrightarrow{\delta^n} ((K')^\times/p^n)^{\oplus 2} \otimes ((K')^\times/p^n)^{\oplus 2} \xrightarrow{(\cdot, \cdot)_{p^n}^{\oplus 4}} \mu_{p^n}^{\oplus 4} \quad (4.3)$$

for each finite extension  $K'/K$ .

**Theorem 4.1.** *Let  $E_1, E_2$  be elliptic curves defined over  $K$ . Assume that their  $p^n$ -torsion points are  $K$ -rational. We put  $X = E_1 \times E_2$ . Then  $T(X)/p^n$  has the following structure.*

(1) *If both  $E_1$  and  $E_2$  have ordinary good reduction over  $K$ , then*

$$T/p^n \simeq \mathbb{Z}/p^n.$$

(2) *If one of  $E_1, E_2$  has split multiplicative reduction over  $K$  and the other has ordinary good reduction over  $K$ , then*

$$T(X)/p^n \simeq (\mathbb{Z}/p^n)^{\oplus 2}.$$

*Proof.* (1) For each finite extension  $K'/K$ , by Proposition 3.1 the image of (4.3) is isomorphic to the direct sum of the following four images:  $(U_{K',n}^{(0)}, U_{K',n}^{(0)})_{p^n}$ ,  $(U_{K',n}^{(0)}, A)_{p^n}$ ,  $(A, U_{K',n}^{(0)})_{p^n}$  and  $(A, A)_{p^n}$ , where  $A$  is the annihilator of  $U_{K',n}^{(0)}$  in the pairing (2.1). By Proposition 2.5 (3), we have  $(U_{K',n}^{(0)}, U_{K',n}^{(0)})_{p^n} = \mu_{p^n}$ . By the definition of  $A$ , we have  $(U_{K',n}^{(0)}, A)_{p^n} = (A, U_{K',n}^{(0)})_{p^n} = (A, A)_{p^n} = 1$ . These images are independent of the finite extension  $K'/K$ . Therefore  $T(X)/p^n$  is isomorphic to  $\mathbb{Z}/p^n$  by (4.2) and the injectivity of the cycle map (4.1).

(2) For each finite extension  $K'/K$ , the image of (4.3) is isomorphic to the direct sum of the following four images:  $((K')^\times/p^n, U_{K',n}^{(0)})_{p^n}$ ,  $((K')^\times/p^n, A)_{p^n}$ ,  $(1, U_{K',n}^{(0)})_{p^n}$  and  $(1, A)_{p^n}$  by (3.3) and Proposition 3.1. By Proposition 2.5 (1), we have  $((K')^\times/p^n, U_{K',n}^{(0)})_{p^n} = \mu_{p^n}$ . Since the group  $A$  is cyclic of order  $p^n$  and the Hilbert symbol is a nondegenerate pairing, we have  $((K')^\times/p^n, A)_{p^n} = \mu_{p^n}$ . Hence we have  $T(X)/p^n \simeq (\mathbb{Z}/p^n)^{\oplus 2}$  by an argument similar to (1).  $\square$

When an elliptic curve  $E$  has supersingular good reduction over  $K$ , we have not succeeded in calculating the image of  $\delta^n$  yet. It is not also clear whether the cycle map is injective in this case. However, when  $n = 1$ , by Kawachi the image was calculated (Remark 3.2 (3)). Then we have the following result.

**Theorem 4.2.** *Let  $E_1, E_2$  be elliptic curves defined over  $K$  and assume that their  $p$ -torsion points are  $K$ -rational. We put  $X = E_1 \times E_2$ . Then*

(1) *If one of the  $E_1, E_2$  has split multiplicative reduction over  $K$  and the other has supersingular good reduction over  $K$ , then the image of  $T(X)/p$  by the cycle map is isomorphic to  $(\mathbb{Z}/p)^{\oplus 2}$ .*

(2) *If one of the  $E_1, E_2$  has ordinary good reduction over  $K$  and the other has supersingular good reduction over  $K$ , then the image of  $T(X)/p$  by the cycle map is isomorphic to  $(\mathbb{Z}/p)^{\oplus 2}$ .*

(3) *If both  $E_1$  and  $E_2$  have supersingular good reduction over  $K$ , then the image of  $T(X)/p$  by the cycle map is isomorphic to the following.*

$$\begin{cases} (\mathbb{Z}/p)^{\oplus 2} & \text{if } t_1 \neq t_2 \text{ and } t_1 + t_2 \neq \frac{e}{p-1}, \\ \mathbb{Z}/p & \text{if } t_1 = t_2 \neq \frac{e}{2(p-1)} \text{ or } "t_1 \neq t_2 \text{ and } t_1 + t_2 = \frac{e}{p-1} ", \\ 0 & \text{if } t_1 = t_2 = \frac{e}{2(p-1)}, \end{cases}$$

where  $e$  is the ramification index of  $K/\mathbb{Q}_p$ , and  $t_1$  and  $t_2$  are respectively the invariants of  $E_1$  and  $E_2$  defined in (3.4).

*Proof.* Since the proofs of (1), (2) and (3) are similar, we shall prove here only (1). We argue in a similar way as in the proof of Theorem 4.1. By Remark 3.2 (1) and (3), it is sufficient to calculate the following four images:  $(K^\times/p, U_{K,1}^{(1-pt+c_1)})_p$ ,  $(K^\times/p, U_{K,1}^{(1+pt)})_p$ ,  $(1, U_{K,1}^{(1-pt+c_1)})_p$ , and  $(1, U_{K,1}^{(1+pt)})_p$ . Since  $1 \leq t < e/(p-1)$ , we have  $(K^\times/p, U_{K,1}^{(1-pt+c_1)})_p = (K^\times/p, U_{K,1}^{(1+pt)})_p = \mu_p$  by Proposition 2.5 (1). Hence the image of  $T(X)/p$  by the cycle map is isomorphic to  $(\mathbb{Z}/p)^{\oplus 2}$ .  $\square$

## Acknowledgement

The author wishes to thank Professor Takao Yamazaki for his valuable advice. And he is also grateful to Professor Yuichiro Taguchi for his helpful comments.

## References

- [CT95] Jean-Louis Colliot-Thélène, *L'arithmétique du groupe de Chow des zéro-cycles*, J. Théor. Nombres Bordeaux **7** (1995), no. 1, 51–73, Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).
- [FV02] I. B. Fesenko and S. V. Vostokov, *Local fields and their extensions*, second ed., Translations of Mathematical Monographs, vol. 121, American Mathematical Society, Providence, RI, 2002.
- [Iwa86] Kenkichi Iwasawa, *Local class field theory*, Oxford Science Publications, The Clarendon Press Oxford University Press, New York, 1986, Oxford Mathematical Monographs.
- [Kat79] Kazuya Kato, *A generalization of local class field theory by using  $K$ -groups. I*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **26** (1979), no. 2, 303–376.
- [Kaw02] Mayumi Kawachi, *Isogenies of degree  $p$  of elliptic curves over local fields and Kummer theory*, Tokyo J. Math **25** (2002), no. 2, 247–259.
- [Mat55] Arthur Mattuck, *Abelian varieties over  $p$ -adic ground fields*, Ann. of Math. (2) **62** (1955), 92–119.
- [Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.
- [PS95] R. Parimala and V. Suresh, *Zero-cycles on quadric fibrations: finiteness theorems and the cycle map*, Invent. Math. **122** (1995), no. 1, 83–117.
- [RS00] Wayne Raskind and Michael Spiess, *Milnor  $K$ -groups and zero-cycles on products of curves over  $p$ -adic fields*, Compositio Math. **121** (2000), no. 1, 1–33.
- [Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979.
- [Yam05] Takao Yamazaki, *On Chow and Brauer groups of a product of Mumford curves*, Math. Ann. **333** (2005), no. 3, 549–567.

Takashi Takemoto  
Graduate School of Mathematics  
Kyushu University  
Fukuoka 812-8581, Japan  
Email address: takemoto@math.kyushu-u.ac.jp