REVISTA DE LA
UNIÓN MATEMÁTICA ARGENTINA
Vol. 56, No. 1, 2015, Pages 63–71
Published online: April 6, 2015

COMPUTATION OF THE CANONICAL LIFTING VIA DIVISION POLYNOMIALS

ALTAN ERDOĞAN

Abstract. We study the canonical lifting of ordinary elliptic curves over the ring of Witt vectors. We prove that the canonical lifting is compatible with the base field of the given ordinary elliptic curve which was first proved in Finotti, *J. Number Theory* 130 (2010), 620–638. We also give some results about division polynomials of elliptic curves defined over the ring of Witt vectors.

1. Introduction

Let k be a perfect field of characteristic $p > 0$ and $W(k)$ be the ring of p-typical Witt vectors of k. Let E be an ordinary elliptic curve over k. A consequence of the Serre–Tate theorem is that up to isomorphism there exists a unique elliptic curve $\mathbb{E}$ over $W(k)$ such that

(1) $\mathbb{E} \otimes_{W(k)} k \overset{\sim}{\to} E$

(2) $\mathrm{End}_{W(k)}(\mathbb{E}) \overset{\sim}{\to} \mathrm{End}_k(E)$,

where both isomorphisms are obtained via the reduction $\pmod{p} : \mathbb{E} \to E$. The elliptic curve $\mathbb{E}$ is called the canonical lifting of E over $W(k)$. If the base ring $W(k)$ is understood we may only call it the canonical lifting of E. If $\mathbb{E}'$ is any elliptic curve over $W(k)$ satisfying only the first condition we say that $\mathbb{E}'$ is a lifting of E. General references for a complete proof and a detailed analysis of the Serre–Tate theorem and in particular the canonical lifting are [5] and [8].

We can formulate the problem of finding the canonical lifting in terms of the j-invariants as follows. By definition, the j-invariant of $\mathbb{E}$, denoted by $j(\mathbb{E}) \in W(k)$ depends only on the j-invariant of E, say j_0. So we can define the following function:

$$\begin{aligned} \Theta : k^{\mathrm{ord}} &\longrightarrow W(k), \\ j_0 &\longmapsto j(\mathbb{E}) = (j_0, j_1, \dots), \end{aligned}$$

where $k^{\mathrm{ord}} = \{j_0 \in k \mid \text{elliptic curves with } j\text{-invariant } j_0 \text{ are ordinary}\}$, $\mathbb{E}$ is the canonical lifting of E, and each j_i is a function of j_0. The question of finding

2010 *Mathematics Subject Classification.* Primary 14H52; Secondary 14G05.

Key words and phrases. elliptic curves, Serre-Tate theorem, canonical lifting, division polynomials.

This work has been supported by TÜBİTAK (an agency of the Turkish government).

the canonical lifting in this form was first given in [7]. The first solution of this question was also given there using the classical modular equation. This method has been studied by Satoh, Skjernaa and Taguchi to give an algorithm to find the canonical lifting and to count the rational points on elliptic curves over finite fields [9]. Another remarkable approach was given by Voloch and Walker for finite k. They proved the existence of a section of the reduction mod p map of the homomorphism $\mathbb{E}(W(\bar{k})) \to E(\bar{k})$. This section is called the elliptic Teichmüller lift and its existence is equivalent to say that $\mathbb{E}$ is the canonical lifting in the case of k being a finite field. The study of the elliptic Teichmüller lift has been made by Finotti and it has been used to determine the structure of Θ [3].

Here we will consider elliptic curves defined over imperfect fields and study the canonical lifting of these elliptic curves. We will work on the reduction of the canonical lifting modulo prime powers, i.e. on the canonical lifting over Witt vectors of finite length denoted by $W_n(k)$. We will prove that the canonical lifting is compatible with the field over which the given ordinary elliptic curve is defined. Explicitly we will prove the following theorem.

Theorem 1. *Let K be a field of characteristic $p \geq 5$, $n \geq 2$ be an arbitrary integer and E be an ordinary elliptic curve over K. Let $\mathrm{Can}(E)$ be the class of isomorphisms of the canonical lifting of E over $W_n(\bar{K})$. Then there exists $\mathbb{E} \in \mathrm{Can}(E)$ which is defined over $W_n(K)$, i.e. which can be given by a single Weierstrass equation with coefficients in $W_n(K)$. In particular if we denote the j-invariant of $\mathbb{E}$ by $j(\mathbb{E}) = (j_0, j_1, \dots, j_n)$ then each j_n is an element of K.*

This theorem was proved in [3] in a computational way using Greenberg transforms and elliptic Teichmüller lift. Also a similar result for separably closed K using fppf-cohomology theory has been given in [1]. Here we give another proof based on a simple fact which is directly used in the proof of the Serre–Tate theorem in [5]. Naively we can state the idea of the proof as follows: the canonical lifting is the unique lifting which has “lots of” nontrivial p-th power torsion points and the existence of these points force the existence of the desired Weierstrass model.

We proceed as follows. First we give a brief overview of some aspects of the Serre–Tate theorem. We restrict ourselves only to facts which we will need in the proof. We will need some basic computational facts about Witt vectors. The statements which we do not prove here in detail are easy consequences of results in [10, §2.4-5]. We may also use some well known results about division polynomials without any reference.

We fix the following notation. For any field k we denote by k' and k^s the perfect and separable closures of k respectively. For any scheme T and any group scheme G/T, $G[N]$ denotes the kernel of the multiplication by N on G. If G is a p-divisible group then we may write $G = (G_n, i_n)$, where $G_n = \ker(p^n : G \longrightarrow G)$ and $i_n : G_n \hookrightarrow G_{n+1}$. For any elliptic curve X/k, T_pX denotes the usual Tate module. If G is the p-divisible group associated to an elliptic curve X/T then we may use $X[p^\infty]$ for G. For any group G, we write G^0 and G^{et} for the maximal connected subgroup and the étale quotient of G respectively (see [12] and [13] for the definition-construction of these groups).

2. An overview of the Serre–Tate theorem

Let X be an ordinary elliptic curve over an algebraically closed field k of characteristic $p > 0$, and B be an Artin local ring with residue field k. We denote any lifting of X/k over B by $\mathbb{X}$. Then we have the following exact sequences

$$0 \to \hat{X}(= X[p^\infty]^0) \to X[p^\infty] \to X[p^\infty]^{et} \to 0,$$
$$0 \to \hat{\mathbb{X}}(= \mathbb{X}[p^\infty]^0) \to \mathbb{X}[p^\infty] \to \mathbb{X}[p^\infty]^{et} \to 0,$$

where the first and the last nonzero p-divisible groups are of height 1, and so the middle one is of height 2 in both sequences. Also $\hat{X}$ and $\hat{\mathbb{X}}$ are Cartier duals of $X[p^\infty]^{et}$ and $\mathbb{X}[p^\infty]^{et}$ respectively. Since k is algebraically closed we have the isomorphism $X[p^\infty]^{et} \overset{\sim}{\to} \mathbb{Q}_p/\mathbb{Z}_p = (X(k)[p^n], i_n)$ where we see $X(k)[p^n]$ as the constant étale group $\mathbb{Z}/p^n\mathbb{Z}$ over k. By the same reason the first sequence splits. Now for each n the isomorphism of B-groups

$$\hat{\mathbb{X}}[p^n] \overset{\sim}{\to} \mathrm{Hom}_{\mathbb{Z}}(X(k)[p^n], \mu_{p^n})$$
$$\hat{\mathbb{X}} \overset{\sim}{\to} \mathrm{Hom}_{\mathbb{Z}_{\mathrm{l}}}(T_pX(k), \mathbb{G}_m),$$

which are obtained from the isomorphism of k-groups

$$\hat{X}[p^n] \overset{\sim}{\to} \mathrm{Hom}_{\mathbb{Z}}(X(k)[p^n], \mu_{p^n})$$
$$\hat{X} \overset{\sim}{\to} \mathrm{Hom}_{\mathbb{Z}_{\mathrm{l}}}(T_pX(k), \mathbb{G}_m),$$

give us the perfect pairings

$$E_{p^n,\mathbb{X}} : \hat{\mathbb{X}}[p^n] \times X(k)[p^n] \to \mu_{p^n}$$
$$E_{\mathbb{X}} : \hat{\mathbb{X}} \times T_pX(k) \to \mathbb{G}_m$$

for each n, where $\mathbb{G}_m := \operatorname{Spec} k[x, x^{-1}]$ is the multiplicative group and $\mu_{p^n} := \mathbb{G}_m[p^n]$.

Now we can construct a map $T_pA(k) \to \hat{\mathbb{X}}(R)$. Let I be the maximal ideal of B and r be a sufficiently large integer such that $I^{r+1} = 0$. Since $\hat{\mathbb{X}}$ is a formal Lie group over B, every element of $\hat{\mathbb{X}}$ is killed by p^r. Now for any $P \in X(k)$ define $\phi_r(P) = p^r(\hat{P})$, where $\hat{P} \in \mathbb{X}(B)$ is any lifting of P. This gives a map from $X(k)$ into $\mathbb{X}(B)$. Note that this map is independent of the choice of $\hat{P}$ and so well-defined. The image of $X(k)[p^n]$ is in $\hat{\mathbb{X}}(B)$. So we get a homomorphism $\phi_r : X(k)[p^n] \to \hat{\mathbb{X}}(B)$ which is compatible with $p^i : X(k)[p^{r+i}] \to X(k)[p^r]$. Thus we obtain a single homomorphism

$$\phi_{\mathbb{X}} : T_pX(k) \xrightarrow{\pi_{\mathrm{r}}} X(k)[p^r] \xrightarrow{\phi_{\mathrm{r}}} \hat{\mathbb{X}}(B).$$

We define

$$q_{\mathbb{X}/B} : T_pX(k) \otimes T_pX(k) \to \mathbb{G}_m(B)$$
$$q_{\mathbb{X}/B}(\alpha, \beta) = E_{\mathbb{X}}(\phi_{\mathbb{X}}, \beta).$$

Since the pairing $E_{\mathbb{X}}$ is perfect, $q = 1$ if and only if $\phi_{\mathbb{X}} = O$, where O is the identity element. The canonical lifting of X is defined to be the elliptic curve $\mathbb{X}$ such that the corresponding q is identically one. In other words $\mathbb{X}$ is the canonical lifting of X if and only if $\phi_r = O$. Note that the only condition on r is that $I^{r+1} = 0$. If we set $r' = \min\{r \in \mathbb{N} : I^{r+1} = 0\}$ we obtain the following corollary.

Corollary 1. *With the previous notation the following are equivalent.*

(1) $\mathbb{X}$ *is the canonical lifting of* X.
(2) $\phi_{r'} = O$.
(3) $\phi_r = O$ *for some (hence all)* $r \geq r'$.

3. Proof of the main theorem

Here we will prove Theorem 1. We will use Corollary 1 for $B = W_{n+1}(k)$ and $r = n+1$. Note that $X(k)[p^{n+1}] \xrightarrow{\sim} \mathbb{Z}/p^{n+1}\mathbb{Z}$ is cyclic so it is enough to show that $\phi_r(P) = O$ for some generator $P \in X(k)[p^{n+1}]$. We will need the following lemma.

Lemma 1. *Let* K *be any field of characteristic* $p > 0$ *and* E *be an ordinary elliptic curve over* K *given by an affine Weierstrass equation*

$$E : f(x_0, y_0) = 0.$$

Let $P = (x_0, y_0) \in E(\bar{K})$ *be any point. If* $p^n P \in E(K)$ *then* $x_0^{p^n} \in K^s$. *In particular if* $P = (x_0, y_0) \in E[p^n](\bar{K})$ *then* $x_0^{p^n} \in K^s$.

Proof. Let $E^{(p^n)} = E \otimes_K K$, where the product is taken via the p^n-th power homomorphism $p^n : K \to K$. Then we have the relative Frobenius $F^n : E \to E^{(p^n)}$ which simply sends (x_0, y_0) to $(x_0^{p^n}, y_0^{p^n})$. Now $p^n : E \to E$ factors through F^n as $p^n : E \xrightarrow{\mathrm{F^n}} E^{(p^n)} \xrightarrow{\mathrm{V^n}} E$, where V^n is the dual of F^n called Verschiebung. Since E is ordinary, V^n is an étale map [6, §12.3.6]. Let $P : \operatorname{Spec} \bar{K} \to E$ be a point such that $p^n P$ is a K-point. This means that $p^n P : \operatorname{Spec} \bar{K} \to E$ factors through $\operatorname{Spec} K$. Then we have the following commutative diagram.

$$\begin{tikzcd}
\operatorname{Spec} \bar{K} \arrow[r, "F^n \circ P"] \arrow[d] & E^{(p^n)} \arrow[d, "V^n"] \\
\operatorname{Spec} K \arrow[r] & E
\end{tikzcd}$$

Let $Q \in E$ be the image of $\operatorname{Spec} K$. Then $\hat{Q} := F^n \circ P(\operatorname{Spec} \bar{K}) \in (V^n)^{-1}(Q)$. Since V^n is étale we have that the residue field of $E^{(p^n)}$ at $\hat{Q}$ denoted by $\kappa(\hat{Q})$ is a separable extension of the residue field of E at Q which is just K. This implies that $F^n \circ P$ factors through $\operatorname{Spec} K^s$, i.e. we have the composition

$$F^n \circ P : \operatorname{Spec} \bar{K} \to \operatorname{Spec} K^s \to E^{(p^n)}.$$

Thus $F^n \circ P$ is a K^s-point, i.e. $x_0^{p^n} \in K^s$. □

By Corollary 1 it is enough to work with p-th power torsion points to find the canonical lifting. Now we will give some basic facts about division polynomials which we will need in the proof. Any elliptic curve C over any scheme on which 6 is invertible can be (Zariski) locally given by equations of the form $Y^2 = X^3 + AX + B$ [6, §2.2]. This condition is satisfied in our case as we assume $p \geq 5$. Since we will work on the local ring $W_n(K)$ we may assume that we have a single global Weierstrass equation of this form. Let N be a positive integer. Let $\Psi = \Psi_{C,N}$ be the N-division polynomial, i.e. the polynomial whose roots give the x-coordinates of the nontrivial N-torsion points. We say that a point $P \in C(W_n(\bar{K}))$ is nontrivial if $P \pmod p \neq O$. It is well known that if N is odd, then $\Psi \in \mathbb{Z}[A,B][x]$ [11].

Now we explain what we mean by saying that the canonical lifting has "lots of" nontrivial p-th power torsion points. Let $\mathbb{E}$ be the canonical lifting of E. Take a non-identity point $P = (x_0, y_0) \in E(\bar{K})[p^r]$ for some $r \geq n$. Take any lifting $\hat{P} \in \mathbb{E}(W_n(\bar{K}))$. Then by Corollary 1, $\hat{P}$ must be a p^r-torsion point. The converse is also true, i.e. if any lifting $\hat{P} \in \mathbb{E}(W_n(\bar{K}))$ of any $P \in E(\bar{K})[p^r]$ for some $r \geq n$ is a p^r-torsion point then $\mathbb{E}$ is the canonical lifting. If we put $\hat{P} = ((x_0, x_1, \ldots, x_{n-1}), (y_0, y_1, \ldots, y_{n-1}))$ then $\Psi((x_0, x_1, \ldots, x_{n-1})) = 0$ for infinitely many $x_1, x_2, \ldots, x_n$. This obviously puts a condition on the coefficients of Ψ. As the coefficients of Ψ are completely determined by A and B this *a posteriori* puts a condition on A and B.

In [2], Cassels shows that for any N, the division polynomials $\Psi = \Psi_N$ of such a cubic equation is defined over $\mathbb{Z}[A,B]$ and satisfy $(\Psi^2)' \equiv 0 \,(\mathrm{mod}\ N)$, where $()'$ means the derivative with respect to x. This result will play a key role in the proof.

Now fix K, p, n and an ordinary elliptic curve

$$E : y_0^2 = x_0^3 + a_0 x_0 + b_0$$

as stated in Theorem 1, where $a_0, b_0 \in K$. Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be algebraically independent indeterminates and consider the Weierstrass equation

$$\begin{aligned}\mathbb{E} : (y_0, y_1, \ldots, y_n)^2 = (x_0, x_1, \ldots, x_n)^3 &+ (a_0, a_1, \ldots, a_n)(x_0, x_1, \ldots, x_n) \\ &+ (b_0, b_1, \ldots, b_n)\end{aligned}$$

defined over $W_{n+1}(F)$, where $F = K(\{a_i, b_i\})$. It maps to E under the reduction map $W_{n+1}(F) \to F$ so it defines an elliptic curve over $W_{n+1}(F)$. Since $\mathrm{char}(K) \neq 2$ we have that for any odd N, $\Psi\Psi' \in N.W_{n+1}(F)[x]$. We can state this in a different way as the following technical lemma.

Lemma 2. *The p^{n+1}-division polynomial Ψ of $\mathbb{E}$ satisfies $\Psi' \in p^{n+1}.W_{n+1}(F)[x]$, i.e. $\Psi' = 0$ in $W_{n+1}(F)[x]$.*

Proof. Since $p^{n+1} = 0$ in $W_{n+1}(F)[x]$, $\Psi' \neq 0$ implies that Ψ is a zero divisor in the polynomial ring $W_{n+1}(F)[x]$. This can occur if and only if there exists a nonzero $A \in W_{n+1}(F)$ such that $A\Psi = 0$. But by construction $\Psi(\mathrm{mod}\ p) = \Psi_{E,p^n}(x)$ is not identically zero. Thus coefficients of some terms of Ψ are nonzero modulo p, i.e. they are units in $W_{n+1}(F)$. So $A\Psi = 0$ can not occur for any nonzero A, i.e. Ψ can not be a zero divisor. So we have $\Psi' = 0$. □

Now we give a proposition about the structure of p-th power division polynomials of $\mathbb{E}$.

Proposition 1. *Let E and $\mathbb{E}$ be given as above. Then the p^{n+1}-division polynomial Ψ of $\mathbb{E}$ is of the form $\Psi = (\Psi_0, \Psi_1, \ldots, \Psi_n)$, where each Ψ_i is a polynomial of $x_0^{p^{n+1}}$ over the ring $\mathbb{Z}[a_0, a_1, \ldots, a_i, b_0, b_1, \ldots, b_i]$. Moreover Ψ_i is linear with respect to a_i and b_i, i.e. $\Psi_i = \alpha_i a_i + \beta_i b_i + \gamma_i$ for some α_i, β_i, $\gamma_i \in \mathbb{Z}[a_0, a_1, \ldots, a_{i-1}, b_0, b_1, \ldots, b_{i-1}, x_0^{p^{n+1}}]$.*

Proof. Let $\Psi = \Psi_{\mathbb{E},p^{n+1}} = A_l + A_{l-1}X + \cdots + A_1 X^{l-1} + A_0 X^l$, where $A_i \in W_{n+1}(F)$ and $X = (x_0, x_1, \ldots, x_n)$. Indeed A_i are polynomials with integer coefficients in the variables $(a_0, a_1, \ldots, a_n), (b_0, b_1, \ldots, b_n)$. To simplify computations which will be made below, we may consider A_i as an element in $W_{n+1}(\bar{F})$ via the inclusion map $W_{n+1}(F) \hookrightarrow W_{n+1}(\bar{F})$. By Lemma 2 for each monomial $A_i X^{l-i}$ of Ψ we have that $(l-i)A_i \in (p^{n+1})$. Let ν_p denote the p-adic valuation of rational integers. Let $\nu_p(l-i) = t_i$ and $l - i = p^{t_i} v_i$ for some non-negative rational integer v_i. If $t_i > n+1$ then

$$X^{v_i p^{t_i}} = (x_0, x_1, \ldots, x_n)^{v_i p^{t_i}} = (x_0^{v_i p^{t_i}}, 0, \ldots, 0).$$

If $t_i \leq n+1$, then $A_i \in (p^{n+1-t_i})$. Since $\operatorname{char}(F) = p$ we have

$$\begin{aligned} X^{p^{t_i}} = (x_0, x_1, \ldots, x_n)^{p^{t_i}} &= (x_0^{p^{t_i}}, 0, 0 \ldots, 0, y_{j+1}, y_{j+2}, \ldots, y_n) \\ &= (x_0^{p^{t_i}}, 0, 0 \ldots, 0) + (0, 0, 0 \ldots, 0, y'_{j+1}, y'_{j+2}, \ldots, y'_n), \end{aligned}$$

where y_s and y'_s are some polynomials in x_i, $j \geq t_i$ and the coordinates of both y_{j+1} and y'_{j+1} are $(j+1)$. Put $u = (x_0^{p^{t_i}}, 0, 0 \ldots, 0)$ and $\pi = (0, 0, 0 \ldots, 0, y'_{j+1}, y'_{j+2}, \ldots, y'_n)$. So we have $A_i X^{l-i} = A_i(u+\pi)^{v_i}$. To ease notation we set $r = n+1-t_i$ and $A_i = (0, 0, \ldots, 0, c_r, c_{r+1}, \ldots, c_n)$. Note that $\pi p^{n+1-t_i} = 0$ and so $A_i X^{l-i} = A_i u^{v_i}$. Thus in any case we have

$$\begin{aligned} A_i X^{l-i} = A_i(x_0^{v_i p^{t_i}}, 0, 0, \ldots, 0) &= (0, \ldots, 0, c_r (x_0^{v_i p^{t_i}})^{p^r}, c_{r+1} (x_0^{v_i p^{t_i}})^{p^{r+1}}, \ldots) \\ &= (0, \ldots, 0, c_r x_0^{v_i p^{n+1}}, c_{r+1} x_0^{v_i^p p^{n+1}}, \ldots). \end{aligned}$$

But A_i is a polynomial in $(a_0, a_1, \ldots, a_n)$ and $(b_0, b_1, \ldots, b_n)$ with integer coefficients, so we have that each c_s is a polynomial in $a_0, a_1, \ldots, a_s, b_0, b_1, \ldots, b_s$ with integer coefficients. By addition and multiplication rules of the ring of Witt vectors we can see that c_s is linear with respect to a_s and b_s. Adding all the monomials $A_i X^{l-i}$ we can see that Ψ is of the desired form. □

After this preparation we can start the proof of Theorem 1.

Proof of Theorem 1. Since $p \geq 5$ any elliptic curves E/K and $\mathbb{E}/W_n(\bar{K})$ can be given by Weierstrass models

$$\begin{aligned} &E : y_0^2 = x_0^3 + a_0 x_0 + b_0 \\ &\mathbb{E} : (y_0, y_1, \ldots, y_n)^2 = (x_0, x_1, \ldots, x_n)^3 + (a_0, a_1, \ldots, a_n)(x_0, x_1, \ldots, x_n) \\ &\qquad\qquad + (b_0, b_1, \ldots, b_n). \end{aligned}$$

We denote the j-invariant of E by j. If $j \neq 0, 1728$ then we put $t_0 = j/(1728 - j)$, $a_0 = 3t_0$ and $b_0 = 2t_0$. Then E becomes $y_0^2 = x_0^3 + 3t_0 x_0 + 2t_0$. Similarly we put

$(a_0, a_1, \ldots, a_n) = 3(t_0, t_1, \ldots, t_n)$ and $(b_0, b_1, \ldots, b_n) = 2(t_0, t_1, \ldots, t_n)$, where t_i for $i \geq 1$ are independent variables. If $j = 0$ we set $a_i = 0$ and $b_i = t_i$ for $i = 0, 1, \ldots, n$. Similarly if $j = 1728$ then we set $b_i = 0$ and $a_i = t_i$ for $i = 0, 1, \ldots, n$. So in any case Ψ_i can be written as a polynomial in $x_0^{p^{n+1}}$ and t_j over $\mathbb{Z}$ for $j \leq i$, and is linear with respect to t_i. So for $i \geq 1$ we can write $\Psi_i = \alpha_i t_i + \beta_i$, where α_i, $\beta_i \in \mathbb{Z}[t_0, t_1, \ldots, t_{i-1}, x_0^{p^{n+1}}]$. Now we take a generator $P = (x_0, y_0) \in E(\bar{K})[p^{n+1}]$. Note that Ψ_0 is the p^{n+1}-division polynomial of the ordinary elliptic curve E/K. So for $P = (x_0, y_0) \in E[p^{n+1}](\bar{K})$ we have that $\Psi_0(x_0) = 0$.

Now we do induction. For $i = 1$, both α_1 and β_1 is a polynomial in t_0, and $x_0^{p^{n+1}}$. The existence of the canonical lifting guarantees at least one solution of $\alpha_1 t_1 + \beta_1 = 0$ for some $t_1 \in \bar{K}$. So either $\alpha_1 \neq 0$ or $\alpha_1 = \beta_1 = 0$. In the second case we can choose $t_1 \in K$. So we may only consider the first case, i.e. the case where $t_1 = \beta_1/\alpha_1$ is uniquely determined. But note that t_i is independent of the choice of x_0. We can replace $P = (x_0, y_0)$ by any other $P = (x_0', y_0') \in E[p^{n+1}](\bar{K})$. Now let G be the absolute Galois group of K. For any $\sigma \in G$ and $x_0 \in L_n$ we have that $\sigma(x_0) \in L_n$ because the division polynomials are defined over $\mathbb{Z}[t_0]$ and $t_0 \in K$. So we may replace x_0 by $\sigma(x_0)$ for any $\sigma \in G$. If we see α_1 and β_1 as functions of x_0 we have that

$$\sigma(\alpha_1(x_0)) = \alpha_1(\sigma(x_0))$$
$$\sigma(\beta_1(x_0)) = \beta_1(\sigma(x_0)).$$

Thus we can see t_1 as the unique solution of the system of equations

$$\{\sigma(\alpha_1(x_0))t_1 + \sigma(\beta_1(x_0)) = 0\}_{\sigma \in G}.$$

But this implies that β_1/α_1 is fixed by G and so $t_1 = \beta_1/\alpha_1 \in K' \cap K^s = K$. Now assume that we can find $t_j \in K$ such that $\alpha_j t_j + \beta_j = 0$ for any $j = 1, 2, \ldots, i-1$ and $x_0 \in L_n$. Again we obtain a linear equation $\alpha_i t_i + \beta_i = 0$. By the same argument of the initial step we can see that t_i is either uniquely determined or can be arbitrarily chosen in $\bar{K}$ according to whether $\alpha_i = 0$ or not. In the first case we again see that G fixes $\beta_i \alpha_i$ which implies that t_i must be in K. This completes the proof. □

It may be possible to drop the assumption $p \geq 5$ in the theorem. Note that if $p = 2$ or 3 any elliptic curve given by the Weierstrass equation

$$y^2 = x^3 + Ax + B$$

is supersingular. In [2], Cassels starts with an equation of this form and proves that $(\Psi_N^2)' \cong 0 \pmod{N}$. If this result can be improved for other types of Weierstrass equations which correspond to ordinary elliptic curves for $p = 2$ and 3 then Theorem 1 can be easily generalized to any positive characteristic. But in any case we can use the method of the proof to compute the canonical lifting. We give a simple example to illustrate this.

Let $k = \mathbb{F}_3$ and J be an indeterminate. Consider the elliptic curve E defined over $k(J)$

$$E : y_0^2 = x_0^3 + x_0^2 - t_0.$$

Note that $j(E) = 1/t_0$, so E is ordinary. Also for any $t_0 \in \bar{k}^*$, E is an ordinary elliptic curve over $\bar{k}$. One can easily see that $P = (x_0, y_0) = (t_0^{1/3}, t_0^{1/3})$ is a 3-torsion point. Now we take a general Weierstrass equation over $W_2(k(J))$ lifting the above one

$$\mathbb{E} : (y_0, y_1)^2 = (x_0, x_1)^3 + (x_0, x_1)^2 + (-t_0, t_1).$$

So in the notation of Corollary 1 we have $r' = 1$. Although in the proof we used $p^{r'+1}$-torsion points for simplicity, it is enough to work with p^r-torsion points in practice. Let $\hat{P} = ((t_0^{1/3}, x_1), (t_0^{1/3}, y_1))$ be any lifting of P. We want that $3\hat{P} = O$, i.e. $2\hat{P} = -\hat{P}$. So we just need to equate the x-coordinates of $2\hat{P}$ and $-\hat{P}$. Now by an easy computation using the doubling formula we can see that t_1 satisfies the equation

$$x_0^{12} - x_0^3 t_0^3 - x_0^6 t_0 + x_0^3 t_0^2 + t_1 = 0.$$

Putting $x_0 = t_0^{1/3}$ we see that $t_1 = 0$.

References

[1] A. Erdoğan, *A universal formula for the j-invariant of the canonical lifting*, Ph.D. Thesis, Koç University, Turkey, 2013.

[2] J. W. S. Cassels. A note on the division values of $\wp(u)$, *Proc. Cambridge Philos. Soc.*, 45(2): 167–172, 1949. MR 0028358.

[3] L. R. A. Finotti. Lifting the j-invariant: questions of Mazur and Tate, *J. Number Theory*, 130(3): 620–638, 2010. MR 2584845.

[4] A. Grothendieck. EGA IV. Étude locale des schémas et des morphismes de schémas. Inst. Hautes Études Sci. Publ. Math., no. 32, 1967. MR 0238860.

[5] N. Katz. Serre–Tate local moduli, in: Surfaces algébriques, Séminaire de Géométrie Algébrique d'Orsay 1976-78, 138–202, Lecture Notes in Math., 868, Springer, Berlin-New York, 1981. MR 0638600.

[6] N. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, 108, Princeton University Press, 1985. MR 0772569.

[7] J. Lubin, J.-P. Serre and J. Tate. Elliptic curves and formal groups, Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts, July 6-July 31, 1964.

[8] W. Messing. *The crystals associated to Barsotti–Tate groups, with applications to abelian schemes*, Lecture Notes in Mathematics, 264, Springer-Verlag, 1972. MR 0347836.

[9] T. Satoh, B. Skjernaa, Y. Taguchi. Fast computation of canonical lifts of elliptic curves and its application to point counting *Finite Fields Appl.*, 9(2): 89–101, 2003. MR 1954785.

[10] J.-P. Serre. *Local fields*, Springer-Verlag, 1979. MR 0554237.

[11] J. Silverman. *The arithmetic of elliptic curves*, Springer-Verlag, Graduate Texts in Mathematics, 106, 1986. MR 0817210.

[12] J. Tate. Finite flat group schemes, in: *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, 121–154, Springer, 1997. MR 1638478.

[13] J. Tate. p-divisible groups, in: Proc. Conf. Local Fields (Driebergen, 1966), 158–183, Springer, 1967. MR 0231827.

A. Erdoğan
Affiliation at time of submission: Department of Mathematics, Koç University, Rumelifeneri
Yolu, 34450 Sarıyer, İstanbul, Turkey
Affiliation at time of publication: Department of Mathematics, Gebze Institute of Technology,
P.K. 141 41400 Gebze, Kocaeli, Turkey
alerdogan@gyte.edu.tr

Received: October 2, 2013
Accepted: August 26, 2014