A Universal Formula for the j-invariant of the Canonical Lifting

by

Altan Erdoğan

A Thesis Submitted to the
Graduate School of Sciences and Engineering
in Partial Fulfillment of the Requirements for
the Degree of

Doctor of Philosophy
in
Mathematics

Koç University

August 2013

A Universal Formula for the j-invariant of the Canonical Lifting

by

Altan Erdoğan

A Thesis Proposal
submitted to the Thesis Supervisory Committee
in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy

Koç University

August 2013

Koç University

Graduate School of Sciences and Enginerring

This is to certify that I have examined this copy of a PhD thesis by

Altan Erdoğan

and have found that it is complete and satisfactory in all respects, and that any and all revisions required by the final examining committee have been made.

Committee Members:

Sinan Ünver, Ph.D. (Thesis Supervisor)	.....
Kazım Büyükboduk, Ph.D.	.....
Muhammed Uludağ, Ph.D.	.....
Tolga Etgü	.....
Arzu Boysal	.....

DATE: 25.08.2013

ABSTRACT

In this thesis we study the j-invariant of the canonical lifting of an elliptic curve as a Witt vector. It is proved that its Witt coordinates lie in the open affine subset of the j-line determined by the ordinary locus which implies the existence of a universal formula for the j-invariant of the canonical lifting. Canonical lifting of elliptic curves over imperfect fields are also analyzed and the notion of the canonical lifting is generalized for elliptic curves defined over bases which are not necessarily fields. The canonical lifting of the elliptic curves with some specific j-invariants are also explicitly computed.

ÖZET

Bu tezde eliptik eğrilerin kanonik uzamalarının j-invaryantları Witt vektörü olarak incelenmiştir. Bu Witt koordinatlarının j-doğrusunun adi noktalar tarafından belirlenen açık afin altkümesinin içinde olduğu ve bu sayede kanonik uzamanın j-invaryantı için evrensel bir formülün varlığı ispatlanmıştır. Ayrıca mükemmel olmayan cisimler üzerinde tanımlı eliptik eğrilerin kanonik uzamaları incelenmiştir ve kanonik uzama kavramı cisimler üzerinde tanımlı olmayan eliptik eğrilere genelleştirilmiştir. Bazı özel j-invaryantlara sahip eliptik eğrilerin kanonik uzamaları da açıkça bulunmuştur.

ACKNOWLEDGEMENTS

It was an honor to have Sinan Ünver as my thesis supervisor. I am deeply thankful for his endless guidance, support and patience he showed me throughout the years I spent in the department.

I also deeply thank to Kazım Büyükboduk, Muhammed Uludağ, Tolga Etgü and Arzu Boysal for participating in my thesis committee. I would like to express my sincere gratitude to all faculty members of mathematics department for their contributions to such a supporting, motivating and encouraging ambient of this department.

I would like to express my gratitude to Brian Conrad for his invaluable comments and suggestions about the topic of this thesis.

I am thankful to all of my officemates for the years we spent with frienship, support and efforts for the will of mathematics.

I thank to TÜBTAK for the financial support provided throughout my graduate study.

Finally I am deeply grateful to my love Cansu for her sincere support and encouragement.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

Let k be an algebraically closed field of characteristic p and $W(k)$ be the ring of p-typical Witt vectors of k. Let A be an ordinary abelian variety over k. A consequence of the Serre-Tate theorem is that up to isomorphism there exists a unique abelian scheme $\mathbb{A}$ over $W(k)$ such that

1. $\mathbb{A} \otimes_{W(k)} k \xrightarrow{\sim} A$,
2. $\mathrm{End}_{W(k)}(\mathbb{A}) \xrightarrow{\sim} \mathrm{End}_k(A)$

where both isomorphisms are obtained via the reduction $(\mathrm{mod}\ p) : \mathbb{A} \to A$. This abelian scheme $\mathbb{A}$ is called the canonical lifting of A. We will see and use some of the other equivalent characterizations of the canonical lifting throughout this thesis.

In general it is not an easy question to completely determine the canonical lifting of a given abelian variety. There are various works on the computation of the canonical lifting of elliptic curves which allow us to derive algorithms with satisfactory complexities with different applications (See [9], [14]) .

In the case of elliptic curves we can reformulate the problem of finding canonical lifting in terms of the j-invariants as follows. Let E be an ordinary elliptic curve over k and $\mathbb{E}$ be its canonical lifting. 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. If we set

$$k^{\mathrm{ord}} = \{j_0 \in k | \text{ elliptic curves with } j\text{-invariant } j_0 \text{ are ordinary}\}$$

then we can define the following function;

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

where $\mathbb{E}$ is the canonical lifting of E and each j_i is a function of j_0. The question of finding the canonical lifting in this form was first given in [7]. The first solution of this question which uses the classical modular equation was also given there.

In this thesis we will focus on the structure of j_i considered as a function of j_0. It was proved that j_i is a rational function of j_0 [2], but a complete description of j_i was not given. A first guess is that each j_i may be a polynomial of j_0. We will see that this is almost true, i.e. each j_i is a rational function of j_0 where the set of all poles of all j_i is a subset of supersingular j-values and hence finite. We also obtain a complete result for the coefficients of j_i seen as a rational function of j_0. Explicitly we will prove the following theorem.

Theorem 1.1 (Main theorem)**.** *Let F be a perfect field of characteristic $p > 0$ with a fixed algebraic closure k, and J be an indeterminate. Let $\phi_p(J)$ denote the* Hasse polynomial*, i.e. the polynomial in $\mathbb{F}_p[J]$ whose roots are the supersingular j-values in characteristic p. Let*

$$A = F[J, 1/\phi_p(J)].$$

(i) *There exist* $f_i \in A$ *for all* $i \in \mathbb{Z}_{\geq 1}$ *such that for any* $j_0 \in k^{\mathrm{ord}}$,

$$\Theta(j_0) = (j_0, f_1(j_0), f_2(j_0), ...f_n(j_0), ...)$$

where for any such j_0 *we see* $f_i \in A$ *as the homomorphism defined as*

$$j_i : A \longrightarrow k, \quad J \longmapsto j_0$$

(ii) *If* $j_0 = 0$ *is an ordinary* j*-value then* $\Theta(0) = 0 \in \mathbb{Z}_p$*, and similarly if* $j_0 = 1728$ *is an ordinary* j*-value then* $\Theta(1728) = 1728 \in \mathbb{Z}_p$.

The first assertion of the theorem mean that we have a universal formula for the j-invariant of the canonical lifting, and Witt entries of this universal formula are almost polynomials. The second assertion is independent of the previous one and proved with a different argument.

We proceed as follows. In §2 we give a brief overview of the Serre-Tate theorem. In §3, we generalize the notion of the canonical lifting for elliptic curves defined over $\mathbb{F}_p$-schemes satisfying certain hypotheses. In §4 we use fppf-Kummer theory to analyze the canonical lifting of an elliptic curve defined over an imperfect field. In §5 we give a purely elementary and computational proof of the main results of §4 which allow us to compute the canonical lifting with a different method. Finally in the last chapter we apply the results of §3 and §4 to universal families of ordinary elliptic curves to prove (i) of Theorem 1.1. We also prove (ii) in the last chapter.

We fix the following notation. For any schemes X/T and U/T we set $X_U := X \times_T U$. If $U = \mathrm{Spec}\, C$ is affine, we may use X_C instead of X_U. If $T = \mathrm{Spec}\, B$ is also affine, we may also use $X \otimes_B C$ for X_U. For $t \in T$ with residue field $\kappa(t)$, we denote $X \times_T \mathrm{Spec}\, \kappa(t)$ by X_t. For 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 $G_n = \ker(p^n : G_{n+1} \longrightarrow G_{n+1})$ and $i_n : G_n \longrightarrow G_{n+1}$. If X is an abelian variety, we denote the p-divisible group $(X[p^n], i_n)$ associated to X by $X[p^\infty]$.

Chapter 2

AN OVERVIEW OF THE SERRE-TATE THEOREM

In this chapter we briefly recall some aspects of the Serre-Tate theorem. We restrict ourselves to the definition-construction of the canonical lifting which is directly used in the proofs. General references for a complete proof and a detailed analysis of the Serre-Tate theorem are [5] and [8]. For the sake of completeness we quote the following theorem from [5] and call it as the *general Serre-Tate theorem.*

Theorem 2.1 (General Serre-Tate theorem)**.** *Let A be a ring in which p is nilpotent. Let I be a nilpotent ideal of A, and put $A_0 = A/I$. Let* $\mathrm{AS}(A)$ *denote the category of abelian schemes over A, and let* $\mathrm{Def}(A, A_0)$ *denote the category of triples (X_0, L, ϵ) where X_0 is an abelian scheme over A_0, L is a p-divisible group over A and $\epsilon : L_0 := L \otimes_A A_0 \longrightarrow A_0[p^\infty]$ is an isomorphism. Then the functor*

$$X \longmapsto (X_0, X[p^\infty], \text{the natural map})$$

is an equivalence of the categories $\mathrm{AS}(A)$ *and* $\mathrm{Def}(A, A_0)$*.*

Let k be an algebraically closed field of characteristic $p > 0$ and A be an Artin local ring with residue field k. In general we say that a lifting of a scheme $X \longrightarrow \operatorname{Spec} k$ is a pair $(\mathbb{X}, \iota)$ where $\mathbb{X} \longrightarrow \operatorname{Spec} A$ is a scheme over $\operatorname{Spec} A$ and $\iota : \mathbb{X} \otimes_A k \xrightarrow{\sim} X$ is an isomorphism.

If ι is unique we omit it and just say that $\mathbb{X} \longrightarrow \operatorname{Spec} A$ is a lifting of $X \longrightarrow \operatorname{Spec} k$. We can replace $\operatorname{Spec} A$ by any scheme with some residue field k and still can define a lifting in a similar way, but for our purposes we only consider lifting over Artin local rings. Given an ordinary abelian variety X over k, the Serre-Tate theorem classifies all abelian schemes defined over A that lift X. For such an ordinary abelian variety $X \longrightarrow \operatorname{Spec} k$ and an abelian scheme $\mathbb{X} \longrightarrow \operatorname{Spec} A$ lifting X/k, there are the associated p-divisible groups (= Barsotti-Tate groups) denoted by $X[p^\infty]$ and $\mathbb{X}[p^\infty]$ respectively which play an important role summarized in the following diagram;

$$\{\text{Isomorphism classes of } \mathbb{X}/A \text{ lifting } X/k\} \quad \xrightarrow{\sim} \tag{2.1}$$

$$\{\text{Isomorphism classes of } \mathbb{X}[p^\infty]/A \text{ lifting } X[p^\infty]/k\} \quad \xrightarrow{\sim} \tag{2.2}$$

$$\operatorname{Ext}_A(T_p(X)(k) \otimes \mathbb{Q}_p/\mathbb{Z}_p, \operatorname{Hom}_{\mathbb{Z}_p}(T_p(X^D)(k), \hat{\mathbb{G}}_m)) \quad \xrightarrow{\sim} \tag{2.3}$$

$$\operatorname{Hom}_{\mathbb{Z}_p}(T_p(X)(k) \otimes T_p(X^D)(k), \hat{\mathbb{G}}_m(A)),$$

where $T_p(X)(k)$ is the Tate module of X, X^D denotes the dual abelian variety, $\hat{\mathbb{G}}_m$ denotes the formal completion of the multiplicative group $\mathbb{G}_m$ and $\operatorname{Ext}_A(-,-)$ denotes the extension group of A-groups. General references for the properties of p-divisible groups are [13] and [8].

This diagram is the core ingredient of this thesis. We will not give a proof of these equivalences but use them widely. A complete proof can be found in [5] and [8]. Indeed (2.1) is just the general Serre-Tate theorem. We will use it in almost all chapters. The next equivalence (2.2) will be used in §3 and §4 and the last equivalence (2.3) will be used in an indirect way in §5.

The above diagram shows that the set

$$\{\text{Isomorphism classes of } \mathbb{X}/A \text{ lifting } X/k\}$$

has a natural group structure.

Definition. *With the above notation the unique abelian scheme $\mathbb{X}/A$ which corresponds to the identity element of the group*

$$\mathrm{Ext}_A(T_p(X)(k) \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mathrm{Hom}_{\mathbb{Z}_p}(T_p(X^D)(k), \hat{\mathbb{G}}_m))$$

is called the canonical lifting of X/k over A.

Remark 1. In the introduction, the base of the canonical lifting is given to be a characteristic zero integral domain, but here we define it over an Artin local ring which indeed fits well to our purposes. At the end of this chapter we will see that this definition is justified.

Remark 2. If we only assume that k is perfect than the above diagram and the definition still remain valid by a slight change of the objects involved. A complete study of equivalent definitions of the canonical lifting for perfect k can be found in [8, V.3 and the Appendix].

The particular case we are concerned with here is the case where $A = W_n(k)$, the ring of p-typical Witt vectors of length n. Recall that if k is a perfect field of characteristic p then $W_n(k)$ is an Artin local ring with residue field k and maximal ideal (p). See [11] for the definition and basic facts about Witt vectors which we use here. In this case the

canonical liftings $\mathbb{X}_m/W_m(k)$ are compatible with each other, i.e. for any $m \leq n$,

$$\mathbb{X}_n \otimes_{W_n(k)} W_m(k) \xrightarrow{\sim} \mathbb{X}_m.$$

Thus the inverse system $(\mathbb{X}_m/W_m(k))_m$ defines a formal abelian scheme over $W(k)$ which can be algebraicized ([8], §V.3.3). This abelian scheme is defined as the canonical lifting of X/k over $W(k)$, and hence justifies our definition above. If there is no confusion about the base we will just say the canonical lifting of X/k.

Chapter 3

CANONICAL LIFTING OF FAMILIES OF ELLIPTIC CURVES

In this chapter we will show that we can extend the definition of the canonical lifting to elliptic curves defined over $\mathbb{F}_p$-schemes under some hypothesis. This will allow us to mention about the canonical lifting of a family of elliptic curves. Main result of this chapter is Theorem 3.4 which is stated and proved at the end of this chapter.

We fix the following notation for this chapter. Let F be a perfect field of characteristic p and R be a Noetherian integral F-algebra with fields of fractions K. We fix an algebraic closure of K, and denote it by $\bar{K}$. Let K' be the perfect closure of K (i.e. the maximal purely inseparable extension of K) in $\bar{K}$ and R' be the integral closure of R in K'. We also define the subrings

$$R_n = R^{1/p^n} = \{x \in \bar{K} | x^{p^n} \in R\}.$$

Note that R_n is Noetherian, and $R' = \cup_n R_n$. Also the morphism of schemes $\operatorname{Spec} R' \longrightarrow \operatorname{Spec} R$ induced by the inclusion $R \hookrightarrow R'$ is a homeomorphism. If $s' \in \operatorname{Spec} R'$ maps to $s \in \operatorname{Spec} R$ then $\kappa(s')$ is the perfect closure of $\kappa(s)$ [3]. Let E/R be an ordinary elliptic curve in the sense of [6, §2 and §12]. Let $E_n := E \otimes_R R_n$ where the base change is done via the p^n-th root homomorphism $R \longrightarrow R_n$.

Throughout this chapter E/R and E_n/R_n will always denote these elliptic curves defined here. To simplify notation we use E also to denote the base extensions $E \otimes_{R,i} R_n$ and $E \otimes_{R,i} R'$ where i is the inclusion map.

Now let T be the spectrum of a complete Noetherian local ring. Then for any finite locally free group scheme G/T, there is a unique exact sequence called the *connected-étale sequence* of G,

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow G^{et} \longrightarrow 0$$

where G^0 and G^{et} are connected and étale T-group schemes respectively. It is characterized by the fact that for any étale T-group H, any T-group homomorphism $G \longrightarrow H$ factors through $G \longrightarrow G^{et}$ [12]. By passage to limit we have a similar construction for p-divisible groups. If $G = (G_n, i_n)_n$ is a p-divisible group, then $G^0 := (G_n^0, i_n)$ and $G^{et} := (G_n^{et}, i_n)$ are connected and étale p-divisible groups respectively. By [13] we have an exact sequence of p-divisible groups

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow G^{et} \longrightarrow 0.$$

Note that if $T =$Spec F then the connected-étale sequence of G splits. In particular if $\tilde{E}$ is an ordinary elliptic curve over F then the connected-étale sequence of $\tilde{E}[p^\infty]$ splits over F. This fact is very crucial in the construction of the canonical lifting (Recall Remark 2). So in order to generalize the notion of the canonical lifting we need a similar result when F is replaced by another scheme. But *a priori* we don't even know that $E[p^\infty]$ has

a connected-étale sequence over an arbitrary base. The following theorems of Messing which we directly quote from [8] and the Proposition 3.1 below allow us to overcome this problem.

Theorem 3.1. *Let S be any scheme and $f : X \longrightarrow S$ be a finite locally free morphism of schemes. Then the function $s \longmapsto$ (separable rank of X_s) is locally constant on S if and only if there are morphisms $i : X \longrightarrow X'$ and $f' : X' \longrightarrow S$ which are finite and locally free with i radiciel and surjective, f' étale and $f = f' \circ i$. The factorization is unique up to unique isomorphism and is functorial in X/S.*

Proof. [8, §II.4.8]. □

Theorem 3.2. *Let S be a scheme on which p is locally nilpotent, and G be a p-divisible group over S. Then the following conditions are equivalent.*

(i) *G is an extension of an étale p-divisible group by a connected p-divisible group.*

(ii) *The function $s \longmapsto$ (separable rank of $G[p]_s$) is locally constant on S.*

Proof. We only take the relevant parts of [8, §II.4.9]. □

Proposition 3.1. *Let $E[p^n]$ denote the kernel of $p^n : E \longrightarrow E$ and $E[p^\infty]$ be the p-divisible group of E.*

(i) *For each n there is a unique connected- étale sequence*

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

which splits over R_n.

(ii) *There is a unique connected- étale sequence of p-divisible groups*

$$0 \longrightarrow E[p^\infty]^0 \longrightarrow E[p^\infty] \longrightarrow E[p^\infty]^{et} \longrightarrow 0,$$

which splits over R'.

Proof. By hypothesis E is ordinary, so the p-divisible group $G = E[p^\infty]$ satisfy the last condition of Theorem 3.2, and the existence of both sequences follow. Recall the notation we adopted for E, i.e. we can take the base to be R, R_n or R' and so we have the relevant connected- étale sequences over any of these bases. But by the uniqueness assertion of Theorem 3.1 these sequences are compatible with each other in the sense that $E_{R'}[p^n]^0 = (E[p^n]^0)_{R'}$ and similarly for other groups and the other base R_n. Thus the uniqueness of the sequences in the theorem also follow.

The remaining thing is to prove the splitting of the sequences over the specified bases. First note that the splitting of the sequences given in (i) for all n imply the splitting of the sequence given in (ii). Thus we only need to show that

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

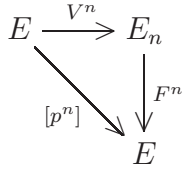
splits over R_n. Also the groups involved here are all commutative, so splitting amounts to giving a chapter of $E[p^n] \longrightarrow E[p^n]^{et}$ over R_n.

Let $F^n : \operatorname{Spec} R_n \longrightarrow \operatorname{Spec} R_n$ be the n-th iterate of the absolute Frobenius of

Spec R_n. Then we have

$$E_n^{(p^n)} := E_n \otimes_{R_n, F^n} R_n = E \otimes_{R,i} R_n (= E).$$

To simplify notation we use F^n also to denote the n-th iterate of the relative Frobenius of E_n; $F^n : E_n \longrightarrow E_n^{(p^n)}$. We denote the dual isogeny of F^n by V^n. Then we have the following commutative diagram



which shows that $\ker(V^n)$ is a subgroup of $E[p^n]$. But since E is ordinary then $\ker(V^n)$ is a finite étale group over R_n [6, §12.3.6]. The inclusion $\ker(V^n) \hookrightarrow E[p^n]$ will give a required section once we can show that $\ker(V^n) \xrightarrow{\sim} E[p^n]^{et}$. Note that this isomorphism holds over algebraically closed fields; since then $E[p^n] = \mu_{p^n} \times \mathbb{Z}/p^n\mathbb{Z}$, and V^n is the identity on μ_{p^n} and kills $\mathbb{Z}/p^n\mathbb{Z}$. Our aim is to reduce to this case. In general the composition

$$\ker(V^n) \longrightarrow E[p^n] \longrightarrow E[p^n]^{et} \tag{3.1}$$

is a group homomorphism, so necessarily commutes with the action of the étale fundamental group (see [12] for the definition of the étale fundamental group). Finally we remark that R_n is Noetherian for any n. Now the following theorem of Grothendieck completes

the proof. □

Theorem. *Let S be a locally Noetherian scheme, α be a geometric point, and $\pi = \pi(S, \alpha)$ be the étale fundamental group of S centered at α. Then the functor $Y \longmapsto Y(\alpha)$ establishes an equivalence between the category of finite étale schemes over S and the category of finite sets with a continuous π action.*

Remark. We need Noetherian hypothesis only in the last step of the proof, i.e. only to use the above theorem of Grothendieck. So the sequences in (i) and (ii) still exist if we drop the Noetherian condition on R.

Remark. The sequence given in (ii) of Proposition 3.1 also captures the connected- étale sequence of the fibre $\kappa(s')$ for any $s' \in \operatorname{Spec} R'$ in the following sense;

$$(E[p^\infty]^{et})_{s'} = (E_{s'}[p^\infty])^{et} \quad \text{and} \quad (E[p^\infty]^0)_{s'} = (E'_s[p^\infty])^0.$$

Now we will use Proposition 3.1, and the general Serre-Tate theorem to find a good lifting of $E(= E_{R'})$ to $W_m(R')$ for each m. We will need the following important theorem of Grothendieck.

Theorem 3.3. *Let A be a ring, I an ideal of A. Suppose that A is complete and separated with respect to topology defined by the ideal I. Put $A_0 = A/I$. Then the functor*

$$X \longmapsto X \otimes_A A_0$$

establishes an equivalence between the category of finite étale A-schemes and the category of finite étale A_0-schemes.

Proof. [4, §18.3.2]. □

Theorem 3.4. *Let R be a Noetherian, integral F-algebra with perfect closure R', and E be an ordinary elliptic curve over R. Then for each m there exists a unique elliptic curve $\mathbb{E}_m/W_m(R')$ lifting E/R' such that the p-divisible group $\mathbb{E}_m[p^\infty]$ has a split exact connected-étale sequence. Moreover for any $s' \in \operatorname{Spec} R'$ with residue field $\kappa(s')$, the elliptic curve*

$$\mathbb{E}_m \otimes_{W_m(R')} W_m(\kappa(s'))$$

is the canonical lifting of $E_{s'}$ over $W_m(\kappa(s'))$.

Proof. Let $m \geq 2$ be a fixed integer. Since R' is a perfect ring, $A = W_m(R')$ satisfies the hypothesis of Theorem 3.3. So for any n there exists a unique étale group scheme H_n over $W_m(R')$ such that

$$H_n \otimes_{W_m(R')} R' \xrightarrow{\sim} E[p^n]^{et}.$$

It also follows that H_n form an inductive system, and so the limit gives a p-divisible group H_∞ lifting $E[p^\infty]^{et}$. Applying Cartier duality to $E[p^n]^{et}$, we see that $E[p^n]^0$ and so $E[p^\infty]^0$ has also a unique lifting G_∞ to $W_m(R')$. Since the sequence given in (ii) of Proposition 3.1 is split exact, the product $G_\infty \times H_\infty$ lifts the p-divisible group $E[p^\infty]$.

By the general Serre-Tate theorem there is a unique abelian scheme $\mathbb{E}_m$ over $W_m(R')$

lifting E which corresponds to $G_\infty \times H_\infty$, and so has a split exact connected- étale sequence

$$0 \longrightarrow \mathbb{E}_m[p^\infty]^0 \longrightarrow \mathbb{E}_m[p^\infty] \longrightarrow \mathbb{E}_m[p^\infty]^0 \longrightarrow 0.$$

By checking fibers or dimension we can see that $\mathbb{E}_m$ is indeed an elliptic curve.

Now by construction for any $s' \in \operatorname{Spec} R'$, the elliptic curve $\mathbb{E}_m \otimes_{W_m(R')} W_m(\kappa(s'))$ lifts $E_{s'}$ and the associated p-divisible group

$$\mathbb{E}_m[p^\infty] \otimes_{W_m(R')} W_m(\kappa(s'))$$

has a split exact connected- étale sequence. So $\mathbb{E}_m \otimes_{W_m(R')} W_m(\kappa(s'))$ must be the canonical lifting of $E_{s'}$. □

We may call the elliptic curve $\mathbb{E}_m$ as the canonical lifting of E over $W_m(R')$. The j-invariant of $\mathbb{E}_m$, denoted by $j(\mathbb{E}_m)$ will be the universal formula for the canonical lifting of the fibers in the following sense: Let

$$j(\mathbb{E}_m) = (j_0, j_1, ..., j_{m-1})$$

and let $f_{s'} : R' \longrightarrow \kappa(s')$ be the canonical map for $s' \in \operatorname{Spec} R'$. Then the j-invariant of the canonical lifting of $E_{s'}$ over $W_m(\kappa(s'))$ is given by

$$j = (f_{s'}(j_0), f_s(j_1), ..., f_s(j_{m-1})).$$

Chapter 4

CANONICAL LIFTING OVER IMPERFECT FIELDS

In this chapter we will prove that the base of the canonical lifting has a well behaviour with respect to the base of the given ordinary elliptic curve. Explicitly we will prove the following theorem.

Theorem 4.1. *Let K be any field of characteristic $p > 0$, and let E be an ordinary elliptic curve over K. Let $\mathbb{E}$ be the canonical lifting of E over $W(\bar{K})$. We denote the j-invariant of $\mathbb{E}$ by $j(\mathbb{E}) = (j_0, j_1, ..., j_n, ...)$. Then each j_n is an element of K.*

Proof. This theorem for $p \geq 5$ was proved by Finotti, L.R.A. in [2] using Greenberg transforms and elliptic Teichmüller lifts. Here we give a different proof. The theorem holds for perfect K by definition of the canonical lifting. Let K' and K^{sep} denote the perfect and separable closures of K respectively. Then we have $K' \cap K^s = K$. Since $j_n \in K'$ it suffices to show that $j_n \in K^{\text{sep}}$. Thus we may assume K to be a separably closed field and $K' = \bar{K}$. In this case for any integer $n \geq 1$ we have the following isomorphisms over K,

$$\begin{aligned} E[p^n]^0 &\xrightarrow{\sim} \mu_{p^n}, \\ E[p^n]^{et} &\xrightarrow{\sim} \mathbb{Z}/p^n\mathbb{Z} \end{aligned}$$

where $\mu_{p^n} = \ker(p^n : \mathbb{G}_m \longrightarrow \mathbb{G}_m)$ and $\mathbb{Z}/p^n\mathbb{Z}$ is the Cartier dual of μ_{p^n}. We may fix these isomorphisms to be compatible with Cartier duality. Then we have the exact sequence

$$0 \longrightarrow \mu \longrightarrow E[p^\infty] \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0$$

where μ and $\mathbb{Q}_p/\mathbb{Z}_p$ denote the p-divisible groups (μ_{p^n}, i_n) and $(\mathbb{Z}/p^n\mathbb{Z}, i_n)$ respectively. By the general Serre-Tate theorem it suffices to show that there exists a p-divisible group $\mathbb{G}/W_m(K)$ lifting $E[p^\infty]$ given with an extension

$$0 \longrightarrow \mu \longrightarrow \mathbb{G} \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0$$

which splits after base change to $W_m(K')$. So the result follows from the following more general theorem. □

Theorem 4.2. *Let K be any field of characteristic $p > 0$ and $G = (G_n, i_n)$ be a p-divisible group over K given with an extension*

$$0 \longrightarrow \mu \longrightarrow G \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0. \tag{4.1}$$

Then there exists a p-divisible group $\mathbb{G}/W_m(K)$ lifting G with an extension

$$0 \longrightarrow \mu \longrightarrow \mathbb{G} \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0.$$

which splits over $W_m(K')$.

Before we go into the proof we briefly give some facts which is crucial in the proof. Further details of this part can be completely found in [6, §8.7-10]. We define a finite locally free group scheme $T[N]$ for any $N > 0$ over $\mathbb{Z}[q, q^{-1}]$ as follows. As a scheme $T[N]$ is the disjoint union of

$$T_i[N] = \mathrm{Spec}\,(Z[q, q^{-1}][X]/(X^N - q^i))$$

for $i = 0, 1, ..., N-1$. For any connected $\mathbb{Z}[q, q^{-1}]$-algebra C we have

$$T[N](C) = \{(X, i/N) | X \in C,\, 0 \leq i \leq N-1,\, X^N = q^i\}$$

The group law is defined by

$$(X, i/N).(Y, j/N) = \begin{cases} (XY, (i+j)/N) & \text{if } i+j \leq N-1, \\ (XY/q, (i+j-N)/N) & \text{if } i+j \geq N. \end{cases}$$

It is easy to see that $T[N]$ is a finite locally free group scheme of order N^2 killed by N and the elements of the form $(X, 0)$ is a subgroup isomorphic to μ_N. So that we have an exact sequence

$$0 \longrightarrow \mu_N \longrightarrow T[N] \longrightarrow \mathbb{Z}/N\mathbb{Z} \longrightarrow 0.$$

This exact sequence splits over C if and only if the image of q in C has an N-th root. Indeed $T[N]$ is universal in the following sense.

Proposition 4.1. *Let S be any scheme and G/S be a finite locally free group scheme over S of order N^2 which is killed by N given with an extension structure*

$$0 \longrightarrow \mu_N \longrightarrow G \longrightarrow \mathbb{Z}/N\mathbb{Z} \longrightarrow 0. \tag{4.2}$$

Then Zariski locally on S there exists $q \in \mathbb{G}_m(S)$ such that

$$G \xrightarrow{\sim} T[N] \otimes_{\mathbb{Z}[q,q^{-1}]} S$$

and this isomorphism is compatible with extension structures.

Proof. A complete proof can be found in [6, §8.10.5]. Here we do not give a complete proof. For our purposes we briefly recall the construction of the given isomorphism in the case $S = \operatorname{Spec} A$ is affine and $\operatorname{Pic}(A) = 0$. So that we may remove the Zariski local condition on the relevant isomorphism.

Now locally fppf (4.2) splits. So G is an fppf form of the product group scheme $\mu_{p^n} \times \mathbb{Z}/p^n\mathbb{Z}$. But the set isomorphism classes of fppf forms of $\mu_{p^n} \times \mathbb{Z}/p^n\mathbb{Z}$ is bijective to the set of isomorphism classes of Aut-torsors where Aut is the group scheme whose set of

T-valued points denoted by $\mathrm{Aut}(T)$ is

$$\left\{ \text{automorphisms of } \mu_{p^n} \times \mathbb{Z}/p^n\mathbb{Z} \text{ of the form } \begin{pmatrix} 1 & \phi \\ 0 & 1 \end{pmatrix}, \phi \in \mathrm{Hom}_T(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n}) \right\}$$

But the later set is just $H^1(\mathrm{Spec}\, A, \mathrm{Aut})$. Also $\mathrm{Aut} \xrightarrow{\sim} \mu_{p^n}$ and so the group $H^1(\mathrm{Spec}\, A, \mu_{p^n})$ classifies the isomorphism classes of forms of $\mu_{p^n} \times \mathbb{Z}/p^n\mathbb{Z}$. Note that the torsor corresponding to G is just the inverse image of 1 in $G \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$. Now consider the Kummer sequence

$$0 \longrightarrow \mu_{p^n} \longrightarrow \mathbb{G}_m \longrightarrow \mathbb{G}_m \longrightarrow 0.$$

Since $H^1(\mathrm{Spec}\, A, \mathbb{G}_m) = \mathrm{Pic}(A) = 0$ we have the following relevant part of the corresponding long exact sequence

$$\mathbb{G}_m(A) \xrightarrow{p^n} \mathbb{G}_m(A) \longrightarrow H^1(\mathrm{Spec}\, A, \mu_{p^n}) \longrightarrow 0.$$

So for any cocycle in $H^1(\mathrm{Spec}\, A, \mu_{p^n})$ the corresponding μ_{p^n}-torsor is just $[p^n]^{-1}(q)$ for some $q \in A^*$. Note that q is unique up to multiplying by a p^n-th power in A^*. In particular the class of G in $H^1(\mathrm{Spec}\, A, \mu_{p^n})$ denoted by $\mathrm{cl}(G)$ corresponds to a μ_{p^n}-torsor $[p^n]^{-1}(q)$ for some $q \in A^*$. For any A-scheme T, the T-valued points of $[p^n]^{-1}(q)$ is the

set $\{x \in \mathbb{G}_m(T) : x^{p^n} = q\}$. Now consider the following extension of group schemes

$$0 \longrightarrow \mu_{p^n} \longrightarrow T[p^n] \otimes_{\mathbb{Z}[q,q^{-1}]} A \xrightarrow{\epsilon} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0.$$

The μ_{p^n}-torsor corresponding to $T[p^n] \otimes_{\mathbb{Z}[q,q^{-1}]} A$ is then $\epsilon^{-1}(1) = [p^n]^{-1}(q)$, so that the images of G and $T[p^n] \otimes_{\mathbb{Z}[q,q^{-1}]} A$ in $H^1(\operatorname{Spec} A, \mu_{p^n})$ are the same and hence

$$G_n \xrightarrow{\sim} T[p^n] \otimes_{\mathbb{Z}[q,q^{-1}]} A.$$

□

Proof of 4.2. First note that any p-divisible group $\mathbb{G}$ lifting G necessarily has an extension structure

$$0 \longrightarrow \mu \longrightarrow \mathbb{G} \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0.$$

This follows from Theorem 3.2. So we only need to show the splitting. Now giving an extension as (4.1) is same as giving a compatible family of extensions

$$0 \longrightarrow \mu_{p^n} \longrightarrow G_n \xrightarrow{\pi} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0 \tag{4.3}$$

for all n. Since G_n satisfies the conditions of Proposition 4.1 there exists $q \in K^*$ such

that

$$G_n \xrightarrow{\sim} T[p^n] \otimes_{\mathbb{Z}[q,q^{-1}]} K.$$

By hypothesis we have that

$$G_{n-1} = \ker(p^{n-1} : G_n \longrightarrow G_n) \xrightarrow{\sim} T[p^{n-1}] \otimes_{\mathbb{Z}[q,q^{-1}]} K.$$

This shows that the class of G_{n-1} in $H^1(\operatorname{Spec} K, \mu_{p^{n-1}})$ is the $\mu_{p^{n-1}}$-torsor $[p^{n-1}]^{-1}(q)$. So $G = (G_n, i_n)$ determines a non-unique sequence of elements (q_n) in K^* where $\overline{q_n} \in H^1(\operatorname{Spec} K, \mu_{p^n}) \xrightarrow{\sim} K^*/(K^*)^{p^n}$ and $\overline{q_n} = u_n^{p^{n-1}}\overline{q_{n-1}}$ for some $u_n \in K^*$, i.e. G determines an element of the inverse limit

$$\varprojlim_n K^*/(K^*)^{p^n}.$$

Conversely given an element $(\overline{q_n}) \in \varprojlim_n K^*/(K^*)^{p^n}$ choose a sequence (q_n) in K^* such that $q_n \mapsto \overline{q_n}$. Then we have that $q_n = u_n^{p^{n-1}} q_{n-1}$ and that $G = (T[p^n] \otimes_{\mathbb{Z}[q_n, q_n^{-1}]} A, i_n)_n$ is a p-divisible group. Thus

$$\operatorname{Ext}_K(\mathbb{Q}_p/\mathbb{Z}_p, \mu) \xrightarrow{\sim} \varprojlim_n K^*/(K^*)^{p^n}$$

Up to now we didn't use that K is indeed a field, we only used that $\mathrm{Pic}(K) = 0$. We can carry out the same procedure to obtain a p-divisible group over $W_m(K)$, i.e. we need to specify a sequence (Q_n) in $W_m(K)^*$ such that $Q_n = U_n^{p^{n-1}} Q_{n-1}$. Then the p-divisible group

$$\mathbb{G} = (T[p^n] \otimes_{\mathbb{Z}[Q_n, Q_n^{-1}]} W_m(K), i_n)$$

is the p-divisible group corresponding to the chosen sequence (Q_n). Now we impose the condition that $\mathbb{G}$ lifts G, i.e. $\mathbb{G}_n \otimes_{W_m(K)} K \xrightarrow{\sim} G_n$ via the surjection $W_m(K) \longrightarrow K$ and the isomorphims are compatible with the maps $i_n : G_n \longrightarrow G_{n+1}$. This condition is satisfied if we choose Q_n and U_n such that $Q_n \mapsto q_n$ and $U_n \mapsto u_n$ under $W_m(K) \longrightarrow K$. Also we want the connected-étale sequence of $\mathbb{G}$ to split over $W_m(K')$. This means that Q_n must have a p^n-th root in $W_m(K')$. All of these are satisfied if we set Q_n and U_n to be the Teichmüller lifts of q_n and u_n respectively. Let

$$\begin{aligned} f : K^* &\longrightarrow W_m(K)^*, \\ a &\longmapsto (a, 0, 0, ..., 0) \end{aligned}$$

be the Teichmüller map. Thus if we set $Q_n = f(q_n) = (q_n, 0, 0, ..., 0)$ and $U_n = f(u_n) = (u_n, 0, 0, ..., 0)$, the corresponding $\mathbb{G}$ is the required p-divisible group. □

Chapter 5

CANONICAL LIFTING AND DIVISION POLYNOMIALS

In the previous chapter we proved that if K is a separably closed field and E is an ordinary elliptic curve over K then the canonical lifting of E is defined over $W_m(K)$. In this chapter we will show that if $\mathrm{char}(K) = p \geq 5$ then we can drop the assumption that K is separably closed. Explicitly we prove the following theorem.

Theorem 5.1. *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. Then the canonical lifting $\mathbb{E}$ of E is defined over $W_n(K)$. In particular if we denote the j-invariant of $\mathbb{E}$ by $j(\mathbb{E}) = (j_0, j_1, ..., j_n)$ then each j_n is an element of K.*

Note that we proved this theorem for separably closed K in the previous chapter. Here we give a more elementary proof for any K. But before we go into the proof we need do to some setup. We first obtain some simple results which leads another characterization of the canonical lifting. In this chapter we will use the division polynomials extensively. The only preliminary about division polynomials is [10, §3, Exercise 3.7]

First we give an equivalent characterization of the canonical lifting. We omit most of the details referring the reader to [5]. 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. Let $\mathbb{X}$ be any lifting of X/k over B. Then by Theorem 3.2 we have the

following exact sequences

$$0 \to \hat{X}(= X[p^\infty]^0) \to X[p^\infty] \to X[p^\infty]^{et} \to 0, \tag{5.1}$$

$$0 \to \hat{\mathbb{X}}(= \mathbb{X}[p^\infty]^0) \to \mathbb{X}[p^\infty] \to \mathbb{X}[p^\infty]^{et} \to 0 \tag{5.2}$$

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 (See [12] and [13] for Cartier duality). Since k is algebraically closed we have that $X[p^\infty]^{et} \xrightarrow{\sim} \mathbb{Q}_p/\mathbb{Z}_p = (X(k)[p^n], i_n)$ 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. For each n we have the following isomorphisms of k-groups;

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

Since B is an Artin local ring by Theorem 3.3 these isomorphisms extend to the following isomorphisms of B-groups;

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

Thus we obtain the the perfect pairings

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

for each n.

Now we construct a map $T_p A(k) \to \hat{\mathbb{X}}(R)$. 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 homomorphism

$$\phi_{\mathbb{X}} : T_p X(k) \xrightarrow{\pi_r} X(k)[p^r] \xrightarrow{\phi_r} \hat{\mathbb{X}}(B).$$

We define $q_{\mathbb{X}/B} : T_p X(k) \otimes T_p X(k) \to \mathbb{G}_m(B)$ as $q_{\mathbb{X}/B}(\alpha, \beta) := E_{\mathbb{X}}(\phi_{\mathbb{X}}, \beta)$. Thus starting with an extension of the form (5.2) we obtain an element $q \in \mathrm{Hom}_{\mathbb{Z}_p}(T_p(X)(k) \otimes T_p(X^D)(k), \hat{\mathbb{G}}_m(B))$ which indeed gives the equivalence (2.3) of §2 [5].

Since the pairing $E_{\mathbb{X}}$ is perfect, $q = 1$ if and only if $\phi_{\mathbb{X}} = O$ where O is the identity element. So canonical lifting of X is 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 5.1. *With the previous notation the followings are equivalent.*

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

We will use Corollary 5.1 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 5.1. *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.

$$\begin{array}{ccc} \operatorname{Spec} \bar{K} & \xrightarrow{F^n \circ P} & E^{(p^n)} \\ \downarrow & & \downarrow{\scriptstyle V^n} \\ \operatorname{Spec} K & \longrightarrow & E \end{array}$$

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

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 5.1 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 $\Psi \in \mathbb{Z}[A, B][x]$.

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 5.1, $\hat{P}$ 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 $\hat{P} = ((x_0, x_1, ...x_{n-1}), (y_0, y_1, ..., y_{n-1}))$ then $\Psi((x_0, x_1, ..., x_{n-1})) = 0$ for infinitely many $x_1, x_2, ..., x_n$. 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 [1], 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

$$(\Psi^2)' \equiv 0 \,(\text{mod } N), \tag{5.3}$$

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 5.1 where $a_0, b_0 \in K$. Let $a_1, ...a_n$ and $b_1, ...b_n$ be algebraically independent indeterminates and consider the Weierstrass equation

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

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 5.2. *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 5.1. *Let E and $\mathbb{E}$ be given as above. Then the p^{n+1}-division polynomial Ψ of $\mathbb{E}$ is of the form*

$$\Psi = (\Psi_0, \Psi_1, ..., \Psi_n)$$

where each Ψ_i is a polynomial of $x_0^{p^{n+1}}$ over the ring $\mathbb{Z}[a_0, a_1, ..., a_i, b_0, b_1, ..., b_i]$. 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, $\gamma_i \in \mathbb{Z}[a_0, a_1, ..., a_{i-1}, b_0, b_1, ..., b_{i-1}, x_0^{p^{n+1}}]$.

Proof. Let

$$\Psi = \Psi_{\mathbb{E},p^{n+1}} = A_l + A_{l-1}X + ... + A_1X^{l-1} + A_0X^l$$

where $A_i \in W_{n+1}(F)$ and $X = (x_0, x_1, ...x_n)$. Indeed A_i are polynomials with integer coefficients in the variables $(a_0, a_1, ..., a_n), (b_0, b_1, ..., b_n)$. To simplify computations which will be made below, we may consider A_i as an element $W_{n+1}(\bar{F})$ via the inclusion $W_{n+1}(F) \hookrightarrow W_{n+1}(\bar{F})$. By the lemma for each monomial A_iX^{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

$$X^{v_ip^{t_i}} = (x_0, x_1, ..., x_n)^{v_ip^{t_i}} = (x_0^{v_ip^{t_i}}, 0, ..., 0).$$

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

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

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 $u = (x_0^{p^{t_i}}, 0, 0..., 0)$ and $\pi = (0, 0, 0..., 0, y'_{j+1}, y'_{j+2}, ..., y'_n)$. So we have

$$A_i X^{l-i} = A_i (u + \pi)^{v_i}.$$

For notational simplicity let $r = n + 1 - t_i$ and $A_i = (0, 0, ..., 0, c_r, c_{r+1}, ..., c_n)$. 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

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

But A_i is a polynomial in $(a_0, a_1, ..., a_n)$ and $(b_0, b_1, ..., b_n)$ with integer coefficients, so we have that each c_s is a polynomial in $a_0, a_1, ..., a_s, b_0, b_1, ..., b_s$ 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. $\square$

After this preparation we can start the proof of the Theorem 5.1.

Proof. (Proof of Theorem 5.1). Since $p \geq 5$ any elliptic curve over K and $W_n(\bar{K})$ can be given by Weierstrass models

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

and

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

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 $(a_0, a_1, ..., a_n) = 3(t_0, t_1, ..., t_n)$ and $(b_0, b_1, ..., b_n) = 2(t_0, t_1, ..., t_n)$ where t_i for $i \geq 1$ are independent variables. If $j = 0$ we set $a_i = 0$ and $b_i = t_i$ for $i = 0, 1, ..., n$. Similarly if $j = 1728$ then we set $b_i = 0$ and $a_i = t_i$ for $i = 0, 1, ..., n$. 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, $\beta_i \in \mathbb{Z}[t_0, t_1, ..., t_{i-1}, x_0^{p^{n+1}}]$. 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 may apply 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 $j = 1, 2, ..., i-1$ 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 β_i/α_i which implies that t_i must be in K. This completes the proof. □

In [1], Cassels starts with an equation of the form

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

and proves that $(\Psi_N^2)' \cong (\text{mod } N)$. For $p = 2$ or 3 such an equation is always supersingular so we have to put the condition $p \geq 5$ in the theorem. 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 5.1 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 $t_1 = 0$.

Chapter 6

THE UNIVERSAL FORMULA

Now we can use the results of the previous chapters to prove Theorem 1.1 stated in §1.

Proof of Theorem 1.1. Let p be any prime number. Recall that we defined the ring A as

$$A = F[J, 1/\phi_p(J)].$$

Let K be the fields of fractions of A with a fixed algebraic closure $\bar{K}$. We define the ring R to be the localization of A at the element $J(J - 1728)$, i.e.

$$R = F[J, 1/J(J - 1728)\Phi_p(J)].$$

We define the elliptic curve E/R as

$$E : y^2 + xy = x^3 - 36x/(J - 1728) - 1/(J - 1728).$$

Note that $j(E) = J$, $\Delta(E) = J^2/(J-1728)^2$ and E is ordinary. So the hypotheses of Theorem 3.4 is satisfied. With the same notation of Theorem 3.4, for any positive integer m we have the elliptic curve $\mathbb{E}_m$ over $W_m(R')$ with j-invariant $j(\mathbb{E}_m) = (j_0, j_1, j_2, ..., j_{m-1})$ and with a split exact connected-étale sequence. Now for any $j_0 \in k^{\text{ord}} \setminus \{0, 1728\}$, the homomorphism $R' \longrightarrow k$ induced by $J \longmapsto j_0$ maps E to an ordinary elliptic curve over k with j-invariant j_0, say $\tilde{E}$. Similarly it maps $\mathbb{E}_m$ to the canonical lifting of $\tilde{E}$. We set $f_i = j_i$ for all i. Now we show that $j_i \in R$.

Let K and K' be the fields of fractions of R and R' respectively. Consider the elliptic curve

$$\mathbb{E}_m \otimes_{W_m(R')} W_m(K')$$

obtained via the inclusion $W_m(R') \hookrightarrow W_m(K')$. It is a lifting of the generic fiber of E denoted by $E_{K'} = E \otimes_{R'} K'$ and has a split exact connected-étale sequence over $W_m(K')$. So it is the canonical lifting of $E_{K'}$. Its j-invariant is in $W_m(R')$ as it is obtained from $\mathbb{E}_m$. But Theorem 4.1 implies that the j-invariant of the canonical lifting of E_K which is tautologically equal to the j-invariant of $\mathbb{E}_m \otimes_{W_m(R')} W_m(K')$ is indeed in $W_m(K)$. So each $j_i \in R' \cap K = R$ since R is integrally closed. Now we will show that $j_i \in A$, i.e. j_i are regular at 0 and 1728 provided that these are ordinary. We will also prove that $(0, j_1(0), j_2(0)...,)$ is the j-invariant of the canonical lifting of the elliptic curve with j-invariant zero, and similarly for 1728.

We may assume $p \geq 5$ because $0 = 1728$ is supersingular in characteristic 2 and 3. Let $\mu_3 \neq 1$ be a fixed cube root of 1. Let $L = F(\mu_3, \sqrt{3})$, $a = \sqrt[3]{J}$ and $b = 2.3^{-1}.\sqrt{J-1728}/\sqrt{3}$.

Let $B = L[J, \sqrt[3]{J}, \sqrt{J - 1728}, 1/\phi_p(J)]$ and E be the scheme over B defined as

$$E' : y^2 = x^3 + ax + b.$$

Note that B is an integral extension of A and E' is an elliptic curve over B with $j(E') = J$ and $\Delta(E) = -4^3.1728 \neq 0$. Now E' and E are isomorphic over $\bar{K}$ since they have the same j-invariant. So the j-invariants of the canonical lifting of E and E' denoted by $\mathbb{E}_m$ and $\mathbb{E}'_m$ are the same. But by Theorem 3.4 we have $j(\mathbb{E}') \in W_m(B')$ where B' is the perfect closure of B. So $j(\mathbb{E}') = j(\mathbb{E}) = (j_0, j_1, j_2, ..., j_{m-1})$ where $j_i \in B'$. But previously we proved that $j_i \in R$. Now B' is an integral extension of A and A is integrally closed in R. Thus $R \cap B' = A$, and so $j_i \in A$. In particular j_i are regular at any element of k^{ord}.

Now let $j_0 = 0 \in k^{\text{ord}}$. Consider the maximal ideal $(J) \subset A$. Since S' is an integral extension of A there exists a prime ideal q' of S' such that $q' \cap A = (J)$. Integrality of S' also implies that q' is a maximal ideal. Let $\kappa = S'/q'$. Since $J \pmod{q'} = 0$ we have that

$$\mathbb{E}'_m \otimes_{W_m(S')} W_m(\kappa)$$

is the canonical lifting of the elliptic curve with j-invariant zero. The j-invariant of this canonical lifting is just

$$(0, \overline{j_1}, \overline{j_2}, ..., \overline{j_{m-1}})$$

where $\overline{j_i} = j_i \pmod{q'}$. But $A/(J) \to S'/q'$ is injective and $j_i \in A$, so $j_i \pmod{q'}$ is the image of $j_i \pmod{(J)}$ under this injection. But $j_i \pmod{(J)} = j_i(0)$. The same argument also works for the maximal ideal $(J - 1728)$ provided that $j_0 = 1728$ is in k^{ord}. This completes the proof of (i).

Now we prove (ii). Since $J = 0 = 1728$ is supersingular for $p = 2, 3$, we may assume that $p \geq 5$. Let E be any ordinary elliptic curve over k with $j(E) = j_0 \in k$, and let $\mathbb{E}$ be its canonical lifting over $W(k)$. Let Ω be a fixed algebraic closure of the field of fractions of $W(k)$. By [8, §V.3] we have that

$$\text{End}_W(k)(\mathbb{E}) \xrightarrow{\sim} \text{End}_k(E)$$

via the reduction modulo p map. Now take any p such that $j_0 = 0$ is an ordinary j-value in k. Then the automorphism group of E/k, $\text{Aut}_k(E)$ has order 6 and by the above isomorphism we also have that $\text{Aut}_\Omega(\mathbb{E} \otimes \Omega)$ has order at least 6. But this can happen if and only if $j(\mathbb{E}) = 0$, i.e. in Witt vector notation $\Theta(0) = (0, 0, 0...)$. Similarly if E/k with $j(E) = j_0 = 1728$ is ordinary for some p, then we have that $\text{Aut}_{\bar{k}}(E)$ has order 4. So that $j(\mathbb{E}) = 1728$. □

BIBLIOGRAPHY

[1] J. W. S. Cassels. A Note on the Division Values of $\wp(u)$, *Mathematical Proceedings of the Cambridge Philosophical Society*, 45(2) (1949), 167-172.

[2] L. R. A. Finotti. Lifting the j-Invariant: Questions of Mazur and Tate, *Journal of Number Theory*, 130(3) (2010), 620-638.

[3] M. J. Greenberg. Perfect Closure of Rings and Schemes, *Proc. Amer. Math. Soc.*, 16 (1965), 313-317.

[4] A. Grothendieck. EGA IV. Étude locale des schémas et des morphismes de schémas. *Inst. Hautes Études Sci. Publ. Math.*, 32 (1967).

[5] N. Katz. Serre-Tate Local Moduli, *Surfaces Algébriques*, Séminaire de Géométrie Algébrique d'Orsay, (1976-1978), 138-202.

[6] N. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves*, Annals of Mathematics Studies, Princeton University Press, (1985).

[7] J. Lubin, J.-P. Serre and J. Tate. Elliptic curves and formal groups by J. Lubin, J.-P. Serre and J. Tate, 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*, Springer-Verlag, (1972).

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

[10] J. Silverman. *Arithmetic of Elliptic Curves*, Springer-Verlag, (1986).

[11] J.-P. Serre. *Local Fields*, Springer-Verlag, (1980).

[12] J. Tate. Finite Flat Group Schemes, *Modular Forms and Fermat's Last Theorem*, Springer, (1997), 121-154.

[13] J. Tate. p-Divisible Groups, *Proceedings of a conference on local fields*, Driebergen, (1966), 158-183.

[14] J.F. Voloch and J. L. Walker. Euclidean weights of codes from elliptic curves over rings, *Trans. Amer. Math. Soc.*, 352(11) (2000), 5063-5076.