THE DISCRIMINANT IN UNIVERSAL FORMULAS FOR THE CANONICAL LIFTING

LUÍS R. A. FINOTTI AND DELONG LI

ABSTRACT. In this paper we study formulas for the coordinates of the Weierstrass coefficients $\boldsymbol{a} = (a, A_1, A_2, \ldots)$ and $\boldsymbol{b} = (b, B_1, B_2, \ldots)$ of the canonical lifting. More precisely we show that there are formulas for A_1 and B_1 that are given by modular functions, universal (meaning, single formulas that work in every possible case), and with no factor of Δ in their denominators. Two possible constructions are given. Moreover, a sufficient condition is given for the existence of A_2 and B_2 with these properties. Finally, we prove that the Hasse invariant, given as a polynomial on the Weierstrass coefficients of an elliptic curve of characteristic $p \geq 5$, has no repeated factor.

1. INTRODUCTION

Let $\Bbbk$ be a perfect field of characteristic $p \geq 5$ and

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

be an ordinary elliptic curve. As first proved by Deuring in [Deu41] and later generalized by Serre and Tate in [LST64], there is then a unique (up to isomorphism) elliptic curve

$$\boldsymbol{E}/\boldsymbol{W}(\Bbbk) \ : \ \boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{a}\boldsymbol{x} + \boldsymbol{b},$$

over the ring of Witt vectors $\boldsymbol{W}(\Bbbk)$ that reduces to E modulo p and for which we can lift the Frobenius of E. Therefore, there are functions $A_i(a, b)$ and $B_i(a, b)$ (where a and b are variables) such that if the pair (a_0, b_0) are the Weierstrass coefficients of an ordinary elliptic curve, then the Weierstrass coefficients of the canonical lifting of this curve can be given by

$$\boldsymbol{a} = (a_0, A_1(a_0, b_0), A_2(a_0, b_0), A_3(a_0, b_0), \ldots),$$
$$\boldsymbol{b} = (b_0, B_1(a_0, b_0), B_2(a_0, b_0), B_3(a_0, b_0), \ldots).$$

Obviously, since the canonical lifting is only unique up isomorphism, these functions are not uniquely determined. In [Fin20] the first author gave a description of "nice" properties

2010 *Mathematics Subject Classification.* Primary 11G07; Secondary 11F03.
Key words and phrases. elliptic curves, canonical lifting, Weierstrass coefficients, modular functions.

(to be made clear below) that these functions can satisfy, and describe methods to compute them. Before we can precisely state these properties, we need a few definitions.

Definition 1.1. (1) Let

$$\Bbbk^2_{\mathrm{ord}} \stackrel{\mathrm{def}}{=} \{(a_0,b_0)\in \Bbbk^2 \ : \ y_0^2 = x_0^3 + a_0x_0 + b_0 \text{ is ordinary}\}.$$

(2) The functions A_i's and B_i's (as above) are called *universal* if they are defined for all $(a_0,b_0)\in \Bbbk^2_{\mathrm{ord}}$.

(3) Let a and b be indeterminates in $\mathbb{F}_p[a,b]$, and assign them weights 4 and 6 respectively. Then, let

$$\mathcal{S}_n \stackrel{\mathrm{def}}{=} \left\{ \frac{f}{g} \in \mathbb{F}_p(a,b) \ : \ f,g\in\mathbb{F}_p[a,b] \text{ homog., and } \operatorname{wgt}(f)-\operatorname{wgt}(g)=n \right\} \cup \{0\}.$$

The elements of $\mathcal{S}_n$ are then called *modular functions of weight n*.

Then, [Fin20, Theorem 2.3] states:

Theorem 1.2. *There are universal modular functions $A_i\in\mathcal{S}_{4p^i}$ and $B_i\in\mathcal{S}_{6p^i}$ (and, in particular, these are rational functions with coefficients in $\mathbb{F}_p$), for $i\in\{1,2,3,\ldots\}$, such that if $(a_0,b_0)\in\Bbbk^2_{\mathrm{ord}}$ gives the Weierstrass coefficients of an ordinary elliptic curve, then*

$$((a_0,A_1(a_0,b_0),A_2(a_0,b_0),\ldots),(b_0,B_1(a_0,b_0),B_2(a_0,b_0),\ldots))$$

gives Weierstrass coefficients of its canonical lifting.

This reference also describes a method to compute examples of these formulas and how to obtain every other possibility (satisfying the conditions of the theorem) from these. These computations are based on an algorithm for the computation of the canonical lifting first introduced by Voloch and Walker (partially described in [VW00]) and later extended by the first author. (We review a few ideas of this method in Section 5.) We shall refer to this construction as the *Greenberg transform construction*. (The name will also be made clear in Section 5.)

Since we will deal with formulas, let's consider the field $\mathbb{K}=\mathbb{F}_p(a,b)$, where again a and b are indeterminates, as the field of definition of our elliptic curve

$$E/\mathbb{K} \ : \ y_0^2 = x_0^3 + ax_0 + b. \tag{1.1}$$

Then, let $\Delta = 4a^3+27b^2$ be the *discriminant* of this elliptic curve E and $\mathfrak{h}$ be the coefficient of x_0^{p-1} of $(x_0^3+ax_0+b)^{(p-1)/2}$, i.e., $\mathfrak{h}$ is the *Hasse invariant* of E. Since an elliptic curve is ordinary if and only if the Hasse invariant is non-zero, we have that A_i and B_i being

universal rational functions is the same as to say that $A_i, B_i \in \mathbb{U} \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, 1/(\Delta\mathfrak{h})]$ and always yield the Weierstrass coefficients of the canonical lifting.

On the other hand, the explicit computations in fact gave $A_i, B_i \in \mathbb{U}_\Delta \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, 1/\mathfrak{h}]$, i.e., the discriminant Δ never appeared in the denominators.

This led to the following conjecture:

Conjecture 1.3. (1) *There are universal modular functions $A_i \in \mathcal{S}_{4p^i}$ and $B_i \in \mathcal{S}_{6p^i}$ giving the Weierstrass coefficients of the canonical lifting with $A_i, B_i \in \mathbb{U}_\Delta$.*

(2) *The Greenberg transform construction (given in* [Fin20]*) yields such modular functions.*

In [FL20], the authors could prove that the first part of the conjecture is true for $p \equiv 11 \pmod{12}$. The idea behind it was to use a different construction for the A_i and B_i, using the j-invariant.

Since the canonical lifting is unique up to isomorphism, there are *uniquely determined* functions J_i for $i \geq 1$ such that if $j_0 = 1728 \cdot 4a_0^3/(4a_0^3 + 27b_0^2)$ is the j-invariant of an ordinary elliptic curve, then

$$\boldsymbol{j} = (j_0, J_1(j_0), J_2(j_0), J_3(j_0), \ldots)$$

is the j-invariant of its canonical lifting.

But then, if $\boldsymbol{j} \neq 0, 1728$, we have that

$$\boldsymbol{y}^2 = \boldsymbol{x}^3 + \frac{27\boldsymbol{j}}{4(1728 - \boldsymbol{j})}\boldsymbol{x} + \frac{27\boldsymbol{j}}{4(1728 - \boldsymbol{j})} \tag{1.2}$$

is a Weierstrass equation for the canonical lifting.

We can then apply this to elliptic curve given by Eq. (1.1) (i.e., we use $j = 1728 \cdot 4a^3/\Delta$), and obtain an Weierstrass equation for its canonical lifting. Although the equation above does not reduce to $y_0^2 = x_0^3 + ax_0 + b$, this can be fixed by setting:

$$\boldsymbol{a} \stackrel{\text{def}}{=} \boldsymbol{\lambda}^4 \cdot \frac{27\boldsymbol{j}}{4(1728 - \boldsymbol{j})} = (a, A_1, A_2, \cdots) \tag{1.3}$$

$$\boldsymbol{b} \stackrel{\text{def}}{=} \boldsymbol{\lambda}^6 \cdot \frac{27\boldsymbol{j}}{4(1728 - \boldsymbol{j})} = (b, B_1, B_2, \cdots), \tag{1.4}$$

where

$$\boldsymbol{\lambda} \stackrel{\text{def}}{=} \left(\left(\frac{b}{a}\right)^{1/2}, 0, 0, \ldots\right). \tag{1.5}$$

With these $\boldsymbol{a}$ and $\boldsymbol{b}$, we obtain a Weierstrass equation

$$\boldsymbol{E} : \boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{a}\boldsymbol{x} + \boldsymbol{b},$$

for the canonical lifting of E that reduces to the equation of E.

Since the functions J_i were extensively studied by the first author in [Fin10], [Fin11], [Fin12], and [Fin13], the two authors could establish a good amount of information about the denominator of the A_i's and B_i's obtained by this new construction.

We shall refer to this second construction as the *j-invariant construction.*

In [FL20] we have the following theorem:

Theorem 1.4. *Let A_i and B_i be the coordinate functions obtained by the j-invariant construction and let $\mathbb{V}_\Delta \overset{\text{def}}{=} \mathbb{F}_p[a,b,1/(\mathfrak{h}ab)]$. Then, we have that $A_i \in \mathcal{S}_{4p^i} \cap \mathbb{V}_\Delta$ and $B_i \in \mathcal{S}_{6p^i} \cap \mathbb{V}_\Delta$, and thus no Δ appears in their denominators.*

So, the authors could show that we have no Δ in the denominator in this construction, but its draw back is that, in general, they are not universal, as they might not be defined for elliptic curves with either a_0 or b_0 equal to 0. But, since $a, b \mid \mathfrak{h}$ if $p \equiv 11 \pmod{12}$, i.e., no ordinary elliptic curve can have either a_0 or b_0 equal to zero in this case, this proved the first part of Conjecture 1.3 in this case. (The above reference gives further details on the possible powers of a and b that can appear in the denominators of A_i and B_i, as we make explicit in Section 2 below.)

One idea in proving the first part of Conjecture 1.3 in general is to start with the A_i's and B_i's from this j-invariant construction, and then find $\boldsymbol{\lambda}$ such that

$$\boldsymbol{\lambda}^4(a, A_1, A_2, A_3, \ldots) = (a, A_1', A_2', A_3', \ldots),$$
$$\boldsymbol{\lambda}^6(b, B_1, B_2, B_3, \ldots) = (b, B_1', B_2', B_3', \ldots)$$

where $A_i' \in \mathcal{S}_{4p^i} \cap \mathbb{U}_\Delta$ and $B_i' \in \mathcal{S}_{6p^i} \cap \mathbb{U}_\Delta$, since clearly these new Witt vectors still give Weierstrass coefficients to the canonical lifting.

In Section 3 we find $\boldsymbol{\lambda}_1 = (1, \lambda_1)$ such that if

$$\boldsymbol{\lambda}_1^4(a, A_1) = (a, A_1') \quad \text{and} \quad \boldsymbol{\lambda}_1^6(b, B_1) = (b, B_1'),$$

then $A_1' \in \mathcal{S}_{4p} \cap \mathbb{U}_\Delta$ and $B_1' \in \mathcal{S}_{6p} \cap \mathbb{U}_\Delta$, effectively proving the first part of Conjecture 1.3 for $i = 1$ (and now with no restriction on p).

In Section 4 we are not quite able to extend the previous result to the third coordinate, but we find a condition to the existence of λ_2 such that if $\boldsymbol{\lambda}_2 = (1, 0, \lambda_2)$, then letting

$$\boldsymbol{\lambda}_2^4(a, A_1', A_2') = (a, A_1', A_2''), \quad \text{and} \quad \boldsymbol{\lambda}_2^6(b, B_1', B_2') = (b, B_1', B_2''),$$

we have that $A_2'' \in \mathcal{S}_{4p^2} \cap \mathbb{U}_\Delta$ and $B_2'' \in \mathcal{S}_{6p^2} \cap \mathbb{U}_\Delta$.

In Section 5 we turn back to the Greenberg transform construction and prove that A_1 and B_1 (from this Greenberg transform construction now) indeed are in $\mathcal{S}_{4p} \cap \mathbb{U}_\Delta$ and $\mathcal{S}_{6p} \cap \mathbb{U}_\Delta$,

thus proving the *second part* (and giving a second proof for the first part) of Conjecture 1.3 for $i = 1$.

Finally, in Section 6, we prove that the Hasse invariant $\mathfrak{h}$ has no repeated factors. (The authors are unsure if this was a known result. In any event, a new proof is given.) Although this is of independent interest, it also has an application to the formulas for the A_i and B_i coming from the j-invariant construction: let

$$\bar{\mathfrak{h}} \stackrel{\text{def}}{=} \frac{\mathfrak{h}}{a^{\nu_a(\mathfrak{h})}\, b^{\nu_b(\mathfrak{h})}}$$

i.e., $\bar{\mathfrak{h}}$ is obtained from $\mathfrak{h}$ by removing any factor of a and b. Then, the maximum power of $\bar{\mathfrak{h}}$ that can appear in the denominator (after reduction) of A_i and B_i is $ip^{i-1} + (i-1)p^{i-2}$. Moreover, this bound is sharp. In fact, in all cases computed, we have that $\bar{\mathfrak{h}}^{ip^{i-1}+(i-1)p^{i-2}}$ always appear in the denominators.

We observe that throughout this paper we are always assuming that the characteristic is $p \geq 5$.

2. Previous Results

Before we prove the main results of this paper, we need to introduce some previous results from [FL20]. In this reference the denominators of A_i and B_i *from the j-invariant construction* are studied in detail. We know from the construction that denominator has to be made up of powers of a, b, Δ, and $\mathfrak{h}$. Of those only $\mathfrak{h}$ is not necessarily irreducible, and in fact a and b might be factors of $\mathfrak{h}$. Thus, to study what powers of $\mathfrak{h}$ can appear in the denominator independently of other factors of a and b, the authors introduce a new variable $\mathfrak{H}$.

The construction via the j-invariant allows us to track exactly where the factors of $\mathfrak{h}$ are introduced in the denominators, so one can simply replace those occurrences of $\mathfrak{h}$ (before any simplification) by the associated variable $\mathfrak{H}$. This way we obtain $\hat{A}_i, \hat{B}_i \in \mathbb{F}_p[a, b, 1/(ab\mathfrak{H})]$ such that $\hat{A}_i(a, b, \mathfrak{h}) = A_i(a, b)$, and $\hat{B}_i(a, b, \mathfrak{h}) = B_i(a, b)$.

With this notation, we can state [FL20, Theorem 10.1], which deals with possible powers of $\mathfrak{H}$ in the denominators:

Theorem 2.1. *Let $\nu_{\mathfrak{H}}$ denote the valuation at $\mathfrak{H}$. We have that $\nu_{\mathfrak{H}}(\hat{A}_i), \nu_{\mathfrak{H}}(\hat{B}_i) = -(ip^{i-1} + (i-1)p^{i-2})$.*

Also, as a corollary, we have [FL20, Corollary 10.2]:

Corollary 2.2. *Let $h \in \mathbb{F}_p[a, b]$ be an irreducible factor of $\mathfrak{h}$ with $h \neq a, b$ and ν_h be the valuation at h. Then, for $i \geq 1$, we have $\nu_h(A_i), \nu_h(B_i) \geq -\nu_h(\mathfrak{h})\left(ip^{i-1} + (i-1)p^{i-2}\right)$.*

Also, [FL20, Theorem 11.2] gives bounds for the powers of a and b in the denominators of $\hat{A}_i$ and $\hat{B}_i$:

Theorem 2.3. *We have:*

(1) *If* $p \equiv 1 \pmod 6$, *then:*
   (a) $\nu_a(\hat{A}_i) \geq -2p^i$ *for* $i \geq 1$;
   (b) $\nu_a(\hat{B}_i) \geq -3p^i$ *for* $i \geq 1$.

(2) *If* $p \equiv 5 \pmod 6$, *then:*
   (a) $\nu_a(\hat{A}_i) \geq -2p^i$, *for* $i = 1, 2, 3$, *and* $\nu_a(\hat{A}_i) \geq -((i-1)p^i - (i-1)p^{i-2})$ *for* $i \geq 4$;
   (b) $\nu_a(\hat{B}_i) \geq -3p^i$ *for* $i = 1, 2, 3$, *and* $\nu_a(\hat{B}_i) \geq -(ip^i - (i-1)p^{i-2})$ *for* $i \geq 4$.

(3) *For every* $p \geq 5$ *we have:*
   (a) $\nu_b(\hat{A}_i) \geq -2ip^i$, *for all* $i \geq 1$;
   (b) $\nu_b(\hat{B}_i) \geq -(2i-1)p^i$, *for all* $i \geq 1$.

Finally, [FL20, Corollary 12.2] and [FL20, Corollary 12.3] give better results about powers of a and b in the denominators of A_1 and B_1 (and not $\hat{A}_1$ and $\hat{B}_1$):

Corollary 2.4. *Let* ν_a *and* ν_b *denote the valuations at* a *and* b *respectively. Then, we have*

$$\nu_a(A_1) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 6, \\ -1, & \text{if } p \equiv 5 \pmod 6, \end{cases} \quad \text{and} \quad \nu_a(B_1) = \begin{cases} -(p-1), & \text{if } p \equiv 1 \pmod 6, \\ -(p+1), & \text{if } p \equiv 5 \pmod 6, \end{cases}$$

and

$$\nu_b(A_1) \geq \begin{cases} -p+1, & \text{if } p \equiv 1 \pmod 4, \\ -(p+1), & \text{if } p \equiv 3 \pmod 4, \end{cases} \quad \text{and} \quad \nu_b(B_1) \geq \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

3. Universality of the Second Coordinate

Let A_1 and B_1 be the coordinate functions obtained from the j-invariant construction. As stated in the introduction, the goal here is to find λ_1 such that if

$$(1, \lambda_1)^4(a, A_1) = (a, A_1') \quad \text{and} \quad (1, \lambda_1)^6(b, B_1) = (b, B_1'),$$

then $A_1' \in \mathcal{S}_{4p} \cap \mathbb{U}_\Delta$ and $B_1' \in \mathcal{S}_{6p} \cap \mathbb{U}_\Delta$, where $\mathbb{U}_\Delta \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, 1/\mathfrak{h}]$ and $\mathcal{S}_k$ as in Definition 1.1. In particular, we want $\lambda_1 \in \mathcal{S}_0$, so that $A_1' \in \mathcal{S}_{4p}$ and $B_1' \in \mathcal{S}_{6p}$. In other words, we want to prove the following theorem:

Theorem 3.1. *There are* $A_1' \in \mathcal{S}_{4p} \cap \mathbb{U}_\Delta$ *and* $B_1' \in \mathcal{S}_{6p} \cap \mathbb{U}_\Delta$, *such that if* $(a_0, b_0) \in \Bbbk^2_{\text{ord}}$ *gives the Weierstrass coefficients of an elliptic curve, then* $((a_0, A_1'(a_0, b_0)), (b_0, B_1'(a_0, b_0)))$ *gives the first two coordinates of its canonical lifting. Therefore,* A_1' *and* B_1' *are then universal*

modular functions with no Δ in the denominator. In particular, the first part of Conjecture 1.3 is true for $i = 1$.

A quick note on terminology: we shall use the term *monomial* for a product of unknowns, and hence we disregard its coefficient. We then use the term *monomial term* for the monomial with its coefficient. For instance, $2a^2 + 3ab$ has monomials a^2 and ab and monomial terms $2a^2$ and $3ab$.

Proof of Theorem 3.1. Let A_1 and B_1 be the modular functions given by the j-invariant construction, i.e., by Eqs. (1.3) and (1.4). (By Theorem 1.4, note that they are in $\mathcal{S}_{4p}$ and $\mathcal{S}_{6p}$, respectively.) Note that Eqs. (1.3) and (1.4) give us that $B_1 = (b^p/a^p)A_1$. Observing that

$$\nu_a(\mathfrak{h}) = \begin{cases} 0, & \text{if } p \equiv 1 \pmod 6, \\ 1, & \text{if } p \equiv 5 \pmod 6, \end{cases} \quad \text{and} \quad \nu_b(\mathfrak{h}) = \begin{cases} 0, & \text{if } p \equiv 1 \pmod 4, \\ 1, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

by Corollaries 2.2 and 2.4, we can write

$$A_1 = \frac{C_1 + D_1}{b^p \mathfrak{h}}$$

with $C_1, D_1 \in \mathbb{F}_p[a, b]$, where we can take C_1 to have all monomial terms of the numerator with valuation at b less than p. Now, since $b^p\mathfrak{h}$ is homogeneous of weight $7p-1$ and $A_1 \in \mathcal{S}_{4p}$, we have that C_1 and D_1 are homogeneous of weight $11p - 1$.

Then, let

$$\lambda_1 \stackrel{\text{def}}{=} \frac{-6C_1 - 4D_1}{24a^p b^p \mathfrak{h}} \tag{3.1}$$

(note that $\lambda_1 \in \mathcal{S}_0$) and $\boldsymbol{\lambda} \stackrel{\text{def}}{=} (1, \lambda_1)$. Then, $\boldsymbol{\lambda}^k = (1, k\lambda_1)$, and so $\boldsymbol{\lambda}^4(a, A_1) = (a, A_1')$, $\boldsymbol{\lambda}^6(b, B_1) = (b, B_1')$ are such that A_1' and B_1' are in $\mathcal{S}_{4p}$ and $\mathcal{S}_{6p}$ and $((a_0, A_1'(a_0, b_0)), (b_0, B_1'(a_0, b_0)))$ give the canonical lifting of the curve given by (a_0, b_0), if A_1' and B_1' are regular at (a_0, b_0). So, it suffices to show that $A_1', B_1' \in \mathbb{U}_\Delta$.

But, we have

$$A_1' = A_1 + 4a^p\lambda_1 = \frac{D_1}{3b^p\mathfrak{h}}.$$

As seen above, the monomials of D_1 have valuation at b greater than or equal to p, so $A_1' \in \mathbb{U}_\Delta$.

Now

$$B_1 = \frac{b^p}{a^p}A_1 = \frac{C_1 + D_1}{a^p\mathfrak{h}}.$$

Since the monomials in C_1 have valuation at b less than p, for its monomials to have weight $11p - 1$, we must have that their valuation at a has to be greater than or equal to p. Then,

as

$$B_1' = B_1 + 6b^p\lambda_1 = -\frac{C_1}{2a^p\mathfrak{h}},$$

we have that $B_1' \in \mathbb{U}_\Delta$. □

4. Universality of the Third Coordinate

We now turn our attention to the third coordinate. The situation is considerably more complicated in this case.

As in the previous section, we have that if λ_1 is as in Eq. (3.1), and

$$(1, \lambda_1, 0, 0, \ldots)^4(a, A_1, A_2, A_3, \ldots) = (a, A_1', A_2', A_3', \ldots),$$
$$(1, \lambda_1, 0, 0, \ldots)^6(b, B_1, B_2, B_3, \ldots) = (b, B_1', B_2', B_3', \ldots),$$

then $A_1' \in \mathbb{U}_\Delta \cap \mathcal{S}_{4p}$ and $B_1' \in \mathbb{U}_\Delta \cap \mathcal{S}_{6p}$. Therefore, now we want some λ_2 such that if we let

$$(1, 0, \lambda_2, 0, \ldots)^4(a, A_1', A_2', A_3', \ldots) = (a, A_1', A_2'', A_3'', \ldots), \tag{4.1}$$
$$(1, 0, \lambda_2, 0, \ldots)^6(b, B_1', B_2', B_3', \ldots) = (b, B_1', B_2'', B_3'', \ldots), \tag{4.2}$$

then $A_2'' \in \mathbb{U}_\Delta \cap \mathcal{S}_{4p^2}$ and $B_2'' \in \mathbb{U}_\Delta \cap \mathcal{S}_{6p^2}$.

With the notation from Theorem 3.1, we write

$$A_1 = \frac{C_1 + D_1}{b^p\mathfrak{h}}, \quad B_1 = \frac{C_1 + D_1}{a^p\mathfrak{h}},$$

with $C_1, D_1 \in \mathbb{F}_p[a, b]$, and where C_1 contains all the monomial terms with valuation at b less than p.

By Theorems 2.1 and 2.3, we can also write

$$A_2 = \frac{C_2 + D_2 + E_2}{a^{2p^2}b^{4p^2}\mathfrak{h}^{2p+1}}, \quad B_2 = \frac{C_2 + D_2 + E_2}{a^{3p^2}b^{3p^2}\mathfrak{h}^{2p+1}}, \tag{4.3}$$

where D_2 contains all the terms with monomials a^ib^j such that $i \geq 2p^2$ and $j \geq 4p^2$, E_2 contains all the terms with monomials a^ib^j such that either $i < 2p^2$ or $j < 3p^2$, and C_2 contains the remaining terms.

Lemma 4.1. *In C_2 (as above), we have that every monomial a^ib^j satisfies $i, j \geq 3p^2$.*

Proof. Of course, by definition, we must have that the monomials a^ib^j from C_2 must satisfy $i \geq 2p^2$ and $3p^2 \leq j < 4p^2$. But note that we have $\mathrm{wgt}(A_2) = 4p^2$ (and $\mathrm{wgt}(\mathfrak{h}) = p - 1$), so

if $i < 3p^2$, we would have

$$\begin{aligned} 4p^2 &= 4i + 6j - (8p^2 + 24p^2 + (2p+1)(p-1)) \\ &< 12p^2 + 24p^2 - (32p^2 + (2p+1)(p-1)) \\ &= 4p^2 - (2p+1)(p-1), \end{aligned}$$

a contradiction. □

Let now $F_1 \stackrel{\text{def}}{=} -(C_1/4 + D_1/6)$, and so $\lambda_1 = F_1/(a^p b^p \mathfrak{h})$. Our main goal in this section is to prove the following result:

Theorem 4.2. *With the notation above, if all the monomials $a^i b^j$ of*

$$E_2 - 12F_1^{2p} a^{p^2} b^{2p^2} \mathfrak{h}$$

are such that $i \geq 2p^2$ and $j \geq 3p^2$, then there is λ_2 (as in Eqs. (4.1) and (4.2)) that yields $A_2'' \in \mathbb{U}_\Delta \cap \mathcal{S}_{4p^2}$ and $B_2'' \in \mathbb{U}_\Delta \cap \mathcal{S}_{6p^2}$.

Unfortunately we were unable to prove that the above condition holds in general, but it allowed us, with the help of the computer, to show such λ_2 exists for p between 5 and 31.

First we need to study how λ_1 affected A_2 and B_2, i.e., we need to describe A_2' and B_2'.

Lemma 4.3. *We can write*

$$\begin{aligned} A_2' &= \frac{F_2 + 4E_2' + 6F_1^{2p} a^{p^2} b^{2p^2} \mathfrak{h} + E_2}{a^{2p^2} b^{4p^2} \mathfrak{h}^{2p+1}}, \\ B_2' &= \frac{G_2 + 6E_2' + 15F_1^{2p} a^{p^2} b^{2p^2} \mathfrak{h} + E_2}{a^{3p^2} b^{3p^2} \mathfrak{h}^{2p+1}}, \end{aligned}$$

where $E_2' \stackrel{\text{def}}{=} F_1^p (C_1 + D_1)^p a^{p^2} b^{2p^2} \mathfrak{h}$, and each monomial $a^i b^j$ of either F_2 or G_2 is such that $i \geq 2p^2$ and $j \geq 3p^2$. Moreover, $A_2' \in \mathcal{S}_{4p^2}$ and $B_2' \in \mathcal{S}_{6p^2}$.

Proof. We start by observing that

$$(1, \lambda_1, 0)^r = \left(1, r\lambda_1, \binom{r}{2}\lambda_1^{2p} + \frac{r - r^p}{p}\lambda_1^p\right). \tag{4.4}$$

(Of course, note that $(r - r^p)/p \in \mathbb{Z}$.) This gives us

$$A_2' = 6\lambda_1^{2p} a^{p^2} + \frac{4 - 4^p}{p}\lambda_1^p a^{p^2} + 4\lambda_1^p A_1^p + A_2 - \sum_{k=1}^{p-1} \left(\frac{1}{p}\binom{p}{k}\right) (4\lambda_1 a^p)^{p-k} A_1^k. \tag{4.5}$$

Now, since $A_1 = (C_1 + D_1)/(b^p \mathfrak{h}) \in \mathcal{S}_{4p}$ and $\lambda_1 = -(6C_1 + 4D_1)/(24 a^p b^p \mathfrak{h})$, it is clear that $\operatorname{wgt}(\lambda_1) = 0$, and therefore $A_2' \in \mathcal{S}_{4p^2}$.

We now consider each term in Eq. (4.5) above. First, we have

$$6\lambda_1^{2p}a^{p^2} = \frac{6F_1^{2p}a^{p^2}b^{2p^2}\mathfrak{h}}{a^{2p^2}b^{4p^2}\mathfrak{h}^{2p+1}}.$$

Then, if we let

$$F_{2,1} \stackrel{\text{def}}{=} \frac{4-4^p}{p}F_1^p a^{2p^2}b^{3p^2}\mathfrak{h}^{p+1},$$

we have

$$\frac{4-4^p}{p}\lambda_1^p a^{p^2} = \frac{F_{2,1}}{a^{2p^2}b^{4p^2}\mathfrak{h}^{2p+1}}.$$

Observe that each monomial a^ib^j of $F_{2,1}$ is such that $i \geq 2p^2$ and $j \geq 3p^2$.

Next, letting

$$E_2' \stackrel{\text{def}}{=} F_1^p(C_1+D_1)^p a^{p^2}b^{2p^2}\mathfrak{h},$$

we have

$$4\lambda_1^p A_1^p = 4\frac{F_1^p(C_1+D_1)^p}{a^{p^2}b^{2p^2}\mathfrak{h}^{2p}} = \frac{4E_2'}{a^{2p^2}b^{4p^2}\mathfrak{h}^{2p+1}}.$$

Then, by letting $F_{2,2} \stackrel{\text{def}}{=} C_2 + D_2$, we have

$$A_2 = \frac{F_{2,2}+E_2}{a^{2p^2}b^{4p^2}\mathfrak{h}^{2p+1}}.$$

Observe that, by the definition of D_2 and Lemma 4.1, each monomial a^ib^j of $F_{2,2}$ is such that $i \geq 2p^2$ and $j \geq 3p^2$.

Finally, letting

$$F_{2,3,k} \stackrel{\text{def}}{=} -\left(\frac{1}{p}\binom{p}{k}\right)(4F_1)^{p-k}(C_1+D_1)^k a^{2p^2}b^{3p^2}\mathfrak{h}^{p+1},$$

we have

$$-\left(\frac{1}{p}\binom{p}{k}\right)(4\lambda_1 a^p)^{p-k}A_1^k = -\left(\frac{1}{p}\binom{p}{k}\right)\frac{(4a^pF_1)^{p-k}}{a^{p(p-k)}b^{p(p-k)}\mathfrak{h}^{p-k}}\frac{(C_1+D_1)^k}{b^{kp}\mathfrak{h}^k}$$

$$= \frac{F_{2,3,k}}{a^{2p^2}b^{4p^2}\mathfrak{h}^{2p+1}}.$$

Note that, clearly, each monomial a^ib^j of $F_{2,3,k}$ is such that $i \geq 2p^2$ and $j \geq 3p^2$.

Defining then

$$F_2 \stackrel{\text{def}}{=} F_{2,1} + F_{2,2} + \sum_{k=1}^{p-1} F_{2,3,k},$$

it's clear that each monomial a^ib^j of F_2 is such that $i \geq 2p^2$ and $j \geq 3p^2$, and the formula for A_2' in the statement holds.

The proof of the formula for B_2' is obtained in a similar way. □

The next lemma has the crucial idea behind the proof of Theorem 4.2:

Lemma 4.4. *Suppose that all the monomials $a^i b^j$ of*

$$E_2 - 12F_1^{2p} a^{p^2} b^{2p^2} \mathfrak{h}$$

are such that $i \geq 2p^2$ and $j \geq 3p^2$. Then, we can write

$$A_2' = \frac{C_2' + D_2' + 4E_2''}{a^{2p^2} b^{4p^2} \mathfrak{h}^{2p+1}}, \quad B_2' = \frac{C_2'' + D_2'' + 6E_2''}{a^{3p^2} b^{3p^2} \mathfrak{h}^{2p+1}},$$

where:

- *each monomial $a^i b^j$ of either C_2' or C_2'' is such that $i \geq 3p^2$ and $j \geq 3p^2$,*
- *each monomial $a^i b^j$ of either D_2' or D_2'' is such that $i \geq 2p^2$ and $j \geq 4p^2$,*
- *each monomial $a^i b^j$ of E_2'' is such that $i < 2p^2$ or $j < 3p^2$.*

Proof. Remember that, by Lemma 4.3, we have

$$A_2' = \frac{F_2 + 4E_2' + 6F_1^{2p} a^{p^2} b^{2p^2} \mathfrak{h} + E_2}{a^{2p^2} b^{4p^2} \mathfrak{h}^{2p+1}}.$$

Let $C_{2,1}$ be the sum of the terms from F_2 with monomials $a^i b^j$ such that $i \geq 3p^2$ and $j \geq 3p^2$, and let $D_{2,1}$ be the sum of the remaining terms. (Thus, $F_2 = C_{2,1} + D_{2,1}$.)

Now, by construction, each monomial of $a^i b^j$ of F_2 is such that $i \geq 2p^2$ and $j \geq 3p^2$. Moreover, since $A_2' \in \mathcal{S}_{4p^2}$, we have that $F_2 \in \mathcal{S}_{38p^2-p-1}$. So, if $a^i b^j$ is a monomial of F_2 with $i < 3p^2$, then $6j > 26p^2 - p - 1 > 24p^2$, so $j \geq 4p^2$. Therefore, each monomial $a^i b^j$ of $D_{2,1}$ is such that $2p^2 \leq i < 3p^2$ and $j \geq 4p^2$.

We now write

$$E_2' = C_{2,2} + D_{2,2} + E_{2,2}, \quad F_1^{2p} a^{p^2} b^{2p^2} \mathfrak{h} = C_{2,3} + D_{2,3} + E_{2,3},$$

where, for $k = 2, 3$, where $D_{2,k}$ contains all the terms with monomials $a^i b^j$ such that $i \geq 2p^2$ and $j \geq 4p^2$, $E_{2,k}$ contains all the terms with monomials $a^i b^j$ such that either $i < 2p^2$ or $j < 3p^2$, and $C_{2,k}$ contains the remaining terms. Note that, similar to Lemma 4.1, we have that the monomials $a^i b^j$ from $C_{2,k}$ are such that $i, j \geq 3p^2$.

Now, by assumption, each monomial $a^i b^j$ of $E_2 - 12(C_{2,3} + D_{2,3} + E_{2,3})$ must have $i \geq 2p^2$ and $j \geq 3p^2$. Thus, by construction of $C_{2,3}$ and $D_{2,3}$, we must have that each monomial $a^i b^j$ of $E_2 - 12E_{2,3}$ must have $i \geq 2p^2$ and $j \geq 3p^2$. Therefore, similar to what was done for F_2 above, we can break

$$E_2 - 12E_{2,3} = C_{2,4} + D_{2,4},$$

where $C_{2,4}$ is the sum of every term with monomial a^ib^j such that $i \geq 3p^2$ and $j \geq 3p^2$, and $D_{2,4}$ contains the remaining terms. Again, similar to the case of F_2 above, we have that each monomial a^ib^j of $D_{2,4}$ is such that $2p^2 \leq i < 3p^2$ and $j \geq 4p^2$.

Hence, letting

$$\begin{aligned} C_2' &\stackrel{\text{def}}{=} C_{2,1} + 4C_{2,2} + 6C_{2,3} + C_{2,4}, \\ D_2' &\stackrel{\text{def}}{=} D_{2,1} + 4D_{2,2} + 6D_{2,3} + D_{2,4}, \\ E_2'' &\stackrel{\text{def}}{=} E_{2,2} + \frac{9}{2}E_{2,3}, \end{aligned}$$

gives the desired expression for A_2'.

Now, since again by Lemma 4.3 we have

$$B_2' = \frac{G_2 + 6E_2' + 15F_1^{2p}a^{p^2}b^{2p^2}\mathfrak{h} + E_2}{a^{3p^2}b^{3p^2}\mathfrak{h}^{2p+1}},$$

proceeding as above and writing $G_2 = C_{2,1}' + D_{2,1}'$, where $C_{2,1}'$ is the sum of terms from G_2 with monomials a^ib^j such that $i \geq 3p^2$ and $j \geq 3p^2$, and $D_{2,1}'$ is the sum of the remaining terms (and hence, as before, we have that each monomial a^ib^j of $D_{2,1}'$ is such that $2p^2 \leq i < 3p^2$ and $j \geq 4p^2$), we can define

$$\begin{aligned} C_2'' &\stackrel{\text{def}}{=} C_{2,1}' + 6C_{2,2} + 15C_{2,3} + C_{2,4}, \\ D_2'' &\stackrel{\text{def}}{=} D_{2,1}' + 6D_{2,2} + 15D_{2,3} + D_{2,4}, \end{aligned}$$

to establish the desired expression for B_2'. □

We finally can prove Theorem 4.2.

Proof of Theorem 4.2. By Lemma 4.4, we have

$$A_2' = \frac{C_2' + D_2' + 4E_2''}{a^{2p^2}b^{4p^2}\mathfrak{h}^{2p+1}}, \quad B_2' = \frac{C_2'' + D_2'' + 6E_2''}{a^{3p^2}b^{3p^2}\mathfrak{h}^{2p+1}}.$$

Let

$$\lambda_2 \stackrel{\text{def}}{=} \frac{-\frac{1}{4}C_2' - \frac{1}{6}D_2'' - E_2''}{a^{3p^2}b^{4p^2}\mathfrak{h}^{2p+1}}.$$

As $(1, 0, \lambda_2, \ldots)^k = (1, 0, k\lambda_2, \ldots)$, we have that

$$(1, 0, \lambda_2, 0, \ldots)^4(a, A_1', A_2', \ldots) = (a, A_1', A_2' + 4\lambda_2 a^{p^2}, \ldots)$$

and

$$(1, 0, \lambda_2, 0, \ldots)^6(b, B_1', B_2', B_3', \ldots) = (b, B_1', B_2' + 6\lambda_2 b^{p^2}, \ldots).$$

Then,

$$A_2'' = A_2' + 4\lambda_2 a^{p^2} = \frac{a^{p^2} D_2' - \frac{4}{6} a^{p^2} D_2''}{a^{3p^2} b^{4p^2} \mathfrak{h}^{2p+1}} \tag{4.6}$$

and

$$B_2'' = B_2' + 6\lambda_2 b^{p^2} = \frac{b^{p^2} C_2'' - \frac{6}{4} b^{p^2} C_2'}{a^{3p^2} b^{4p^2} \mathfrak{h}^{2p+1}}. \tag{4.7}$$

Now, the conditions on C_2', C_2'', D_2', and D_2'' (as stated in Lemma 4.4) give that $A_2'', B_2'' \in \mathbb{U}_\Delta$.

Finally, note that since $A_2' \in \mathcal{S}_{4p^2}$ and $B_2' \in \mathcal{S}_{6p^2}$ (as show in Lemma 4.3), the formulas from Lemma 4.4 give us that C_2', C_2'', D_2', and D_2'' all have weight $38p^2 - p - 1$, and therfore λ_2 has weight 0. Thus, Eqs. (4.6) and (4.7) give that $A_2'' \in \mathcal{S}_{4p^2}$ and $B_2'' \in \mathcal{S}_{6p^2}$. □

5. Denominator of Greenberg Transform Construction

We now turn back to the Greenberg transform construction. The main goal of this section is to prove the following result:

Theorem 5.1. *Let A_1 and B_1 be the coordinate function obtained by the Greenberg transform construction. Then, $A_1 \in \mathcal{S}_{4p} \cap \mathbb{U}_\Delta$ and $B_1 \in \mathcal{S}_{6p} \cap \mathbb{U}_\Delta$. Therefore, both parts of Conjecture 1.3 are true for $i = 1$.*

Before we can prove this, we need to review the Greenberg transform construction. Since we will only deal with the second coordinate, we will only look at the first two coordinates of this construction, which is much simpler, but the general construction for any length can be found in [Fin20].

The construction is based on an algorithm for the computation of the canonical lifting by Voloch and Walker, which instead of using the modular polynomial (as in [LST64]), uses the *elliptic Teichmüller lift*: if σ denotes the Frobenius of both $\Bbbk$ and $\boldsymbol{W}(\Bbbk)$, $\phi : E \to E^\sigma$ denotes the p-th power Frobenius, and $\boldsymbol{\phi} : \boldsymbol{E} \to \boldsymbol{E}^\sigma$ denotes its lift to $\boldsymbol{E}$, the elliptic Teichmüller lift $\tau : E(\Bbbk) \to \boldsymbol{E}(\boldsymbol{W}(\Bbbk))$ is a section of the reduction modulo p (and an injective homomorphism of groups) that makes the following diagram commute:

$$\begin{array}{ccc} \boldsymbol{E}(\boldsymbol{W}(\Bbbk)) & \xrightarrow{\boldsymbol{\phi}} & \boldsymbol{E}^\sigma(\boldsymbol{W}(\Bbbk)) \\ {\scriptstyle\pi}\downarrow \uparrow{\scriptstyle\tau} & & {\scriptstyle\pi}\downarrow \uparrow{\scriptstyle\tau^\sigma} \\ E(\Bbbk) & \xrightarrow{\phi} & E^\sigma(\Bbbk) \end{array}$$

In [VW00, Theorem 4.2], we have:

Theorem 5.2. *Let $\Bbbk$ be a perfect field of characteristic $p > 0$ and*

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

be an ordinary elliptic curve with Hasse invariant $\mathfrak{h}_0 = \mathfrak{h}(a_0, b_0)$. *Suppose that:*

(1) $\boldsymbol{E}/\boldsymbol{W}_2(\Bbbk)$, *where* $\boldsymbol{W}_2(\Bbbk)$ *is the ring of Witt vectors of length* 2 *over* $\Bbbk$, *is an elliptic curves that reduces to* E *modulo* p;
(2) *there is a section of the reduction* $\tau : E(\Bbbk) \setminus \{\mathcal{O}\} \to \boldsymbol{E}(\boldsymbol{W}_2(\Bbbk)) \setminus \{\boldsymbol{\mathcal{O}}\}$, *where* $\mathcal{O}$ *and* $\boldsymbol{\mathcal{O}}$ *represent the points at infinity of* E *and* $\boldsymbol{E}$ *respectively;*
(3) $\tau(x_0, y_0) = ((x_0, F_1(x_0)), (y_0, y_0 H_1(x_0)))$, *with* $F_1, H_1 \in \Bbbk[x_0]$ *and* $\deg F_1 \leq (3p-1)/2$ *and* $\deg H_1 \leq (4p-3)/2$.

Then τ *is regular at* $\mathcal{O}$, $\boldsymbol{E}$ *is the canonical lifting of* E *(modulo* p^2*), and* τ *is the elliptic Teichmüller lift.*

Moreover, if $\tau(x_0, y_0) = ((x_0, F_1(x_0)), (y_0, y_0 H_1(x_0)))$ *is the elliptic Teichmüler lift, then*

$$F_1' = \mathfrak{h}_0^{-1}(x_0^3 + a_0 x_0 + b_0)^{(p-1)/2} - x_0^{p-1}. \tag{5.1}$$

(Note that Eq. (5.1) is not in the statement of [VW00, Theorem 4.2], but is proved in its proof.)

We then use the theorem above to compute the canonical lifting in this construction. Since we want to obtain general formulas, we will consider again

$$E/\mathbb{K} \ : \ y_0^2 = f(x_0) \stackrel{\text{def}}{=} x_0^3 + a x_0 + b,$$

where, as before, $\mathbb{K} \stackrel{\text{def}}{=} \mathbb{F}_p(a, b)$, with a and b indeterminates. Let's also denote $\mathbb{S} \stackrel{\text{def}}{=} \mathbb{F}_p[a, b]$. Since $\mathfrak{h}$ (the coefficient of x_0^{p-1} in $f^{(p-1)/2}$) is not zero, we can find its canonical lifting. Let then,

$$\boldsymbol{E}/\boldsymbol{W}_2(\mathbb{K}) \ : \ \boldsymbol{y}^2 = \boldsymbol{x}^3 + (a, A_1)\boldsymbol{x} + (b, B_1)$$

be the first two coordinates of its canonical lifting, where A_1 and B_1 are still unknown. By replacing $\boldsymbol{x}$ by (x_0, x_1) and $\boldsymbol{y}$ by (y_0, y_1), where x_0, y_0, x_1, and y_1 are all indeterminates, we can expand the equation for $\boldsymbol{E}$ above using sums and products of Witt vectors. The variety over $\mathbb{K}$ obtained by equating the coordinates of the Witt vectors obtained this way is called the *Greenberg transform* of $\boldsymbol{E}$ and denoted by $G(\boldsymbol{E})$. (To be precise, the Greenberg transform is given by the infinitely many equations we obtain when we use infinite Witt vectors. But here we will only consider the first two coordinates.) It's clear then that we have a natural bijection between $\boldsymbol{E}(\boldsymbol{W}_2(\mathbb{K}))$ and $G(\boldsymbol{E})(\mathbb{K})$, given by $((x_0, x_1), (y_0, y_1)) \mapsto (x_0, y_0, x_1, y_1)$.

The second coordinate of the Greenberg transform of $\boldsymbol{E}$ is given by

$$2y_0^p y_1 = (f')^p x_1 + A_1 x_0^p + B_1 + \eta_1(f), \tag{5.2}$$

where $\eta_1(f)$ is defined as follows: consider the polynomial

$$\eta_1(X,Y,Z) \stackrel{\text{def}}{=} \frac{X^p + Y^p + Z^p - (X+Y+Z)^p}{p}.$$

Then, $\eta_1 \in \mathbb{Z}[X,Y,Z]$ and we can define $\eta_1(f) \stackrel{\text{def}}{=} \eta_1(x_0^3, a_0x_0, b_0)$. (This notation for η_1 is the same used in [Fin14], where a more general formula for the Greenberg transform is given.) Therefore, it is clear that $\eta_1(f) \in \mathbb{S}[x_0]$.

Following Theorem 5.2, we need that $\tau(x_0, x_1) = ((x_0, F_1), (y_0, y_0H_1))$, for some polynomials F_1 and H_1, should give a point in $G(\boldsymbol{E})$. Therefore, we must have

$$2y_0^{p+1}H_1 = (f')^pF_1 + A_1x_0^p + B_1 + \eta_1(f),$$

or, using $y_0^2 = f$, we have

$$2f^{(p+1)/2}H_1 = (f')^pF_1 + A_1x_0^p + B_1 + \eta_1(f), \tag{5.3}$$

where now we have no term in y_0 left.

Again, by Theorem 5.2, we know $F_1' = \mathfrak{h}^{-1}f^{(p-1)/2} - x_0^{p-1}$. Of course, since we are in characteristic $p > 0$, this means we know, by formal integration, all terms of F_1 except for terms in x_0^{kp}, for $k \geq 0$. On the other hand, we also know that $\deg F_1 \leq (3p-1)/2$, and therefore we can write

$$F_1 = \hat{F}_1 + c_1x_0^p + c_0,$$

where $\hat{F}_1$ is the formal integral of $\mathfrak{h}^{-1}f^{(p-1)/2} - x_0^{p-1}$, and only c_1 and c_0 are unknown. (Note that $\hat{F}_1 \in \mathbb{U}_\Delta[x_0]$, where $\mathbb{U}_\Delta \stackrel{\text{def}}{=} \mathbb{F}_p[a,b,1/\mathfrak{h}]$.)

By letting $g \stackrel{\text{def}}{=} \eta_1(f) + (f')^p\hat{F}_1$, and thus $g \in \mathbb{U}_\Delta[x_0]$, we can rewrite Eq. (5.3) as

$$2f^{(p+1)/2}H_1 = (f')^p(c_1x_0^p + c_0) + A_1x_0^p + B_1 + g. \tag{5.4}$$

Thus, the unknowns on the right-hand side are c_0, c_1, A_1, and B_1. Although we do not know much about the left-hand side, we do know that H_1 must be a polynomial, and thus if divide the right-hand side by $2f^{(p+1)/2}$, we must have that remainder is zero.

Performing this division and setting the remainder equal to zero gives us a linear system in the four unknowns. By Theorem 5.2, finding a solution will give us the canonical lifting (i.e., A_1 and B_1) and F_1 (i.e., c_0 and c_1), from which we can find H_1 (as the quotient of the division).

Now, [Fin20] states that (in this case) if we take $c_1 = 0$, then the obtained A_1 and B_1 are in $\mathcal{S}_{4p} \cap \mathbb{U}$ and $\mathcal{S}_{6p} \cap \mathbb{U}$, where $\mathbb{U} \stackrel{\text{def}}{=} \mathbb{F}_p[a,b,1/(\Delta\mathfrak{h})]$. This is what we call *the Greenberg transform construction* (for two coordinates) of A_1 and B_1.

Therefore, to prove Theorem 5.1, we need to prove that choosing $c_1 = 0$ gives $A_1, B_1 \in \mathbb{U}_\Delta$.

Proof of Theorem 5.1. We take then $c_1 = 0$, and hence Eq. (5.4) becomes

$$2f^{(p+1)/2}H_1 = (f')^p c_0 + A_1 x_0^p + B_1 + g. \tag{5.5}$$

We need to look at the remainder of the division of the right-hand side when divided by $f^{(p+1)/2}$.

Let

$$\begin{aligned}(f')^p &= f^{(p+1)/2}q_1 + r_1,\\ g &= f^{(p+1)/2}q_2 + r_2,\end{aligned}$$

with $\deg r_i \leq (3p+1)/2$. Note that since $f^{(p+1)/2}$ is monic and $g, (f')^p \in \mathbb{U}_\Delta[x_0]$, we have that $q_i, r_i \in \mathbb{U}_\Delta[x_0]$. Then,

$$(f')^p c_0 + A_1 x_0^p + B_1 + g = f^{(p+1)/2}(c_0 q_1 + q_2) + (c_0 r_1 + r_2 + A_1 x_0^p + B_1).$$

Let then

$$r \stackrel{\text{def}}{=} (c_0 r_1 + r_2 + A_1 x_0^p + B_1). \tag{5.6}$$

So, $\deg r \leq (3p+1)/2$, and hence r is the remainder in question. We shall now explicitly find r_1.

Let

$$f^{(p-1)/2} = \sum_{i=0}^{(3p-3)/2} e_i x_0^i,$$

and define

$$\hat{q} \stackrel{\text{def}}{=} \sum_{i=0}^{p-1} e_i x_0^i \qquad \text{and} \qquad q \stackrel{\text{def}}{=} 3\,\frac{f^{(p-1)/2} - \hat{q}}{x_0^p}.$$

Therefore, we have $q \in \mathbb{S}[x_0]$ and

$$\begin{aligned}(f')^p - f^{(p+1)/2}q &= (3x_0^{2p} + a^p) - 3\,\frac{f^p - f^{(p+1)/2}\hat{q}}{x_0^p}\\ &= (3x_0^{2p} + a^p) - \frac{3x_0^{3p} + 3a^p x_0^p + 3b^p - 3f^{(p+1)/2}\hat{q}}{x_0^p}\\ &= -2a^p + 3\,\frac{f^{(p+1)/2}\hat{q} - b^p}{x_0^p}.\end{aligned}$$

(Note that since $q \in \mathbb{S}[x_0]$, clearly the expression above is in $\mathbb{S}[x_0]$.) One can clearly see that the degree of the expression above is equal to $(3p+1)/2$ with leading coefficient $3e_{p-1} = 3\mathfrak{h}$. Therefore, the expression above must be r_1 and $q_1 = q$.

We then look at the coefficient of $x_0^{(3p+1)/2}$ in r (given by Eq. (5.6)). Since the remainder must be zero, this coefficient must be zero. On the other hand, this coefficient is clearly equal to c_0 times the coefficient of $x_0^{(3p+1)/2}$ in r_1, which, as we have just seen, is equal to $3\mathfrak{h}$, plus the coefficient of $x_0^{(3p+1)/2}$ in r_2, which must be in $\mathbb{U}_\Delta$, as observed above. Hence, solving for c_0, we get that $c_0 \in \mathbb{U}_\Delta$.

Now, since then $c_0 r_1, r_2 \in \mathbb{U}_\Delta[x_0]$, the equations for the coefficients of x_0^p and the constant term in $r = 0$, give us that $A_1, B_1 \in \mathbb{U}_\Delta$. □

6. Factors of the Hasse Invariant

In [FL20], the authors checked (with MAGMA) that for all primes $p \leq 997$, the Hasse invariant has no repeated irreducible factor. We now prove this result in general:

Theorem 6.1. *The Hasse invariant polynomial $\mathfrak{h}$ (for $p \geq 5$) has no repeated irreducible factor, i.e., if h is an irreducible factor of $\mathfrak{h}$, then $h^2 \nmid \mathfrak{h}$.*

As a consequence, we can improve on [FL20, Corollary 10.2]:

Corollary 6.2. *Let $h \in \mathbb{F}_p[a,b]$ be an irreducible factor of $\mathfrak{h}$, with $h \neq a, b$. Then, for $i \geq 1$, we have $\nu_h(A_i), \nu_h(B_i) \geq -\left(ip^{i-1} + (i-1)p^{i-2}\right)$.*

Proof. Corollary 2.2 states that

$$\nu_h(A_i), \nu_h(B_i) \geq -\nu_h(\mathfrak{h})\left(ip^{i-1} + (i-1)p^{i-2}\right),$$

and by Theorem 6.1, we have $\nu_h(\mathfrak{h}) = 1$. □

The remaining of this section will be devoted to the proof of Theorem 6.1. The proof is based on the relation between the Hasse invariant and the *supersingular polynomial* ss_p, as outlined in [Fin09]. (Although we will not need it here, remember that the supersingular polynomial is the polynomial given by $\mathrm{ss}_p(X) \stackrel{\text{def}}{=} \prod_{j \text{ supersing.}}(X - j)$.)

We shall need some notation and definitions from [Fin09]: let $r \stackrel{\text{def}}{=} (p-1)/2$, $r_1 \stackrel{\text{def}}{=} \lceil r/3 \rceil$, and $r_2 \stackrel{\text{def}}{=} \lfloor r/2 \rfloor$. Then, define

$$F(X) \stackrel{\text{def}}{=} \sum_{i=r_1}^{r_2} \binom{r}{i}\binom{i}{3i-r} X^{i-r_1}. \tag{6.1}$$

As seen right before [Fin09, Proposition 4.1], we have

$$\mathfrak{h} = \frac{b^{r-2r_1}}{a^{r-3r_1}} \cdot F\left(\frac{a^3}{b^2}\right). \tag{6.2}$$

We also have:

Lemma 6.3. *The polynomial F has no repeated irreducible factor.*

Proof. By [Fin09, Proposition 4.2], we have that F satisfies the following differential equation:

$$X(4X+27)F'' + (8(r_1+1)X + 27(2r_1+1))F' + \left(4r_1 + \frac{31}{36}\right)F = 0. \tag{6.3}$$

It's clear from it's definition that $F(0) \neq 0$. Also, as observed after [Fin09, Lemma 3.1], we have $F(-27/4) \neq 0$. Therefore, if $F(x_0) = F'(x_0) = 0$, we have that $x_0 \neq 0, -27/4$, and thus $F''(x_0) = 0$. But, taking derivatives of Eq. (6.3), we'd then have that $F^{(k)}(x_0) = 0$ for all $k \geq 0$, which is a contradiction.

Hence, F has no repeated root, and therefore no repeated irreducible factor. □

Now, by Eq. (6.2), we have

$$\mathfrak{h} = \sum_{i=r_1}^{r_2} \binom{r}{i}\binom{i}{3i-r} a^{3i-r} b^{r-2i}.$$

Thus, if we let

$$\bar{\mathfrak{h}} \stackrel{\text{def}}{=} \frac{\mathfrak{h}}{a^{3r_1-r}b^{r-2r_2}} = \sum_{i=r_1}^{r_2} \binom{r}{i}\binom{i}{3i-r} a^{3(i-r_1)} b^{2(r_2-i)} \in \mathbb{F}_p[a,b], \tag{6.4}$$

we have that $a, b \nmid \bar{\mathfrak{h}}$, and $\bar{\mathfrak{h}} \in \mathcal{S}_{12(r_2-r_1)}$. Furthermore, note that since $3r_1 - r, r - 2r_2 \in \{0,1\}$, in order to prove Theorem 6.1, it suffices to show that $\bar{\mathfrak{h}}$ has no repeated irreducible factor.

Lemma 6.4. *Let $\bar{\mathbb{F}}_p$ denote the algebraic closure of $\mathbb{F}_p$. Then, every factor of $\bar{\mathfrak{h}}$ is in $\bar{\mathbb{F}}_p[a^3, b^2]$.*

Proof. Let $h \in \bar{\mathbb{F}}_p[a,b]$ be a irreducible factor of $\bar{\mathfrak{h}}$. Since $\bar{\mathfrak{h}}$ is homogeneous (with $\operatorname{wgt}(a) = 4$, $\operatorname{wgt}(b) = 6$), we have that h must also be homogeneous, say $\operatorname{wgt}(h) = k$. Since, moreover, $h \notin \bar{\mathbb{F}}_p$ and $a, b \nmid \bar{\mathfrak{h}}$, we have that

$$h = c_1 a^m + c_2 b^n + abh_1,$$

with $c_1, c_2 \in \bar{\mathbb{F}}_p^\times$ and $h_1 \in \bar{\mathbb{F}}_p[a,b]$. But then, if $a^i b^j$ is a monomial of h, we have $4i + 6j = k = 4m = 6n$, and so $3 \mid i$ and $2 \mid j$. □

Therefore, if we let

$$\bar{\mathfrak{h}}_1 \stackrel{\text{def}}{=} \sum_{i=r_1}^{r_2} \binom{r}{i}\binom{i}{3i-r} u^{i-r_1} v^{r_2-i} \in \mathbb{F}_p[u,v], \tag{6.5}$$

and assign $\operatorname{wgt}(u) = \operatorname{wgt}(v) = 1$, then $\bar{\mathfrak{h}}_1$ is homogeneous of weight $r_2 - r_1$, it has no factors of u or v, $\bar{\mathfrak{h}}_1(a^3, b^2) = \bar{\mathfrak{h}}$ (by Eq. (6.4)), and the lemma above tells us if $\bar{\mathfrak{h}}_1$ has no repeated factors, then neither does $\bar{\mathfrak{h}}$, which would finish the proof of Theorem 6.1. But that is indeed the case:

Lemma 6.5. *We have that $\bar{\mathfrak{h}}_1$ has no repeated irreducible factor.*

Proof. Suppose then that $\bar{\mathfrak{h}}_1(u,v) = P(u,v)^2 \cdot Q(u,v)$, with P irreducible. But note that, by Eqs. (6.1) and (6.5), we have $\bar{\mathfrak{h}}_1(X,1) = F(X)$, and then by Lemma 6.3, we must have that $P(X,1) \in \bar{\mathbb{F}}_p^{\times}$. But, since $P(u,v)$ must be homogeneous of positive weight and $v \nmid \bar{\mathfrak{h}}_1$, we must have $P(u,v)$ has a monomial of the form u^m, and hence $P(X,1)$ cannot be constant. Therefore, we have a contradiction, and $\bar{\mathfrak{h}}_1$ has no repeated factors. □

Note that $\mathfrak{h}$ does not need to be irreducible. For instance, for $p = 11$, we have $\mathfrak{h} = 9ab$. Moreover, if $p = 29$ we have $\mathfrak{h} = a(a^3 + 2b^2)(a^3 + 22b^2)$, so $\bar{\mathfrak{h}}$ is not irreducible in general either.

References

[Deu41] M. Deuring. Die typen der multiplikatorenringe elliptischer funktionenköper. *Abh. Math. Sem. Univ. Hamburg*, 14:197–272, 1941.

[Fin09] L. R. A. Finotti. A formula for the supersingular polynomial. *Acta Arith.*, 139(3):265–273, 2009.

[Fin10] L. R. A. Finotti. Lifting the j-invariant: Questions of Mazur and Tate. *J. Number Theory*, 130(3):620 – 638, 2010.

[Fin11] L. R. A. Finotti. Computations with Witt vectors of length 3. *J. Théor. Nombres Bordeaux*, 23(2):417–454, 2011.

[Fin12] L. R. A. Finotti. Nonexistence of pseudo-canonical liftings. *Int. J. Number Theory*, 8(1):31–51, 2012.

[Fin13] L. R. A. Finotti. Coordinates of the j-invariant of the canonical lifting. *Funct. Approx. Comment. Math.*, 49(1):57–72, 2013.

[Fin14] L. R. A. Finotti. Computations with Witt vectors and the Greenberg transform. *Int. J. Number Theory*, 10(6):1431–1458, 2014.

[Fin20] L. R. A Finotti. Weierstrass coefficients of the canonical lifting. *Int. J. Number Theory*, 16(2):397–422, 2020.

[FL20] L. R. A. Finotti and D. Li. Denominator of the weierstrass coefficients of the canonical lifting. Available at `http://www.math.utk.edu/~finotti`, 2020.

[LST64] J. Lubin, J-P. Serre, and J. Tate. Elliptic curves and formal groups. *Proc. of Woods Hole summer institute in algebraic geometry*, 1964. Unpublished. Available at `http://www.ma.utexas.edu/users/voloch/lst.html`.

[VW00] J. F. Voloch and J. L. Walker. Euclidean weights of codes from elliptic curves over rings. *Trans. Amer. Math. Soc.*, 352(11):5063–5076, 2000.

Department of Mathematics, University of Tennessee, Knoxville, TN, 37996
Email address: `lfinotti@utk.edu`
URL: `www.math.utk.edu/~finotti`

Department of Mathematics, University of Tennessee, Knoxville, TN, 37996
Email address: `dli24@vols.utk.edu`
URL: `sites.google.com/vols.utk.edu/delongli/home`