DENOMINATORS OF THE WEIERSTRASS COEFFICIENTS OF THE CANONICAL LIFTING

LUÍS R. A. FINOTTI AND DELONG LI

ABSTRACT. Given an ordinary elliptic curve $E/\Bbbk : y_0^2 = x_0^3 + a_0x_0 + b_0$ over a field $\Bbbk$ of characteristic $p \geq 5$ with j-invariant j_0, the j-invariant of its canonical lifting $\boldsymbol{E}/\boldsymbol{W}(\Bbbk)$: $\boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{a}\boldsymbol{x} + \boldsymbol{b}$ is $\boldsymbol{j} = (j_0, J_1(j_0), J_2(j_0), \ldots)$, for some $J_i \in \mathbb{F}_p(X)$. Thus the Weierstrass coefficients of $\boldsymbol{E}$ can be given by $\boldsymbol{a} = \boldsymbol{\lambda}^4 \cdot 27\boldsymbol{j}/(6912 - 4\boldsymbol{j})$, $\boldsymbol{b} = \boldsymbol{\lambda}^6 \cdot 27\boldsymbol{j}/(6912 - 4\boldsymbol{j})$, where $\boldsymbol{\lambda} = ((b_0/a_0)^{1/2}, 0, 0, \ldots)$, and therefore can be seen as functions on (a_0, b_0). Here we study the denominators of the coordinates of these $\boldsymbol{a}$ and $\boldsymbol{b}$. We show that the only possible factors for these denominators are powers of a_0, b_0, and the Hasse invariant $\mathfrak{h}$. Upper bounds for these powers are given for each one of them.

1. INTRODUCTION

In this introduction we shall give a general idea of the main focus and results of this paper, while in order to not overextend this overview, we shall leave more precise definitions and statements for the following sections.

The main topic of this paper is explicit computations of the Weierstrass coefficients of the canonical lifting. In [Fin19] the first author gave an algorithm to produce formulas for these coefficients and then discussed their properties. The formulas are not unique, since the canonical lifting is only unique up to isomorphism, and so the Weierstrass coefficients can be changed. But the formulas derived in this reference have many desirable properties. More precisely, here is one of the its main results, namely [Fin19, Theorem 2.3]:

Theorem 1.1. *Given a prime $p \geq 5$, there are (explicitly computable) rational functions $A_i, B_i \in \mathbb{U} \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, 1/(\Delta\mathfrak{h})]$, where $\Delta = 4a^3 + 27b^2$ and $\mathfrak{h}$ is the coefficient of x_0^{p-1} in $(x_0^3 + ax_0 + b)^{(p-1)/2}$, such that if $\Bbbk$ is a field of characteristic p and*

$$E/\Bbbk \ : \ y_0^2 = x_0^3 + a_0x_0 + b_0$$

is any *ordinary elliptic curve, then the elliptic curve over the ring of Witt vectors $\boldsymbol{W}(\Bbbk)$ given by*

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

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

with $\boldsymbol{a} = (a_0, A_1(a_0,b_0), A_2(a_0,b_0), \ldots)$, *and* $\boldsymbol{b} = (b_0, B_1(a_0,b_0), B_2(a_0,b_0), \ldots)$, *is the canonical lifting of* E.

Moreover, if a *and* b *have weights* 4 *and* 6 *respectively, then these functions can be taken so that* A_i *and* B_i *are modular functions of weights* $4p^i$ *and* $6p^i$ *respectively.*

The algorithm described in [Fin19] allows us to compute many explicit examples, and some of these can be found in the first author's GitHub page, more precisely, at `https://github.com/lrfinotti/cl_examples`.

Inspecting these examples (and others), one notices that this algorithm seems to always give $A_i, B_i \in \mathbb{U}_\Delta \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, 1/\mathfrak{h}]$, i.e., it seems that Δ does not show up in the denominators. This led us to the following conjecture:

Conjecture 1.2. *There are modular functions* A_i *and* B_i *as described in Theorem 1.1 with* $A_i, B_i \in \mathbb{U}_\Delta \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, 1/\mathfrak{h}]$. *Moreover, the algorithm given in* [Fin19] *yields such modular functions.*

The problem is that it is not trivial to obtain a precise description of the denominators from the algorithm in question. In fact, the result that $A_i, B_i \in \mathbb{U}$ in the first place, follows from theoretical considerations, not from an analysis of the algorithm.

On the other hand, the j-invariant of the canonical lifting has been extensively studied by the first author (see, for instance, [Fin13]) and these can also be used to obtain (different) formulas for its Weierstrass coefficients. These known results about the j-invariant allow us to obtain more detailed information about the Weierstrass coefficients (when computed this way), and will be the approach we shall take here. (This will be more carefully discussed in Section 3.) In particular, we can get more precise information about the denominators of the rational functions that appear in these coefficients, unlike when using the algorithm from [Fin19], taking us closer the first part of Conjecture 1.2.

Unfortunately this approach has its own problems as, although the A_i's and B_i's obtained this way are indeed modular functions of the stated weight (as in Theorem 1.1), these may fail to be defined for *every* ordinary elliptic curve: in principle they give $A_i, B_i \in \mathbb{V} \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, 1/(\Delta \cdot \mathfrak{h} \cdot a \cdot b)]$, and so these might not work when the j-invariant of the ordinary elliptic curve in characteristic p is either 0 or 1728.

Although one cannot immediately remove the a's and b's from the denominators, we do prove that the formulas are in fact in $\mathbb{V}_\Delta \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, 1/(\mathfrak{h} \cdot a \cdot b)]$. (See Theorem 9.2 below.) In particular, if $p \equiv 11 \pmod{12}$, then it's known that $a, b \mid \mathfrak{h}$, which implies that $\mathbb{U}_\Delta = \mathbb{V}_\Delta$, and therefore this result proves the first part of Conjecture 1.2 for $p \equiv 11 \pmod{12}$. (This is stated as Corollary 9.3 below.)

It's also worth observing that although having single formulas (with "good" properties) that work in all cases is desirable, the cases when the ordinary elliptic curve has either $a_0 = 0$ (i.e., j-invariant 0) or $b_0 = 0$ (i.e., j-invariant 1728), for which these new formulas might fail, have well known canonical liftings: their canonical liftings have j-invariant $\boldsymbol{j} = 0$ and $\boldsymbol{j} = 1728$ respectively. Thus, in these cases we can take $A_i = B_i = 0$ for all $i \geq 1$. In other words, the formulas lose some of their desired properties, namely, the continuity at $a = 0$ and/or $b = 0$, but we *do* know values for A_i and B_i that work in those cases.

Finally, this new method also allows us to obtain a better description of the actual denominators of A_i and B_i: since $A_i, B_i \in \mathbb{V}_\Delta$, the denominators can only contain powers of a, b, or of factors of $\mathfrak{h}$, and we give upper bounds for these powers. More precisely, Corollary 10.2 gives sharp upper bounds for the power of factors of $\mathfrak{h}$ different from a and b (if either is a factor of $\mathfrak{h}$), while Theorem 11.3 gives upper bounds for the powers of a and b. These last bounds are far from sharp (as Table 11.1 shows), but in the last section, sharp bounds in the case of A_1 and B_1 are given.

2. Terminology and Definitions

We now introduce some notation and review some of the theory that will be needed throughout this paper.

Let $\Bbbk$ be a perfect field of characteristic $p > 0$. Associated to an *ordinary* elliptic curve E over $\Bbbk$, there exists a unique (up to isomorphisms) elliptic curve $\boldsymbol{E}$ over $\boldsymbol{W}(\Bbbk)$, the ring of Witt vectors over $\Bbbk$, called the *canonical lifting* of E, and a map $\tau : E(\bar{\Bbbk}) \to \boldsymbol{E}(\boldsymbol{W}(\bar{\Bbbk}))$, i.e., a *lift of points*, called the *elliptic Teichmüller lift*, characterized by the following properties:

(1) the reduction modulo p of $\boldsymbol{E}$ is E;
(2) τ is an injective group homomorphism and a section of the reduction modulo p, which we denote by π;
(3) let σ denote the Frobenius of both $\Bbbk$ and $\boldsymbol{W}(\Bbbk)$; if $\phi : E \to E^\sigma$ denotes the p-th power Frobenius, then there exists a map $\boldsymbol{\phi} : \boldsymbol{E} \to \boldsymbol{E}^\sigma$, such that the diagram

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

commutes. (In other words, there exists a *lifting of the Frobenius.*)

This concept of canonical lifting of elliptic curves was first introduced by Deuring in [Deu41] and then generalized to Abelian varieties by Serre and Tate in [LST64]. Apart from being

of independent interest, this theory has been used in many interesting applications, such as counting rational points in ordinary elliptic curves, as in Satoh's [Sat00], coding theory, as in Voloch and Walker's [VW00], and counting torsion points of curves of genus $g \geq 2$, as in Poonen's [Poo01] or Voloch's [Vol97].

In [Fin13] the first author studied the j-invariant of the canonical lifting $\boldsymbol{E}$. More precisely, there are functions J_i, for $i \in \{1, 2, \ldots\}$, such that if j_0 is the j-invariant of an *ordinary* elliptic curve, then

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

is the j-invariant of its canonical lifting (as a Witt vector). We describe in the reference above many of the properties of these functions J_i. (These are reviewed in Section 4 below.)

In a similar manner, in [Fin19] the first author studied the Weierstrass coefficients of the canonical lifting. Before we can state the main results of this last reference, we need to introduce some notation and terminology.

Definition 2.1. If $\Bbbk$ is a field of characteristic different from 2 and 3, we refer to the elliptic curve given by the Weierstrass equation

$$E/\Bbbk \ : \ y^2 = x^3 + ax + b, \tag{2.1}$$

simply as *the curve given by* (a, b). We shall implicitly assume that $\Delta \stackrel{\text{def}}{=} 4a^3 + 27b^2 \neq 0$, i.e., that the curve is non-singular.

We also need the following definition:

Definition 2.2. Let $\Bbbk$ be a field with $\mathrm{char}(\Bbbk) = p \geq 5$. We define

$$\Bbbk^2_{\mathrm{ord}} \stackrel{\text{def}}{=} \{(a_0, b_0) \in \Bbbk^2 \ : \ 4a_0^3 + 27b_0^2 \neq 0 \text{ and the curve given by } (a_0, b_0) \text{ is } \textit{ordinary}\}.$$

So, let's fix some field $\Bbbk$ with $\mathrm{char}(\Bbbk) = p \geq 5$ and $(a_0, b_0) \in \Bbbk^2_{\mathrm{ord}}$. Then, the ordinary elliptic curve

$$E/\Bbbk \ : \ y_0^2 = x_0^3 + a_0 x_0 + b_0 \tag{2.2}$$

has a canonical lifting, say $\boldsymbol{E}$, given by some pair $(\boldsymbol{a}, \boldsymbol{b}) \in \boldsymbol{W}(\Bbbk)^2$, i.e., by

$$\boldsymbol{E}/\boldsymbol{W}(\Bbbk) \ : \ \boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{a}\boldsymbol{x} + \boldsymbol{b}, \tag{2.3}$$

where $\boldsymbol{a} = (a_0, a_1, \ldots)$ and $\boldsymbol{b} = (b_0, b_1, \ldots)$. Note that we are requiring that the reduction modulo p of $\boldsymbol{a}$ and $\boldsymbol{b}$ are a_0 and b_0 respectively, and therefore $\boldsymbol{E}$ reduces to E.

Unlike with the j-invariant, the pair of Weierstrass coefficients (a_0, b_0) of E does not uniquely determine $(\boldsymbol{a}, \boldsymbol{b})$, as the canonical lifting is unique only up to isomorphism. But

certainly there are (non-unique) functions

$$A_i : \Bbbk^2_{\mathrm{ord}} \to \Bbbk, \qquad B_i : \Bbbk^2_{\mathrm{ord}} \to \Bbbk, \qquad \text{for } i \in \{1, 2, 3, \ldots\}$$

such that, if $(a_0, b_0) \in \Bbbk^2_{\mathrm{ord}}$, then the curve given by $(\boldsymbol{a}, \boldsymbol{b}) \in \boldsymbol{W}(\Bbbk)^2$, with

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

is the canonical lifting of the (ordinary) curve given by (a_0, b_0).

As observed in [Fin19], if we impose $a_0 \neq 0$ (i.e., $j_0 \neq 0$), then we can choose A_i, for all $i \geq 1$, to be *any* function, making then the choice of B_i uniquely determined, but likely undefined at $a_0 = 0$. Or, similarly, if it we impose $b_0 \neq 0$ (i.e., $j_0 \neq 1728$), then we can choose B_i, for all $i \geq 1$, to be any function. The problem then is that formulas obtained this way are not necessarily defined for *all* pairs $(a_0, b_0) \in \Bbbk^2_{\mathrm{ord}}$. This led us to the following definition:

Definition 2.3. The functions A_i's and B_i's are called *universal* if they are defined for all $(a_0, b_0) \in \Bbbk^2_{\mathrm{ord}}$.

Also, in concrete computations it could be observed that the functions A_i's and B_i's were, depending on choices made, often *modular functions*:

Definition 2.4. Let a and b be indeterminates in $\mathbb{F}_p[a, b]$, and assign them weights 4 and 6 respectively. Then, let

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

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

Note that the given weights make $\mathbb{F}_p[a, b]$ into a graded ring. Then, the sums of quotients (in $\mathbb{F}_p(a, b)$) of *homogeneous* polynomials in $\mathbb{F}_p[a, b]$ also form a graded ring $\mathcal{S}$. The set $\mathcal{S}_n$ is simply the homogeneous component of weight n of this graded ring.

We now can restate Theorem 1.1, the main result of [Fin19], with this terminology:

Theorem 2.5. *There are (explicitly computable) universal modular functions $A_i \in \mathcal{S}_{4p^i}$ and $B_i \in \mathcal{S}_{6p^i}$ (and, in particular, 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 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 its canonical lifting.

Note that if we let $\Delta = 4a^3 + 27b^2$ (the *discriminant*) and $\mathfrak{h}$ be the coefficient of x_0^{p-1} in $(x_0^3 + ax_0 + b)^{(p-1)/2}$ (the *Hasse invariant*), then $\Delta \in \mathcal{S}_{12}$, $\mathfrak{h} \in \mathcal{S}_{p-1}$, and the universality of the rational functions A_i and B_i from the theorem above is equivalent to saying that they belong to the ring $\mathbb{U} \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, 1/(\Delta\mathfrak{h})]$, as our elliptic curve is non-singular (and hence $\Delta \neq 0$) and ordinary (and hence $\mathfrak{h} \neq 0$). In fact, observe that $\Bbbk^2_{\text{ord}} = \{(a_0, b_0) \in \Bbbk^2 \ : \Delta(a_0, b_0) \cdot \mathfrak{h}(a_0, b_0) \neq 0\}$.

Also, as observed in the introduction, in all concrete examples computed with the algorithm given in [Fin19] that gives functions as in the theorem, we seem to always get $A_i, B_i \in \mathbb{U}_\Delta \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, 1/\mathfrak{h}]$, i.e., no factor of Δ appeared in the denominator of these functions, which led to Conjecture 1.2 above. But, in general, there certainly are A_i's and B_i's as in Theorem 2.5 that *do* have Δ in their denominators. Indeed, in [Fin19, Section 8] the following result is proven:

Theorem 2.6. *Suppose that both*

$$((a, A_1, \ldots, A_{n-1}, A_n), (b, B_1, \ldots, B_{n-1}, B_n))$$

and

$$((a, A_1, \ldots, A_{n-1}, A'_n), (b, B_1, \ldots, B_{n-1}, B'_n))$$

give the Weierstrass coefficients of the canonical lifting. Then there is a function λ such that

$$A'_n = A_n + 4\lambda a^{p^n}, \tag{2.4}$$

$$B'_n = B_n + 6\lambda b^{p^n}. \tag{2.5}$$

Moreover, if $A_i \in \mathcal{S}_{4p^i}$ and $B_i \in \mathcal{S}_{6p^i}$, for $i = 1, \ldots, n$, and are all universal, then $A'_n \in \mathcal{S}_{4p^n}$, $B'_n \in \mathcal{S}_{6p^n}$, and are both universal if and only if $\lambda \in \mathbb{U} \cap \mathcal{S}_0$.

So, together with the algorithm from [Fin19] to compute universal modular functions A_i's and B_i's as in Theorem 2.5 above, the result above tells us how to obtain *all* functions satisfying the properties of the theorem. And, depending on the choice of λ above, one can certainly introduce Δ in the denominator, thus obtaining $A_n, B_n \in \mathbb{U} \setminus \mathbb{U}_\Delta$ (while still satisfying all the conditions in the statement of Theorem 2.5).

Now, if this Conjecture 1.2 is true, i.e., we can get A_i's and B_i's without Δ in the denominator, then their denominators (in this case) are powers of factors of $\mathfrak{h}$, and it is therefore natural to ask if one can find upper bounds for these powers.

The problem with answering these questions is that the algorithm described involves solving an enormous linear system, in which it is hard to control the coefficients enough to know which denominators are introduced when solving it.

3. Choice of A_i's and B_i's

Since the universal modular functions from the algorithm from [Fin19] are difficult to analyze, we turn to another way to obtain the functions A_i and B_i (also described in [Fin19]): since we can compute the canonical liftings via the j-invariants (see [Fin13], for instance), another approach is to use the fact that if $\boldsymbol{j}$ is the j-invariant of the canonical lifting, then, if $\boldsymbol{j} \neq 0, 1728$, we have that

$$\boldsymbol{y}^2 = \boldsymbol{x}^3 + \frac{27\boldsymbol{j}}{4(1728-\boldsymbol{j})}\boldsymbol{x} + \frac{27\boldsymbol{j}}{4(1728-\boldsymbol{j})} \tag{3.1}$$

is an equation for the canonical lifting. On the other hand, this equation does not reduce to $y_0^2 = x_0^3 + ax_0 + b$, but this problem can be easily resolved by setting:

$$\boldsymbol{a} \stackrel{\text{def}}{=} \boldsymbol{\lambda}^4 \cdot \frac{27\boldsymbol{j}}{4(1728-\boldsymbol{j})} = (a, A_1, A_2, \cdots) \tag{3.2}$$

$$\boldsymbol{b} \stackrel{\text{def}}{=} \boldsymbol{\lambda}^6 \cdot \frac{27\boldsymbol{j}}{4(1728-\boldsymbol{j})} = (b, B_1, B_2, \cdots), \tag{3.3}$$

where

$$\boldsymbol{\lambda} \stackrel{\text{def}}{=} \left(\left(\frac{b}{a}\right)^{1/2}, 0, 0, \dots \right). \tag{3.4}$$

As observed in the introduction, the advantage of this method is that the first author has extensively studied the j-invariant of the canonical lifting as a function of the j-invariant of the ordinary elliptic curve in characteristic p. We shall review these results below, but before that we observe that in the case of $p = 5$ this method gives

$$A_1 = (2a^{12} + 3a^9b^2 + 3a^6b^4 + 3a^3b^6 + 3b^8)/(ab^4), \tag{3.5}$$

$$B_1 = (2a^{12}b + 3a^9b^3 + 3a^6b^5 + 3a^3b^7 + 3b^9)/a^6. \tag{3.6}$$

The key issue, as perhaps to be expected from the restrictions that $\boldsymbol{j} \neq 0, 1728$, is that even though these functions are modular functions of the expected weights, as we see in Theorem 5.3 below, they are *not* in general universal: in this example above, for instance, the formulas do not work for the *ordinary* elliptic curve (in characteristic 5) given by $y_0^2 = x_0^3 + x_0$, as $b_0 = 0$ (i.e., with $j_0 = 1728$) and we have b in the denominator of A_1. (But do note that $A_1 \in \mathcal{S}_{20}$ and $B_1 \in \mathcal{S}_{30}$.)

One can find MAGMA routines to compute this choice of A_i's and B_i's at GitHub, more precisely at `https://github.com/lrfinotti/witt`. The file `lift_j.m` provides the routine

```
> load 'lift_j.m';
Loading "lift_j.m"
Loading "gt.m"
Loading "witt.m"
Loading "etas.m"
> jweier(5,1);
[
  [
      a0,
      (2*a0^12 + 3*a0^9*b0^2 + 3*a0^6*b0^4 + 3*a0^3*b0^6 + 3*b0^8)/(a0*b0^4)
  ],
  [
      b0,
      (2*a0^12*b0 + 3*a0^9*b0^3 + 3*a0^6*b0^5 + 3*a0^3*b0^7 + 3*b0^9)/a0^6
  ]
]
```

FIGURE 3.1. Example of computation of Eqs. (3.5) and (3.6).

`jweier` that allows one to compute these liftings. Figure 3.1 shows how one can use it to compute the example given by Eqs. (3.5) and (3.6). The first argument of `jweier` is the characteristic, and the second is the length of the lifting minus one. (So, if the second argument is n, then the `jweier` gives $((a_0, A_1, \ldots, A_n), (b_0, B_1, \ldots, B_n))$.)

4. Lifting the j-Invariant

We now review what we know about $\boldsymbol{j}$. Since the canonical lifting is unique up to isomorphism, given an ordinary elliptic curve $E/\Bbbk$ with j-invariant j_0, we have that the j-invariant of its canonical lifting is given by $\boldsymbol{j} = (j_0, J_1(j_0), J_2(j_0), \ldots)$ for some *uniquely defined* functions $J_i : \Bbbk_{\text{ord}} \to \Bbbk$, where $\Bbbk_{\text{ord}}$ denotes the set of ordinary values of j-invariants in $\Bbbk$. B. Mazur and J. Tate asked about the nature of these functions, which motivated the first author to publish a few results on the subject: see [Fin10], [Fin11], [Fin12], and [Fin13]. Before we can quote the main results of these references, we need a little more notation.

Let

$$\mathcal{S}_p(X) \stackrel{\text{def}}{=} \frac{\text{ss}_p(X)}{X^\delta (X - 1728)^\epsilon},$$

where

$$\text{ss}_p(X) \stackrel{\text{def}}{=} \prod_{j \text{ supersing.}} (X - j)$$

is the *supersingular polynomial* (as in, for instance, [Fin09]),

$$\delta \stackrel{\text{def}}{=} \begin{cases} 0, & \text{if } p \equiv 1 \pmod 6; \\ 1, & \text{if } p \equiv 5 \pmod 6; \end{cases} \qquad \text{and} \qquad \epsilon \stackrel{\text{def}}{=} \begin{cases} 0, & \text{if } p \equiv 1 \pmod 4; \\ 1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

(Note that $\Bbbk_{\mathrm{ord}} = \{j_0 \in \Bbbk \,:\, \mathrm{ss}_p(j_0) \neq 0\}$.) Hence, $\mathcal{S}_p(X) \in \mathbb{F}_p[X]$, and $\mathcal{S}_p(0), \mathcal{S}_p(1728) \neq 0$. (Again, see, for instance, [Fin09].) Also, let

$$\iota = \begin{cases} 1, & \text{if } p \neq 31; \\ 2, & \text{if } p = 31. \end{cases}$$

We can now state the main result of [Fin13], more precisely, its Theorems 1.1 and 1.2:

Theorem 4.1. *Let J_i, for $i = 1, 2, \ldots$ be the functions giving the j-invariant of the canonical lifting described above.*

(1) *We have $J_i(X) \in \mathbb{F}_p(X)$.*
(2) *Let $p \geq 5$, $J_i = F_i/G_i$, with $F_i, G_i \in \mathbb{F}_p[X]$, $(F_i, G_i) = 1$, and G_i monic. Also, let $s_i = (i-1)p^{i-1}$, $t_i = ((i-3)p^i + ip^{i-1})/3$ and $t_i' = \max\{0, t_i\}$. Then, for* all *$i \in \mathbb{Z}_{>0}$ we have:*
   (a) $\deg F_i - \deg G_i = p^i - \iota$;
   (b) $G_i = \mathcal{S}_p(X)^{ip^{i-1}+(i-1)p^{i-2}} \cdot H_i$, *where* $H_1 = 1$, $H_2 = (X - 1728)^{\epsilon s_2}$, $H_3 = X^{\delta p^2}(X - 1728)^t$, *for some* $t \in \{0, \ldots, \epsilon s_3\}$, *and* $H_i \mid X^{\delta t_i'} \cdot (X - 1728)^{\epsilon s_i}$ *for* $i \geq 4$.

So, Theorem 4.1 above gives a relatively precise description of the denominators in the functions J_i, which in turn we use to study the denominators of the functions A_i and B_i coming from Eqs. (3.2) and (3.3), which is the main goal of this paper.

5. Witt Vectors

In this section we will briefly review some of the basic facts about Witt vectors. More details, including motivation and proofs, can be found in many sources such as Hazewinkel's [Haz09] and Borger's [Bor11]. A more friendly introduction can be found in Rabinoff's notes [Rab14].

Let p be a prime and for each non-negative integer n consider

$$W^{(n)}(X_0, \ldots, X_n) \stackrel{\text{def}}{=} X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^{n-1}X_{n-1}^p + p^n X_n,$$

the corresponding *Witt polynomial*. Then, there exist polynomials $S_i, P_i \in \mathbb{Z}[X_0, \ldots, X_i, Y_0, \ldots, Y_i]$ satisfying:

$$W^{(n)}(S_0, \ldots, S_n) = W^{(n)}(X_0, \ldots, X_n) + W^{(n)}(Y_0, \ldots, Y_n)$$

and

$$W^{(n)}(P_0, \ldots, P_n) = W^{(n)}(X_0, \ldots, X_n) \cdot W^{(n)}(Y_0, \ldots, Y_n).$$

More explicitly, we have the following recursive formulas:

$$S_n = (X_n + Y_n) + \frac{1}{p}(X_{n-1}^p + Y_{n-1}^p - S_{n-1}^p) + \cdots + \frac{1}{p^n}(X_0^{p^n} + Y_0^{p^n} - S_0^{p^n}) \tag{5.1}$$

and

$$\begin{aligned} P_n &= \frac{1}{p^n}\Big[(X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) - \\ &\qquad \Big(P_0^{p^n} + \cdots + p^{n-1} P_{n-1}^p\Big)\Big] \\ &= (X_0^{p^n} Y_n + X_1^{p^{n-1}} Y_{n-1}^p + \cdots + X_n Y_0^{p^n}) \\ &\quad + \frac{1}{p}(X_0^{p^n} Y_{n-1}^p + \cdots + X_{n-1}^p Y_0^{p^n}) \\ &\quad \vdots \\ &\quad + \frac{1}{p^n}(X_0^{p^n} Y_0^{p^n}) - \frac{1}{p^n} P_0^{p^n} - \cdots - \frac{1}{p} P_{n-1}^p \\ &\quad + p\left(X_1^{p^{n-1}} Y_n + X_2^{p^{n-2}}(Y_{n-1}^p + pY_n) + \cdots\right). \end{aligned} \tag{5.2}$$

Note that despite the denominators in the formulas, cancellations yield polynomials with coefficients in $\mathbb{Z}$.

We can then define sums and products of infinite vectors in $A^{\mathbb{Z}_{\geq 0}}$, where A is a commutative ring (with 1), say $\boldsymbol{a} = (a_0, a_1, \dots)$ and $\boldsymbol{b} = (b_0, b_1, \dots)$, by

$$\boldsymbol{a} + \boldsymbol{b} \stackrel{\text{def}}{=} (S_0(a_0, b_0), S_1(a_0, a_1, b_0, b_1), \dots)$$

and

$$\boldsymbol{a} \cdot \boldsymbol{b} \stackrel{\text{def}}{=} (P_0(a_0, b_0), P_1(a_0, a_1, b_0, b_1), \dots).$$

These operations make $A^{\mathbb{Z}_{\geq 0}}$ into a commutative ring (with 1) called the *ring of Witt vectors over* A and denoted by $\boldsymbol{W}(A)$.

Since we will deal with Witt vectors over fields of characteristic p, we may use $\bar{S}_n, \bar{P}_n \in \mathbb{F}_p[X_0, \dots, X_n, Y_0, \dots, Y_n]$, defined to be the reductions modulo p of S_n, P_n respectively, to define the addition and the multiplication of Witt vectors.

First, observe that, if we introduce a grading on $\mathbb{Z}[X_0, \dots, X_n, Y_0, \dots, Y_n]$ by defining $\operatorname{wgt}(X_i) = \operatorname{wgt}(Y_i) = p^i$, then both S_n and P_n are homogeneous of weights p^n and $2p^n$ respectively in this graded ring. This gives the following trivial lemmas:

Lemma 5.1. *The monomials $\prod_i X_i^{s_i} \prod_j Y_j^{t_j}$ occurring in $\bar{S}_n$ satisfies*

$$\sum_i s_i p^i + \sum_j t_j p^j = p^n.$$

Lemma 5.2. *Let* $\mathcal{S}^{(r)} \stackrel{\text{def}}{=} \{\boldsymbol{f} = (f_0, f_1, \ldots) \in \boldsymbol{W}(\mathbb{F}_p(a,b)) \ : \ f_i \in \mathcal{S}_{rp^i}\}$. *Then, if* $\boldsymbol{f} \in \mathcal{S}^{(r)}$ *and* $\boldsymbol{g} \in \mathcal{S}^{(s)}$, *we have that* $\boldsymbol{f} \cdot \boldsymbol{g} \in \mathcal{S}^{(r+s)}$. *Moreover, if* $r = s$, *then* $\boldsymbol{f} + \boldsymbol{g} \in \mathcal{S}^{(r)}$.

This lemma immediately gives us:

Theorem 5.3. *The functions* A_i *and* B_i *given by Eqs.* (3.2) *and* (3.3) *are in* $\mathcal{S}_{4p^i}$ *and* $\mathcal{S}_{6p^i}$ *respectively.*

Proof. The theorem follows immediately from the lemma, noticing that $J_i(1728 \cdot 4a^3/\Delta) \in \mathcal{S}_0$, by the first item of Theorem 4.1, and so $\boldsymbol{j} \in \mathcal{S}^{(0)}$, and $\boldsymbol{\lambda}^2 \in \mathcal{S}^{(2)}$ (with $\boldsymbol{\lambda}$ as in Eq. (3.4)). □

Moreover, we shall need the following lemma:

Lemma 5.4. *The monomials* $\prod_i X_i^{s_i} \prod_j Y_j^{t_j}$ *occurring in* $\bar{P}_n$ *satisfies*

$$\sum_i s_i p^i = \sum_j t_j p^j = p^n, \qquad \sum_i i s_i p^i + \sum_j j t_j p^j \leq n p^n,$$

and, for $n \geq 1$, *we also have* $s_0 + t_0 \leq p^n$. *Moreover,*

$$\bar{P}_n = \sum_{i=0}^{n} X_i^{p^{n-i}} Y_{n-i}^{p^i} + \bar{Q}_n,$$

where $\bar{Q}_n \in \mathbb{F}_p[X_0, \ldots, X_{n-1}, Y_0, \ldots, Y_{n-1}]$ *and has its monomials (as above) satisfying* $\sum_i i s_i p^i + \sum_j j t_j p^j \leq (n-1)p^n$.

Proof. The lemma, except for the $s_0 + t_0 \leq p^n$ part, is [Fin02, Lemma 2.1]. Although the lemma states

$$\sum_i i s_i p^i + \sum_j j t_j p^j < n p^n$$

for the second part, its proof actually shows the result stated above.

We now prove $s_0 + t_0 \leq p^n$ for $n \geq 1$. We proceed by induction: we have that $P_1 = X_0^p Y_1 + X_1 Y_0^p$, so the statement is true for $n = 1$.

Now, assume the statement true for P_t for $t \in \{1, \ldots, (n-1)\}$. By Eq. (5.2), noticing $(X_0^{p^n} Y_0^{p^n})/p^n - P_0^{p^n}/p^n = 0$, the statement is clear for the terms

$$\begin{aligned}
&(X_0^{p^n} Y_n + X_1^{p^{n-1}} Y_{n-1}^p + \cdots + X_n Y_0^{p^n}) \\
&\quad + \frac{1}{p}(X_0^{p^n} Y_{n-1}^p + \cdots + X_{n-1}^p Y_0^{p^n}) \\
&\quad \vdots \\
&\quad + \frac{1}{p^{n-1}}(X_0^{p^n} Y_1^{p^{n-1}} + X_1^{p^{n-1}} Y_0^{p^n}).
\end{aligned}$$

So, it remains to check for the monomials coming from $P_r^{p^{n-r}}$, for $r = 1, \dots, (n-1)$, as the remaining terms from Eq. (5.2) are multiples of p, and hence do not affect $\bar{P}_n$. But a monomial in $P_r^{p^{n-r}}$ is a product of p^{n-r} monomials of P_r:

$$\prod_{k=1}^{p^{n-r}} \left[\prod_i X_i^{s_{i,k}} \prod_j Y_j^{t_{j,k}} \right] = \prod_i X_i^{\sum_k s_{i,k}} \prod_j Y_j^{\sum_k t_{j,k}}.$$

But, by the induction hypothesis, we have that $s_{0,k} + t_{0,k} \leq p^r$, and hence

$$\sum_{k=1}^{p^{n-r}} s_{0,k} + \sum_{k=1}^{p^{n-r}} t_{0,k} = \sum_{k=1}^{p^{n-r}} (s_{0,k} + t_{0,k}) \leq p^{n-r} p^r = p^n.$$

□

We will also need the following lemma about the polynomials P_n:

Lemma 5.5. *Let $R_0 \stackrel{\text{def}}{=} X_0 Y_0$ and, recursively define*

$$\begin{aligned} R_n \stackrel{\text{def}}{=} & (X_0^{p^n} Y_n + X_1^{p^{n-1}} Y_{n-1}^p + \cdots + X_n Y_0^{p^n}) \\ & + \frac{1}{p}(X_0^{p^n} Y_{n-1}^p + \cdots + X_{n-1}^p Y_0^{p^n}) \\ & \vdots \\ & + \frac{1}{p^n}(X_0^{p^n} Y_0^{p^n}) - \frac{1}{p^n} R_0^{p^n} - \cdots - \frac{1}{p} R_{n-1}^p. \end{aligned}$$

Then R_n has integer coefficients and $\bar{P}_n = \bar{R}_n$.

Proof. The result is clear for $n = 0$, as $P_0 = R_0$. Now, assume for $i \in \{0, \dots, n-1\}$ we have $P_i = R_i + p \cdot T_i$, for some polynomials T_i with integer coefficients.

By Eq. (5.2) we have

$$\begin{aligned} P_n = & (X_0^{p^n} Y_n + X_1^{p^{n-1}} Y_{n-1}^p + \cdots + X_n Y_0^{p^n}) \\ & + \frac{1}{p}(X_0^{p^n} Y_{n-1}^p + \cdots + X_{n-1}^p Y_0^{p^n}) \\ & \vdots \\ & + \frac{1}{p^n}(X_0^{p^n} Y_0^{p^n}) - \frac{1}{p^n} P_0^{p^n} \\ & - \frac{1}{p^{n-1}}(R_1 + pT_1)^{p^{n-1}} - \cdots - \frac{1}{p}(R_{n-1} + pT_{n-1})^p. \end{aligned}$$

Now, since $(R_i + pT_i)^{p^{n-i}} \equiv R_i^{p^{n-i}} \pmod{p^{n-i+1}}$, we have that $P_n \equiv R_n \pmod{p}$, which finishes the proof. □

We also observe the following basic facts about Witt vectors:

Lemma 5.6. *We have:*

(1) *if p is odd, then*

$$-(a_0, a_1, a_2, \ldots) = (-a_0, -a_1, -a_2, \ldots);$$

(2) $(a_0, a_1, a_2, \ldots) \in \boldsymbol{W}(R)^\times$ *if and only if* $a_0 \in R^\times$*;*
(3) $(\lambda, 0, 0, \ldots) \cdot (a_0, a_1, a_2, \ldots) = (\lambda a_0, \lambda^p a_1, \lambda^{p^2} a_2, \ldots)$.

6. Valuations and Witt Vectors

In this section we state and prove a few lemmas on Witt vectors and valuations which will be our main tools in the proofs of the main results.

First we need a couple of lemmas for sums and products. We first state a more general lemma from which we can derive the results we actually need as particular cases.

Lemma 6.1. *Let ν be a valuation (considering $\nu(0) = \infty$), $\boldsymbol{u} = (u_0, u_1, \ldots)$, $\boldsymbol{v} = (v_0, v_1, \ldots)$, and suppose that, for some $k \geq 0$, we have:*

- $\nu(u_i), \nu(v_i) \geq 0$ *for* $i = 0, \ldots, (k-1)$*;*
- $\nu(u_i) \geq \nu_i$ *for* $i \geq k$*, where* $\nu_k < 0$ *and* $\nu_{i+1} < p\nu_i$ *for all* $i \geq k$.

Also, let $\boldsymbol{u} + \boldsymbol{v} = (r_0, r_1, \ldots)$ and $\boldsymbol{u} \cdot \boldsymbol{v} = (s_0, s_1, \ldots)$.

Then, $\nu(r_i), \nu(s_i) \geq 0$ for $i \leq k-1$, and:

(1) *If $\nu(v_k) \geq \nu_k$ and $\nu(v_i) > \nu_i$ for $i > k$, then $\nu(r_n) \geq \nu_n$ for $n \geq k$. Moreover, if $\nu(v_k) > \nu_k = \nu(u_k)$, then $\nu(r_k) = \nu_k$, and if $\nu(u_i) = \nu_i$ for $i > k$, then $\nu(r_n) = \nu_n$ for $n > k$. (Note that the two "if" statements are independent.)*
(2) *If $\nu(v_i) \geq p^i \nu(v_0)$ for $i > 0$, with $\nu_k < -p^k \nu(v_0)$, then $\nu(s_n) \geq \nu_n + p^n \nu(v_0)$ for $n \geq k$. Moreover, if $\nu_k = \nu(u_k)$, then $\nu(s_k) = \nu_k + p^k \nu(v_0)$, and if $\nu(u_i) = \nu_i$ for $i > k$, then $\nu(s_n) = \nu_n + p^n \nu(v_0)$ for $n > k$. (Again, these "if" statements are independent.)*

Proof. First, since $\nu(u_i), \nu(v_i) \geq 0$ for $i = 0, \ldots, (k-1)$, it is clear that $\nu(r_n), \nu(s_n) \geq 0$ for $n = 0, \ldots, (k-1)$.

Let then $\prod_i X_i^{s_i} \prod_j Y_j^{t_j}$ be a monomial from $\bar{S}_n$ different from X_n and Y_n, the only monomials containing either X_n or Y_n. (Hence, we have that $i, j < n$.)

Then, clearly, if $n = k$, we have that $\nu\left(\prod_i u_i^{s_i} \prod_j v_j^{t_j}\right) \geq 0$. And since $\nu(u_k), \nu(v_k) \geq \nu_k$, with $\nu_k < 0$, we have that $\nu(r_k) \geq \nu_k$. And observe that if $\nu(v_k) > \nu_k = \nu(u_k)$, then $\nu(r_k) = \nu_k$.

So now let $n > k$. We want to argue that $\nu\left(\prod_i u_i^{s_i}\prod_j v_j^{t_j}\right) > \nu_n$. First note that if for all $k \le i < n$ and $k \le j < n$ we have that $s_i = t_j = 0$, then

$$\nu\left(\prod_i u_i^{s_i}\prod_j v_j^{t_j}\right) \ge \sum_{k\le i<n} s_i\nu_i + \sum_{k\le j<n} t_j\nu_j = 0 > \nu_n.$$

Now, observe that the condition on the ν_i's imply that if $n > i \ge k$, then $\nu_i > \nu_n/p^{n-i}$. And hence, if either some s_i or some t_j is not zero for some $k \le i < n$ or some $k \le j < n$, then, by Lemma 5.1, we also have

$$\begin{aligned}\nu\left(\prod_i u_i^{s_i}\prod_j v_j^{t_j}\right) &\ge \sum_{k\le i<n} s_i\nu_i + \sum_{k\le j<n} t_j\nu_j > \sum_{k\le i<n} s_i\frac{\nu_n}{p^{n-i}} + \sum_{k\le j<n} t_j\frac{\nu_n}{p^{n-j}}\\ &= \frac{\nu_n}{p^n}\left[\sum_{k\le i<n} s_ip^i + \sum_{k\le j<n} t_jp^j\right] \ge \frac{\nu_n}{p^n}\left[\sum_i s_ip^i + \sum_j t_jp^j\right] = \nu_n.\end{aligned}$$

Therefore, since also $\nu(u_n) \ge \nu_n$ and $\nu(v_n) > \nu_n$, we get $\nu(r_n) \ge \nu_n$. Note that if $\nu(u_n) = \nu_n$, then we have $\nu(r_n) = \nu_n$.

For the second part, first note that if $k = 0$, then $s_k = s_0 = u_0 \cdot v_0$, and $\nu(s_0) = \nu(u_0) + \nu(v_0) \ge \nu_0 + p^0\nu(v_0)$. And notice that if $\nu_0 = \nu(u_0)$, we have equality.

So assume now $k > 0$ and let now $\prod_i X_i^{s_i}\prod_j Y_j^{t_j}$ be a monomial from $\bar{P}_n$, for $n \ge k$, different from $Y_0^{p^n}X_n$ and $X_0^{p^n}Y_n$, the only monomials containing either X_n or Y_n. (Hence, we have that $i, j < n$.)

For $n = k$, again $\nu\left(\prod_i u_i^{s_i}\prod_j v_j^{t_j}\right) \ge 0$. As $k > 0$, we have that $\nu(u_0) \ge 0 > \nu_k$, and so $\nu(u_0^{p^k}v_k) > \nu_k + p^k\nu(v_0)$. Since $\nu(v_0^{p^k}u_k) \ge \nu_k + p^k\nu(v_0)$ and $\nu_k + p^k\nu(v_0) < 0$ (by hypothesis), we have $\nu(s_k) \ge \nu_k + p^k\nu(v_0)$, and observe that if $\nu(u_k) = \nu_k$, we have the equality. (This concludes the case $n = k$ for both cases, $k = 0$ and $k > 0$.)

So, assume now $n > k$. We want to argue that $\nu\left(\prod_i u_i^{s_i}\prod_j v_j^{t_j}\right) > \nu_n + p^n\nu(v_0)$. If $s_i = 0$ for all i with $k \le i < n$, then, by Lemma 5.4, we have

$$\begin{aligned}\nu\left(\prod_i u_i^{s_i}\prod_j v_j^{t_j}\right) &\ge \sum_{k\le i<n} s_i\nu_i + \sum_j t_jp^j\nu(v_0)\\ &= \nu(v_0)\sum_j t_jp^j = p^n\nu(v_0) > \nu_n + p^n\nu(v_0).\end{aligned}$$

Now, if $s_{i_0} \neq 0$ for some $k \leq i_0 < n$, then, as again $\nu_i > \nu_n/p^{n-i}$, we would have by Lemma 5.4,

$$\begin{aligned}
\nu\left(\prod_i u_i^{s_i}\prod_j v_j^{t_j}\right) &\geq \sum_{k\leq i<n} s_i\nu_i + \sum_j t_j p^j \nu(v_0)\\
&> \sum_{k\leq i<n} s_i \frac{\nu_n}{p^{n-i}} + \nu(v_0)\sum_j t_j p^j\\
&= \frac{\nu_n}{p^n}\sum_{k\leq i<n} s_i p^i + \nu(v_0)\sum_j t_j p^j\\
&\geq \frac{\nu_n}{p^n}\sum_i s_i p^i + \nu(v_0)\sum_j t_j p^j\\
&= \nu_n + p^n\nu(v_0).
\end{aligned}$$

Now, $\nu(u_0^{p^n}v_n) \geq p^n\nu(u_0) + \nu(v_n) \geq p^n\nu(u_0) + p^n\nu(v_0)$. If $k = 0$, and as $n > k$, then $\nu_n < p^n\nu_0 \leq p^n\nu(u_0)$, and so $\nu(u_0^{p^n}v_n) > \nu_n + p^n\nu(v_0)$. If $k > 0$, then $\nu(u_0) \geq 0 > \nu_n$, and again $\nu(u_0^{p^n}v_n) > \nu_n + p^n\nu(v_0)$.

Finally, we have $\nu(v_0^{p^n}u_n) \geq \nu_n + p^n\nu(v_0)$, and hence $\nu(s_n) \geq \nu_n + p^n\nu(v_0)$, and note that if $\nu(u_n) = \nu_n$, then we have $\nu(s_n) = \nu_n + p^n\nu(v_0)$. □

In Section 10 we shall use the following particular case of Lemma 6.1:

Lemma 6.2. *Let ν be a valuation (considering $\nu(0) = \infty$), $\boldsymbol{u} = (u_0, u_1, \ldots)$, $\boldsymbol{v} = (v_0, v_1, \ldots)$, and suppose that $\nu(u_i) \geq \nu_i$, with $\nu_0 \leq 0$ and $\nu_{i+1} < p\nu_i$ for all i. Then, if $\boldsymbol{u}+\boldsymbol{v} = (r_0, r_1, \ldots)$ and $\boldsymbol{u}\cdot\boldsymbol{v} = (s_0, s_1, \ldots)$, we have:*

1. *If $\nu(v_0) \geq \nu_0$ and $\nu(v_i) > \nu_i$ for all $i \geq 1$, then $\nu(r_n) \geq \nu_n$ for $n \geq 1$. Moreover, if $\nu(u_i) = \nu_i$ for all i, then $\nu(r_n) = \nu_n$ for $n \geq 1$.*
2. *Now, if $\nu_0 < 0$, assume $\nu_0 < -\nu(v_0)$, while if $\nu_0 = 0$, assume both $\nu_1 < -p\nu(v_0)$ and $\nu(v_0) \geq 0$. Then, in either case, we have that if $\nu(v_i) \geq p^i\nu(v_0)$ for all i, then $\nu(s_n) \geq \nu_n + p^n\nu(v_0)$ for $n \geq 1$. Moreover, if $\nu(u_i) = \nu_i$ for all i, then $\nu(s_n) = \nu_n + p^n\nu(v_0)$ for $n \geq 1$.*

Proof. The lemma immediately follows from Lemma 6.1 with $k = 0$ if $\nu_0 < 0$ or $k = 1$ if $\nu_0 = 0$. □

In Section 11 we need the following particular case of Lemma 6.1:

Lemma 6.3. *Let k be a non-negative integer, ν be a valuation (considering $\nu(0) = \infty$), $\boldsymbol{u} = (u_0, u_1, \ldots)$, $\boldsymbol{v} = (v_0, v_1, \ldots)$, $\boldsymbol{u} + \boldsymbol{v} = (r_0, r_1, \ldots)$, and $\boldsymbol{u} \cdot \boldsymbol{v} = (s_0, s_1, \ldots)$. Assume also:*

- *$\nu(u_i) \geq 0$ for $i = 0, \ldots, (k-1)$;*
- *$\nu(u_i) \geq \nu_i$ for $i \geq k$, where $\nu_k < 0$ and $\nu_{i+1} < p\nu_i$ for all $i \geq k$;*
- *$\nu(v_0) = 0$;*
- *$\nu(v_i) \geq 0$ for all $i \geq 1$.*

We then have:

(1) *$\nu(r_n) \geq 0$ for $n = 0, \ldots, (k-1)$ and $\nu(r_n) \geq \nu_n$ for $n \geq k$.*
(2) *$\nu(s_n) \geq 0$ for $n = 0, \ldots, (k-1)$ and $\nu(s_n) \geq \nu_n$ for $n \geq k$.*

Moreover, if we also have $\nu(u_i) = \nu_i$ for $i \geq k$, then $\nu(r_n) = \nu(s_n) = \nu_n$ for all $n \geq k$.

Proof. The lemma immediately follows from Lemma 6.1, since $\nu(v_i) \geq 0 > \nu_i$ for $i \geq k$, and $\nu(v_i) \geq 0 = p^i \nu(v_0)$ for $i > 0$. □

We also need the two following lemmas to deal with inverses.

Lemma 6.4. *Let k be a positive integer, ν be a valuation (considering $\nu(0) = \infty$), $\boldsymbol{u} = (u_0, u_1, \ldots)$, and suppose that:*

- *$\nu(u_0) = 0$;*
- *$\nu(u_i) \geq 0$ for $i = 1, \ldots, (k-1)$;*
- *there are $\alpha, \beta \in \mathbb{R}_{>0}$ such that $\nu(u_i) \geq \nu_i \stackrel{\text{def}}{=} p^i(\alpha - \beta i)$, for all $i \geq k$, and with $\alpha - \beta k < 0$.*

Then, if $\boldsymbol{u}^{-1} = (v_0, v_1, \ldots)$, we have that $\nu(v_i) \geq 0$ for $i = 1, \ldots, (k-1)$ and $\nu(v_i) \geq \nu_i$ for all $i \geq k$. Moreover, if $\nu(u_i) = \nu_i$ for $i \geq k$, then we have that $\nu(v_i) = \nu_i$ for $i \geq k$.

Proof. Since $\nu(u_0) = 0$, it is clear that $\nu(v_0) = \nu(1/u_0) = 0$ and, from Item 2 of Lemma 5.6, that $\nu(v_i) \geq 0$ for $i < k$.

As $k \geq 1$, we have $P_k(u_0, \ldots, u_k, v_0, \ldots, v_k) = 0$, and by Eq. (5.2) we get that $\nu(u_0^{p^k} v_k + u_k v_0^{p^k}) \geq 0$. Now, if $\nu(v_k) < \nu_k$, then $\nu(u_0^{p^k} v_k) < \nu(u_k v_0^{p^k}) = \nu_k < 0$, and hence $\nu(u_0^{p^k} v_k + u_k v_0^{p^k}) = \nu(v_k) < 0$, a contradiction. Therefore, $\nu(v_k) \geq \nu_k$. Moreover, if $\nu(u_k) = \nu_k$, we must also have $\nu(v_k) = \nu_k$.

So, now let $n > k$. By Lemma 5.5 we have that $R_n(u_0, \ldots, u_n, v_0, \ldots, v_n) = 0$. Now let $m = M(u_0, \ldots, u_n, v_0, \ldots, v_n)$, where M is a monomial from R_n, different from $X_0^{p^n} Y_n$ and $X_n Y_0^{p^n}$, i.e., M involves neither X_n nor Y_n. We prove, by induction on n that $\nu(m) > \nu_n$, which suffices to finish the proof.

Observing that $\nu_k < 0$, the case $n = k$ can be seen in the argument above. So, assume true for all $i \in \{k, \dots, n-1\}$. By Lemma 5.5, we have that either M is of the form $X_i^{p^{n-i}} Y_j^{p^{n-j}}$, with $i + j \leq n$, or it is a monomial coming from $R_i^{p^{n-i}}$ for some $i \in \{1, \dots, n-1\}$.

If M comes from $R_i^{p^{n-i}}$ for some $i \in \{1, \dots, k-1\}$, then clearly $\nu(m) = 0 > \nu_n$. If M comes from $R_i^{p^{n-i}}$ for some $i \in \{k, \dots, n-1\}$, then, by the induction hypothesis, $\nu(m) \geq p^{n-i}\nu_i = p^n(\alpha - \beta i) > \nu_n$, as $\beta > 0$.

So, assume $M = X_i^{p^{n-i}} Y_j^{p^{n-j}}$, with $i + j \leq n$, and $i, j \neq n$. If i and j are less than k, then clearly $\nu(m) \geq 0 > \nu_n$.

If $i \geq k$ and $j < k$, then $\nu(m) \geq p^n(\alpha - \beta i) > \nu_n$. Similarly, if $i < k$ and $j \geq k$, then $\nu(m) \geq p^n(\alpha - \beta j) > \nu_n$.

Finally, if $i, j \geq k$, then $\nu(m) \geq p^n(\alpha - \beta i) + p^n(\alpha - \beta j) = p^n(2\alpha - \beta(i+j)) \geq p^n(2\alpha - \beta n) > \nu_n$, as $\alpha > 0$. □

Lemma 6.5. *Let ν be a valuation, $\boldsymbol{u} = (u_0, u_1, \dots)$, with $\nu_0 \stackrel{\text{def}}{=} \nu(u_0) > 0$, $\nu(u_1) \geq 0$ and $\nu(u_i) > -p^i(i-1)\nu_0$ for $i \geq 2$. Then, if $\boldsymbol{u}^{-1} = (v_0, v_1, \dots)$, we have $\nu(v_n) \geq -p^n(n+1)\nu_0$ for $n \geq 0$. Moreover, if $\nu(u_1) = 0$, then $\nu(v_n) = -p^n(n+1)\nu_0$ for $n \geq 0$.*

Proof. Notice first that $\nu(v_0) = \nu(1/u_0) = -\nu_0$.

We again prove it by induction. Let $n \geq 1$ and $\prod_i X_i^{s_i} \prod_j Y_j^{t_j}$ be a monomial from $\bar{P}_n$ coming from $\bar{Q}_n$, as in Lemma 5.4. Then:

$$\begin{aligned}
\nu\left(\prod_i u_i^{s_i} \prod_j v_j^{t_j}\right) &\geq s_0\nu_0 - \sum_{i\geq 1} s_i p^i(i-1)\nu_0 - \sum_j t_j p^j(j+1)\nu_0 \\
&\geq \nu_0 \left[s_0 - \left[\sum_{i\geq 1} s_i i p^i + \sum_j t_j j p^j \right] + \sum_{i\geq 1} s_i p^i - \sum_j t_j p^j \right] \\
&\geq -p^n(n-1)\nu_0 > -p^n n\nu_0.
\end{aligned}$$

Now, for $i \in \{2, \dots, n\}$, we have $\nu(u_i^{p^{n-i}} v_{n-i}^{p^i}) > -p^n(i-1)\nu_0 - p^n(n-i+1)\nu_0 = -p^n n\nu_0$, while $\nu(u_1^{p^{n-1}} v_{n-1}^{p}) \geq p^{n-1}\nu(u_1) - p^n n\nu_0 \geq -p^n n\nu_0$, with equalities if $\nu(u_1) = 0$, and $\nu(u_0^{p^n} v_n) = \nu_0 p^n + \nu(v_n)$. Since

$$u_0^{p^n} v_n + \left[\sum_{i=1}^{n} u_i^{p^{n-i}} v_{n-i}^{p^i} \right] + \bar{Q}_n(u_0, \dots, u_{n-1}, v_0, \dots, v_{n-1}) = P_n(\boldsymbol{u}, \boldsymbol{v}) = 0,$$

we have $\nu(v_n) \geq -p^n(n+1)\nu_0$, with equality if $\nu(u_1) = 0$. □

7. Supersingular Polynomial and the Hasse Invariant

Since we will switch from functions on the j-invariant j, to functions on the Weierstrass coefficients (a,b), we need to relate the supersingular polynomial ss_p, which tells when the elliptic curve with j-invariant j is supersingular, to the Hasse invariant $\mathfrak{h}$, which tells us when an elliptic curve given by the Weierstrass coefficients (a,b) is supersingular. (Most of what we discuss here can be found in [Fin09].)

As a consequence of [Fin09, Lemma 2.2], we can easily see that the Hasse invariant is given by

$$\mathfrak{h} = \sum_{i=r_1}^{r_2} \binom{r}{i}\binom{i}{3i-r} a^{3i-r} b^{r-2i}, \tag{7.1}$$

where $r \stackrel{\text{def}}{=} (p-1)/2$, $r_1 \stackrel{\text{def}}{=} \lceil r/3 \rceil$, and $r_2 \stackrel{\text{def}}{=} \lfloor r/2 \rfloor$. (We shall keep this notation throughout this paper.)

Moreover, in [Fin09, Sections 2 and 3], we see that

$$\mathcal{S}_p(j) = \left(-\frac{2}{9}\right)^r \left(\frac{1728}{\Delta}\right)^{r_2-r_1} \frac{(-27)^{r_2}}{4^{r_1}} \frac{1}{a^{3r_1-r}b^{r-2r_2}}\mathfrak{h}, \tag{7.2}$$

where $j \stackrel{\text{def}}{=} 1728 \cdot 4a^3/\Delta$, with $\Delta = 4a^3 + 27b^2$. (Note that leading coefficient in [Fin09] is incorrect, and was fixed in the formula above.)

This immediately gives the following proposition:

Proposition 7.1. *The denominator of the function $J_i(j) \in \mathbb{F}_p(a,b)$ (with j as above) involves only powers of Δ, $\mathfrak{h}$, a, and b, i.e., $J_i(j) \in \mathbb{V} \stackrel{\text{def}}{=} \mathbb{F}_p[a,b,1/(\Delta\cdot\mathfrak{h}\cdot a\cdot b)]$.*

Proof. By Theorem 4.1, the denominator of J_i involves only powers of X, which gives a denominator that is a power of a in $J_i(j)$, $X - 1728$, which gives a denominator that is a power of b in $J_i(j)$, and $\mathcal{S}_p(X)$, which gives a power of $\mathfrak{h}$ in $J_i(j)$ by Eq. (7.2).

Finally, again by Theorem 4.1, the numerator J_i has degree larger than its denominator (as polynomials in X), and therefore can introduce powers of Δ in the denominator of $J_i(j)$ (as a rational function in (a,b)). □

8. General Denominator

We now start the study the denominators of the functions A_i and B_i given by Eqs. (3.2) and (3.3). We start by finding what are the possible denominators of these functions:

Theorem 8.1. *The functions A_i and B_i given by Eqs.* (3.2) *and* (3.3) *are in the ring $\mathbb{V}$.*

Proof. By Proposition 7.1, as $\boldsymbol{j} = (j, J_1(j), J_2(j), \ldots)$ (the j-invariant of the canonical lifting of the curve given by (a,b)), then we have that $27\boldsymbol{j}, 4(1728-\boldsymbol{j}) \in \boldsymbol{W}(\mathbb{V})$. Clearly we also

have that $\boldsymbol{\lambda}^2 \in \boldsymbol{W}(\mathbb{V})$. Furthermore, observe that $4(1728 - \boldsymbol{j}) = (1728 \cdot 4 \cdot 27b^2/\Delta, \cdots)$, and so, since $1728 \cdot 4 \cdot 27b^2/\Delta$ is a unit of $\mathbb{V}$, we have that $(4(1728 - \boldsymbol{j}))^{-1} \in \boldsymbol{W}(\mathbb{V})$. Therefore, we have that $\boldsymbol{a}$ and $\boldsymbol{b}$ from Eqs. (3.2) and (3.3) are in $\boldsymbol{W}(\mathbb{V})$. □

We now turn our attention to what powers of Δ, $\mathfrak{h}$, a, and b appear in the denominators of A_i and B_i. The typical tool to do so is *valuations*. But, observe that while a, b, and Δ are irreducibles in $\mathbb{F}_p[a, b]$, we have that $\mathfrak{h}$ might not be so. For instance, for $p = 11$ we have that $\mathfrak{h} = 9ab$. Moreover, in some cases, like for $p = 5$, where $\mathfrak{h} = 2a$, tracking powers of $\mathfrak{h}$ is the same as tracking powers of a. Some of these will be introduced by $\mathfrak{h}$ coming from Eq. (7.2), while some will come from the a in the denominator of $\boldsymbol{\lambda}$ (from Eq. (3.4)).

Hence, it is harder to actually track powers of $\mathfrak{h}$ showing in the denominators. The approach we take here is to view the $\mathfrak{h}$ coming from Eq. (7.2) as an *unknown*, rather than an expression on a and b, as this is the only place where $\mathfrak{h}$ is explicitly introduced. To avoid confusion, we will use $\mathfrak{H}$ for this new variable, while keeping $\mathfrak{h} \in \mathbb{F}_p[a, b]$ as defined by Eq. (7.1). So, in Eq. (7.2) we replace $\mathcal{S}_p(j)$ by

$$\hat{\mathcal{S}}_p \stackrel{\text{def}}{=} \left(-\frac{2}{9}\right)^r \left(\frac{1728}{\Delta}\right)^{r_2 - r_1} \frac{(-27)^{r_2}}{4^{r_1}} \frac{1}{a^{3r_1 - r} b^{r - 2r_2}} \mathfrak{H}. \tag{8.1}$$

Again, to avoid confusion, we consider $\hat{A}_i, \hat{B}_i \in \hat{\mathbb{V}} \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, \mathfrak{H}, 1/(\Delta \cdot \mathfrak{H} \cdot a \cdot b)]$ corresponding to A_i and B_i, respectively, when replacing $\mathfrak{h}$ with the variable $\mathfrak{H}$ in the term coming from $\mathcal{S}_p$. Thus, we have that $A_i(a, b) = \hat{A}_i(a, b, \mathfrak{h})$ and $B_i(a, b) = \hat{B}_i(a, b, \mathfrak{h})$. Similarly, we introduce $\hat{J}_i \in \hat{\mathbb{V}}$ as $J_i(j)$, but again with the $\mathfrak{h}$ replaced by the variable $\mathfrak{H}$.

So, in the next sections we shall look at $\nu(\hat{A}_i)$ and $\nu(\hat{B}_i)$, where ν is one of the valuations ν_a, ν_b, ν_Δ, or $\nu_\mathfrak{H}$, i.e., valuations of $\mathbb{F}_p(a, b, \mathfrak{H})$ at a, b, Δ, and $\mathfrak{H}$ respectively.

9. Powers of Δ

We first prove the following result:

Lemma 9.1. *We have that $\Delta \nmid \mathfrak{h}$, i.e., Δ and $\mathfrak{h}$ are relatively prime in $\mathbb{F}_p[a, b]$.*

Proof. From Eq. (7.2) we have that

$$\mathfrak{h} = c \cdot \Delta^{r_2 - r_1} \cdot a^{3r_1 - r} b^{r - 2r_2} \mathcal{S}_p(j),$$

with $c \in \mathbb{F}_p$. Since $\deg(\mathcal{S}_p) = r_2 - r_1$ (see, for instance, [Fin09] again) and $\mathcal{S}_p \in \mathbb{F}_p[X]$, we have that

$$\nu_\Delta(\mathfrak{h}) = (r_2 - r_1) + \nu_\Delta(\mathcal{S}_p(j)) = (r_2 - r_1) + \deg(\mathcal{S}_p) \cdot \nu_\Delta(j) = 0.$$

□

The main goal now is to prove the following theorem:

Theorem 9.2. *We have that $\nu_\Delta(\hat{A}_i), \nu_\Delta(\hat{B}_i) \geq 0$, i.e., $\hat{A}_i, \hat{B}_i \in \hat{\mathbb{V}}_\Delta \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, \mathfrak{H}, 1/(\mathfrak{H}\cdot a\cdot b)]$. Therefore, by Lemma 9.1, Δ does not appear in the denominator of either A_i or B_i.*

Note that this result is similar to Conjecture 1.2, which states that, as observed in concrete examples, the (universal) A_i's and B_i's coming from the algorithm described in [Fin19] do not seem to have Δ in their denominators, i.e., are in $\mathbb{U}_\Delta \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, 1/\mathfrak{h}]$. In fact, the theorem has the following corollary:

Corollary 9.3. *For $p \equiv 11 \pmod{12}$ there are* universal *modular functions A_i and B_i giving the canonical lifting, as in Theorem 2.5, with $A_i, B_i \in \mathbb{U}_\Delta$.*

Proof. Just observe that by Eq. (7.1), for $p \equiv 11 \pmod{12}$ we have that $a, b \mid \mathfrak{h}$. □

Note that this corollary does *not* prove Conjecture 1.2 in the case of $p \equiv 11 \pmod{12}$, as the A_i's and B_i's from its statement come from a specific (and different) algorithm, but it is closely related, as it gives functions with the same required properties.

We shall need the following lemma (to prove Theorem 9.2):

Lemma 9.4. *We have that $\nu_\Delta(\hat{J}_i) = -p^i + \iota$.*

Proof. With the notation of Theorem 4.1 we have that

$$\hat{J}_i = \frac{F_i(j)}{\hat{\mathcal{S}}_p^{m_i} \cdot H_i(j)},$$

with $\hat{\mathcal{S}}_p$ as in Eq. (8.1) and $m_i \stackrel{\text{def}}{=} ip^{i-1} + (i-1)p^{i-2}$. Now, since $\deg \mathcal{S}_p = r_2 - r_1$, as observed above, we have that $\nu_\Delta(\hat{\mathcal{S}}_p) = -(r_2 - r_1) = -\deg(\mathcal{S}_p)$.

So, by Theorem 4.1, we have

$$\begin{aligned}\nu_\Delta(\hat{J}_i) &= \nu_\Delta(F_i(j)) - m_i\nu_\Delta(\hat{\mathcal{S}}_p) - \nu_\Delta(H_i(j)) \\ &= -\deg(F_i) + m_i \deg(\mathcal{S}_p) + \deg(H_i) \\ &= -\deg(F_i) + \deg(G_i) = -p^i + \iota.\end{aligned}$$

□

We can now proceed with the proof of the theorem:

Proof of Theorem 9.2. Let $\hat{\boldsymbol{j}} \stackrel{\text{def}}{=} (j, \hat{J}_1, \hat{J}_2, \ldots)$ and $\tau(\Delta) = (\Delta, 0, 0, \ldots)$, the *Teichmüller lift* of Δ. Then, by the previous lemma, we have that

$$27 \cdot \tau(\Delta) \cdot \hat{\boldsymbol{j}} = 27 \cdot (1728 \cdot 4a^3, \Delta^p \hat{J}_1, \Delta^{p^2} \hat{J}_2, \ldots) \in \boldsymbol{W}(\hat{\mathbb{V}}_\Delta).$$

Similarly,

$$4 \cdot \tau(\Delta) \cdot (1728 - \hat{\boldsymbol{j}}) = 4 \cdot 1728 \cdot \tau(\Delta) - 4 \cdot \tau(\Delta) \cdot \hat{\boldsymbol{j}} = (4 \cdot 1728 \cdot 27b^2, \ldots) \in \boldsymbol{W}(\hat{\mathbb{V}}_\Delta).$$

Moreover, since $4 \cdot 1728 \cdot 27 \cdot b^2$ is a unit of $\hat{\mathbb{V}}_\Delta$, we have that $4 \cdot \tau(\Delta) \cdot (1728 - \hat{\boldsymbol{j}})$ is a unit of $\boldsymbol{W}(\hat{\mathbb{V}}_\Delta)$, and hence,

$$\frac{27\hat{\boldsymbol{j}}}{4(1728 - \hat{\boldsymbol{j}})} = \frac{\tau(\Delta) \cdot 27\hat{\boldsymbol{j}}}{\tau(\Delta) \cdot 4(1728 - \hat{\boldsymbol{j}})} \in \boldsymbol{W}(\hat{\mathbb{V}}_\Delta).$$

Since clearly $\boldsymbol{\lambda}^2 = (b/a, 0, 0, \ldots) \in \boldsymbol{W}(\hat{\mathbb{V}}_\Delta)$, we have that $\hat{A}_i, \hat{B}_i \in \hat{\mathbb{V}}_\Delta$ (by Eqs. (3.2) and (3.3)). □

10. Powers of $\mathfrak{h}$

We now turn to powers of $\mathfrak{H}$. First we observe that, by Eq. (8.1) and Theorem 4.1, we have that if $m_0 \stackrel{\text{def}}{=} 0$ and $m_i \stackrel{\text{def}}{=} ip^{i-1} + (i-1)p^{i-2}$ for $i \geq 1$, then $\nu_{\mathfrak{H}}(\hat{J}_i) = -m_i$. We prove the following result:

Theorem 10.1. *We have that* $\nu_{\mathfrak{H}}(\hat{A}_i), \nu_{\mathfrak{H}}(\hat{B}_i) = -m_i = -(ip^{i-1} + (i-1)p^{i-2})$.

Proof. Let again $\hat{J} = (\hat{J}_0, \hat{J}_1, \hat{J}_2, \ldots)$, with $\hat{J}_0 \stackrel{\text{def}}{=} j$. Then, we have that $\nu_{\mathfrak{H}}(\hat{J}_0) = 0$, $\nu_{\mathfrak{H}}(\hat{J}_1) = -m_1 = -1 < p \cdot 0$, and for $i \geq 1$, we have

$$\begin{aligned}\nu_{\mathfrak{H}}(\hat{J}_{i+1}) = -m_{i+1} = -(i+1)p^i - ip^{i-1} &= -p[(i+1)p^{i-1} + ip^{i-2}] \\ &< -p[ip^{i-1} + (i-1)p^{i-2}] = -pm_i = p\,\nu_{\mathfrak{H}}(\hat{J}_i).\end{aligned}$$

Then, by Lemma 6.2, we have that if $1728 - \hat{\boldsymbol{j}} = (r_0, r_1, \ldots)$, then $\nu_{\mathfrak{H}}(r_i) = \nu_{\mathfrak{H}}(\hat{J}_i) = -m_i$ for all $i \geq 0$. Now, by Lemma 6.4 (with $k = 1$, $\alpha = 1/p^2$, and $\beta = (p+1)/p^2$), we have that if $(1728 - \hat{\boldsymbol{j}})^{-1} = (s_0, s_1, \ldots)$, then $\nu_{\mathfrak{H}}(s_i) = \nu_{\mathfrak{H}}(r_i) = -m_i$. And, finally, applying Lemma 6.2 a few more times, we have that

$$\frac{27\boldsymbol{\lambda}^4}{4}\left(1728 \cdot \frac{1}{1728 - \hat{\boldsymbol{j}}} - 1\right) = \boldsymbol{\lambda}^4 \cdot \frac{27\hat{\boldsymbol{j}}}{4(1728 - \hat{\boldsymbol{j}})} = (a, \hat{A}_1, \hat{A}_2, \ldots), \tag{10.1}$$

$$\frac{27\boldsymbol{\lambda}^6}{4}\left(1728 \cdot \frac{1}{1728 - \hat{\boldsymbol{j}}} - 1\right) = \boldsymbol{\lambda}^6 \cdot \frac{27\hat{\boldsymbol{j}}}{4(1728 - \hat{\boldsymbol{j}})} = (b, \hat{B}_1, \hat{B}_2, \ldots), \tag{10.2}$$

are such that $\nu_{\mathfrak{H}}(\hat{A}_i) = \nu_{\mathfrak{H}}(\hat{B}_i) = -m_i$. □

So, Theorem 10.1 gives an *equality* for the valuations $\nu_{\mathfrak{H}}(\hat{A}_i)$ and $\nu_{\mathfrak{H}}(\hat{B}_i)$, but how does this translate to the powers of $\mathfrak{h}$ in the denominators of A_i and B_i? As seen in Eq. (3.6), for which $p = 5$ and so $\mathfrak{h} = 2a$, we see $\mathfrak{h}^6$ appearing in the denominator. But the problem here is that, as we observed before, extra powers of a and b can appear in the denominator.

(We shall discuss these in more details in the next section.) So, it is not surprising that a larger power shows up. Similar problems occur for $p = 7$ and $p = 11$, for which $\mathfrak{h} = 3b$ and $\mathfrak{h} = 9ab$ respectively. For $p = 13$ and $p = 17$, for which $\mathfrak{h} = 7a^3 + 2b^2$ and $\mathfrak{h} = 2a^4 + 15ab^2$ respectively, we see the exact powers m_1 and m_2 appearing on the denominators of A_i and B_i for $i = 1, 2$ (along with some extra factors of a and b).

In general, we can expect a power less than or equal to m_i in the denominators of A_i and B_i (with some extra factors of a and b), as, although unlikely, the numerator might be itself divisible by $\mathfrak{h}$, or by factors of $\mathfrak{h}$, which Theorem 10.1 does not account for. I.e., we have:

Corollary 10.2. *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 $\nu_h(A_i), \nu_h(B_i) \geq -\nu_h(\mathfrak{h})\, m_i = -\nu_h(\mathfrak{h}) \left(ip^{i-1} + (i-1)p^{i-2}\right)$.*

The authors verified in MAGMA that for $p \leq 997$ the Hasse invariant $\mathfrak{h}$ has no repeated irreducible factor, i.e, $\nu_h(\mathfrak{h}) = 1$ for all irreducible factors h of $\mathfrak{h}$, but they are unaware if this is true in general.

11. Powers of a and b

We now turn our attention to a and b. Our main tool, Theorem 4.1, does not give as much information in this case, as it only gives *upper bounds* for the powers of X and $X - 1728$ in the denominator of $J_i(X)$. This limitation makes the bounds given in this section be very far from sharp.

In any event, we have:

Theorem 11.1. *We have:*

1. *If $p \equiv 1 \pmod 6$, then $\nu_a(\hat{J}_i) \geq 0$ for all i.*
2. *If $p \equiv 5 \pmod 6$, then $\nu_a(\hat{J}_1) \geq 1$, $\nu_a(\hat{J}_2) \geq (2p+1)$, $\nu_a(\hat{J}_3) = 2p$, and for $i \geq 4$ we have $\nu_a(\hat{J}_i) \geq -((i-3)p^i - (i-1)p^{i-2})$.*
3. *If $p \equiv 1 \pmod 4$, then $\nu_b(\hat{J}_i) \geq 0$ for all i.*
4. *If $p \equiv 3 \pmod 4$, then $\nu_b(\hat{J}_1) \geq 1$, $\nu_b(\hat{J}_2) = 1$, and for $i \geq 3$ we have that $\nu_b(\hat{J}_i) \geq -((i-2)p^{i-1} - (i-1)p^{i-2})$.*

Proof. Equation (8.1) gives us that $\nu_a(\hat{\mathcal{S}}_p) = -(3r_1 - r) = -\delta$ and $\nu_b(\hat{\mathcal{S}}_p) = -(r - 2r_2) = -\epsilon$ (with ϵ and δ as defined in Section 4). Since

$$\hat{J}_i = \frac{F_i(j)}{\hat{\mathcal{S}}_p^{m_i} \cdot H_i(j)},$$

with $m_i \stackrel{\text{def}}{=} ip^{i-1} + (i-1)p^{i-2}$, we have, for ν either ν_a or ν_b, that $\nu(\hat{J}_i) = \nu(F_i(j)) - m_i\nu(\hat{\mathcal{S}}_p) - \nu(H_i(j))$. Observe that if $H_i = X^\alpha(X - 1728)^\beta$, then $\nu_a(H_i(j)) = 3\alpha$ and $\nu_b(H_i(j)) = 2\beta$.

Thus, from Theorem 4.1, we have:

$$\nu_a(\hat{J}_1) = \nu_a(F_1(j)) + \delta \geq \delta, \quad \nu_b(\hat{J}_1) = \nu_b(F_1(j)) + \epsilon \geq \epsilon. \tag{11.1}$$

Also

$$\begin{aligned}\nu_a(\hat{J}_2) &= \nu_a(F_2(j)) + (2p+1)\delta \geq (2p+1)\delta,\\ \nu_b(\hat{J}_2) &= \nu_b(F_2(j)) + (2p+1)\epsilon - 2p\epsilon \geq \epsilon,\end{aligned}$$

noting that we have equality if $\epsilon = 1$ (since $(F_2, G_2) = 1$),

$$\nu_a(\hat{J}_3) = \nu_a(F_3(j)) + (3p^2+2p)\delta - 3\delta p^2 \geq 2p\delta,$$

with equality if $\delta = 1$,

$$\begin{aligned}\nu_b(\hat{J}_i) &\geq \nu_b(F_i(j)) + m_i\epsilon - 2s_i\epsilon\\ &= \nu_b(F_i(j)) - ((i-2)p^{i-1} - (i-1)p^{i-2})\epsilon\\ &\geq -((i-2)p^{i-1} - (i-1)p^{i-2})\epsilon\end{aligned}$$

for $i \geq 3$, and finally,

$$\begin{aligned}\nu_a(\hat{J}_i) &\geq \nu_a(F_i(j)) + m_i\delta - 3t_i\delta\\ &= \nu_a(F_i(j)) - ((i-3)p^{i} - (i-1)p^{i-2})\delta\\ &\geq -((i-3)p^{i} - (i-1)p^{i-2})\delta\end{aligned}$$

for $i \geq 4$. □

Here is the main theorem of this section:

Theorem 11.2. *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* $i \geq 1$.

Proof. Although we have many cases to prove, the basic idea will be the same for all. Theorem 11.1 deals with

$$\hat{\boldsymbol{j}} = (j, \hat{J}_1, \hat{J}_2, \ldots).$$

Then, we apply Lemma 6.3 to get valuations of the coordinates of

$$1728 - \hat{\boldsymbol{j}} = (u_0, u_1, \ldots).$$

With either Lemma 6.4 or Lemma 6.5 we can get valuations of

$$(1728 - \hat{\boldsymbol{j}})^{-1} = (v_0, v_1, \ldots).$$

Using either Lemma 6.2 or Lemma 6.3 again, we get the valuations of

$$\frac{27}{4}\left(1728 \cdot \frac{1}{1728 - \hat{\boldsymbol{j}}} - 1\right) = (w_0, w_1, \ldots),$$

in fact, the lemmas give that $\nu(v_i)$ and $\nu(w_i)$ satisfy the same bounds. Then, by Eqs. (10.1) and (10.2), we get that

$$\begin{aligned} \nu_a(\hat{A}_i) &= \nu_a(w_i) - 2p^i, & \nu_a(\hat{B}_i) &= \nu_a(w_i) - 3p^i, \\ \nu_b(\hat{A}_i) &= \nu_b(w_i) + 2p^i, & \nu_b(\hat{B}_i) &= \nu_b(w_i) + 3p^i. \end{aligned}$$

(We shall keep the notation for the u_i's, v_i's, and w_i's above throughout this proof.)

If $p \equiv 1 \pmod 6$, then, by Theorem 11.1, we have that $\hat{J}_i \in \mathbb{U}_a$, where $\mathbb{U}_a \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, \mathfrak{H}, 1/(\Delta\mathfrak{H}b)]$. Moreover,

$$1728 - j = 1728\frac{27b^2}{4a^3 + 27b^2},$$

so, $1728 - \hat{\boldsymbol{j}} \in \boldsymbol{W}(\mathbb{U}_a)$.

Then, since $(1728 - j)^{-1} \in \mathbb{U}_a$, we get that $(1728 - \hat{\boldsymbol{j}})^{-1} \in \boldsymbol{W}(\mathbb{U}_a)$, and hence

$$\frac{27}{4}\left(1728 \cdot \frac{1}{1728 - \hat{\boldsymbol{j}}} - 1\right) \in \boldsymbol{W}(\mathbb{U}_a).$$

Then, from our previous observations, we have that $\nu_a(\hat{A}_i) \geq -2p^i$ and $\nu_a(\hat{B}_i) \geq -3p^i$, for $i \geq 1$.

Now suppose that $p \equiv 5 \pmod 6$. Then, by Theorem 11.1, we have $\nu_a(\hat{J}_i) \geq 0$ for $i = 1, 2, 3$ and $\nu_a(\hat{J}_i) \geq -((i-3)p^i - (i-1)p^{i-2})$ for $i \geq 4$. By Lemma 6.3, we have that $\nu_a(u_i) \geq 0$ for $i = 1, 2, 3$ and $\nu_a(u_i) \geq -((i-3)p^i - (i-1)p^{i-2})$ for $i \geq 4$. Now, $\nu_a(1728 - j) = 0$, and so, by Lemma 6.4 (with $k = 4$, $\alpha = 3 - 1/p^2$, $\beta = 1 - 1/p^2$) and Lemma 6.3, $\nu_a(w_i) \geq 0$, for $i = 1, 2, 3$, and $\nu_a(w_i) \geq -((i-3)p^i - (i-1)p^{i-2})$ for $i \geq 4$.

Hence, $\nu_a(\hat{A}_i) \geq -2p^i$ for $i = 1, 2, 3$ and $\nu_a(\hat{A}_i) \geq -((i-1)p^i - (i-1)p^{i-2})$ for $i \geq 4$, while $\nu_a(\hat{B}_i) \geq -3p^i$ for $i = 1, 2, 3$ and $\nu_a(\hat{B}_i) \geq -(ip^i - (i-1)p^{i-2})$ for $i \geq 4$.

If $p \equiv 1 \pmod 4$, then, by Theorem 11.1, we have that $\hat{J}_i \in \boldsymbol{W}(\mathbb{U}_b)$, where $\mathbb{U}_b \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, \mathfrak{H}, 1/(\Delta\mathfrak{H}a)]$. Since we also have that $j \in \mathbb{U}_b$, we have that $1728 - \hat{\boldsymbol{j}} \in \boldsymbol{W}(\mathbb{U}_b)$.

Now, we have that $u_0 = 1728 - j$, and so $\nu_b(u_0) = 2$. Then, by Lemmas 6.3 and 6.5, we get that $\nu_b(w_i) \geq -2(i+1)p^i$.

So, $\nu_b(\hat{A}_i) \geq -2ip^i$ and $\nu_b(\hat{B}_i) \geq -(2i-1)p^i$ for $i \geq 0$.

Finally, if $p \equiv 3 \pmod 4$, then by Theorem 11.1 and Lemma 6.3, we have $\nu_b(u_i) \geq 0$ for $i = 0, 1, 2$ and $\nu_b(u_i) \geq -((i-2)p^{i-1} - (i-1)p^{i-2})$ for $i \geq 3$. As above, we have that $\nu_b(u_0) = 2$, and hence, by Lemmas 6.3 and 6.5, we have that $\nu_b(w_i) \geq -2(i+1)p^i$.

Thus, $\nu_b(\hat{A}_i) \geq -2ip^i$ and $\nu_b(\hat{B}_i) \geq -(2i-1)p^i$ for $i \geq 0$. □

We can then apply Theorem 11.2 together with Theorem 10.1 to get bounds, although still far from sharp, for A_i and B_i themselves:

Theorem 11.3. *We have:*

(1) *If $p \equiv 1 \pmod 6$, then:*
   (a) $\nu_a(A_i) \geq -2p^i$ *for* $i \geq 1$;
   (b) $\nu_a(B_i) \geq -3p^i$ *for* $i \geq 1$.

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

(3) *For every $p \equiv 1 \pmod 4$ we have:*
   (a) $\nu_b(A_i) \geq -2ip^i$, *for all* $i \geq 1$;
   (b) $\nu_b(B_i) \geq -(2i-1)p^i$, *for all* $i \geq 1$.

(4) *For every $p \equiv 3 \pmod 4$ we have:*
   (a) $\nu_b(A_i) \geq -2ip^i - ip^{i-1} - (i-1)p^{i-2}$, *for all* $i \geq 1$;
   (b) $\nu_b(B_i) \geq -(2i-1)p^i - ip^{i-1} - (i-1)p^{i-2}$, *for all* $i \geq 1$.

Proof. The proof follows immediately from Theorems 10.1 and 11.2 after observing that Eq. (7.1) gives that

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

	$p=5$		$p=7$	
	Actual	Bound	Actual	Bound
$\nu_a(A_1)$	-1	-11	1	-14
$\nu_a(A_2)$	-35	-61	-35	-98
$\nu_a(A_3)$	-325	-335	-539	-686
$\nu_a(A_4)$	-1775	-2375	-4067	-4802
$\nu_a(B_1)$	-6	-16	-6	-21
$\nu_a(B_2)$	-60	-86	-84	-147
$\nu_a(B_3)$	-450	-460	-882	-1029
$\nu_a(B_4)$	-2400	-3000	-6468	-7203
$\nu_b(A_1)$	-4	-10	-8	-15
$\nu_b(A_2)$	-40	-100	-112	-211
$\nu_b(A_3)$	-300	-750	-1176	-2219
$\nu_b(A_4)$	-1600	-5000	-10976	-20727
$\nu_b(B_1)$	1	-5	-1	-8
$\nu_b(B_2)$	-15	-75	-63	-162
$\nu_b(B_3)$	-175	-625	-833	-1876
$\nu_b(B_4)$	-975	-4375	-8575	-18326

TABLE 11.1. Actual valuations versus bounds.

□

As mentioned, these bounds are far from sharp. Table 11.1 illustrates this point.

12. Improved Bounds for A_1 and B_1

Due to some specific results from [Fin10] on J_1, we can obtain improved bounds for the valuations of A_1 and B_1.

We start by stating these results:

Theorem 12.1. *Let $p \geq 5$ be prime. Then,*

$$\operatorname{ord}_{X=0}\left(J_1(X)\right) = \begin{cases} (2p+1)/3 & \text{if } p \equiv 1 \pmod 6, \\ (2p-1)/3 & \text{if } p \equiv 5 \pmod 6, \end{cases}$$

and

$$\operatorname{ord}_{X=1728}\left(J_1(X)\right) = \begin{cases} 1 & \text{if } 1728^p \equiv 1728 \pmod{p^2}, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, if $\boldsymbol{j} = (j, J_1(j))$ *and* $1728 - \boldsymbol{j} = (u_0, u_1)$*, then*

$$\nu_b(u_1) \geq \begin{cases} p+1, & \text{if } p \equiv 1 \pmod 4, \\ p-1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. The first part follows from [Fin10, Theorem 3.2], which was originally proved by Kaneko and Zagier in [KZ98], while the second part follows from Proposition 5.6 of the same reference.

The last part is proved within the proof of [Fin10, Proposition 5.6]. □

Although of no real consequence for us here, we've checked using Sage that the only primes p, with $5 \leq p \leq 436263290$, for which $1728^p \equiv 1728 \pmod{p^2}$ are 2693 and 123653.

Also, note that if $1728 = (\alpha_0, \alpha_1) \in \boldsymbol{W}_2(\mathbb{F}_p)$, then $\alpha_0 = 1728$ (in $\mathbb{F}_p$) and $\alpha_1 = (1728 - 1728^p)/p$. So, $\alpha_1 = 0$ if and only if $1728^p \equiv 1728 \pmod{p^2}$.

We immediately get from Theorem 12.1:

Corollary 12.2. *We have*

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

Proof. Since $j = 1728 \cdot 4a^3/(4a^3 + 27b^2)$, we have that $\nu_a(J_1(j)) = 3 \cdot \operatorname{ord}_{X=0} J_1(X)$. Now, let $1728 = (\alpha_0, \alpha_1) \in \boldsymbol{W}_2(\mathbb{F}_p)$, as above, and $1728 - \boldsymbol{j} = (u_0, u_1)$. Then

$$u_1 = \alpha_1 - J_1(j) - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} \alpha_0^{p-i} (-j)^i$$

(observing that $\frac{1}{p}\binom{p}{i} \in \mathbb{Z}$). So, we have $\nu_a(u_0) = 0$, and $\nu_a(u_1) = 0$ if $\alpha_1 \neq 0$ and $\nu_a(u_1) \geq 3$ if $\alpha_1 = 0$.

Then, if $(1728 - \boldsymbol{j})^{-1} = (v_0, v_1)$, we have that $v_0 = 1/u_0$, and $v_1 = -u_1/u_0^{2p}$. So, $\nu_a(v_0) = 0$ and $\nu_a(v_1) = \nu_a(u_1) \geq 0$.

Similarly, if we let $27/4 = (\beta_0, \beta_1)$ and $27/(4(1728 - \boldsymbol{j})) = (w_0, w_1)$, then we have $\nu_a(w_0) = \nu_a(\beta_0 v_0) = 0$, and $\nu_a(w_1) = \nu_a(\beta_0^p v_1 + v_0^p \beta_1)$, and so $\nu_a(w_1) = \nu_a(v_1) \geq 0$ if $\beta_1 = 0$, and $\nu_a(w_1) \geq 0$ if $\beta_1 \neq 0$. Therefore, in either case, we have $\nu_a(w_1) \geq 0$.

Hence, if $27\boldsymbol{j}/(4(1728 - \boldsymbol{j})) = (z_0, z_1)$, then $(z_0, z_1) = (jw_0, j^p w_1 + w_0^p J_1(j))$, and thus $\nu_a(z_0) = 3$ and $\nu_a(z_1) = \nu_a(J_1(j))$, since, by Theorem 12.1, we have $\nu_a(j^p w_1) \geq 3p > 2p + 1 \geq \nu_a(J_1(j))$.

Now, by Eq. (3.2), we have $\nu_a(A_1) = \nu_a(J_1(j)) - 2p$, and by Eq. (3.3) we have $\nu_a(B_1) = \nu_a(J_1(j)) - 3p$. The result then follows from Theorem 12.1. □

We proceed in a similar manner for ν_b.

Corollary 12.3. *We have*

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

Proof. If $1728 - \boldsymbol{j} = (u_0, u_1)$, then by Theorem 12.1, we have that $\nu_b(u_0) = 2$ and $\nu_b(u_1) \geq p \pm 1$ with the positive sign if $p \equiv 1 \pmod 4$ and negative sign if $p \equiv 3 \pmod 4$.

Then, if $(1728 - \boldsymbol{j})^{-1} = (v_0, v_1)$, we have that $v_0 = 1/u_0$, and $v_1 = -u_1/u_0^{2p}$. So, $\nu_b(v_0) = -2$ and $\nu_b(v_1) \geq -3p \pm 1$.

Similarly, the formulas for the Witt product give that if $27/(4(1728 - \boldsymbol{j})) = (w_0, w_1)$, then $\nu_b(w_0) = -2$, $\nu_b(w_1) \geq -3p \pm 1$.

Now, observe that from the second part of Theorem 12.1, we have that $\operatorname{ord}_{X=1728} J_1(X) \in \{0, 1\}$, and so $\nu_b(J_1(j)) \in \{0, 2\}$. Therefore

$$\nu_b(J_1(j)w_0^p + w_1 j^p) \geq -3p \pm 1,$$

i.e., if $27\boldsymbol{j}/(4(1728 - \boldsymbol{j})) = (z_0, z_1)$, then $\nu_b(z_0) = -2$ and $\nu_b(z_1) \geq -3p \pm 1$.

Thus, by Eq. (3.2), we have $\nu_b(A_1) \geq -p \pm 1$, and by Eq. (3.3) we have $\nu_b(B_1) \geq \pm 1$. □

Acknowledgments. The computations mentioned were done with MAGMA.

References

[Bor11] J. Borger. The basic geometry of Witt vectors, I: The affine case. *Algebra Number Theory*, 5(2):231–285, 2011.

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

[Fin02] L. R. A. Finotti. Degrees of the elliptic Teichmüller lift. *J. Number Theory*, 95(2):123–141, 2002.

[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.

[Fin19] L. R. A Finotti. Weierstrass coefficients of the canonical lifting. To appear at the *Int. J. of Number Theory*. Available at `http://www.math.utk.edu/~finotti/`, 2019.

[Haz09] M. Hazewinkel. Witt vectors. I. In *Handbook of algebra. Vol. 6*, volume 6 of *Handb. Algebr.*, pages 319–472. Elsevier/North-Holland, Amsterdam, 2009.

[KZ98] M. Kaneko and D. Zagier. Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 97–126. Amer. Math. Soc., Providence, RI, 1998.

[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`.

[Poo01] B. Poonen. Computing torsion points on curves. *Experiment. Math.*, 10(3):449–465, 2001.

[Rab14] J. Rabinoff. The Theory of Witt Vectors. *arXiv e-prints*, page arXiv:1409.7445, September 2014.

[Sat00] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.

[Vol97] J. F. Voloch. Torsion points of $y^2 = x^6 + 1$. *unpublished manuscript*, 1997. available at `http://www.ma.utexas.edu/users/voloch/oldpreprint.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`