5-2020

Denominators of the Weierstrass Coefficients of the Canonical Lifting

Delong Li
University of Tennessee, dli24@vols.utk.edu

To the Graduate Council:

I am submitting herewith a dissertation written by Delong Li entitled "Denominators of the Weierstrass Coefficients of the Canonical Lifting." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

Luis Finotti, Major Professor

We have read this dissertation and recommend its acceptance:

Shashikant Mulay, Marie Jameson, Michael Berry

Accepted for the Council:

Dixie L. Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

Denominators of the Weierstrass Coefficients of the Canonical Lifting

A Dissertation Presented for the

Doctor of Philosophy

Degree

The University of Tennessee, Knoxville

Delong Li

May 2020

I dedicate this work to my parents, my advisor: Luis Finotti, and my professors Shashikant Mulay, Marie Jameson, Dustin Cartwright, and Morwen Thistlethwaite.

Acknowledgments

I would like to thank: Luis Finotti, for his ideas and guidance. I also acknowledge the use of Magma for the computation in the dissertation.

Abstract

Given an ordinary elliptic curve $E/k : y_0^2 = x_0^3 + a_0x_0 + b_0$ with characteristic $p \geq 5$, the canonical lifting $\mathbf{E}$ over the ring of Witt vectors is given by $\mathbf{E}/W(k) : y^2 = x^3 + ax + b$, where $a = (a_0, A_1, A_2, \ldots)$ and $b = (b_0, B_1, B_2, \ldots)$ are functions of a_0 and b_0. Finotti has proved that these functions A_i and B_i can be taken to be rational functions on a_0 and b_0 and raised questions about their denominators. In this dissertation we will find all the possible factors of the denominators, and give an upper bound for each factor, in the case when these functions are obtained from formulas for the j-invariant of the canonical lifting. We will also find an isomorphic canonical lifting that is universal up to the second coordinates. In addition, we will show some computations done with Magma.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

In this chapter, I will talk informally about the problems I am trying to solve, and also the motivation of the dissertation.

This dissertation is about the canonical lifting of elliptic curves. Elliptic curve is an important topic in the area of number theory. It is also a difficult topic because we must have studied commutative algebra, algebraic number theory, and algebraic geometry in order to understand it fully. There are also a lot of aspects in elliptic curves and many people are working on it. It also has many applications such as cryptography.

The underlying field of an elliptic curve can have either characteristic zero or positive characteristic. In the second case, we can define the canonical lifting of the curve to be another elliptic curve which satisfies some nice properties. The coefficients of the canonical lifting are infinite vectors with special addition and multiplication, which are called Witt vectors. This concept of canonical lifting of elliptic curves was first introduced by Deuring in [1] and then generalized to Abelian varieties by Serre and Tate in [10]. This theory has many applications, such as counting rational points in ordinary elliptic curves, as in Satoh's [12], coding theory, as in Voloch and Walker's [16], and counting torsion points of curves of genus $g \geq 2$, as in Poonen's [11] or Voloch's [15].

It is known that the canonical lifting is unique up to isomorphism. Dr. Finotti has asked the question: can we find formulas for the canonical lifting that satisfies good properties? In Finotti's [8], he gave two ways to construct the canonical lifting. The first way is by solving a system of linear equations. The canonical lifting obtained this way satisfies nice

properties. For example, it is universal and modular. We will explain what these mean in the next chapter. Finotti has asked me to find out more properties about this canonical lifting. Especially, through computations, he observed that Δ does not appear in the denominators of each coordinate, so he would like to prove it is true in general. But the study of this canonical lifting is very difficult because the computation involves solving a big system of equations.

The second way is by using j-invariant. This method gives an explicit formula which is easier to study. Finotti has shown that the coordinates are modular functions and wondered about other properties. For example, he asked the following questions.

1. What are the possible factors of the denominators?
2. What are the powers of each factor?
3. Starting with this formula, can we obtain an isomorphic canonical lifting with better properties such as universal?

The main goal of this dissertation is to answer these three questions as much as possible. I will answer question 1 fully. For question 2, I will give an upper bound for the powers. For question 3, I will only be able to obtain canonical lifting that is universal up to the second coordinates. In the future, I would like to improve these results.

In this dissertation, I used Magma to do the computations with Witt vectors. It gives a good prediction and also helps me test some conjectures.

In this dissertation, I used many results from Finotti. All his papers can be found in his website at https://www.math.utk.edu/ finotti/. In addition to the references that I will mention, I also used Dummit and Foote's [2] a lot.

In this dissertation, I will post some questions that I will be working on in the future. They will be labeled as future questions.

Chapter 2

Preliminaries

In this chapter, I will give some definitions and theorems that are needed to understand the problems I am trying to solve. The main goal of this chapter is to explain what the canonical lifting of elliptic curve mean.

2.1 Elliptic curves

This section gives a brief introduction to elliptic curves and some related concepts. For more information on the definition of elliptic curves, please read Silverman and Tate's [14], which requires some knowledge of algebraic geometry. For the related concepts, please read Silverman's [13], which is harder to read.

Let k be a field of characteristic $p \geq 5$, $\overline{k}$ be the algebraic closure of k, $a, b \in k$, $f(x) = x^3 + ax + b$, and assume that the roots of $f(x)$ are distinct. Then the curve given by the equation

$$E/k : y^2 = x^3 + ax + b$$

is called an *elliptic curve E over k*, and a, b are called the *Weierstrass coefficients* of E. Sometimes, I will just call them the coefficients of E for short. We also call E the elliptic curve given by (a, b).

Let R be an integral domain and k its field of fractions. Let $E/k : y^2 = x^3 + ax + b$ be an elliptic curve over k. If a, b are in R, then we say E is an *elliptic curve over R*. Let

$E_1 : y^2 = x^3 + ax + b$ and $E_2 : y^2 = x^3 + cx + d$ be two elliptic curves over R. We say E_1/R and E_2/R are *isomorphic* if there is $\lambda \in \overline{k}$ such that $c = \lambda^4 a$ and $d = \lambda^6 b$.

Since we consider elliptic curve a *projective curve*, we have one extra point "at infinity": the corresponding equation in the projective plane is the set of solutions in $\overline{k}$ to $Y^2Z = X^3 + aXZ^2 + bZ^3$. We identify (x, y) with $[x, y, 1]$. Then the projective curve has one more point $\mathcal{O} = [0, 1, 0]$, which we refer to as the point at infinity.

If K is a field extension of k, we denote by

$$E(K) = \{(x_0, y_0) \in K^2 : y_0^2 = x_0^3 + ax_0 + b\} \cup \{\mathcal{O}\},$$

the set of points of E with coordinates in K.

We can roughly define addition on $E(K)$ as follows: let $P, Q \in E(K)$. The line connecting P and Q intersects the projective curve in a third point in $E(K)$. Reflect that point about the x-axis, and the resulting point is defined to be $P + Q$. It is known that $E(K)$ is a group under this addition. Let

$$E[p] = \{P \in E(\bar{k}) : pP = \mathcal{O}\}.$$

Then it is known that $E[p]$ is either 0 or $\mathbb{Z}/p\mathbb{Z}$. E is called *supersingular* if $E[p] = 0$, and *ordinary* otherwise.

2.2 The ring of Witt vectors

This section gives a brief introduction to the ring of Witt vectors. For more detail, please read Jacobson's [9] which gives a clear definition, and the material does not require a lot of background. Please also read Finotti's [8], which gives more details about the computational aspects of the Witt vectors.

We introduce this concept because the canonical lifting of an elliptic curve is an elliptic curve with coefficients in the ring of Witt vectors.

Let p be a prime. Let $X_0, Y_0, X_1, Y_1, \ldots$ be indeterminates. Let $S_0(X_0, Y_0) = X_0 + Y_0$ and $P_0(X_0, Y_0) = X_0 Y_0$. For $n \geq 1$, define S_n, P_n inductively:

$$\begin{aligned} S_n(X_0, Y_0, \ldots, X_n, Y_n) &= (X_n + Y_n) + \frac{1}{p}(X_{n-1}^p + Y_{n-1}^p - S_{n-1}^p) \\ &\quad + \cdots + \frac{1}{p^n}(X_0^{p^n} + Y_0^{p^n} - S_0^{p^n}), \\ P_n(X_0, Y_0, \ldots, X_n, Y_n) &= \frac{1}{p^n}((X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) \\ &\quad - (P_0^{p^n} + \cdots + p^{n-1} P_{n-1}^p)). \end{aligned} \tag{2.1}$$

Then it is known that $S_n, P_n \in \mathbb{Z}[X_0, Y_0, \ldots, X_n, Y_n]$. Let $\overline{S_n}, \overline{P_n}$ be the reduction modulo p of S_n, P_n, respectively. Let A be a commutative ring with $1 \neq 0$ of characteristic p. Let

$$W(A) = \{(a_0, a_1, \ldots) : a_i \in A\}.$$

Let $a = (a_0, a_1, \ldots), b = (b_0, b_1, \ldots) \in W(A)$. Define

$$\begin{aligned} a + b &= (\overline{S_0}(a_0, b_0), \overline{S_1}(a_0, b_0, a_1, b_1), \ldots), \\ ab &= (\overline{P_0}(a_0, b_0), \overline{P_1}(a_0, b_0, a_1, b_1), \ldots). \end{aligned}$$

Then it is known that $W(A)$ forms a commutative ring with $1 = (1, 0, 0, \ldots) \neq 0 = (0, 0, \ldots)$. We call $W(A)$ the *ring of Witt vectors over* A.

We observe that the expressions for S_n, P_n are complicated. For instance, for $p = 7$ the polynomial $S_2 \in \mathbb{Z}[X_0, X_1, X_2, Y_0, Y_1, Y_2]$ has 412 monomials. Magma has been used to do the computations of Witt vectors. Finotti has written programs that can compute the sum, product, and inverse of Witt vectors for the first few coordinates and for small prime p.

The ring of Witt vectors is closely related to p-adic integers. In fact, it is known that $W(\mathbb{F}_p) \cong \mathbb{Z}_p$ as rings, where $\mathbb{Z}_p$ is the ring of p-adic integers.

We need one more definition to define the canonical lifting: define $\sigma : W(A) \to W(A)$ by $\sigma(a_0, a_1, \ldots) = (a_0^p, a_1^p, \ldots)$. It is known that σ is a ring endomorphism of $W(A)$, called the *Frobenius endomorphism of* $W(A)$. Sometimes, we will call it the Frobenius of $W(A)$ for short.

2.3 The canonical lifting of elliptic curves

This section gives the definition of the canonical lifting of elliptic curves. Please read Finotti's [8] for more details. We will first introduce some terminologies and notations.

Let k be a perfect field of characteristic $p \geq 5$.

If $\mathbf{E}/W(k) : y^2 = x^3 + ax + b$ is an elliptic curve over $W(k)$, where $a = (a_0, a_1, \ldots)$ and $b = (b_0, b_1, \ldots)$, then $E/k : y_0^2 = x_0^3 + a_0 x_0 + b_0$ is an elliptic curve over k, called the *reduction modulo p of* $\mathbf{E}$, since $(c_0, c_1, \ldots) \mapsto c_0$ is the reduction modulo p in $W(k)$.

If $E/k : y_0^2 = x_0^3 + a_0 x_0 + b_0$ is an elliptic curve over k, then $y_0^2 = x_0^3 + a_0^p x_0 + b_0^p$ is also an elliptic curve over k, which we denote by E^σ. Here, the σ denotes the Frobenius of k. Similarly, if $\mathbf{E}/W(k) : y^2 = x^3 + ax + b$ is an elliptic curve over $W(k)$, then $y^2 = x^3 + a^\sigma x + b^\sigma$ is also an elliptic curve over $W(k)$, which we denote by $\mathbf{E}^\sigma$, where $a^\sigma = \sigma(a)$ and σ is the Frobenius of $W(k)$.

If $\mathbf{E}$ is an elliptic curve over $W(k)$ and E is its reduction modulo p, define $\pi : \mathbf{E}(W(k)) \to E(k)$ by

$$\pi((c_0, c_1, \ldots), (d_0, d_1, \ldots)) = (c_0, d_0). \tag{2.2}$$

Then π is well defined and is called the *reduction modulo p*. Similarly, E^σ is the reduction modulo p of $\mathbf{E}^\sigma$, and we also use π to denote the reduction modulo p map.

If E is an elliptic curve over k, define $\phi : E(k) \to E^\sigma(k)$ by $\phi(c, d) = (c^p, d^p)$. Then ϕ is well defined and is a curve homomorphism, i.e., it is given by rational functions and it also maps $\mathcal{O}$ to $\mathcal{O}$. This map ϕ is called the *Frobenius (for curves over fields of characteristic p)*.

With the notations given above, we are now able to give the definition of canonical lifting of elliptic curves.

Given an ordinary elliptic curve E, it is known that there exists a unique elliptic curve $\mathbf{E}$ over $W(k)$, up to isomorphism, and a homomorphism of curves $\Phi : \mathbf{E} \to \mathbf{E}^\sigma$ such that E is the reduction modulo p of $\mathbf{E}$ (and so E^σ is the reduction modulo p of $\mathbf{E}^\sigma$), and the following diagram commutes:

$$\begin{array}{ccc} \mathbf{E}(W(k)) & \xrightarrow{\Phi} & \mathbf{E}^{\sigma}(W(k)) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ E(k) & \xrightarrow{\phi} & E^{\sigma}(k) \end{array}$$

The elliptic curve $\mathbf{E}$ described above is called the *canonical lifting* of E.

Notice that we assumed k to be perfect at the beginning. In fact, we can extend the definition to non-perfect fields.

If E/k and k is a field of characteristic $p \geq 5$, not perfect, Finotti showed that the canonical lifting of E can be defined over $W(k)$. Hence we can extend the definition of canonical lifting of elliptic curves to non-perfect fields of characteristic $p \geq 5$.

Chapter 3

The canonical lifting through j-invariant

In this chapter, I will introduce the previous results about the canonical lifting and lead to the problems I am trying to solve.

3.1 Some terminology

In this section, we introduce some terminology that is used in the constructions of canonical lifting.

Let k be a field of characteristic $p \geq 5$. Let

$$E/k : y^2 = x^3 + ax + b$$

be an elliptic curve over k. Define the *discriminant* of E to be $4a^3 + 27b^2$, denoted by Δ. Then $\Delta \neq 0$, since we required that the cubic in x has no multiple roots. Define the *Hasse invariant* of E to be the coefficient of x^{p-1} in $(x^3 + ax + b)^{(p-1)/2}$, denoted by $\mathcal{H}$. Then it is known that E is ordinary if $\mathcal{H} \neq 0$, and E is supersingular if $\mathcal{H} = 0$. Define the *j-invariant* of E to be

$$1728 \cdot \frac{4a^3}{4a^3 + 27b^2},$$

denoted by j. It is known that two elliptic curves are isomorphic if and only if they have the same j-invariant.

3.2 The set up of the problems and the properties of the canonical lifting

In this section, we will introduce the set up of the problems and we will talk about the properties of the canonical lifting that we want.

Let $R = \mathbb{F}_p[a_0, b_0]$ and $k = \mathbb{F}_p(a_0, b_0)$, where a_0 and b_0 are *indeterminates* and $p \geq 5$. Then, the elliptic curve given by $E/k : y_0^2 = x_0^3 + a_0 x_0 + b_0$ is ordinary. It is an elliptic curve because $\Delta = 4a_0^3 + 27b_0^2$ is a non-zero element in k. It is ordinary because by Equation (2.3) from [4], we have

$$\mathcal{H} = \left(\frac{b_0}{a_0}\right)^r \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} \left(\frac{a_0^3}{b_0^2}\right)^i,$$

where $r = (p-1)/2$, $r_1 = \lceil r/3 \rceil$, and $r_2 = \lfloor r/2 \rfloor$. Hence $\mathcal{H}$ is a non-zero element in k.

So we can let $\mathbf{E}/W(k) : y^2 = x^3 + ax + b$ be the canonical lifting of E, where $a = (a_0, A_1, A_2, \ldots), b = (b_0, B_1, B_2, \ldots)$. Because the canonical lifting is unique only up to isomorphism, these A_n, B_n are not uniquely defined. We want to find formulas for A_n, B_n that satisfy nice properties.

One of the properties we want is universal. If the formulas for A_n, B_n are well defined for all specializations of a_0, b_0 that give ordinary elliptic curves, then A_n, B_n are called *universal*.

Another property is modular functions. Define the weights of a_0, b_0 to be $4, 6$, respectively, denoted by $\mathrm{wt}(a_0) = 4, \mathrm{wt}(b_0) = 6$. Define

$$\mathrm{S}_n = \{f/g \in \mathbb{F}_p(a_0, b_0) : f, g \in \mathbb{F}_p[a_0, b_0] \text{ homogeneous, and } \mathrm{wt}(f) - \mathrm{wt}(g) = n\} \cup \{0\}.$$

If h is in S_n for some integer n, then h is called a *modular function of weight* n.

3.3 The first construction of canonical lifting

In this section, we will talk about the first construction of canonical lifting.

In Finotti's [8], he gave two ways to construct the canonical lifting. The first way is by solving a system of equations. Finotti has shown the following theorem for the first construction.

Theorem 3.1 (Finotti)**.** *The A_n, B_n obtained in the first way are universal and modular functions. In particular, $A_n \in \mathrm{S}_{4p^n}$ and $B_n \in \mathrm{S}_{6p^n}$.*

We see that the A_n, B_n obtained in the first way satisfies nice properties. Finotti has asked more questions about these A_n, B_n. For example, the theorem implies that A_n, B_n have only Δ and $\mathcal{H}$ in the denominator, that is, $A_n, B_n \in \mathbb{F}_p[a_0, b_0, 1/(\Delta\mathcal{H})]$. Finotti asked about the powers for each factor. From computations, he observed that Δ does not appear in the denominators. Therefore, he conjectured that this is true in general. Here is Dr. Finotti's conjecture:

Conjecture 3.2. *(1) There are universal modular functions A_n, B_n such that $A_n, B_n \in \mathbb{F}_p[a_0, b_0, 1/\mathcal{H}]$.*

(2) The A_n, B_n obtained in the first construction give such modular functions.

To answer the questions, we need to study the construction which involve solving a big system of equations. I do not have a solution yet, so I will post them as future questions.

Future question 1. Show that Δ does not appear in the denominators of A_n, B_n in the first construction. Or find a counter example.

Future question 2. What are the powers of $\mathcal{H}$ in the denominators of A_n, B_n in the first construction?

3.4 The second construction of canonical lifting

In this section, we will talk about the second construction of canonical lifting. My dissertation will be mainly focused on this construction.

The second way is by using j-invariant. It says that the coefficients a, b of the canonical lifting can be given by the following explicit formulas:

$$\begin{aligned} a &= \lambda^4 \frac{27j}{4(1728-j)} = (a_0, A_1, A_2, \ldots), \\ b &= \lambda^6 \frac{27j}{4(1728-j)} = (b_0, B_1, B_2, \ldots), \end{aligned} \tag{3.1}$$

where $\lambda = (\sqrt{b_0/a_0}, 0, 0, \ldots)$, and j is the j-invariant of the canonical lifting. Using Magma, we have that, for $p = 5$,

$$\begin{aligned} A_1 &= (2a_0^{12} + 3a_0^9 b_0^2 + 3a_0^6 b_0^4 + 3a_0^3 b_0^6 + 3b_0^8)/(a_0 b_0^4), \\ B_1 &= (2a_0^{12} b_0 + 3a_0^9 b_0^3 + 3a_0^6 b_0^5 + 3a_0^3 b_0^7 + 3b_0^9)/a_0^6. \end{aligned}$$

This can be seen in Figure 3.1. We will give more details about the codes in the last chapter computations section.

We know that for $p = 5$, $\mathcal{H} = 2a_0$. If $b_0 = 0$, then these formulas does not work. So these formulas are not universal. But we still want to study these formulas because the formulas are very simple and therefore we can get a very good understanding of each A_n, B_n. In this dissertation, we will answer the following questions:

Dissertation question 1. We show that A_n, B_n are modular functions.

Dissertation question 2. We will find all the possible factors for the denominators of A_n, B_n.

Dissertation question 3. We will give an upper bound for the power of each factor.

We still can try to find universal A_n, B_n's from these construction. If $\lambda = (\lambda_0, \lambda_1, \ldots)$, then the elliptic curve given by $(\lambda^4 a, \lambda^6 b)$ is also the canonical lifting. We can choose λ_n so that the new formulas are universal. We have not done too much in this part yet. The difficulty is that we need more information about the numerators of A_n, B_n.

Future question 3. Find λ so that $\lambda^4 a, \lambda^6 b$ are universal.

```
> 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 computations.

Chapter 4

Modular functions

The main goal of this chapter is to answer the first dissertation question. That is, we will show that A_n, B_n are modular functions. We will introduce some tools we need to solve the problem.

4.1 Properties of j-invariant

In this section, I provide more results about j-invariant. More details can be found in Finotti's [6] and [4].

Given an ordinary elliptic curve E/k with j-invariant j_0, we have that the j-invariant of its canonical lifting is $j = (j_0, J_1(j_0), J_2(j_0), \ldots)$ for some uniquely defined functions J_i. To describe more about these functions J_i, we need a few more definitions.

It is known that, for a fixed characteristic $p > 0$, there are, up to isomorphism, finitely many supersingular elliptic curves. Let s be the number of supersingular elliptic curves for a fixed characteristic p and $j_1, \ldots, j_s$ be the j-invariants of these curves. The *supersingular polynomial* is defined as

$$\mathrm{ss}_p(X) = \prod_{i=1}^{s}(X - j_i).$$

Define

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

Let

$$r = (p-1)/2, \quad r_1 = \lceil r/3 \rceil, \quad r_2 = \lfloor r/2 \rfloor, \quad r_1' = \lfloor r/3 \rfloor, \quad r_2' = \lceil r/2 \rceil.$$

Then we have the following lemma.

Lemma 4.1. *We have*

(1) Let $p = 12k + s$, where $0 < s < 12$. Then $r_2 - r_1 = k \geq 0$,

(2) $\delta = r_1 - r_1' = 3r_1 - r \geq 0$,

(3) $\epsilon = r_2' - r_2 = r - 2r_2 \geq 0$.

Proof. For (1), we have four cases $s = 1, 5, 7, 11$. If $s = 1$, then $r_1 = 2k$ and $r_2 = 3k$, hence $r_2 - r_1 = k \geq 0$. Other cases and (2), (3) can be proved similarly. □

Define

$$\mathcal{S}_p(X) = \frac{\mathrm{ss}_p(X)}{X^\delta (X - 1728)^\epsilon}.$$

Lemma 4.2. *We have $\mathcal{S}_p(X) \in \mathbb{F}_p[X]$ is monic, and $\mathcal{S}_p(0), \mathcal{S}_p(1728) \neq 0$. Also, we have* $\deg \mathcal{S}_p = r_2 - r_1$.

Proof. From [4], we have

$$\mathrm{ss}_p(X) = \left(-\frac{2}{9}\right)^r \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} \left(-\frac{27}{4}\right)^i X^{i-r_1'} (X - 1728)^{r_2' - i}.$$

So $\mathrm{ss}_p(X) \in \mathbb{F}_p[X]$, and $\mathrm{ss}_p(X) = X^{r_1 - r_1'}(X - 1728)^{r_2' - r_2} Q(X)$ for some $Q(X) \in \mathbb{F}_p[X]$ such that $X, (1728 - X) \nmid Q(X)$. Hence $\mathcal{S}_p(X) \in \mathbb{F}_p[X]$, and $\mathcal{S}_p(0), \mathcal{S}_p(1728) \neq 0$ by Lemma 4.1. Since $\mathrm{ss}_p(X)$ is monic, we have $\mathcal{S}_p(X)$ is monic. From [4] under (2.6), we have $\deg \mathrm{ss}_p(X) = r_2' - r_1'$. So $\deg \mathcal{S}_p = r_2' - r_1' - \delta - \epsilon = r_2 - r_1$. □

Let

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

We state the main result of [6].

Theorem 4.3. *We have*

(1) $J_i(X) \in \mathbb{F}_p(X)$ *for all* $i \geq 1$.

(2) Let $p \geq 5$, *and for* $i \geq 1$, *let* $J_i = F_i/G_i$ *be such that* $F_i, G_i \in \mathbb{F}_p[X]$, $(F_i, G_i) = 1$, *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 we have:*

(a) $\deg F_i - \deg G_i = p^i - \iota$;

(b) $G_i = \mathcal{S}_p(X)^{ip^{i-1}+(i-1)p^{i-2}} H_i$, *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* $H_i \mid X^{\delta t_i'}(X - 1728)^{\epsilon s_i}$ *for* $i \geq 4$.

This theorem is very helpful because we can get a better understanding of the factors of $J_n(j_0)$. Then we can use Equation (3.1) to study a and b.

4.2 Properties of Witt vectors

Previously, we defined the ring of Witt vectors. In this section, we give more properties of this ring.

Let A be a commutative ring with $1 \neq 0$ of characteristic $p > 0$. Let $W(A)$ be the ring of Witt vectors over A. Remember that

$$\begin{aligned} S_n(X_0, Y_0, \ldots, X_n, Y_n) &= (X_n + Y_n) + \frac{1}{p}(X_{n-1}^p + Y_{n-1}^p - S_{n-1}^p) \\ &\quad + \cdots + \frac{1}{p^n}(X_0^{p^n} + Y_0^{p^n} - S_0^{p^n}), \\ P_n(X_0, Y_0, \ldots, X_n, Y_n) &= \frac{1}{p^n}((X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) \\ &\quad - (P_0^{p^n} + \cdots + p^{n-1} P_{n-1}^p)). \end{aligned}$$

We first show a few basic results about Witt vectors.

Lemma 4.4. *Let* $(c_0, c_1, \ldots) \in W(A)$, *and* $\lambda, \mu \in A$. *Then we have*

(i) We have $p = (0, 1, 0, 0, \ldots)$ *and if* A *is perfect, then the map* $\varphi : W(A) \to A$ *defined by* $\varphi((a_0, a_1, \ldots)) = a_0$ *is a ring homomorphism, called the* reduction modulo p.

(ii) $(c_0, c_1, \ldots) \in W(A)^\times$ *if and only if* $c_0 \in A^\times$,

(iii)

$$(\lambda, 0, 0, \ldots)(c_0, c_1, \ldots) = (\lambda c_0, \lambda^p c_1, \lambda^{p^2} c_2, \ldots),$$

(iv) If p is odd, then

$$-(c_0, c_1, \ldots) = (-c_0, -c_1, \ldots),$$

(v) Let $n \geq 0$. Then

$$(\lambda, 0, 0, \ldots)(\mu, 0, 0, \ldots) = (\lambda\mu, 0, 0, \ldots), \quad (\lambda, 0, 0, \ldots)^n = (\lambda^n, 0, 0, \ldots),$$

(vi) Let $n \geq 1$. Then in $W(A)$, we have

$$\begin{aligned} n &= n \cdot 1 = (n, *, *, \ldots), \\ (\lambda, *, *, \ldots) &+ (\mu, *, *, \ldots) = (\lambda + \mu, *, *, \ldots), \\ (\lambda, *, *, \ldots)&(\mu, *, *, \ldots) = (\lambda\mu, *, *, \ldots), \end{aligned}$$

where $*$ indicates that we do not have any information of its value. If $\lambda \in A^\times$, then

$$(\lambda, *, *, \ldots)^{-1} = (\lambda^{-1}, *, *, \ldots).$$

Proof. The proof of (i) and (ii) can be found in Jacobson's [9] section 8.10.

For (iii), we show that $P_n(X_0, Y_0, 0, Y_1, \ldots, 0, Y_n) = X_0^{p^n} Y_n$ for $n \geq 0$ by induction on n. If $n = 0$, $P_0(X_0, Y_0) = X_0 Y_0$. Let $n \geq 1$. By (2.1), we have

$$\begin{aligned} P_n(X_0, Y_0, 0, Y_1, \ldots, 0, Y_n) = \frac{1}{p^n}(&X_0^{p^n}(Y_0^{p^n} + \cdots + p^{n-1} Y_{n-1}^p + p^n Y_n) \\ &- (P_0(X_0, Y_0)^{p^n} + \cdots + p^{n-1} P_{n-1}(X_0, Y_0, 0, Y_1, \ldots, 0, Y_{n-1})^p)). \end{aligned}$$

By induction hypothesis,

$$\begin{aligned} P_n(X_0, Y_0, 0, Y_1, \ldots, 0, Y_n) = \frac{1}{p^n}(&X_0^{p^n} Y_0^{p^n} + \cdots + p^{n-1} X_0^{p^n} Y_{n-1}^p + p^n X_0^{p^n} Y_n) \\ - ((X_0 Y_0)^{p^n} + \cdots + p^{n-1}&(X_0^{p^{n-1}} Y_{n-1})^p)) = X_0^{p^n} Y_n. \end{aligned}$$

Therefore, $P_n = X_0^{p^n} Y_n + X_1 Q_1 + \cdots + X_n Q_n$ for some $Q_1, \ldots, Q_n \in \mathbb{Z}[X_0, Y_0, \ldots, X_n, Y_n]$. Let $(d_0, d_1, \ldots) = (\lambda, 0, 0, \ldots)(c_0, c_1, \ldots)$. Then, we have $d_n = \overline{P_n}(\lambda, c_0, 0, c_1, \ldots, 0, c_n) = \lambda^{p^n} c_n$ for $n \geq 0$. This proves (iii).

For (iv), we show that $S_n(X_0, -X_0, \ldots, X_n, -X_n) = 0$ for $n \geq 0$ by induction on n. If $n = 0$, then $S_0(X_0, -X_0) = X_0 - X_0 = 0$. Let $n \geq 1$. Then, by (2.1) and since p is odd, we have

$$\begin{aligned} S_n(X_0, -X_0, \ldots, X_n, -X_n) &= X_n - X_n \\ &+ \frac{1}{p}(X_{n-1}^p - X_{n-1}^p - S_{n-1}(X_0, -X_0, \ldots, X_{n-1}, -X_{n-1})^p) + \cdots \\ &+ \frac{1}{p^n}(X_0^{p^n} - X_0^{p^n} - S_0(X_0, -X_0)^{p^n}) = 0, \end{aligned}$$

by induction hypothesis. Let $(d_0, d_1, \ldots) = (c_0, c_1, \ldots) + (-c_0, -c_1, \ldots)$. Then, for $n \geq 0$, we have $d_n = \overline{S_n}(c_0, -c_0, \ldots, c_n, -c_n) = 0$. This proves (iv).

(v) follows from (iii).

For (vi), we prove by induction on n. If $n = 1$, we are done. Let $n \geq 2$. Then since $S_0 = X_0 + Y_0$, by induction hypothesis, we have

$$n = 1 + (n-1) = (1, 0, 0, \ldots) + (n-1, *, *, \ldots) = (n, *, *, \ldots).$$

The last three equations are true since $S_0 = X_0 + Y_0$ and $P_0 = X_0 Y_0$. We can also prove the first part of (vi) by using (i). □

4.3 Weight function

Next, we want to study the monomials of S_n and P_n. Let

$$m = cX_0^{\alpha_0} Y_0^{\beta_0} \cdots X_n^{\alpha_n} Y_n^{\beta_n}$$

be a non-zero monomial in $\mathbb{Z}[X_0, Y_0, \ldots, X_n, Y_n]$. Define the *weight* of m to be

$$\alpha_0 + \beta_0 + p(\alpha_1 + \beta_1) + \cdots + p^n(\alpha_n + \beta_n),$$

denoted by $\mathrm{wt}(m)$. The *weight* of a non-zero polynomial in $\mathbb{Z}[X_0, Y_0, \ldots, X_n, Y_n]$ is defined to be the largest weight of its monomials. We say that 0 has every weight.

Let $R = \mathbb{Z}[X_0, Y_0, \ldots, X_n, Y_n]$.

Lemma 4.5. *Let m, M be non-zero monomials in R. Then $\mathrm{wt}(mM) = \mathrm{wt}(m) + \mathrm{wt}(M)$. Let $f, g \in R$ and $f, g \neq 0$. Then $\mathrm{wt}(fg) = \mathrm{wt}(f) + \mathrm{wt}(g)$.*

Proof. The first statement is true by definition. For the second statement, let $f = f_0 + \cdots + f_s$ and $g = g_0 + \cdots + g_t$, where for each $0 \leq i \leq s$, f_i is the sum of the terms in f of weight i, similarly for g, and $f_s, g_t \neq 0$. Then $\mathrm{wt}(f) = s$ and $\mathrm{wt}(g) = t$. We have

$$fg = f_s g_t + h,$$

where $h = 0$ or $\mathrm{wt}(h) < s + t$. Since $f_s g_t \neq 0$, it contains some term of weight $s + t$. This term cannot be like term with any term in h, since they have different weights. All other terms have weights less than or equal to $s + t$. So $\mathrm{wt}(fg) = s + t = \mathrm{wt}(f) + \mathrm{wt}(g)$. □

Let $f \in R$ and $f \neq 0$. Let $t \geq 0$. Then f is said to be *homogeneous of weight t* if each term in f has weight t.

Lemma 4.6. *Let $t \geq 0$ and $N \geq 1$. Let $m_1, \ldots, m_N \in R$ be monomials of weight t. Assume that $m_1 + \cdots + m_N \neq 0$. Then $m_1 + \cdots + m_N$ is homogeneous of weight t.*

Proof. We prove by induction on N. If $N = 1$, then m_1 is homogeneous of weight t by definition. Let $N \geq 2$. If no terms in $m_1 + \cdots + m_N$ are like term, then $m_1 + \cdots + m_N$ is homogeneous of weight t by definition. If $m_1 + \cdots + m_N$ has like terms, say $m_1 = cm$ and $m_2 = dm$, where $c, d \in \mathbb{Z}$ and $c, d \neq 0$ and m is a monomial with coefficient 1. Then $m_1 + \cdots + m_N = (c + d)m + m_3 + \cdots + m_N$ is homogeneous of weight t by induction hypothesis. □

Lemma 4.7. *Let $t \geq 0$ and $N \geq 1$. Let $f_1, \ldots, f_N \in R$ be homogeneous of weight t. Assume $f_1 + \cdots + f_N \neq 0$. Then $f_1 + \cdots + f_N$ is homogeneous of weight t.*

Proof. For $1 \leq i \leq N$, write f_i as the sum of its monomials. Then the conclusion is true by Lemma 4.6. □

Lemma 4.8. *Let $s, t \geq 0$. Let $f, g \in R$ be homogeneous of weight s, t, respectively. Then fg is homogeneous of weight $s + t$.*

Proof. Let $f = f_1 + \cdots + f_N$ and $g = g_1 + \cdots + g_M$, where $f_1, \ldots, f_N$ are the monomials appearing in f, similarly for g. Then $fg \neq 0$, and $fg = f_1 g_1 + \cdots + f_N g_M$. For each $1 \leq i \leq N$ and $1 \leq j \leq M$, we have $\mathrm{wt}(f_i g_j) = s + t$. By Lemma 4.6, fg is homogeneous of weight $s + t$. □

Lemma 4.9. *Let $n \geq 0$. Then S_n is homogeneous of weight p^n, and P_n is homogeneous of weight $2p^n$.*

Proof. We prove by induction on n. If $n = 0$, then $S_0 = X_0 + Y_0$ and $P_0 = X_0 Y_0$, so S_0 is homogeneous of weight 1, and P_0 is homogeneous of weight 2. Let $n \geq 1$. By (2.1), we have

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

Since X_n is the only term in S_n containing X_n, we have $S_n \neq 0$. Also, we have $\mathrm{wt}(X_i^{p^{n-i}}) = \mathrm{wt}(Y_i^{p^{n-i}}) = p^n$ for $0 \leq i \leq n$. By induction hypothesis, S_i is homogeneous of weight p^i for $0 \leq i \leq n-1$. So by Lemma 4.8, $S_i^{p^{n-i}}$ is homogeneous of weight p^n. Hence S_n is homogeneous of weight p^n. Similarly, by (2.1), we have

$$P_n = \frac{1}{p^n}((X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) - (P_0^{p^n} + \cdots + p^{n-1} P_{n-1}^p)).$$

The term $X_0^{p^n} Y_n$ in P_n cannot be combined with other terms, so $P_n \neq 0$. Since $\mathrm{wt}(X_i^{p^{n-i}}) = \mathrm{wt}(Y_i^{p^{n-i}}) = p^n$ for $0 \leq i \leq n$, we have $X_0^{p^n} + \cdots + p^n X_n$ and $Y_0^{p^n} + \cdots + p^n Y_n$ are homogeneous of weight p^n. By induction hypothesis and Lemma 4.8, we have $P_i^{p^{n-i}}$ is homogeneous of weight $2p^n$ for $0 \leq i \leq n-1$. So P_n is homogeneous of $2p^n$. □

Lemma 4.10. *Let $\prod_{i=0}^n X_i^{s_i} \prod_{j=0}^n Y_j^{t_j}$ be a term in $\overline{S_n}$. Then*

$$\sum_{i=0}^n s_i p^i + \sum_{j=0}^n t_j p^j = p^n.$$

Proof. We have $\prod_{i=0}^n X_i^{s_i} \prod_{j=0}^n Y_j^{t_j}$ is also a term of S_n. So by Lemma 4.9, we have

$$p^n = \mathrm{wt}\left(\prod_{i=0}^n X_i^{s_i} \prod_{j=0}^n Y_j^{t_j}\right) = \sum_{i=0}^n s_i p^i + \sum_{j=0}^n t_j p^j.$$

□

Lemma 4.11. *Let* $\prod_{i=0}^{n} X_i^{s_i} \prod_{j=0}^{n} Y_j^{t_j}$ *be a term in* $\overline{P_n}$. *Then*

$$\sum_{i=0}^{n} s_i p^i = \sum_{j=0}^{n} t_j p^j = p^n, \quad \sum_{i=0}^{n} i s_i p^i + \sum_{j=0}^{n} j t_j p^j \leq n p^n,$$

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

$$\overline{P_n} = \sum_{i=0}^{n} X_i^{p^{n-i}} Y_{n-i}^{p^i} + \overline{Q_n},$$

where $\overline{Q_n} \in \mathbb{F}_p[X_0, Y_0, \ldots, X_{n-1}, Y_{n-1}]$ *and has its monomials (as above) satisfying* $\sum_{i=0}^{n-1} i s_i p^i + \sum_{j=0}^{n-1} j t_j p^j \leq (n-1)p^n$.

Proof. The lemma, except for the $s_0 + t_0 \leq p^n$ part, is Lemma 2.1 of [3]. Although Lemma 2.1 of [3] states

$$\sum_{i=0}^{n-1} i s_i p^i + \sum_{j=0}^{n-1} j t_j p^j < n p^n$$

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 prove by induction on n. If $n = 1$, we have $P_1 = X_0^p Y_1 + X_1 Y_0^p$, so the statement is true. Let $n \geq 2$. We have

$$P_n = \frac{1}{p^n}((X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) - (P_0^{p^n} + \cdots + p^{n-1} P_{n-1}^p)).$$

Notice that $X_0^{p^n} Y_0^{p^n} - P_0^{p^n} = 0$. Also, every term from $(X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n)$ except $X_0^{p^n} Y_0^{p^n}$ satisfies the condition $s_0 + t_0 \leq p^n$. So, it remains to check for the terms coming from $P_r^{p^{n-r}}$, for $r = 1, \ldots, n-1$. Any term in $P_r^{p^{n-r}}$ is a product of p^{n-r} terms of P_r:

$$\prod_{k=1}^{p^{n-r}} \left(\prod_{i=0}^{r} X_i^{s_{ik}} \prod_{j=0}^{r} Y_j^{t_{jk}} \right) = \prod_{i=0}^{r} X_i^{\sum_{k=1}^{p^{n-r}} s_{ik}} \prod_{j=0}^{r} Y_j^{\sum_{k=1}^{p^{n-r}} t_{jk}}.$$

By induction hypothesis, we have $s_{0k} + t_{0k} \leq p^r$ for all k. So

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

□

Let v_p denote the valuation at p over $\mathbb{Q}$. For example, we have $v_2(2^2 3) = 2$.

Lemma 4.12. *Let $n \geq 1$. Then we have $n > v_p(n)$.*

Proof. Let $n = p^\alpha m$ where $p \nmid m$. Then

$$\begin{aligned} n - v_p(n) &= p^\alpha m - \alpha \geq 2^\alpha - \alpha = (1+1)^\alpha - \alpha \\ &= \sum_{i=0}^{\alpha} \binom{\alpha}{i} - \alpha \geq \sum_{i=0}^{\alpha} 1 - \alpha > 0. \end{aligned}$$

□

The following lemma is Lemma 8.1 from [7].

Lemma 4.13. *Let $1 \leq a < p^k$. We have that*

$$v_p\binom{p^k}{a} = k - v_p(a).$$

Note that the lemma originally had $1 < a < p^k$, but the case $a = 1$ can be checked directly.

Lemma 4.14. *Let M be a term in $\overline{P_n}$. Then M is either of the form $X_i^{p^{n-i}} Y_j^{p^{n-j}}$ where $i + j \leq n$ or a like term to a term in $\overline{P_i}^{p^{n-i}}$ where $i \leq n - 1$.*

Proof. We have

$$\begin{aligned} P_n &= \frac{1}{p^n}((X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) - (P_0^{p^n} + \cdots + p^{n-1} P_{n-1}^p)) \\ &= \frac{1}{p^n}\left(\sum_{i+j \leq n} p^{i+j} X_i^{p^{n-i}} Y_j^{p^{n-j}} - (P_0^{p^n} + \cdots + p^{n-1} P_{n-1}^p)\right) + \sum_{i+j > n} p^{i+j-n} X_i^{p^{n-i}} Y_j^{p^{n-j}}. \end{aligned}$$

The terms $\sum_{i+j>n} p^{i+j-n} X_i^{p^{n-i}} Y_j^{p^{n-j}}$ will not appear in $\overline{P_n}$ because p divides them.

Now, we want to study the terms coming from $P_i^{p^{n-i}}$ where $i \leq n-1$. We show that the terms in P_i that are divisible by p will not contribute to $\overline{P_n}$. That is, let $P_i = Q_i + pR_i$ where the coefficients of Q_i are in $\{0, 1, \ldots, p-1\}$. Then

$$-\frac{1}{p^n} p^i P_i^{p^{n-i}} = -\frac{1}{p^n} p^i (Q_i + pR_i)^{p^{n-i}}$$

are some terms of P_n. We show that all the terms except $-p^i Q_i^{p^{n-i}}/p^n$ will be divisible by p. Let N be such a term. Then $N = -p^{i-n}\binom{p^{n-i}}{j} Q_i^{n-j} p^j R_i^j$, where $1 \leq j \leq p^{n-i}$. If $j = p^{n-i}$, then

$$v_p\left(p^{i-n}\binom{p^{n-i}}{j} p^j\right) = i - n + j = p^{n-i} - (n-i) = p^{n-i} - v_p(p^{n-i}) > 0,$$

by Lemma 4.12. If $j \neq p^{n-i}$, then by Lemma 4.12 and Lemma 4.13, we have

$$v_p\left(p^{i-n}\binom{p^{n-i}}{j} p^j\right) = i - n + n - i - v_p(j) + j = j - v_p(j) > 0.$$

Hence $p \mid N$. Therefore, the terms in P_i that are divisible by p will not contribute to $\overline{P_n}$. So we have M is either of the form $X_i^{p^{n-i}} Y_j^{p^{n-j}}$ where $i + j \leq n$ or a like term to a term in $\overline{P_i}^{p^{n-i}}$ where $i \leq n-1$. □

4.4 Modular functions

Recall that we define $\mathrm{wt}(a_0) = 4, \mathrm{wt}(b_0) = 6$, and define

$$\mathrm{S}_n = \{f/g \in \mathbb{F}_p(a_0, b_0) : f, g \in \mathbb{F}_p[a_0, b_0] \text{ homogeneous, and } \mathrm{wt}(f) - \mathrm{wt}(g) = n\} \cup \{0\}.$$

If h is in S_n for some integer n, then h is called a modular function of weight n.

Lemma 4.15. *Let $F, G \in \mathrm{S}_0$. Then $F + G, FG \in \mathrm{S}_0$. Moreover, if $F \neq 0$, then $1/F \in \mathrm{S}_0$.*

Proof. If F or G is zero, then we are done. Let $F = f/g$ and $G = h/k$, where $f, g, h, k \in \mathbb{F}_p[a_0, b_0]$ are homogeneous, and $\mathrm{wt}(f) = \mathrm{wt}(g)$, and $\mathrm{wt}(h) = \mathrm{wt}(k)$. Then $F + G = (fk +$

$gh)/(gk)$. If $F+G=0$, then we are done. If not, then $fk+gh, gk$ are homogeneous of the same weight. So $F+G \in \mathrm{S}_0$. Also $FG=(fh)/(gk) \in \mathrm{S}_0$. Finally, $1/F = g/f \in \mathrm{S}_0$. □

The following lemma is Lemma 3.1 from [8].

Lemma 4.16. *Let $k=\mathbb{F}_p(a_0,b_0)$. Let $\pi_i : W(k) \to k$ denote the map that gives the i-th coordinate of a Witt vector. Assume $\pi_i(f) \in \mathrm{S}_{rp^i}$ and $\pi_i(g) \in \mathrm{S}_{sp^i}$ for all i. Then $\pi_i(fg) \in \mathrm{S}_{(r+s)p^i}$ for all i. Moreover, if we assume $r=s$, then $\pi_i(f+g) \in \mathrm{S}_{rp^i}$ for all i.*

Define

$$\mathrm{S}^{(r)} = \{f=(f_0,f_1,\ldots) \in W(\mathbb{F}_p(a_0,b_0)) : f_i \in \mathrm{S}_{rp^i} \text{ for all } i\}.$$

Lemma 4.17. *Assume $f \in \mathrm{S}^{(r)}$ and $g \in \mathrm{S}^{(s)}$. Then $fg \in \mathrm{S}^{(r+s)}$. Moreover, if we assume $r=s$, then $f+g \in \mathrm{S}^{(r)}$.*

Proof. We have $f \in \mathrm{S}^{(r)}$ if and only if $\pi_i(f) \in \mathrm{S}_{rp^i}$ for all i, where π_i is same as in Lemma 4.16. Then the results follow from Lemma 4.16. □

Lemma 4.18. *Assume $f \in \mathrm{S}^{(0)}$ and $f \in W(\mathbb{F}_p(a_0,b_0))^\times$. Then $1/f \in \mathrm{S}^{(0)}$.*

Proof. Let $f=(f_0,f_1,\ldots)$ and $1/f=(g_0,g_1,\ldots)$. We show that $g_n \in \mathrm{S}_0$ for all n. We prove by induction on n. If $n=0$, then $g_0=1/f_0$. Since $f_0 \in \mathrm{S}_0$, we have $g_0 \in \mathrm{S}_0$. Let $n \geq 1$. Then $\overline{P_n}(f_0,g_0,\ldots,f_n,g_n)=0$. By (2.1), $g_n f_0^{p^n}$ is the only term in $\overline{P_n}(f_0,g_0,\ldots,f_n,g_n)$ containing g_n. All other terms are of the form $f_0^{s_0}\cdots f_n^{s_n} g_0^{t_0}\cdots g_{n-1}^{t_{n-1}}$, hence are in S_0 by induction hypothesis. Their sum is also in S_0. So $g_n f_0^{p^n} \in \mathrm{S}_0$, hence $g_n \in \mathrm{S}_0$. □

We need a few more lemmas before we can answer the first dissertation question.

Lemma 4.19.

$$j_0 = \frac{1728 \cdot 4a_0^3}{\Delta}, \quad 1728 - j_0 = \frac{1728 \cdot 27b_0^2}{\Delta}, \quad 1728 = 12^3.$$

Proof. The statements are true because $j_0 = 1728 \cdot 4a_0^3/(4a_0^3+27b_0^2)$ and $\Delta = 4a_0^3+27b_0^2$. □

Note that since $p \geq 5$, the lemma implies that $1728^{-1} \in \mathbb{F}_p$.

Lemma 4.20. *Let $\mathcal{H}$ be the Hasse invariant. Then*

$$\mathcal{S}_p(j_0) = \left(-\frac{2}{9}\right)^r \left(\frac{1728}{\Delta}\right)^{r_2-r_1} \frac{(-27)^{r_2}}{4^{r_1} a_0^{\delta} b_0^{\epsilon}} \mathcal{H}, \tag{4.1}$$

and $\mathcal{S}_p(j_0) \neq 0$. Hence $\mathcal{S}_p(j_0) \in \mathbb{F}_p(a_0, b_0)$.

Remember that $r, r_1, r_2, \delta, \epsilon$ are defined in Chapter 4. By Lemma 4.1, all the exponents in the above equation are non-negative.

Proof. By definition of $\mathcal{S}_p(X)$, we have $\mathrm{ss}_p(X) = \mathcal{S}_p(X) X^{\delta} (X - 1728)^{\epsilon}$. As in [4], let

$$G(X) = \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} \left(-\frac{27}{4}\right)^i X^{i-r_1} (X-1728)^{r_2-i}.$$

By Theorem 1.1 of [4] and Lemma 4.1, we have $\mathrm{ss}_p(X) = (-2/9)^r G(X) X^{\delta} (X-1728)^{\epsilon}$. So $\mathcal{S}_p(X) = (-2/9)^r G(X)$. Plugging in j_0 and using 4.19, we have

$$\begin{aligned}
\mathcal{S}_p(j_0) &= \left(-\frac{2}{9}\right)^r \left(\frac{1728}{\Delta}\right)^{r_2-r_1} \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} \left(-\frac{27}{4}\right)^i (4a_0^3)^{i-r_1} (-27 b_0^2)^{r_2-i} \\
&= \left(-\frac{2}{9}\right)^r \left(\frac{1728}{\Delta}\right)^{r_2-r_1} \frac{(-27)^{r_2}}{4^{r_1}} \frac{b_0^{2r_2}}{a_0^{3r_1}} \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} \left(\frac{a_0^3}{b_0^2}\right)^i \\
&= \left(-\frac{2}{9}\right)^r \left(\frac{1728}{\Delta}\right)^{r_2-r_1} \frac{(-27)^{r_2}}{4^{r_1}} \frac{b_0^{2r_2-r}}{a_0^{3r_1-r}} \left(\frac{b_0}{a_0}\right)^r \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} \left(\frac{a_0^3}{b_0^2}\right)^i.
\end{aligned}$$

By Equation (2.3) from [4], we have

$$\mathcal{H} = \left(\frac{b_0}{a_0}\right)^r \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} \left(\frac{a_0^3}{b_0^2}\right)^i. \tag{4.2}$$

Also by Lemma 4.1, we have $r - 2r_2 = \epsilon$ and $3r_1 - r = \delta$. This proves the equation. Since $\mathcal{H}$ is a non-zero polynomial in $\mathbb{F}_p[a_0, b_0]$, we have $\mathcal{S}_p(j_0) \neq 0$. The last statement follows from the equation and the fact that $\mathcal{H} \in \mathbb{F}_p[a_0, b_0]$. □

Let $i \geq 1$. As in Theorem 4.3, let

$$J_i(X) = \frac{F_i(X)}{G_i(X)} = \frac{F_i(X)}{\mathcal{S}_p(X)^{\alpha} X^{\beta} (X-1728)^{\gamma}}, \tag{4.3}$$

where $F_i \in \mathbb{F}_p[X]$, $(F_i, G_i) = 1$, G_i monic, and $\alpha, \beta, \gamma \geq 0$.

Lemma 4.21. *For $i \geq 1$, we have $J_i(j_0) \in \mathbb{F}_p(a_0, b_0)$.*

Proof. Since $j_0 = 1728 \cdot 4a_0^3/(4a_0^3 + 27b_0^2) \in \mathbb{F}_p(a_0, b_0)$, by Lemma 4.20 and Lemma 4.19, we have $F_i(j_0), G_i(j_0) \in \mathbb{F}_p(a_0, b_0)$, and $G_i(j_0) \neq 0$. So $J_i(j_0) \in \mathbb{F}_p(a_0, b_0)$. □

Now we can answer the first dissertation question. That is, A_n, B_n are modular functions. Recall that

$$a = \lambda^4 \frac{27j}{4(1728 - j)} = (a_0, A_1, A_2, \ldots),$$
$$b = \lambda^6 \frac{27j}{4(1728 - j)} = (b_0, B_1, B_2, \ldots),$$

where $\lambda = (\sqrt{b_0/a_0}, 0, 0, \ldots)$, and j is the j-invariant of the canonical lifting.

Theorem 4.22. *Let $i \geq 1$. Then $A_i \in \mathrm{S}_{4p^i}$ and $B_i \in \mathrm{S}_{6p^i}$. In particular, $A_i, B_i \in \mathbb{F}_p(a_0, b_0)$.*

Proof. We have $j = (j_0, J_1(j_0), J_2(j_0), \ldots)$. Also $j_0 = 1728 \cdot 4a_0^3/\Delta \in \mathrm{S}_0$. By Theorem 4.3, $J_i(X) \in \mathbb{F}_p(X)$ for all i. Then by Lemma 4.15, we have $J_i(j_0) \in \mathrm{S}_0$. So $j \in \mathrm{S}^{(0)}$. Since $1 = (1, 0, 0, \ldots) \in \mathrm{S}^{(0)}$, by Lemma 4.17, we have $4, 27, 1728 \in \mathrm{S}^{(0)}$. Hence by Lemma 4.17 and Lemma 4.18, we have $27j/(4(1728 - j)) \in \mathrm{S}^{(0)}$. Also $\lambda^2 = (b_0/a_0, 0, 0, \ldots) \in \mathrm{S}^{(2)}$. Hence $a \in \mathrm{S}^{(4)}$ and $b \in \mathrm{S}^{(6)}$. So $A_i \in \mathrm{S}_{4p^i}$ and $B_i \in \mathrm{S}_{6p^i}$ for all i. □

Chapter 5

The factors of the denominators

In this chapter, I will answer the last two dissertation questions. That is, I will find the possible factors for the denominators of A_n, B_n, and estimate the powers of each factor. Then I will show some computations done by Magma. I will introduce some tools to solve the problem.

Notice that since $A_n \in \mathbb{F}_p(a_0, b_0)$, we have $A_n = a/b$ where $a, b \in \mathbb{F}_p[a_0, b_0]$ and $(a, b) = 1$. If $A_n = c/d$ for $c, d \in \mathbb{F}_p[a_0, b_0]$ with $(c, d) = 1$, then $ad = bc$. Then $b = md$ for some $m \neq 0$ and $m \in \mathbb{F}_p$. So all denominators of A_n in reduced form differ by a constant multiple. Hence when we are talking about the denominator of A_n, we mean the denominator of A_n in reduced form.

5.1 Possible factors of the denominators

In this section, we will answer the second dissertation question. That is, we will find all the possible factors for the denominators of A_n, B_n. We will use a few results from Finotti's papers.

Since $a = \lambda^4 \cdot 27j/(4(1728 - j))$ and $b = \lambda^2 a$, we will first study the denominators of each coordinate of $j = (j_0, J_1(j_0), J_2(j_0), \ldots)$. The results from [6] give us a good understanding of $J_n(X)$. Define

$$\mathbb{V} = \mathbb{F}_p[a_0, b_0, 1/(\Delta \cdot \mathcal{H} \cdot a_0 \cdot b_0)].$$

Proposition 5.1. *We have $j_0 \in \mathbb{V}$. For $i \geq 1$, we have $J_i(j_0) \in \mathbb{V}$.*

Proof. By definition, we have $j_0 \in \mathbb{V}$. As in (4.3), define $J_i(X) = F_i(X)/G_i(X)$. Since $j_0 \in \mathbb{V}$, we have $F_i(j_0) \in \mathbb{V}$. By Lemma 4.19 and Lemma 4.20, we have that $j_0^{-1}, (j_0 - 1728)^{-1}, \mathcal{S}_p(j_0)^{-1} \in \mathbb{V}$. Since

$$G_i(j_0) = \mathcal{S}_p(j_0)^{\alpha} j_0^{\beta} (j_0 - 1728)^{\gamma},$$

we have $G_i(j_0)^{-1} \in \mathbb{V}$. Hence $J_i(j_0) \in \mathbb{V}$. □

Now, we can answer the second dissertation question. That is, we can find all possible factors of the denominators of A_n, B_n. Recall that $a = \lambda^4 \cdot 27j/(4(1728-j))$, $b = \lambda^2 a$, where $\lambda = (\sqrt{b_0/a_0}, 0, 0, \ldots)$.

Theorem 5.2. *Let $n \geq 1$. Then $A_n, B_n \in \mathbb{V}$.*

Proof. By Proposition 5.1, we have $j = (j_0, J_1(j_0), J_2(j_0), \ldots) \in W(\mathbb{V})$. Since $1 = (1, 0, 0, \ldots) \in W(\mathbb{V})$, we have $27, 4, 1728 \in W(\mathbb{V})$. So $27j, 4(1728 - j) \in W(\mathbb{V})$. By Lemma 4.4, we have

$$4(1728 - j) = (4(1728 - j_0), *, *, \ldots) = (4 \cdot 1728 \cdot 27 b_0^2/\Delta, *, *, \ldots).$$

By Lemma 4.4 (ii), we have $(4(1728 - j))^{-1} \in W(\mathbb{V})$. So $27j/(4(1728 - j)) \in W(\mathbb{V})$. Since $\lambda^2 = (b_0/a_0, 0, 0, \ldots) \in W(\mathbb{V})$, we have $a, b \in W(\mathbb{V})$. Hence $A_n, B_n \in \mathbb{V}$. □

5.2 Valuations

Now we will work on the last dissertation question. That is, we want to know how many powers of $\Delta, \mathcal{H}, a_0, b_0$ appear in the denominators of A_n, B_n. We will use the tool of valuations to help us solve the problem. In this section, I will introduce the definition and some properties of valuations.

Remember that my goal is to estimate the powers of each factor. This is exactly what valuations do.

Let R be a unique factorization domain of characteristic $p > 0$. Let q be a prime in R. Let $f \in R$. Define the *valuation in q of f*, denoted $\nu_q(f)$, as follows: if $f = 0$, define

$\nu_q(f) = \infty$. If f is non-zero, then $f = f_0 q^i$ for some $f_0 \in R$ and $i \geq 0$ such that $q \nmid f_0$. Define $\nu_q(f) = i$. Let K be the quotient field of R. Let $h = f/g \in K$ with $f, g \in R$ and $g \neq 0$. Define $\nu_q(h) = \nu_q(f) - \nu_q(g)$.

We need to show that the valuation is well defined on K. We need a lemma first.

We also need to be careful about the infinity appearing as a possible output. We will assume the following:

$$\infty + \infty = \infty, \quad \infty + a = \infty, \quad \infty \geq \infty, \quad \infty \geq a$$

where $a \in \mathbb{Z}$. If we want to subtract the term $\nu_q(f)$ on an equation or inequality, we must deal with the case when $f = 0$ separately. The cases $\infty - \infty$ and $0 \cdot \infty$ will not happen, so we do not need to worry about that.

The following lemmas are standard properties for valuations. I include them here for completeness. We write ν for ν_q.

Lemma 5.3. *Let $f, g \in R$. Then $\nu(f) \geq 0$ and $\nu(fg) = \nu(f) + \nu(g)$.*

Proof. If f or g is zero, then we are done. Assume $f, g \neq 0$. Let $f = f_0 q^i$ and $g = g_0 q^j$, where $f_0, g_0 \in R$, $i, j \geq 0$, and $q \nmid f_0, g_0$. Then $\nu(f) = i \geq 0$, and $\nu(fg) = \nu(f_0 g_0 q^{i+j}) = i + j = \nu(f) + \nu(g)$, since $q \nmid (f_0 g_0)$. □

Now we can show that the valuation is well defined on K. Let $h \in K$, and let $h = f/g = u/v$, where $f, g, u, v \in R$ and $g, v \neq 0$. Then $fv = gu$. So $\nu(f) + \nu(v) = \nu(g) + \nu(u)$. Since $\nu(g), \nu(v) \neq \infty$, we can subtract them on both sides. So $\nu(f) - \nu(g) = \nu(u) - \nu(v)$. Hence the valuation is well defined.

Lemma 5.4. *Let $m \geq 1$. Let $f_1, \ldots, f_m \in R$.*

(i) We have $\nu(f_1 + \cdots + f_m) \geq \min\{\nu(f_1), \ldots, \nu(f_m)\}$,

(ii) Let $1 \leq i \leq m$. If $\nu(f_i) < \nu(f_j)$ for all $j \neq i$, then $\nu(f_1 + \cdots + f_m) = \nu(f_i)$.

Proof. We prove by induction on m. If $m = 1$, then we are done. Let $m \geq 2$. If $f_k = 0$ for some k, then (i) is true by induction hypothesis. Assume $f_j \neq 0$ for all j. Let $f_j = g_j q^{n_j}$ for $1 \leq j \leq m$, where $g_j \in R$, and $q \nmid g_j$ in R. Then $n_j = \nu(f_j)$ for $1 \leq j \leq m$.

(i) Let $1 \leq l \leq m$ be such that $n_l = \min\{n_1, \ldots, n_m\}$. Then

$$f_1 + \cdots + f_m = q^{n_l}(g_1 q^{n_1 - n_l} + \cdots + g_l + \cdots + g_m q^{n_m - n_l}).$$

Hence $\nu(f_1 + \cdots + f_m) \geq n_l = \min\{\nu(f_1), \ldots, \nu(f_m)\}$.

(ii) We have

$$f_1 + \cdots + f_m = q^{n_i}(g_1 q^{n_1 - n_i} + \cdots + g_i + \cdots + g_m q^{n_m - n_i}).$$

Since $n_j > n_i$ for all $j \neq i$, we have

$$q \nmid (g_1 q^{n_1 - n_i} + \cdots + g_i + \cdots + g_m q^{n_m - n_i}).$$

Hence $f_1 + \cdots + f_m \neq 0$, and $\nu(f_1 + \cdots + f_m) = n_i = \nu(f_i)$. □

Lemma 5.5. *Let $f, g \in K$. Then $\nu(fg) = \nu(f) + \nu(g)$. If $g \neq 0$, then $\nu(f/g) = \nu(f) - \nu(g)$.*

Proof. Let $f = f_1/f_2, g = g_1/g_2$ where $f_1, f_2, g_1, g_2 \in R$, and $f_2, g_2 \neq 0$. Then $\nu(fg) = \nu(f_1 g_1/f_2 g_2) = \nu(f_1) + \nu(g_1) - \nu(g_1) - \nu(g_2) = \nu(f) + \nu(g)$. The proof for the second part is similar. □

Lemma 5.6. *Let $m \geq 1$. Let $f_1, \ldots, f_m \in K$.*

(i) We have $\nu(f_1 + \cdots + f_m) \geq \min\{\nu(f_1), \ldots, \nu(f_m)\}$,

(ii) Let $1 \leq i \leq m$. If $\nu(f_i) < \nu(f_j)$ for all $j \neq i$, then $\nu(f_1 + \cdots + f_m) = \nu(f_i)$.

Proof. Let $f_j = g_j/h$ for some $g_j, h \in R$, for $1 \leq j \leq m$, and $h \neq 0$. Then by Lemma 5.4,

$$\begin{aligned}\nu(f_1 + \cdots + f_m) &= \nu((g_1 + \cdots + g_m)/h) = \nu(g_1 + \cdots + g_m) - \nu(h) \\ &\geq \min\{\nu(g_1), \ldots, \nu(g_m)\} - \nu(h) = \min\{\nu(f_1), \ldots, \nu(f_m)\}.\end{aligned}$$

So (i) is true. For (ii), we have $\nu(g_i) - \nu(h) < \nu(g_j) - \nu(h)$ for $j \neq i$. Since $h \neq 0$, we have $\nu(g_i) < \nu(g_j)$ for $j \neq i$. So by Lemma 5.4,

$$\nu(f_1 + \cdots + f_m) = \nu(g_1 + \cdots + g_m) - \nu(h) = \nu(g_i) - \nu(h) = \nu(f_i).$$

□

Lemma 5.7. *Let $f \in K$. Then $\nu(-f) = \nu(f)$.*

Proof. We have $\nu(-f) = \nu(-1) + \nu(f) = \nu(f)$. □

Define

$$S = \{f \in K : \nu(f) \geq 0\}.$$

Lemma 5.8. *We have S is a subring of K.*

Proof. Since $\nu(0) = \infty \geq 0$, we have $S \neq \emptyset$. Let $f, g \in K$. Then $\nu(f - g) \geq \min\{\nu(f), \nu(-g)\} = \min\{\nu(f), \nu(g)\} \geq 0$. So $f - g \in S$. Also, $\nu(fg) = \nu(f) + \nu(g) \geq 0$. So $fg \in S$. Since $\nu(1) = 0$, we have $1 \in S$. □

5.3 Valuations for Witt vectors

This section discusses some special properties of valuations for Witt vectors. We will prove a few technical lemmas. Roughly speaking, if we know that the valuations of the coordinates of two Witt vectors satisfy some properties, the lemmas show that the valuations of the coordinates of their sum, product, inverse also satisfy some related properties.

Let R be a unique factorization domain of characteristic $p > 0$ with quotient field K. Let q be a prime in R. Let ν be the valuation in q. Let $u = (u_0, u_1, \ldots), v = (v_0, v_1, \ldots) \in W(K)$. Let $k \geq 0$. Define

$$C_k = \{\{\nu_i\} : \nu_i \in \mathbb{R} \text{ for } i \geq k, \nu_k < 0, \nu_{i+1} < p\nu_i \text{ for all } i \geq k\}. \tag{5.1}$$

Let $\{\nu_i\} \in C_k$, $u + v = (r_0, r_1, \ldots)$, and $uv = (s_0, s_1, \ldots)$.

Note that $\nu_i < 0$ for all $i \geq k$. Also

$$\nu_i > \nu_n / p^{n-i},$$

for $n > i \geq k$.

Lemma 5.9. *Suppose that $\nu(u_i), \nu(v_i) \geq 0$ for $i = 0, \ldots, k-1$ and $\nu(u_i) \geq \nu_i$ for $i \geq k$.*

(i) We have $\nu(r_i), \nu(s_i) \geq 0$ for $i \leq k-1$.

(ii) Suppose that $\nu(v_k) \geq \nu_k$ and $\nu(v_i) > \nu_i$ for $i > k$. Then $\nu(r_n) \geq \nu_n$ for $n \geq k$.

(a) If $\nu(v_k) > \nu_k = \nu(u_k)$, then $\nu(r_k) = \nu_k$;

(b) If $\nu(u_i) = \nu_i$ for $i > k$, then $\nu(r_n) = \nu_n$ for $n > k$.

(iii) Suppose that $\nu(v_i) \geq p^i \nu(v_0)$ for $i > 0$, with $\nu_k < -p^k \nu(v_0)$. Then $\nu(s_n) \geq \nu_n + p^n \nu(v_0)$ for $n \geq k$.

(a) If $\nu_k = \nu(u_k)$, then $\nu(s_k) = \nu_k + p^k \nu(v_0)$;

(b) If $\nu(u_i) = \nu_i$ for $i > k$, then $\nu(s_n) = \nu_n + p^n \nu(v_0)$ for $n > k$.

Note that let $u - v = (t_0, t_1, \ldots)$. Then, by Lemma 4.4 (iv) and Lemma 5.7, we have that the results for r_i also hold for t_i.

Proof. (i) Since $r_i = \overline{S_i}(u_0, v_0, \ldots, u_i, v_i)$ and S_i is a polynomial, we have r_i is a sum of terms of the form

$$u_0^{\alpha_0} v_0^{\beta_0} \cdots u_i^{\alpha_i} v_i^{\beta_i},$$

where $\alpha_0, \beta_0, \ldots, \alpha_i, \beta_i \geq 0$. The ν of this term is greater than or equal to 0 by assumption and Lemma 5.5. Then by Lemma 5.6, ν of the sum is also greater than or equal to 0.

(ii) By the definition of S_n, we have that r_n is the sum of u_n, v_n, and terms of the form

$$u_0^{\alpha_0} v_0^{\beta_0} \cdots u_{n-1}^{\alpha_{n-1}} v_{n-1}^{\beta_{n-1}}.$$

Call the above monomial M. Let $\alpha_n, \beta_n = 0$. We have $\nu(u_n), \nu(v_n) \geq \nu_n$.

If $n = k$, by assumption, we have $\nu(M) \geq 0 > \nu_k$. Hence $\nu(r_n) \geq \nu_n$.

If $n > k$, we show that $\nu(M) > \nu_n$. If $\alpha_k, \beta_k, \ldots, \alpha_{n-1}, \beta_{n-1} = 0$, then

$$\nu(M) \geq \alpha_k \nu_k + \beta_k \nu_k + \cdots + \alpha_{n-1} \nu_{n-1} + \beta_{n-1} \nu_{n-1} = 0 > \nu_n.$$

If one of $\alpha_k, \beta_k, \ldots, \alpha_{n-1}, \beta_{n-1}$ is non-zero, then

$$\begin{aligned}\nu(M) &\geq \sum_{i=k}^{n-1} \alpha_i \nu_i + \sum_{j=k}^{n-1} \beta_j \nu_j > \sum_{i=k}^{n-1} \alpha_i \frac{\nu_n}{p^{n-i}} + \sum_{j=k}^{n-1} \beta_j \frac{\nu_n}{p^{n-j}} \\ &= \frac{\nu_n}{p^n} \left(\sum_{i=k}^{n-1} \alpha_i p^i + \sum_{j=k}^{n-1} \beta_j p^j \right) \geq \frac{\nu_n}{p^n} \left(\sum_{i=0}^{n} \alpha_i p^i + \sum_{j=0}^{n} \beta_j p^j \right) = \nu_n,\end{aligned}$$

by Lemma 4.10. So $\nu(r_n) \geq \nu_n$.

(a) Similarly as in (ii), we have r_k is the sum of u_k, v_k, and terms of the form $M = u_0^{\alpha_0} v_0^{\beta_0} \cdots u_{k-1}^{\alpha_{k-1}} v_{k-1}^{\beta_{k-1}}$. We have $\nu(u_k) = \nu_k$, and $\nu(v_k) > \nu_k$. Also $\nu(M) \geq 0 > \nu_k$. By Lemma 5.6, we have $\nu(r_k) = \nu_k$.

(b) Similarly as in (ii), we have r_n is the sum of u_n, v_n, and terms of the form $M = u_0^{\alpha_0} v_0^{\beta_0} \cdots u_{n-1}^{\alpha_{n-1}} v_{n-1}^{\beta_{n-1}}$. We have $\nu(u_n) = \nu_n$ and $\nu(v_n) > \nu_n$. Also, from (ii), we have $\nu(M) > \nu_n$. So by Lemma 5.6, we have $\nu(r_n) = \nu_n$.

(iii) By the definition of P_n, we have that s_n is the sum of $u_0^{p^n} v_n$, $v_0^{p^n} u_n$, and terms of the form $M = u_0^{\alpha_0} v_0^{\beta_0} \cdots u_{n-1}^{\alpha_{n-1}} v_{n-1}^{\beta_{n-1}}$.

Case 1: $n = k$.

If $k = 0$, then $s_0 = u_0 v_0$. So $\nu(s_0) = \nu(u_0) + \nu(v_0) \geq \nu_0 + p^0 \nu(v_0)$.

If $k \geq 1$, then we have $\nu(u_0) \geq 0 > \nu_n$. So

$$\nu(u_0^{p^n} v_n) = p^n \nu(u_0) + \nu(v_n) > \nu_n + p^n \nu(v_0).$$

Also, $\nu(v_0^{p^n} u_n) = \nu(u_n) + p^n \nu(v_0) \geq \nu_n + p^n \nu(v_0)$. By hypothesis, we have $\nu(M) \geq 0 > \nu_n + p^n \nu(v_0)$. So $\nu(s_n) \geq \nu_n + p^n \nu(v_0)$.

Case 2: $n > k$.

We show that $\nu(u_0^{p^n} v_n) > \nu_n + p^n \nu(v_0)$.

Since $n > 0$, we have $\nu(u_0^{p^n} v_n) = p^n \nu(u_0) + \nu(v_n) \geq p^n \nu(u_0) + p^n \nu(v_0)$.

If $k = 0$, then since $n > k$, we have $\nu_n < p^n \nu_0 \leq p^n \nu(u_0)$. So $\nu(u_0^{p^n} v_n) > \nu_n + p^n \nu(v_0)$.

If $k \geq 1$, then $p^n \nu(u_0) \geq 0 > \nu_n$. So $\nu(u_0^{p^n} v_n) > \nu_n + p^n \nu(v_0)$.

Next, we have that $\nu(v_0^{p^n} u_n) = \nu(u_n) + p^n \nu(v_0) \geq \nu_n + p^n \nu(v_0)$.

Now, we show that $\nu(M) > \nu_n + p^n \nu(v_0)$.

If $\alpha_k, \dots, \alpha_{n-1} = 0$, then by Lemma 4.11 and the fact that $\nu(v_i) \geq p^i \nu(v_0)$ for $i \geq 0$, we have

$$\nu(M) \geq \sum_{i=k}^{n-1} \alpha_i \nu(u_i) + \sum_{j=0}^{n} \beta_j \nu(v_j) \geq \sum_{j=0}^{n} \beta_j p^j \nu(v_0) = p^n \nu(v_0) > \nu_n + p^n \nu(v_0).$$

If not all $\alpha_k, \dots, \alpha_{n-1}$ are zero, then

$$\nu(M) \geq \sum_{i=k}^{n-1} \alpha_i \nu(u_i) + \sum_{j=0}^{n} \beta_j \nu(v_j) \geq \sum_{i=k}^{n-1} \alpha_i \nu_i + \sum_{j=0}^{n} \beta_j p^j \nu(v_0) > \sum_{i=k}^{n-1} \alpha_i \frac{\nu_n}{p^{n-i}} + p^n \nu(v_0)$$
$$= \frac{\nu_n}{p^n} \sum_{i=k}^{n-1} \alpha_i p^i + p^n \nu(v_0) \geq \frac{\nu_n}{p^n} \sum_{i=0}^{n} \alpha_i p^i + p^n \nu(v_0) = \nu_n + p^n \nu(v_0).$$

Therefore, we have $\nu(s_n) \geq \nu_n + p^n \nu(v_0)$.

(a) Similarly, we have s_k is the sum of $u_0^{p^k} v_k$, $v_0^{p^k} u_k$, and terms of the form $M = u_0^{\alpha_0} v_0^{\beta_0} \cdots u_{k-1}^{\alpha_{k-1}} v_{k-1}^{\beta_{k-1}}$. If $k = 0$, then $\nu(s_0) = \nu(u_0) + \nu(v_0) = \nu_0 + p^0 \nu(v_0)$. If $k > 0$, then as before, we have $\nu(u_0^{p^k} v_k) > \nu_k + p^k \nu(v_0)$, $\nu(v_0^{p^k} u_k) = \nu_k + p^k \nu(v_0)$, and $\nu(M) > \nu_k + p^k \nu(v_0)$. So $\nu(s_k) = \nu_k + p^k \nu(v_0)$.

(b) We have s_n is the sum of $u_0^{p^n} v_n$, $v_0^{p^n} u_n$, and terms of the form $M = u_0^{\alpha_0} v_0^{\beta_0} \cdots u_{n-1}^{\alpha_{n-1}} v_{n-1}^{\beta_{n-1}}$. Also, from before, we have $\nu(u_0^{p^n}) > \nu_n + p^n \nu(v_0)$, $\nu(v_0^{p^n} u_n) = \nu_n + p^n \nu(v_0)$, and $\nu(M) > \nu_n + p^n \nu(v_0)$. So $\nu(s_n) = \nu_n + p^n \nu(v_0)$. □

Define u, v, u_i, v_i, r_i, s_i as before. Define

$$C = \{\{\nu_i\} : \nu_i \in \mathbb{R} \text{ for } i \geq 0, \nu_0 \leq 0, \nu_{i+1} < p\nu_i \text{ for } i \geq 0\}. \tag{5.2}$$

Let $\{\nu_i\} \in C$.

Note that if $\nu_0 < 0$, then $\{\nu_i\} \in C_0$. If $\nu_0 = 0$, then $\{\nu_i\} \in C_1$.

Lemma 5.10. *Assume that $\nu(u_i) \geq \nu_i$ for $i \geq 0$.*

(i) Assume $\nu(v_0) \geq \nu_0$ 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 $i \geq 0$, then $\nu(r_n) = \nu_n$ for $n \geq 1$.

(ii) Assume $\nu(v_i) \geq p^i \nu(v_0)$ for all $i \geq 0$.

(a) Assume also that $\nu_0 < 0$ *and* $\nu_0 < -\nu(v_0)$. *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* $i \geq 0$, *then* $\nu(s_n) = \nu_n + p^n\nu(v_0)$ *for* $n \geq 1$.

(b) Assume also that $\nu_0 = 0$, $\nu_1 < -p\nu(v_0)$, *and* $\nu(v_0) \geq 0$. *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* $i \geq 0$, *then* $\nu(s_n) = \nu_n + p^n\nu(v_0)$ *for* $n \geq 1$.

Proof. (i) If $\nu_0 < 0$, then $\{\nu_i\} \in C_0$. By Lemma 5.9 (ii), we have $\nu(r_n) \geq \nu_n$ for $n \geq 1$.

If $\nu_0 = 0$, then $\{\nu_i\} \in C_1$. Again by Lemma 5.9 (ii), we have $\nu(r_n) \geq \nu_n$ for $n \geq 1$.

Suppose $\nu(u_i) = \nu_i$ for $i \geq 0$. If $\nu_0 < 0$, then $\{\nu_i\} \in C_0$. By Lemma 5.9 (ii) (b), we have $\nu(r_n) = \nu_n$ for $n \geq 1$. If $\nu_0 = 0$, then $\{\nu_i\} \in C_1$. By Lemma 5.9 (ii) (a) and (b), we have $\nu(r_n) = \nu_n$ for $n \geq 1$.

(ii) (a) Since $\nu_0 < 0$, we have $\{\nu_i\} \in C_0$. By Lemma 5.9 (iii), we have $\nu(s_n) \geq \nu_n + p^n\nu(v_0)$ for $n \geq 1$. Assume that $\nu(u_i) = \nu_i$ for $i \geq 0$. By Lemma 5.9 (iii) (b), we have $\nu(s_n) = \nu_n + p^n\nu(v_0)$ for $n \geq 1$.

(b) Since $\nu_0 = 0$, we have $\{\nu_i\} \in C_1$. By Lemma 5.9 (iii), we have $\nu(s_n) \geq \nu_n + p^n\nu(v_0)$ for $n \geq 1$. Assume that $\nu(u_i) = \nu_i$ for $i \geq 0$. By Lemma 5.9 (iii) (a) and (b), we have $\nu(s_n) = \nu_n + p^n\nu(v_0)$ for $n \geq 1$. □

Define $u, v, u_i, v_i, r_i, s_i, k$ as before. Let $\{\nu_i\} \in C_k$.

Lemma 5.11. *Assume* $\nu(u_i) \geq 0$ *for* $0 \leq i \leq k-1$, *and* $\nu(u_i) \geq \nu_i$ *for* $i \geq k$. *Assume also* $\nu(v_0) = 0$ *and* $\nu(v_i) \geq 0$ *for* $i \geq 1$.

(i) We have $\nu(r_n) \geq 0$ *for* $0 \leq n \leq k-1$ *and* $\nu(r_n) \geq \nu_n$ *for* $n \geq k$.

(ii) We have $\nu(s_n) \geq 0$ *for* $0 \leq n \leq k-1$ *and* $\nu(s_n) \geq \nu_n$ *for* $n \geq k$.

(iii) Assume $\nu(u_i) = \nu_i$ *for* $i \geq k$. *Then* $\nu(r_n) = \nu(s_n) = \nu_n$ *for* $n \geq k$.

Proof. (i) By Lemma 5.9 (i), we have $\nu(r_n) \geq 0$ for $0 \leq n \leq k-1$. Also, we have $\nu(v_k) \geq 0 > \nu_k$ and $\nu(v_i) \geq 0 > \nu_i$ for $i > k$. By Lemma 5.9 (ii), we have $\nu(r_n) \geq \nu_n$ for $n \geq k$.

(ii) By Lemma 5.9 (i), we have $\nu(s_n) \geq 0$ for $0 \leq n \leq k-1$. By Lemma 5.9 (iii), we have $\nu(s_n) \geq \nu_n + p^n\nu(v_0) = \nu_n$ for $n \geq k$.

(iii) Since $\nu(v_k) \geq 0 > \nu_k = \nu(u_k)$, by Lemma 5.9 (ii) (a) and (b), we have $\nu(r_n) = \nu_n$ for $n \geq k$. Similarly, by Lemma 5.9 (iii) (a) and (b), we have $\nu(r_n) = \nu_n$ for $n \geq k$. □

Now, let $u = (u_0, u_1, \ldots) \in W(K)$. Let $u^{-1} = (v_0, v_1, \ldots) \in W(K)$. Let $k \geq 1$. Let $\alpha, \beta > 0$. Define

$$\nu_i = p^i(\alpha - \beta i),$$

for $i \geq 1$. Assume $\alpha - \beta k < 0$.

Lemma 5.12. *Assume that $\nu(u_0) = 0$ and $\nu(u_i) \geq 0$ for $i = 1, \ldots, (k-1)$. Also assume $\nu(u_i) \geq \nu_i$ for $i \geq 1$. Then, we have $\nu(v_i) \geq \max\{0, \nu_i\}$ for $i = 1, \ldots, (k-1)$, and $\nu(v_i) \geq \nu_i$ for $i \geq k$. Moreover, if $\nu(u_i) = \nu_i$ for $i \geq k$, then we have $\nu(v_i) = \nu_i$ for $i \geq k$.*

Proof. We have

$$(u_0, u_1, \ldots)(v_0, v_1, \ldots) = (1, 0, 0, \ldots). \tag{5.3}$$

Hence $v_0 = u_0^{-1}$. So $\nu(v_0) = 0$.

We show that $\nu(v_n) \geq 0$ for $n = 1, \ldots, (k-1)$ by induction on n. If $n = 1$, we have $u_0^p v_1 + v_0^p u_1 = 0$. So $v_1 = -v_0^p u_1 / u_0^p$. Hence $\nu(v_1) = \nu(u_1) \geq 0$. Let $2 \leq n \leq k-1$. By the definition of P_n and (5.3), we have $-u_0^{p^n} v_n$ is the sum of $v_0^{p^n} u_n$ and terms of the form $M = u_0^{\alpha_0} v_0^{\beta_0} \cdots u_{n-1}^{\alpha_{n-1}} v_{n-1}^{\beta_{n-1}}$, where $\alpha_0, \beta_0, \ldots, \alpha_{n-1}, \beta_{n-1} \geq 0$. We have $\nu(-u_0^{p^n} v_n) = \nu(v_n)$, $\nu(v_0^{p^n} u_n) = \nu(u_n) \geq 0$, and $\nu(M) \geq 0$ by induction hypothesis. So $\nu(v_n) \geq 0$.

Next, we show that $\nu(v_n) \geq \nu_n$ for $n \geq 1$ by induction on n. If $n = 1$, we have $\nu(v_1) = \nu(u_1) \geq \nu_1$. Let $n \geq 2$. By Lemma 4.11 and (5.3), we have that $-u_0^{p^n} v_n$ is the sum of $u_i^{p^{n-i}} v_{n-i}^{p^i}$ where $i = 1, \ldots, n$, and terms of the form $M = u_0^{\alpha_0} v_0^{\beta_0} \cdots u_{n-1}^{\alpha_{n-1}} v_{n-1}^{\beta_{n-1}}$ where $\sum_{i=0}^{n-1} i\alpha_i p^i + \sum_{j=0}^{n-1} j\beta_j p^j \leq (n-1)p^n$. We have $\nu(-u_0^{p^n} v_n) = \nu(v_n)$ and $\nu(v_0^{p^n} u_n) = \nu(u_n) \geq \nu_n$. For $1 \leq i \leq n-1$, we have

$$\nu(u_i^{p^{n-i}} v_{n-i}^{p^i}) \geq p^{n-i} p^i (\alpha - \beta i) + p^i p^{n-i} (\alpha - \beta(n-i)) = p^n(2\alpha - \beta n) > p^n(\alpha - \beta n) = \nu_n.$$

Also, since $\nu(u_0) = \nu(v_0) = 0$, by induction hypothesis and Lemma 4.11, we have

$$\begin{aligned}
\nu(M) &= \sum_{i=1}^{n-1} \alpha_i \nu(u_i) + \sum_{j=1}^{n-1} \beta_j \nu(v_j) \geq \sum_{i=1}^{n-1} \alpha_i p^i(\alpha - \beta i) + \sum_{j=1}^{n-1} \beta_j p^j(\alpha - \beta j) \\
&= \alpha \left(\sum_{i=1}^{n-1} \alpha_i p^i + \sum_{j=1}^{n-1} \beta_j p^j \right) - \beta \left(\sum_{i=1}^{n-1} i\alpha_i p^i + \sum_{j=1}^{n-1} j\beta_j p^j \right) \\
&> \alpha \left(\sum_{i=0}^{n} \alpha_i p^i + \sum_{j=0}^{n} \beta_j p^j - \alpha_0 - \beta_0 \right) - \beta n p^n = \alpha \left(2p^n - \alpha_0 - \beta_0\right) - \beta n p^n \\
&= p^n(\alpha - \beta n) + \alpha(p^n - \alpha_0 - \beta_0) \geq p^n(\alpha - \beta n) = \nu_n.
\end{aligned}$$

Then by Lemma 5.6, we have $\nu(v_n) \geq \nu_n$. Therefore, we have $\nu(v_i) \geq \max\{0, \nu_i\}$ for $i = 1, \ldots, (k-1)$. Also we have $\nu(v_i) \geq \nu_i$ for $i \geq k$.

Assume $\nu(u_i) = \nu_i$ for $i \geq k$. Let $n \geq k$. As before, we have that $-u_0^{p^n} v_n$ is the sum of $u_i^{p^{n-i}} v_{n-i}^{p^i}$ where $i = 1, \ldots, n$, and terms of the form $M = u_0^{\alpha_0} v_0^{\beta_0} \cdots u_{n-1}^{\alpha_{n-1}} v_{n-1}^{\beta_{n-1}}$ where $\sum_{i=0}^{n-1} i\alpha_i p^i + \sum_{j=0}^{n-1} j\beta_j p^j \leq (n-1)p^n$. We have $\nu(-u_0^{p^n} v_n) = \nu(v_n)$ and $\nu(v_0^{p^n} u_n) = \nu(u_n) = \nu_n$. For $1 \leq i \leq n-1$, we have $\nu(u_i^{p^{n-i}} v_{n-i}^{p^i}) > \nu_n$. Also, we have $\nu(M) > \nu_n$. So by Lemma 5.6 (ii), we have $\nu(v_n) = \nu_n$. □

Let $u = (u_0, u_1, \ldots) \in W(K)$. Let $u^{-1} = (v_0, v_1, \ldots) \in W(K)$. Let $k \geq 1$. Let $\alpha, \beta > 0$. Define

$$\nu_i = p^i(\alpha - \beta i),$$

for $i \geq k$. Assume $\alpha - \beta k < 0$. Hence $\nu_i < 0$ for $i \geq k$.

Lemma 5.13. *Assume that $\nu(u_0) = 0$ and $\nu(u_i) \geq 0$ for $i = 1, \ldots, (k-1)$. Also assume $\nu(u_i) \geq \nu_i$ for $i \geq k$. Then, we have $\nu(v_i) \geq 0$ for $i = 0, 1, \ldots, (k-1)$, and $\nu(v_i) \geq \nu_i$ for $i \geq k$. Moreover, if $\nu(u_i) = \nu_i$ for $i \geq k$, then we have $\nu(v_i) = \nu_i$ for $i \geq k$.*

Proof. We have

$$(u_0, u_1, \ldots)(v_0, v_1, \ldots) = (1, 0, 0, \ldots).$$

We show that $\nu(v_n) \geq 0$ for $n = 0, 1, \ldots, (k-1)$ by induction on n. If $n = 0$, we have $v_0 = u_0^{-1}$. So $\nu(v_0) = 0$. Let $1 \leq n \leq k-1$. By the definition of P_n and (5.3), we have $-u_0^{p^n} v_n$ is the sum of $v_0^{p^n} u_n$ and terms of the form $M = u_0^{\alpha_0} v_0^{\beta_0} \cdots u_{n-1}^{\alpha_{n-1}} v_{n-1}^{\beta_{n-1}}$, where $\alpha_0, \beta_0, \ldots, \alpha_{n-1}, \beta_{n-1} \geq 0$.

We have $\nu(-u_0^{p^n}v_n) = \nu(v_n)$, $\nu(v_0^{p^n}u_n) = \nu(u_n) \geq 0$, and $\nu(M) \geq 0$ by induction hypothesis. So $\nu(v_n) \geq 0$.

Next, we show that $\nu(v_n) \geq \nu_n$ for $n \geq k$.

Let T be a term of $\overline{P_n}$ different from $X_0^{p^n}Y_n$. Let $M = T(u_0, v_0, \ldots, u_n, v_n)$.

We show that $\nu(M) \geq \nu_n$ by induction on n.

If $n = k$, then $M = v_0^{p^k}u_k$ or $u_0^{\alpha_0}v_0^{\beta_0}\cdots u_{k-1}^{\alpha_{k-1}}v_{k-1}^{\beta_{k-1}}$, where $\alpha_0, \beta_0, \ldots, \alpha_{k-1}, \beta_{k-1} \geq 0$. We have $\nu(v_0^{p^k}u_k) = \nu(u_k) \geq \nu_k$. Also we have $\nu(u_0^{\alpha_0}v_0^{\beta_0}\cdots u_{k-1}^{\alpha_{k-1}}v_{k-1}^{\beta_{k-1}}) \geq 0 > \nu_k$. Since $\nu(-u_0^{p^k}v_k) = \nu(v_k)$ and $-u_0^{p^k}v_k$ equals the sum of all the M's, we have $\nu(v_k) \geq \nu_k$.

Let $n \geq k+1$. By Lemma 4.14, we have M is either of the form $X_i^{p^{n-i}}Y_j^{p^{n-j}}$ where $i + j \leq n$ and $j \neq n$, or a like term to a term in $\overline{P_i}^{p^{n-i}}$ where $i \leq n-1$.

First let M be of the form $u_i^{p^{n-i}}v_j^{p^{n-j}}$ where $i + j \leq n$ and $j \neq n$. Note that since $-u_0^{p^j}v_j$ is equal to the sum of all M's in case $n = j$, by induction hypothesis, we have $\nu(v_j) \geq \nu_j$.

If $i = n$, then $j = 0$. We have $\nu(u_n v_0^{p^n}) = \nu(u_n) \geq \nu_n$. Let $i < n$.

Case 1: $i, j \leq k-1$. Then

$$\nu(u_i^{p^{n-i}}v_{n-i}^{p^i}) \geq 0 > \nu_n.$$

Case 2: $i \leq k-1$ and $j \geq k$. Then

$$\nu(u_i^{p^{n-i}}v_j^{p^{n-j}}) \geq p^{n-j}p^j(\alpha - \beta j) > p^n(\alpha - \beta n) = \nu_n.$$

Case 3: $i \geq k$ and $j \leq k-1$. Then

$$\nu(u_i^{p^{n-i}}v_j^{p^{n-j}}) \geq p^{n-i}p^i(\alpha - \beta i) > p^n(\alpha - \beta n) = \nu_n.$$

Case 4: $i, j \geq k$. Then

$$\begin{aligned}\nu(u_i^{p^{n-i}}v_j^{p^{n-j}}) &\geq p^{n-i}p^i(\alpha - \beta i) + p^{n-j}p^j(\alpha - \beta j) = p^n(2\alpha - \beta(i+j)) \\ &> p^n(\alpha - \beta(i+j)) \geq p^n(\alpha - \beta n) = \nu_n,\end{aligned}$$

since $i + j \leq n$.

Let M be a term coming from $\overline{P_i}^{p^{n-i}}$. If $i \leq k-1$, then $\nu(M) \geq 0 > \nu_n$. If $i \geq k$, then $\nu(M) \geq p^{n-i}p^i(\alpha - \beta i) > \nu_n$. So $\nu(M) \geq \nu_n$ for all cases. Hence $\nu(v_n) \geq \nu_n$.

Assume $\nu(u_i) = \nu_i$ for $i \geq k$. Let $n \geq k$. As before, we have that $-u_0^{p^n} v_n$ is the sum of $u_n v_0^{p^n}$ and other terms M. We have $\nu(-u_0^{p^n} v_n) = \nu(v_n)$ and $\nu(v_0^{p^n} u_n) = \nu(u_n) = \nu_n$. For different cases, we have $\nu(M) > \nu_n$. So by Lemma 5.6 (ii), we have $\nu(v_n) = \nu_n$. □

Let u, u^{-1}, u_i, v_i be as for Lemma 5.12. Let $\nu_0 > 0$.

Lemma 5.14. *Assume $\nu(u_0) = \nu_0$, $\nu(u_1) \geq 0$, and $\nu(u_i) > -p^i(i-1)\nu_0$ for $i \geq 2$. Then 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. We prove by induction on n. If $n = 0$, then $\nu(v_0) = \nu(1/u_0) = -\nu_0$. Let $n \geq 1$. Like in the proof of Lemma 5.12, we have $-u_0^{p^n} v_n$ is the sum of $u_i^{p^{n-i}} v_{n-i}^{p^i}$ where $i = 1, \ldots, n$, and terms of the form $M = u_0^{\alpha_0} v_0^{\beta_0} \cdots u_{n-1}^{\alpha_{n-1}} v_{n-1}^{\beta_{n-1}}$ where $\sum_{i=0}^{n-1} i\alpha_i p^i + \sum_{j=0}^{n-1} j\beta_j p^j \leq (n-1)p^n$. By induction hypothesis, we have $\nu(-u_0^{p^n} v_n) = \nu_0 p^n + \nu(v_n)$ and $\nu(u_1^{p^{n-1}} v_{n-1}^{p}) = p^{n-1}\nu(u_1) + p\nu(v_{n-1}) \geq -p^n n\nu_0$. For $i = 2, \ldots, n$, we have $\nu(u_i^{p^{n-i}} v_{n-i}^{p^i}) > -p^n(i-1)\nu_0 - p^n(n-i+1)\nu_0 = -p^n n\nu_0$. Also, we have

$$\begin{aligned}
\nu(M) &\geq \alpha_0\nu_0 - \sum_{i=1}^{n-1} \alpha_i p^i (i-1)\nu_0 - \sum_{j=0}^{n-1} \beta_j p^j (j+1)\nu_0 \\
&= \nu_0 \left(\alpha_0 - \left(\sum_{i=0}^{n-1} \alpha_i i p^i + \sum_{j=0}^{n-1} \beta_j j p^j \right) + \sum_{i=1}^{n-1} \alpha_i p^i - \sum_{j=0}^{n-1} \beta_j p^j \right) \\
&\geq -p^n(n-1)\nu_0 > -p^n n\nu_0.
\end{aligned}$$

So by Lemma 5.6, we have $\nu_0 p^n + \nu(v_n) \geq -p^n n\nu_0$. Hence $\nu(v_n) \geq -p^n(n+1)\nu_0$.

Assume that $\nu(u_1) = 0$. We prove by induction on n. If $n = 0$, we are done. Let $n \geq 1$. Then $-u_0^{p^n} v_n$ is the sum of $u_i^{p^{n-i}} v_{n-i}^{p^i}$ where $i = 1, \ldots, n$, and terms of the form M. By induction hypothesis, we have $\nu(-u_0^{p^n} v_n) = \nu_0 p^n + \nu(v_n)$ and $\nu(u_1^{p^{n-1}} v_{n-1}^{p}) = p^{n-1}\nu(u_1) + p\nu(v_{n-1}) = -p^n n\nu_0$. For $i = 2, \ldots, n$, we have $\nu(u_i^{p^{n-i}} v_{n-i}^{p^i}) > -p^n n\nu_0$. Also, we have $\nu(M) > -p^n n\nu_0$. So by Lemma 5.6 (ii), we have $\nu_0 p^n + \nu(v_n) = -p^n n\nu_0$. Hence $\nu(v_n) = -p^n(n+1)\nu_0$. □

5.4 The general denominator

We now want to know what powers of $\Delta, \mathcal{H}, a_0, b_0$ appear in the denominators of A_i and B_i. We will use the valuations to answer the questions. Since the valuations must be used in primes, we now check each of the four factors.

Remember that $\Delta = 4a_0^3 + 27b_0^2$.

Lemma 5.15. *We have a_0, b_0, Δ are primes in $\mathbb{F}_p[a_0, b_0]$.*

Proof. We know that a_0, b_0 are primes. Now we show Δ is a prime. Since 27 is a unit in $\mathbb{F}_p[a_0, b_0]$, it suffices to show $b_0^2 + ca_0^3$, call it f, is a prime, where $c = 4/27$. Since $\mathbb{F}_p[a_0, b_0]$ is a UFD, we only need to show that f is irreducible. We have f is non-zero and non-unit. Let $f = gh$ where $g, h \in \mathbb{F}_p[a_0, b_0]$.

Case 1: $g = b_0 + g_1(a_0)$ and $h = b_0 + h_1(a_0)$ for some $g_1, h_1 \in \mathbb{F}_p[a_0]$.

Comparing the b_0 and 1 terms in $f = gh$, we have $0 = g_1(a_0) + h_1(a_0)$ and $ca_0^3 = g_1(a_0)h_1(a_0)$. Hence $ca_0^3 = -(g_1(a_0))^2$. The degree in a_0 is odd for the left hand side, but is even for the right hand side, a contradiction.

Case 2: $g = b_0^2 + b_0 g_1(a_0) + g_2(a_0)$ and $h = h_1(a_0)$ for some $g_1, g_2, h_1 \in \mathbb{F}_p[a_0]$.

Comparing the b_0^2 terms in $f = gh$, we have $h_1(a_0) = 1$.

So Δ is a prime. □

Remember, $\mathcal{H}$ is the coefficient of x_0^{p-1} in $(x_0^3 + a_0x_0 + b_0)^{(p-1)/2}$. We have $\mathcal{H}$ may not be a prime in $\mathbb{F}_p[a_0, b_0]$. For example, if $p = 11$, then we have $\mathcal{H} = 9a_0b_0$. Also, if $p = 5$, then $\mathcal{H} = 2a_0$. So tracking powers of $\mathcal{H}$ is the same as tracking powers of a_0. Hence it is harder to track powers of $\mathcal{H}$ showing in the denominators. The approach we take here is to view the $\mathcal{H}$ coming from Equation (4.1) as an unknown, rather than an expression on a_0 and b_0, as this is the only place where $\mathcal{H}$ is explicitly introduced. We use $\mathfrak{H}$ for this new variable.

Let

$$\hat{R} = \mathbb{F}_p[a_0, b_0, \mathfrak{H}], \quad \hat{k} = \mathbb{F}_p(a_0, b_0, \mathfrak{H}).$$

Then all $\Delta, \mathfrak{H}, a_0, b_0$ are primes of $\hat{R}$. Let

$$\hat{\mathcal{S}}_p = \left(-\frac{2}{9}\right)^r \left(\frac{1728}{\Delta}\right)^{r_2 - r_1} \frac{(-27)^{r_2}}{4^{r_1} a_0^{\delta} b_0^{\epsilon}} \mathfrak{H}. \tag{5.4}$$

For $i \geq 1$, by (4.3), we have that $J_i(j_0) = F_i(j_0)/(\mathcal{S}_p(j_0)^\alpha j_0^\beta (j_0 - 1728)^\gamma)$, for some $\alpha, \beta, \gamma \geq 0$. Define

$$\hat{J}_i = \frac{F_i(j_0)}{\hat{\mathcal{S}}_p^\alpha j_0^\beta (j_0 - 1728)^\gamma}.$$

Define $\hat{j} = (j_0, \hat{J}_1, \hat{J}_2, \ldots)$. Let

$$\hat{a} = \lambda^4 \frac{27\hat{j}}{4(1728 - \hat{j})} = (a_0, \hat{A}_1, \hat{A}_2, \ldots),$$
$$\hat{b} = \lambda^6 \frac{27\hat{j}}{4(1728 - \hat{j})} = (b_0, \hat{B}_1, \hat{B}_2, \ldots),$$

where $\lambda = (\sqrt{b_0/a_0}, 0, 0, \ldots)$. Define

$$\hat{\mathbb{V}} = \mathbb{F}_p[a_0, b_0, \mathfrak{H}, 1/(\Delta \cdot \mathfrak{H} \cdot a_0 \cdot b_0)].$$

Then we have $A_i(a_0, b_0) = \hat{A}_i(a_0, b_0, \mathcal{H})$ and $B_i(a_0, b_0) = \hat{B}_i(a_0, b_0, \mathcal{H})$.

By the definition of $\hat{A}_i$ and $\hat{B}_i$ and from the proofs of Proposition 5.1 and Theorem 5.2, we have that $\hat{A}_i, \hat{B}_i \in \hat{\mathbb{V}}$ for $i \geq 1$. Let $\hat{\nu}_\Delta, \hat{\nu}_\mathfrak{H}, \hat{\nu}_{a_0}, \hat{\nu}_{b_0}$ be the valuations over the field $\hat{k}$. In the next few sections, we will study these valuations.

5.5 The bounds for Δ

In this section, we will study the valuations in Δ of A_i and B_i for $i \geq 1$.

We first show the following lemma about Δ and $\mathcal{H}$.

Lemma 5.16. *We have that $\Delta \nmid \mathcal{H}$ in $\mathbb{F}_p[a_0, b_0]$, i.e., Δ and $\mathcal{H}$ are relatively prime in $\mathbb{F}_p[a_0, b_0]$.*

Proof. By (4.1), we have that

$$\mathcal{H} = c\Delta^{r_2 - r_1} a_0^\delta b_0^\epsilon \mathcal{S}_p(j_0),$$

for some $c \in \mathbb{F}_p$ and $c \neq 0$. By Lemma 4.2, we have $\deg \mathcal{S}_p = r_2 - r_1$ and $\mathcal{S}_p(X) \in \mathbb{F}_p[X]$. Say $\mathcal{S}_p(X) = c_n X^n + \cdots + c_0$, where $n = r_2 - r_1$ and $c_n, \ldots, c_0 \in \mathbb{F}_p$. Since $j_0 = 1728 \cdot 4a_0^3/\Delta$, we have $\nu_\Delta(\mathcal{S}_p(j_0)) = r_1 - r_2$ by Lemma 5.6 (ii). So $\nu_\Delta(\mathcal{H}) = r_2 - r_1 + \nu_\Delta(\mathcal{S}_p(j_0)) = 0$. □

Lemma 5.17. *We have that $\nu_{a_0}(\mathcal{H}) = \delta$ and $\nu_{b_0}(\mathcal{H}) = \epsilon$.*

Proof. Remember from (4.2), we have

$$\mathcal{H} = \left(\frac{b_0}{a_0}\right)^r \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} \left(\frac{a_0^3}{b_0^2}\right)^i.$$

Each term above have different degrees in a_0. So $\nu_{a_0}(\mathcal{H})$ equals the smallest power occurring on a_0, which is $3r_1 - r = \delta$, by Lemma 4.1. Similarly, we have $\nu_{b_0}(\mathcal{H}) = r - 2r_2 = \epsilon$. □

Now we can compute the valuations. We first compute the valuation of $\hat{J}_i$. In this section, let $\nu = \nu_\Delta$ and $\hat{\nu} = \hat{\nu}_\Delta$.

Lemma 5.18. *Let $i \geq 1$. Then we have $\hat{\nu}(\hat{J}_i) = -p^i + \iota$.*

Proof. By Theorem 4.3, we have

$$\hat{J}_i = \frac{F_i(j_0)}{\hat{\mathcal{S}}_p^{m_i} H_i(j_0)}, \tag{5.5}$$

where $m_i = ip^{i-1} + (i-1)p^{i-2}$. By the definition of $\hat{\mathcal{S}}_p$, we have $\hat{\nu}(\hat{\mathcal{S}}_p) = -(r_2 - r_1) = -\deg \mathcal{S}_p$. Also, as in the proof of 5.16, we have $\hat{\nu}(F_i(j_0)) = -\deg F_i$ and $\hat{\nu}(H_i(j_0)) = -\deg H_i$.

Since $G_i = \mathcal{S}_p^{m_i} H_i$, by Theorem 4.3, we have

$$\begin{aligned}\hat{\nu}(\hat{J}_i) &= \hat{\nu}(F_i(j_0)) - m_i \hat{\nu}(\hat{\mathcal{S}}_p) - \hat{\nu}(H_i(j_0)) \\ &= -\deg F_i + m_i \deg \mathcal{S}_p + \deg H_i = -\deg F_i + \deg G_i = -p^i + \iota.\end{aligned}$$

□

Now, we can prove the main theorem for Δ. Let

$$\hat{\mathbb{V}}_\Delta = \mathbb{F}_p[a_0, b_0, \mathfrak{H}, 1/(\mathfrak{H} a_0 b_0)].$$

Theorem 5.19. *Let $i \geq 1$. Then we have $\hat{A}_i$, $\hat{B}_i \in \hat{\mathbb{V}}_\Delta$. Hence we have $\hat{\nu}(\hat{A}_i)$, $\hat{\nu}(\hat{B}_i) \geq 0$. Therefore Δ does not appear in the denominators of A_i or B_i.*

Proof. Let $d = (\Delta, 0, 0, \ldots)$. By Lemma 4.4 and Lemma 5.18, we have

$$27d\hat{j} = 27(1728 \cdot 4a_0^3, \Delta^p \hat{J}_1, \Delta^{p^2} \hat{J}_2, \ldots) \in W(\hat{\mathbb{V}}_\Delta).$$

Similarly, we have

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

Also we have $4d(1728 - \hat{j}) = (4 \cdot 1728 \cdot 27b_0^2, \ldots)$. Since $4 \cdot 1728 \cdot 27b_0^2$ is a unit of $\hat{\mathbb{V}}_\Delta$, we have $4d(1728 - \hat{j})$ is a unit of $W(\hat{\mathbb{V}}_\Delta)$. So

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

Since $\lambda^2 = (b_0/a_0, 0, 0, \ldots) \in W(\hat{\mathbb{V}}_\Delta)$, be the definition of $\hat{a}$ and $\hat{b}$, we have $\hat{a}, \hat{b} \in W(\hat{\mathbb{V}}_\Delta)$. So $\hat{A}_i, \hat{B}_i \in \hat{\mathbb{V}}_\Delta$. Hence $\hat{\nu}(\hat{A}_i)$, $\hat{\nu}(\hat{B}_i) \geq 0$. Therefore by Lemma 5.16, we have Δ does not appear in the denominators of A_i or B_i. □

Let

$$\mathbb{U} = \mathbb{F}_p[a_0, b_0, 1/\mathcal{H}].$$

Corollary 5.20. *If $p \equiv 11 \pmod{12}$, then for $i \geq 1$, we have $A_i, B_i \in \mathbb{U}$. Hence the A_i, B_i given by (3.1) are universal.*

Proof. We have that $\delta, \epsilon = 1$. So by Lemma 5.17, we have $a_0, b_0 \mid \mathcal{H}$. By Theorem 5.19, we have $A_i, B_i \in \mathbb{F}_p[a_0, b_0, 1/(\mathcal{H}a_0b_0)] = \mathbb{U}$. Hence A_i, B_i are universal. □

This proves that for $p \equiv 11 \pmod{12}$, we have universal modular functions with no delta in the denominators giving the canonical lifting. This proves part (1) of Conjecture 3.2 for $p \equiv 11 \pmod{12}$.

5.6 The valuations in factors of $\mathcal{H}$

In this section, I will study the valuations in $\mathcal{H}$ of A_n, B_n for $n \geq 1$.

In this section, let $\hat{\nu} = \hat{\nu}_{\mathfrak{H}}$. Let $m_0 = 0$ and $m_i = ip^{i-1} + (i-1)p^{i-2}$ for $i \geq 1$. Then by (5.5) and (5.4), we have that

$$\hat{\nu}(\hat{J}_i) = -m_i,$$

for $i \geq 1$. From this, we can find the valuation for $\hat{A}_i$ and $\hat{B}_i$.

Let $\hat{J}_0 = j_0$. Then $\hat{j} = (\hat{J}_0, \hat{J}_1, \ldots)$.

Theorem 5.21. *Let $i \geq 0$. Then $\hat{\nu}(\hat{A}_i)$, $\hat{\nu}(\hat{B}_i) = -m_i$.*

Proof. We have $-m_0 = 0$, $-m_1 = -1 < p \cdot 0$, and for $i \geq 1$, we have

$$\begin{aligned} -m_{i+1} &= -(i+1)p^i - ip^{i-1} = -p((i+1)p^{i-1} + ip^{i-2}) \\ &< -p(ip^{i-1} + (i-1)p^{i-2}) = -pm_i. \end{aligned}$$

So $\{-m_i\} \in C$ by (5.2). Then $-m_i < 0$ for all $i \geq 0$. Let $1728 = (v_0, v_1, \ldots)$. Then $\hat{\nu}(v_0) \geq 0$ and $\hat{\nu}(v_i) \geq 0 > -m_i$ for $i \geq 1$. Also, we have $\hat{\nu}(\hat{J}_i) = -m_i$ for $i \geq 0$. Let $1728 - \hat{j} = (r_0, r_1, \ldots)$. Then, by Lemma 5.10 (i), we have $\hat{\nu}(r_i) = -m_i$ for all $i \geq 1$. Also $\hat{\nu}(r_0) = \hat{\nu}(4 \cdot 1728 \cdot 27b_0^2/\Delta) = 0 = -m_0$. So $\hat{\nu}(r_i) = -m_i$ for all $i \geq 0$.

Let $(1728 - \hat{j})^{-1} = (s_0, s_1, \ldots)$. Let $k = 1$, $\alpha = 1/p^2$, and $\beta = (p+1)/p^2$. We have $\alpha, \beta > 0$ and $\alpha - \beta = -1/p < 0$. Also, for $i \geq 1$, we have $p^i(\alpha - \beta i) = p^{i-2} - ip^{i-1} - ip^{i-2} = -m_i$. And we have $\hat{\nu}(r_0) = 0$ and $\hat{\nu}(r_i) = -m_i$ for $i \geq 1$. So, by Lemma 5.12, we have that $\hat{\nu}(s_i) = -m_i$ for $i \geq 0$, since $s_0 = \Delta/(4 \cdot 1728 \cdot 27b_0^2)$.

Now, we have

$$\hat{a} = \lambda^4 \frac{27\hat{j}}{4(1728 - \hat{j})} = \frac{27\lambda^4}{4}\left(1728 \cdot \frac{1}{1728 - \hat{j}} - 1\right), \quad \hat{b} = \lambda^2 \hat{a}.$$

We have $\{-m_i\} \in C_1$ by (5.1). Also $\hat{\nu}(s_0) \geq 0$ and $\hat{\nu}(s_i) = -m_i$ for $i \geq 1$. Since $1728 = (v_0, v_1, \ldots)$, we have $\hat{\nu}(v_0) = 0$ and $\hat{\nu}(v_i) \geq 0$ for $i \geq 1$. Let $1728/(1728 - \hat{j}) = (t_0, t_1, \ldots)$. Then, by Lemma 5.11 (iii), we have $\hat{\nu}(t_i) = -m_i$ for $n \geq 0$. Similarly, by Lemma 5.10 (i) and Lemma 5.11 (iii), we have that $\hat{\nu}(\hat{A}_i)$, $\hat{\nu}(\hat{B}_i) = -m_i$ for $i \geq 0$. □

Now we want to translate this theorem to the powers of $\mathcal{H}$ in the denominators of A_i and B_i. Remember that $\mathcal{H}$ may not be prime in $\mathbb{F}_p[a_0, b_0]$, and $\mathcal{H}$ may have a_0 or b_0 as a

factor. And there are also powers of a_0, b_0 coming from parts other than plugging in $\mathfrak{H} = \mathcal{H}$ in $\hat{A}_i, \hat{B}_i$. We will deal with the powers of a_0 and b_0 in the next section. Therefore we give the following corollary about the powers of the irreducible factors of $\mathcal{H}$ that are not a_0 or b_0.

Corollary 5.22. *Let $h \in \mathbb{F}_p[a_0, b_0]$ be an irreducible factor of $\mathcal{H}$ such that $h \neq a_0, b_0$. Then, for $i \geq 1$, we have $\nu_h(A_i)$, $\nu_h(B_i) \geq -m_i \nu_h(\mathcal{H})$.*

Proof. Let $v = \nu_h(\mathcal{H})$. Then $\mathcal{H} = qh^v$, where $h \nmid q$. By Theorem 5.21, we have

$$\hat{A}_i = \frac{f_i}{a_0^\alpha b_0^\beta \mathfrak{H}^{m_i}},$$

where $f_i \in \mathbb{F}_p[a_0, b_0, \mathfrak{H}]$, and $\alpha, \beta \geq 0$. Plugging in $\mathfrak{H} = \mathcal{H}$, we have

$$A_i(a_0, b_0) = \hat{A}_i(a_0, b_0, \mathcal{H}) = \frac{f_i(a_0, b_0, \mathcal{H})}{a_0^\alpha b_0^\beta (qh^v)^{m_i}}.$$

So $\nu_h(A_i) \geq -m_i v = -m_i \nu_h(\mathcal{H})$. Similarly, we have $\nu_h(B_i) \geq -m_i v = -m_i \nu_h(\mathcal{H})$. □

Future question 4. Prove or find a counter example that $\mathcal{H} \in \mathbb{F}_p[a_0, b_0]$ has no repeated factors.

We computed by Magma the $\mathcal{H}$ for $p \leq 997$ and none of them have repeated factors.

5.7 The bounds for a_0, b_0

In this section, we will study the valuation in a_0, b_0 for A_i, B_i. Since the formulas for general case are very complicated, we will give the bounds in different cases depending on the congruences of p modulo 4 and 6.

In this section, let $\hat{\nu}_1 = \hat{\nu}_{a_0}$, $\hat{\nu}_2 = \hat{\nu}_{b_0}$, $\nu_1 = \nu_{a_0}$, and $\nu_2 = \nu_{b_0}$. As before, we will study the valuation of $\hat{J}_i$ first.

Lemma 5.23. *We have,*

(i) If $p \equiv 1 \pmod 6$, then $\hat{\nu}_1(\hat{J}_i) \geq 0$ for $i \geq 0$.

(ii) If $p \equiv 5 \pmod 6$, then $\hat{\nu}_1(\hat{J}_0) = 3$, $\hat{\nu}_1(\hat{J}_1) \geq 1$, $\hat{\nu}_1(\hat{J}_2) \geq 2p + 1$, $\hat{\nu}_1(\hat{J}_3) = 2p$, and for $i \geq 4$, we have $\hat{\nu}_1(\hat{J}_i) \geq -((i-3)p^i - (i-1)p^{i-2})$.

(iii) If $p \equiv 1 \pmod 4$*, then* $\hat{\nu}_2(\hat{J}_i) \geq 0$ *for* $i \geq 0$.

(iv) If $p \equiv 3 \pmod 4$*, then* $\hat{\nu}_2(\hat{J}_0) = 0$*,* $\hat{\nu}_2(\hat{J}_1) \geq 1$*,* $\hat{\nu}_2(\hat{J}_2) = 1$*, and for* $i \geq 3$*, we have* $\hat{\nu}_2(\hat{J}_i) \geq -((i-2)p^{i-1} - (i-1)p^{i-2})$.

Proof. By Equation (5.4), we have $\hat{\nu}_1(\hat{\mathcal{S}}_p) = -\delta$ and $\hat{\nu}_2(\hat{\mathcal{S}}_p) = -\epsilon$. Let $i \geq 1$. By (5.5), we have

$$\hat{J}_i = \frac{F_i(j_0)}{\hat{\mathcal{S}}_p^{m_i} H_i(j_0)},$$

where $m_i = ip^{i-1} + (i-1)p^{i-2}$. Since $H_i = X^\alpha (X - 1728)^\beta$ for some $\alpha, \beta \geq 0$, we have $\hat{\nu}_1(H_i(j_0)) = 3\alpha$ and $\hat{\nu}_2(H_i(j_0)) = 2\beta$. So

$$\hat{\nu}_1(\hat{J}_i) = \hat{\nu}_1(F_i(j_0)) + m_i\delta - 3\alpha, \quad \hat{\nu}_2(\hat{J}_i) = \hat{\nu}_2(F_i(j_0)) + m_i\epsilon - 2\beta.$$

By Theorem 4.3, if $i = 1$, then $H_1 = 1$. So $\alpha, \beta = 0$. Hence we have

$$\hat{\nu}_1(\hat{J}_1) = \hat{\nu}_1(F_1(j_0)) + \delta \geq \delta, \quad \hat{\nu}_2(\hat{J}_1) = \hat{\nu}_2(F_1(j_0)) + \epsilon \geq \epsilon.$$

For $i = 2$, we have $H_2 = (X - 1728)^{\epsilon p}$. So $\alpha = 0$ and $\beta = \epsilon p$. Hence we have

$$\hat{\nu}_1(\hat{J}_2) = \hat{\nu}_1(F_2(j_0)) + (2p+1)\delta \geq (2p+1)\delta, \quad \hat{\nu}_2(\hat{J}_2) = \hat{\nu}_2(F_2(j_0)) + (2p+1)\epsilon - 2p\epsilon \geq \epsilon.$$

For $i = 3$, we have $H_3 = X^{\delta p^2}(X - 1728)^t$, where $t \leq 2\epsilon p^2$. So $\alpha = \delta p^2$ and $\beta \leq 2\epsilon p^2$. Hence we have

$$\hat{\nu}_1(\hat{J}_3) = \hat{\nu}_1(F_3(j_0)) + (3p^2 + 2p)\delta - 3\delta p^2 \geq 2p\delta.$$

For $i \geq 3$, we have $\beta \leq \epsilon(i-1)p^{i-1}$. Hence we have

$$\hat{\nu}_2(\hat{J}_i) \geq \hat{\nu}_2(F_i(j_0)) + m_i\epsilon - 2\epsilon(i-1)p^{i-1} \geq -((i-2)p^{i-1} - (i-1)p^{i-2})\epsilon.$$

For $i \geq 4$, we have $\alpha \leq \delta t_i'$, where $t_i' = \max\{0, t_i\}$ and $t_i = ((i-3)p^i + ip^{i-1})/3$. Then $t_i \geq 0$. So $t_i' = t_i$. Hence we have

$$\hat{\nu}_1(\hat{J}_i) \geq \hat{\nu}_1(F_i(j_0)) + m_i\delta - 3\delta t_i \geq -((i-3)p^i - (i-1)p^{i-2})\delta.$$

(i) We have $\delta = 0$. So $\hat{\nu}_1(\hat{J}_i) \geq 0$ for $i \geq 1$. Also, we have $\hat{\nu}_1(\hat{J}_0) = 2 \geq 0$ since $\hat{J}_0 = j_0 = 1728 \cdot 4a_0^3/\Delta$.

(ii) We have $\delta = 1$. So $\hat{\nu}_1(\hat{J}_0) = 3$, $\hat{\nu}_1(\hat{J}_1) \geq 1$ and $\hat{\nu}_1(\hat{J}_2) \geq 2p+1$.

For $i = 3$, we have $X \mid H_3$. Since $(F_3, G_3) = 1$ where $G_3 = \mathcal{S}_p^{m_3} H_3$. So $X \nmid F_3$. Let

$$F_3(X) = c_n X^n + \cdots + c_1 X + c_0,$$

where $n \geq 0$, $c_n, \ldots, c_0 \in \mathbb{F}_p$, and $c_0 \neq 0$. Since $j_0 = 1728 \cdot 4a_0^3/\Delta$, we have $\hat{\nu}_1(F_3(j_0)) = 0$. So $\hat{\nu}_1(\hat{J}_3) = 2p$.

For $i \geq 4$, we have $\hat{\nu}_1(\hat{J}_i) \geq -((i-3)p^i - (i-1)p^{i-2})$.

(iii) We have $\epsilon = 0$. So $\hat{\nu}_2(\hat{J}_i) \geq 0$ for $i \geq 1$. Also, we have $\hat{\nu}_2(\hat{J}_0) = 0 \geq 0$.

(iv) We have $\epsilon = 1$. So $\hat{\nu}_2(\hat{J}_0) = 0$ and $\hat{\nu}_2(\hat{J}_1) \geq 1$.

For $i = 2$, we have $(X - 1728) \mid H_2$, hence $(X - 1728) \nmid F_2$. So

$$F_2 = d_m (X - 1728)^m + \cdots + d_1 (X - 1728) + d_0,$$

for some $d_0, \ldots, d_m \in \mathbb{F}_p$ and $d_0 \neq 0$. Since $j_0 - 1728 = -1728 \cdot 27 b_0^2/\Delta$, we have $\hat{\nu}_2(F_2(j_0)) = 0$. Hence $\hat{\nu}_2(\hat{J}_2) = 1$.

For $i \geq 3$, we have $\hat{\nu}_2(\hat{J}_i) \geq -((i-2)p^{i-1} - (i-1)p^{i-2})$. □

Now we can study the valuations of $\hat{A}_i$ and $\hat{B}_i$. Let $\hat{A}_0 = a_0$ and $\hat{B}_0 = b_0$.

Theorem 5.24. *We have*

(i) If $p \equiv 1 \pmod 6$, *then*

(a) $\hat{\nu}_1(\hat{A}_i) \geq -2p^i$ *for* $i \geq 0$,

(b) $\hat{\nu}_1(\hat{B}_i) \geq -3p^i$ *for* $i \geq 0$.

(ii) If $p \equiv 5 \pmod 6$, *then*

(a) $\hat{\nu}_1(\hat{A}_i) \geq -2p^i$ *for* $i = 0, 1, 2, 3$, *and* $\hat{\nu}_1(\hat{A}_i) \geq -((i-1)p^i - (i-1)p^{i-2})$ *for* $i \geq 4$,

(b) $\hat{\nu}_1(\hat{B}_i) \geq -3p^i$ *for* $i = 0, 1, 2, 3$, *and* $\hat{\nu}_1(\hat{B}_i) \geq -(ip^i - (i-1)p^{i-2})$ *for* $i \geq 4$.

(iii) For any $p \geq 5$, *we have*

(a) $\hat{\nu}_2(\hat{A}_i) \geq -2ip^i$ *for* $i \geq 0$,

(b) $\hat{\nu}_2(\hat{B}_i) \geq -(2i-1)p^i$ *for* $i \geq 0$.

Proof. (i) Let $i \geq 0$. Let

$$\mathbb{U}_1 = \mathbb{F}_p[a_0, b_0, \mathfrak{H}, 1/(\Delta\mathfrak{H}b_0)].$$

By Lemma 5.23, we have $\hat{J}_i \in \mathbb{U}_1$. So $1728 - \hat{j} \in W(\mathbb{U}_1)$. Since $1728 - j_0 = 1728 \cdot 27b_0^2/\Delta$, we have $(1728 - j_0)^{-1} \in \mathbb{U}_1$. So $(1728 - \hat{j})^{-1} \in W(\mathbb{U}_1)$. Hence

$$\frac{27\hat{j}}{4(1728 - \hat{j})} = \frac{27}{4}\left(1728 \cdot \frac{1}{1728 - \hat{j}} - 1\right) \in W(\mathbb{U}_1).$$

Since $\hat{a} = \lambda^4 27\hat{j}/(4(1728 - \hat{j}))$ and $\lambda^4 = (b_0^2/a_0^2, 0, 0, \ldots)$, by Lemma 4.4 (iii), we have $\hat{\nu}_1(\hat{A}_i) \geq -2p^i$ and $\hat{\nu}_1(\hat{B}_i) \geq -3p^i$.

(ii) By Lemma 5.23, we have $\hat{\nu}_1(\hat{J}_i) \geq 0$ for $i = 0, 1, 2, 3$ and $\hat{\nu}_1(\hat{J}_i) \geq -((i-3)p^i - (i-1)p^{i-2})$ for $i \geq 4$. Let $k = 4$. Let $\nu_i = -((i-3)p^i - (i-1)p^{i-2})$ for $i \geq k$. Then $\nu_4 = -(p^4 - 3p^2) < 0$. Also, for $i \geq k$, we have

$$p\nu_i - \nu_{i+1} = -((i-3)p^{i+1} - (i-1)p^{i-1}) + ((i-2)p^{i+1} - ip^{i-1}) = p^{i+1} - p^{i-1} > 0.$$

Hence $\{\nu_i\} \in C_k$ by (5.1). Let $1728 = (v_0, v_1, \ldots)$. Then $\hat{\nu}_1(v_0) = 0$ and $\hat{\nu}_1(v_i) \geq 0$ for $i \geq 1$. Let $1728 - \hat{j} = (r_0, r_1, \ldots)$. By Lemma 5.11 (i), we have $\hat{\nu}_1(r_i) \geq 0$ for $i = 0, 1, 2, 3$ and $\hat{\nu}_1(r_i) \geq \nu_i$ for $i \geq 4$.

Let $\alpha = 3 - 1/p^2$ and $\beta = 1 - 1/p^2$. Then $\alpha, \beta > 0$. Also we have $p^i(\alpha - \beta i) = \nu_i$ for $i \geq 4$. We have $\alpha - 4\beta = -1 + 3/p^2 < 0$. Also we have $\hat{\nu}_1(r_0) = 0$. Let $(1728 - \hat{j})^{-1} = (s_0, s_1, \ldots)$. By Lemma 5.13, we have $\hat{\nu}_1(s_i) \geq 0$ for $i = 0, 1, 2, 3$ and $\hat{\nu}_1(s_i) \geq \nu_i$ for $i \geq k$. Let

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

By Lemma 5.11 (i) and (ii), we have $\hat{\nu}_1(w_i) \geq 0$ for $i = 0, 1, 2, 3$, and $\hat{\nu}_1(w_i) \geq \nu_i$ for $i \geq 4$. Hence $\hat{\nu}_1(\hat{A}_i) \geq -2p^i$ for $i = 0, 1, 2, 3$, and $\hat{\nu}_1(\hat{A}_i) \geq -((i-1)p^i - (i-1)p^{i-2})$ for $i \geq 4$. Also, we have $\hat{\nu}_1(\hat{B}_i) \geq -3p^i$ for $i = 0, 1, 2, 3$, and $\hat{\nu}_1(\hat{B}_i) \geq -(ip^i - (i-1)p^{i-2})$ for $i \geq 4$.

(iii) If $p \equiv 1 \pmod 4$, then let

$$\mathbb{U}_2 = \mathbb{F}_p[a_0, b_0, \mathfrak{H}, 1/(\Delta\mathfrak{H}a_0)].$$

By Lemma 5.23, we have $\hat{J}_i \in W(\mathbb{U}_2)$ for $i \geq 0$. So $1728 - \hat{j} \in W(\mathbb{U}_2)$. Define r_i, s_i, w_i as in (ii). Let $\nu_0 = 2 > 0$. Then $\hat{\nu}_2(r_0) = \nu_0$, $\hat{\nu}_2(r_1) \geq 0$, and $\hat{\nu}_2(r_i) \geq 0 > -p^i(i-1)\nu_0$ for $i \geq 2$. By Lemma 5.14, we have $\hat{\nu}_2(s_i) \geq -p^i(i+1)\nu_0$ for $i \geq 0$.

Let $k = 0$. Then $-\nu_0 < 0$ and

$$p(-p^i(i+1)\nu_0) + p^{i+1}(i+2)\nu_0 = p^{i+1}\nu_0 > 0.$$

So $\{-p^i(i+1)\nu_0\} \in C_0$ by (5.1). By Lemma 5.11 (i) and (ii), we have $\hat{\nu}_2(w_i) \geq -p^i(i+1)\nu_0$ for $i \geq 0$. Hence $\hat{\nu}_2(\hat{A}_i) \geq -2ip^i$ and $\hat{\nu}_2(\hat{B}_i) \geq -(2i-1)p^i$ for $i \geq 0$.

If $p \equiv 3 \pmod 4$, then by Lemma 5.23, we have $\hat{\nu}_2(\hat{J}_i) \geq 0$ for $i = 0, 1, 2$ and $\hat{\nu}_2(\hat{J}_i) \geq -((i-2)p^{i-1} - (i-1)p^{i-2})$ for $i \geq 3$.

Let $k = 3$. Let $\nu_i = -((i-2)p^{i-1} - (i-1)p^{i-2})$ for $i \geq 3$. We have $\nu_3 = -p^2 + 2p < 0$ and

$$p\nu_i - \nu_{i+1} = -(i-2)p^i + (i-1)p^{i-1} + (i-1)p^i - ip^{i-1} = p^i - p^{i-1} > 0.$$

So $\{\nu_i\} \in C_3$ by (5.1). Let r_i, s_i, w_i be as before. By Lemma 5.11 (i), we have $\hat{\nu}_2(r_i) \geq 0$ for $i = 0, 1, 2$ and $\hat{\nu}_2(r_i) \geq \nu_i$ for $i \geq 3$. Next we have $\hat{\nu}_2(r_0) = 2 > 0$, $\hat{\nu}_2(r_1) \geq 0$, $\hat{\nu}_2(r_2) = 0 > -2p^2$, and for $i \geq 3$, we have

$$\begin{aligned} &-((i-2)p^{i-1} - (i-1)p^{i-2}) + 2p^i(i-1) = p^{i-2}((2p^2 - p + 1)i - 2p^2 + 2p - 1) \\ &> (2p^2 - p + 1)2 - 2p^2 + 2p - 1 = 2p^2 + 1 > 0. \end{aligned}$$

So $\hat{\nu}_2(r_i) \geq \nu_i > -2p^i(i-1)$ for $i \geq 2$. By Lemma 5.14, we have $\hat{\nu}_2(s_i) \geq -2p^i(i+1)$ for $i \geq 0$. As before, we have $\{-2p^i(i+1)\} \in C_0$. By Lemma 5.11 (i) and (ii), we have $\hat{\nu}_2(w_i) \geq -2p^i(i+1)$ for $i \geq 0$. Hence $\hat{\nu}_2(\hat{A}_i) \geq -2ip^i$ and $\hat{\nu}_2(\hat{B}_i) \geq -(2i-1)p^i$ for $i \geq 0$. □

Now we translate this into valuations of A_i and B_i.

Theorem 5.25. *We have*

(i) If $p \equiv 1 \pmod 6$, then

(a) $\nu_1(A_i) \geq -2p^i$ for $i \geq 1$,

(b) $\nu_1(B_i) \geq -3p^i$ for $i \geq 1$.

(ii) If $p \equiv 5 \pmod 6$, then

(a) $\nu_1(A_i) \geq -2p^i - ip^{i-1} - (i-1)p^{i-2}$ *for* $i = 1, 2, 3$ *and* $\nu_1(A_i) \geq -(i-1)p^i - ip^{i-1}$ *for* $i \geq 4$,

(b) $\nu_1(B_i) \geq -3p^i - ip^{i-1} - (i-1)p^{i-2}$ *for* $i = 1, 2, 3$ *and* $\nu_1(B_i) \geq -ip^i - ip^{i-1}$ *for* $i \geq 4$.

(iii) If $p \equiv 1 \pmod 4$, *then*

(a) $\nu_2(A_i) \geq -2ip^i$ *for* $i \geq 1$,

(b) $\nu_2(B_i) \geq -(2i-1)p^i$ *for* $i \geq 1$.

(iv) If $p \equiv 3 \pmod 4$, *then*

(a) $\nu_2(A_i) \geq -2ip^i - ip^{i-1} - (i-1)p^{i-2}$ *for* $i \geq 1$,

(b) $\nu_2(B_i) \geq -(2i-1)p^i - ip^{i-1} - (i-1)p^{i-2}$ *for* $i \geq 1$.

Proof. (i) Let $i \geq 1$. By Theorem 5.24 and Theorem 5.21, we have

$$\hat{A}_i = \frac{f_i}{a_0^{2p^i} b_0^{\beta} \mathfrak{H}^{m_i}},$$

where $f_i \in \mathbb{F}_p[a_0, b_0, \mathfrak{H}]$, $\beta \geq 0$, and $m_i = ip^{i-1} + (i-1)p^{i-2}$. We have $\delta = 0$. By Lemma 5.17, we have $\nu_1(\mathcal{H}) = \delta = 0$. So

$$A_i(a_0, b_0) = \hat{A}_i(a_0, b_0, \mathcal{H}) = \frac{f_i(a_0, b_0, \mathcal{H})}{a_0^{2p^i} b_0^{\beta} \mathcal{H}^{m_i}}.$$

Hence $\nu_1(A_i) \geq -2p^i$. Similarly, we have $\nu_1(B_i) \geq -3p^i$.

(ii) We have $\delta = 1$. So $\nu_1(\mathcal{H}) = 1$. Similarly, for $i = 1, 2, 3$, we have

$$A_i = \frac{f_i(a_0, b_0, \mathcal{H})}{a_0^{2p^i} b_0^{\beta} \mathcal{H}^{m_i}}.$$

So $\nu_1(A_i) \geq -2p^i - m_i = -2p^i - ip^{i-1} - (i-1)p^{i-2}$. For $i \geq 4$, we have

$$A_i = \frac{f_i(a_0, b_0, \mathcal{H})}{a_0^{(i-1)p^i - (i-1)p^{i-2}} b_0^{\beta} \mathcal{H}^{m_i}}.$$

So $\nu_1(A_i) \geq -(i-1)p^i + (i-1)p^{i-2} - m_i = -(i-1)p^i - ip^{i-1}$. Similarly, we have $\nu_1(B_i) \geq -3p^i - ip^{i-1} - (i-1)p^{i-2}$ for $i = 1, 2, 3$ and $\nu_1(B_i) \geq -ip^i - ip^{i-1}$ for $i \geq 4$.

(iii) Let $i \geq 1$. We have $\epsilon = 0$. So $\nu_2(\mathcal{H}) = \epsilon = 0$. We have

$$A_i = \frac{f_i(a_0, b_0, \mathcal{H})}{a_0^{\alpha} b_0^{2ip^i} \mathcal{H}^{m_i}},$$

where $\alpha \geq 0$. So $\nu_2(A_i) \geq -2ip^i$. Similarly, we have $\nu_2(B_i) \geq -(2i-1)p^i$.

(iv) Let $i \geq 1$. We have $\nu_2(\mathcal{H}) = \epsilon = 1$. Also we have

$$A_i = \frac{f_i(a_0, b_0, \mathcal{H})}{a_0^{\alpha} b_0^{2ip^i} \mathcal{H}^{m_i}}.$$

So $\nu_2(A_i) \geq -2ip^i - m_i = -2ip^i - ip^{i-1} - (i-1)p^{i-2}$. Similarly, we have $\nu_2(B_i) \geq -(2i-1)p^i - ip^{i-1} - (i-1)p^{i-2}$. □

5.8 Computations

In this section, I will show some computations done by Magma. Table 5.1 gave some computation of the actual bounds compared to the bounds we got from the theorem. The Magma codes can be found in https://github.com/lrfinotti/witt. The actual bound can be computed similarly as shown in Figure 3.1. For example, if we want to compute $\nu_{a_0}(A_2)$, we load the file `lift_j.m`, then type the code `jweier(5,2)`, where the input means $p = 5$ and $n = 2$. The program returns a list with two items: a and b. For a, it gives A_0, A_1, A_2. In A_2, we can see that the denominator is $a_0^{35} b_0^{40}$. So we have $\nu_{a_0}(A_2) = -35$. This is shown in the Figure 5.1.

We see that the bounds are not sharp. In the future, we would like to improve those bounds.

```
> load 'lift_j.m';
Loading "lift_j.m"
Loading "gt.m"
Loading "witt.m"
Loading "etas.m"
> jweier(5,2);
[
    [
        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),
        (3*a0^120 + 4*a0^105*b0^10 + 3*a0^96*b0^16 + 2*a0^93*b0^18 + a0^90*b0^20
         + 4*a0^87*b0^22 + 4*a0^81*b0^26 + 4*a0^78*b0^28 + a0^75*b0^30
         + 4*a0^72*b0^32 + 3*a0^66*b0^36 + 4*a0^63*b0^38 + 4*a0^60*b0^40
         + 4*a0^57*b0^42 + 2*a0^54*b0^44 + a0^51*b0^46 + 2*a0^45*b0^50
         + 4*a0^36*b0^56 + 4*a0^33*b0^58 + a0^30*b0^60 + 2*a0^27*b0^62
            + 2*a0^24*b0^64 + a0^15*b0^70 + 3*b0^80)/(a0^35*b0^40)
    ],
    [
        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,
        (3*a0^120 + 4*a0^105*b0^10 + 3*a0^96*b0^16 + 2*a0^93*b0^18 + a0^90*b0^20
        + 4*a0^87*b0^22 + 4*a0^81*b0^26 + 4*a0^78*b0^28 + a0^75*b0^30
        + 4*a0^72*b0^32 + 3*a0^66*b0^36 + 4*a0^63*b0^38 + 4*a0^60*b0^40
        + 4*a0^57*b0^42 + 2*a0^54*b0^44 + a0^51*b0^46 + 2*a0^45*b0^50
        + 4*a0^36*b0^56 + 4*a0^33*b0^58 + a0^30*b0^60 + 2*a0^27*b0^62
            + 2*a0^24*b0^64 + a0^15*b0^70 + 3*b0^80)/(a0^60*b0^15)
    ]
]
```

Figure 5.1: Computation for A_2 when $p = 5$.

Table 5.1: Actual bounds versus theorem

	$p=5$ actual	$p=5$ bound	$p=7$ actual	$p=7$ bound
$\nu_{a_0}(A_1)$	-1	-11	1	-14
$\nu_{a_0}(A_2)$	-35	-61	-35	-98
$\nu_{a_0}(A_3)$	-325	-335	-539	-686
$\nu_{a_0}(A_4)$	-1775	-2375	-4067	-4802
$\nu_{a_0}(B_1)$	-6	-16	-6	-21
$\nu_{a_0}(B_2)$	-60	-86	-84	-147
$\nu_{a_0}(B_3)$	-450	-460	-882	-1029
$\nu_{a_0}(B_4)$	-2400	-3000	-6468	-7203
$\nu_{b_0}(A_1)$	-4	-10	-8	-15
$\nu_{b_0}(A_2)$	-40	-100	-112	-211
$\nu_{b_0}(A_3)$	-300	-750	-1176	-2219
$\nu_{b_0}(A_4)$	-1600	-5000	-10976	-20727
$\nu_{b_0}(B_1)$	1	-5	-1	-8
$\nu_{b_0}(B_2)$	-15	-75	-63	-162
$\nu_{b_0}(B_3)$	-175	-625	-833	-1876
$\nu_{b_0}(B_4)$	-975	-4375	-8575	-18326

Bibliography

[1] Deuring, M. (1941). Die typen der multiplikatorenringe elliptischer funktionenköper. *Abh. Math. Sem. Univ. Hamburg*, 14:197–272. 1

[2] Dummit, D. S. and Foote, R. M. (2004). *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition. 2

[3] Finotti, L. R. A. (2002). Degrees of the elliptic Teichmüller lift. *J. Number Theory*, 95(2):123–141. 20

[4] Finotti, L. R. A. (2009). A formula for the supersingular polynomial. *Acta Arith.*, 139(3):265–273. 9, 13, 14, 24

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

[6] Finotti, L. R. A. (2013). Coordinates of the j-invariant of the canonical lifting. *Funct. Approx. Comment. Math.*, 49(1):57–72. 13, 14, 26

[7] Finotti, L. R. A. (2014). Computations with Witt vectors and the Greenberg transform. *Int. J. Number Theory*, 10(6):1431–1458. 21

[8] Finotti, L. R. A. (2019). Weierstrass coefficients of the canonical lifting. To appear at the *Int. J. of Number Theory*. Available at http://www.math.utk.edu/~finotti/. 1, 4, 6, 10, 23

[9] Jacobson, N. (1984). *Basic Algebra*, volume 2. W. H. Freeman and Company, second edition. 4, 16

[10] Lubin, J., Serre, J.-P., and Tate, J. (1964). Elliptic curves and formal groups. *Proc. of Woods Hole summer institute in algebraic geometry*. Unpublished. Available at http://www.ma.utexas.edu/users/voloch/lst.html. 1

[11] Poonen, B. (2001). Computing torsion points on curves. *Experiment. Math.*, 10(3):449–465. 1

[12] Satoh, T. (2000). The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270. 1

[13] Silverman, J. H. (2009). *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition. 3

[14] Silverman, J. H. and Tate, J. T. (2015). *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer, Cham, second edition. 3

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

[16] Voloch, J. F. and Walker, J. L. (2000). Euclidean weights of codes from elliptic curves over rings. *Trans. Amer. Math. Soc.*, 352(11):5063–5076. 1

Vita

Delong Li was born in Xi'an, China, on April 22, 1988. He is the son of Guoying Li and Ying Wang, and he is an only child. Delong grew up in Xi'an and went to Xi'an High School. At age of 18, he went to Xi'an Technological University, where he received his undergraduate degree in Information and computing science. At 2012, he moved to Jonesboro, Arkansas, to pursue Master's degree in Mathematics at Arkansas State University. After that, at 2014, he moved to Knoxville, Tennessee, to study for the doctorate degree in Mathematics at the University of Tennessee.