IMPROVED BOUNDS FOR DENOMINATORS IN THE FORMULAS OF THE CANONICAL LIFTING

LUÍS R. A. FINOTTI AND DELONG LI

Abstract. An ordinary elliptic curve $y_0^2 = x_0^3 + ax_0 + b$ has a canonical lifting $\boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{a}\boldsymbol{x} + \boldsymbol{b}$, where $\boldsymbol{a} = (a, A_1, A_2, \ldots), \boldsymbol{b} = (b, B_1, B_2, \ldots)$ and the A_n's and B_n's are rational functions on a and b. Two constructions have been given for these functions, and some of their properties have been studied in some of the authors' previous work. In this paper, we further study those properties, showing that the Greenberg transform construction gives A_1 and B_1 of the form $C/\mathfrak{h}$, where $\mathfrak{h}$ is the Hasse invariant, and giving better bounds for the powers of a and b in the denominators of A_2 and B_2 given by the j-invariant construction.

1. Introduction

Let $p \geq 5$ be a prime, and a and b be indeterminates. Let E be the elliptic curve

$$E/\mathbb{F}_p(a,b) : \; y_0^2 = x_0^3 + ax_0 + b,$$

and

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

be the canonical lifting of E, where $\boldsymbol{a} = (a, A_1, \ldots), \boldsymbol{b} = (b, B_1, \ldots)$. Note that A_n and B_n are then functions on a and b, but since the canonical lifting is unique only up to isomorphism, these coordinate functions are not uniquely defined.

The first author asked about the nature of these A_n and B_n. In [Fin20] he showed that these functions can be, depending on choices under isomorphisms, universal modular functions, and then asked whether these could also be chosen so that the discriminant Δ does not appear in their denominators. In other words, he asked whether the universal modular functions can be taken in ring $\mathbb{F}_p[a, b, 1/\mathfrak{h}]$, where $\mathfrak{h}$ is the *Hasse invariant* of E. Two approaches were suggested to solve this problem.

2010 *Mathematics Subject Classification.* Primary 11G07; Secondary 11F03.

Key words and phrases. canonical lifting, elliptic curves, Witt vectors.

The first approach is to find the canonical lifting by the *Greenberg transform construction*, as described in [FL21] and reviewed below, and show that A_n and B_n satisfy all the requirements. Computations with MAGMA showed that this is the case for small primes p and short lengths, and the first author conjectured it would be true in general. In [FL21] the authors showed that indeed this construction gives $A_1, B_1 \in \mathbb{F}_p[a, b, 1/\mathfrak{h}]$, and therefore, the conjecture is true for $n = 1$.

The second approach is to find the canonical lifting by the *j-invariant construction*, again introduced in [FL21] and reviewed below, and then create isomorphic canonical liftings that satisfy the requirements, as these might not always be universal. More precisely, in [FL20] it was shown that the j-invariant construction yields A_n's and B_n's of the form $C/(a^\alpha b^\beta \mathfrak{h}^\gamma)$, where C is homogeneous, and hence are not defined for curves with j-invariant equal to either 0 or 1728. On the other hand, one can try to create isomorphic liftings by choosing some $\boldsymbol{\lambda}$ such that $\boldsymbol{a}' = \boldsymbol{\lambda}^4 \boldsymbol{a}$ and $\boldsymbol{b}' = \boldsymbol{\lambda}^6 \boldsymbol{b}$ give coordinate functions satisfying all the requirements (i.e., universal modular functions, with no Δ in the denominator). It was shown in [FL21] this can be done for $n = 1$, and under some extra assumption, also for $n = 2$ (after a second change of coordinates).

Also of interest for computations would be to determine the power of each factor in the denominators of A_n and B_n for each construction. That is, for the Greenberg transform construction, A_n and B_n have the form $C/(\mathfrak{h}^\alpha \Delta^\beta)$, and we would like to find upper bounds for α and β. For the j-invariant construction, A_n and B_n have the form $C/(a^\alpha b^\beta \mathfrak{h}^\gamma)$, and we would like to find upper bounds for α, β, and γ.

Besides having its own intrinsic value, this problem can also help solving the problem of finding universal modular functions in $\mathbb{F}_p[a, b, 1/\mathfrak{h}]$ giving the coefficients of the canonical lifting. For example, the authors studied these bounds for the j-invariant construction in [FL20], and were then able to use them in [FL21] to find the isomorphic liftings with no discriminant in the denominator mentioned above.

In the present paper, we will show that the Greenberg transform construction yields A_1 and B_1 of the form $C/\mathfrak{h}$, i.e., the maximal power of the $\mathfrak{h}$ in their denominators is 1, and give better bounds for the powers of a and b in the denominators of the A_2 and B_2 obtained by the j-invariant construction. (Note that the bounds given for A_1 and B_1 in [FL20] were already improved over the general bound.)

2. Previous Results

We shall assume throughout that p is a prime greater than or equal to 5. Then, let a and b be indeterminates and E be the elliptic curve given by the Weierstrass coefficients (a, b), i.e.,

$$E/\mathbb{F}_p(a,b) : \; y_0^2 = x_0^3 + ax_0 + b.$$

Since E is ordinary, it has a *canonical lifting*

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

over the ring of Witt vectors $\boldsymbol{W}(\mathbb{F}_p(a,b))$ (see [Fin20]). By definition, this means that $\boldsymbol{E}$ reduces to E modulo p, i.e., $\boldsymbol{a} = (a, \ldots)$ and $\boldsymbol{b} = (b, \ldots)$, and has a lifting of the Frobenius.

Let then

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

These coordinates A_n and B_n are then functions on a and b, but since the canonical lifting is only unique up to isomorphism, they are not uniquely determined. In [Fin20] it is shown that A_n and B_n can be chosen as to have some “nice” properties. For instance, they can be *modular functions* of weights $4p^n$ and $6p^n$, respectively. To be clear, if we assign weights $\mathrm{wgt}(a) = 4$ and $\mathrm{wgt}(b) = 6$, and let

$$\mathcal{S}_n = \{f/g : f, g \in \mathbb{F}_p[a,b] \text{ homog.}, \mathrm{wgt}(f) - \mathrm{wgt}(g) = n\} \cup \{0\},$$

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

Moreover, it was shown that these A_n and B_n can also be taken to be *universal*, meaning that they are defined for every $a = a_0$ and $b = b_0$ such that (a_0, b_0) gives Weierstrass coefficients of an *ordinary* elliptic curve. In other words, one can find (modular) functions A_n and B_n in the ring $\mathbb{F}_p[a, b, 1/(\Delta\mathfrak{h})]$, where Δ and $\mathfrak{h}$ are the discriminant and Hasse invariant of E, respectively.

The proofs of the properties above allow the discriminant Δ to appear in the denominators, but concrete examples seem to indicate that there are such universal modular functions A_n and B_n for which it does not, i.e., for which we have $A_n, B_n \in \mathbb{F}_p[a, b, 1/\mathfrak{h}]$ instead of $\mathbb{F}_p[a, b, 1/(\Delta\mathfrak{h})]$, raising the question if this is indeed always the case, and if so, how to find such functions.

In [Fin20], two methods to construct the canonical lifting are introduced. The first method uses the *elliptic Teichmüller lift*, which is a section of the reduction modulo p (from $\boldsymbol{E}$ to E) that commutes with the Frobenius maps, and we call this the *Greenberg transform construction*. But by [Fin20, Theorem 2.3], the A_n and B_n given by this construction are in $\mathcal{S}_{4p^n} \cap \mathbb{F}_p[a, b, 1/(\Delta\mathfrak{h})]$ and $\mathcal{S}_{6p^n} \cap \mathbb{F}_p[a, b, 1/(\Delta\mathfrak{h})]$, respectively, while [FL21, Theorem 5.1] shows that $A_1, B_1 \in \mathbb{F}_p[a, b, 1/\mathfrak{h}]$. In Section 3 we show that the denominators of A_1 and B_1 have no powers of $\mathfrak{h}$ higher than one.

The second method to compute A_n and B_n introduced in [Fin20] is the *j-invariant construction*: if $\boldsymbol{j}$ is the j-invariant of the canonical lifting $\boldsymbol{E}$, which was extensively studied in [Fin10], [Fin12], and [Fin13], then

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

where $\boldsymbol{\lambda} = (\sqrt{b/a}, 0, 0, \ldots)$. By [FL20, Theorems 6.3, 10.2, 11.1, 12.2], we have that this construction gives $A_n \in \mathcal{S}_{4p^n}$, $B_n \in \mathcal{S}_{6p^n}$ of the form

$$A_n = \frac{C}{\mathfrak{h}^{np^{n-1}+(n-1)p^{n-2}} a^{(n-1)p^n-(n-1)p^{n-2}} b^{2np^n}},$$
$$B_n = \frac{D}{\mathfrak{h}^{np^{n-1}+(n-1)p^{n-2}} a^{np^n-(n-1)p^{n-2}} b^{(2n-1)p^n}},$$

where $C, D \in \mathbb{F}_p[a, b]$. Moreover, [FL20, Corollaries 13.2, 13.3] give better bounds for the powers of a and b in the denominators for $n = 1$. More precisely, if ν_q is the valuation at q, then:

$$\nu_a(A_1) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 6, \\ -1, & \text{if } p \equiv 5 \pmod 6, \end{cases} \qquad \nu_a(B_1) = \begin{cases} -p+1, & \text{if } p \equiv 1 \pmod 6, \\ -p-1, & \text{if } p \equiv 5 \pmod 6, \end{cases}$$
$$\nu_b(A_1) \geq \begin{cases} -p+1, & \text{if } p \equiv 1 \pmod 4, \\ -p-1, & \text{if } p \equiv 3 \pmod 4, \end{cases} \qquad \nu_b(B_1) \geq \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Similar improvements for the bounds in the case of $n = 2$ will be given here in Section 4.

Before we proceed, we state some of the results we will use below.

Theorem 2.1. *There are rational functions $J_i \in \mathbb{F}_p(X)$, for $i \geq 1$ such that if j is the j-invariant of an ordinary elliptic curve, then the j-invariant of its canonical lifting is given by $(j, J_1(j), J_2(j), \ldots)$.*

Proof. This is [Fin12, Theorem 1.1]. □

Let ss_p be the *supersingular polynomial* (i.e., the monic polynomial having as simple roots exactly the j-invariants of supersingular curves) and

$$S_p(X) \stackrel{\text{def}}{=} \frac{\mathrm{ss}_p(X)}{X^\delta (X - 1728)^\epsilon}, \tag{2.1}$$

where

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

and hence

$$S_p(X) \in \mathbb{F}_p[X], \quad S_p(0), S_p(1728) \neq 0.$$

Then, we have:

Theorem 2.2. *Let J_2 be defined as in Theorem 2.1. Then, we have that*

$$J_2(X) = F_2(X)/G_2(X) \in \mathbb{F}_p(X),$$

where:

(1) $F_2, G_2 \in \mathbb{F}_p[X]$, *with* $(F_2, G_2) = 1$;
(2) F_2 *has a zero at* 0 *of order* $(2\lfloor (p-1)/6 \rfloor + 1)p$;
(3) $G_2(X) = (X - 1728)^{\epsilon p} S_p(X)^{2p+1}$.

Proof. This is [Fin12, Theorem 7.2]. □

We also have:

Theorem 2.3. *We have*

$$\nu_a(J_1(j)) = \begin{cases} 2p+1, & \textit{if } p \equiv 1 \pmod 6, \\ 2p-1, & \textit{if } p \equiv 5 \pmod 6, \end{cases} \qquad \nu_b(J_1(j)) = \begin{cases} 2, & \textit{if } 1728^p \equiv 1728 \pmod{p^2}, \\ 0, & \textit{otherwise}, \end{cases}$$

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

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

Proof. This is [FL20, Theorem 13.1]. □

Finally, we briefly review some basic results about Witt vectors. (More details can be found in [Ser79], [Jac84], or [Rab14].) Let $S_0 = X_0 + Y_0$, $P_0 = X_0 Y_0$, and define S_n and P_n inductively as follows

$$S_n = X_n + Y_n + \frac{1}{p}(X_{n-1}^p + Y_{n-1}^p - S_{n-1}^p) + \cdots + \frac{1}{p^n}(X_0^{p^n} + Y_0^{p^n} - S_0^{p^n}),$$
$$P_n = \frac{1}{p^n}[(X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) - (P_0^{p^n} + \cdots + p^{n-1} P_{n-1}^p)].$$

Then it is known that S_n and P_n have coefficients in $\mathbb{Z}$, and if A is a ring of characteristic p, then addition and multiplication of $\boldsymbol{a} = (a_0, a_1, \ldots)$ and $\boldsymbol{b} = (b_0, b_1, \ldots)$ in the ring of Witt vectors $\boldsymbol{W}(A)$ are given by

$$\boldsymbol{a} + \boldsymbol{b} = (\bar{S}_0(a_0, b_0), \bar{S}_1(a_0, a_1, b_0, b_1), \ldots), \quad \boldsymbol{ab} = (\bar{P}_0(a_0, b_0), \bar{P}_1(a_0, a_1, b_0, b_1), \ldots),$$

where $\bar{S}_n$ and $\bar{P}_n$ are the reductions modulo p of S_n, P_n, respectively.

Moreover, one has $-(a_0, a_1, \ldots) = (-a_0, -a_1, \ldots)$ for $p \neq 2$, and

$$(\lambda, 0, 0, \ldots)(a_0, a_1, a_2, \ldots) = (\lambda a_0, \lambda^p a_1, \lambda^{p^2} a_2, \ldots).$$

We will also need:

Lemma 2.4. *The monomials $\prod_{i=0}^n X_i^{s_i} \prod_{j=0}^n Y_j^{t_j}$ occurring in $\bar{P}_n$ satisfies*

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

Proof. This is [Fin02, Lemma 2.1]. □

3. The power of Hasse invariant in the Greenberg transform construction

Let A_1 and B_1 be the second coordinates of the Weierstrass coefficients of the canonical lifting *given by the Greenberg transform construction*. In this section we show that the power of Hasse invariant $\mathfrak{h}$ in the denominators of A_1 and B_1 is less than or equal to 1.

We start by giving a sufficient condition for the result. Let

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

where $f = x_0^3 + a x_0 + b$. (Thus, we have that $e_i \in \mathbb{F}_p[a, b]$ and e_{p-1} is the Hasse invariant $\mathfrak{h}$.)

Lemma 3.1. *Assume that* $\mathfrak{h} = e_{p-1}$ *and* e_{p-2} *have no non-trivial common divisor. Then* $A_1 = C_1/\mathfrak{h}, B_1 = D_1/\mathfrak{h}$ *for some* $C_1, D_1 \in \mathbb{F}_p[a, b]$.

The proof is similar to [FL21, Section 5].

Proof. From [FL21, Eqs. (5.4), (5.5)], we have

$$2f^{(p+1)/2}H_1 = (f')^p c_0 + A_1 x_0^p + B_1 + \eta_1(f) + (f')^p \hat{F}_1,$$

where $\hat{F}_1$ is the formal integral of $\mathfrak{h}^{-1} f^{(p-1)/2} - x_0^{p-1}$, $\eta_1(f) \in \mathbb{F}_p[a, b, x_0]$, $H_1 \in \mathbb{F}_p(a, b)[x_0]$, and $c_0 \in \mathbb{F}_p(a, b)$. Then $\eta_1(f) + (f')^p \hat{F}_1 = g_1/\mathfrak{h}$ for some $g_1 \in \mathbb{F}_p[a, b, x_0]$. Therefore

$$2f^{(p+1)/2}H_1 = (f')^p c_0 + A_1 x_0^p + B_1 + g_1/\mathfrak{h}. \tag{3.1}$$

Let

$$\begin{aligned} (f')^p &= 2f^{(p+1)/2} q_1 + r_1, \\ g_1 &= 2f^{(p+1)/2} q_2 + r_2, \end{aligned}$$

where $\deg r_i \leq (3p+1)/2$ (where deg refers to degrees as polynomials in x_0). Since $2f^{(p+1)/2}$ has leading coefficient 2 and $(f')^p, g_1 \in \mathbb{F}_p[a, b, x_0]$, we have $q_i, r_i \in \mathbb{F}_p[a, b, x_0]$. So

$$(f')^p c_0 + A_1 x_0^p + B_1 + g_1/\mathfrak{h} = 2f^{(p+1)/2}(c_0 q_1 + q_2/\mathfrak{h}) + (c_0 r_1 + r_2/\mathfrak{h} + A_1 x_0^p + B_1).$$

Let

$$r \stackrel{\text{def}}{=} c_0 r_1 + r_2/\mathfrak{h} + A_1 x_0^p + B_1. \tag{3.2}$$

So, $\deg r \leq (3p+1)/2$, and hence $r = 0$ by Eq. (3.1). We now determine r_1.

Remember

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

and let

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

Then $q \in \mathbb{F}_p[a, b, x_0]$ and

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

The above expression has degree $(3p+1)/2$ and leading coefficient $3\mathfrak{h}$ (as $\mathfrak{h} = e_{p-1}$). Since it is in $\mathbb{F}_p[a, b, x_0]$, it must be equal to remainder r_1 above.

Comparing the coefficients of $x_0^{(3p+1)/2}$ in Eq. (3.2), we have

$$0 = 3\mathfrak{h}c_0 + t/\mathfrak{h},$$

for some $t \in \mathbb{F}_p[a,b]$. So

$$c_0 = -t/(3\mathfrak{h}^2).$$

Comparing the coefficients of x_0^p and 1 in Eq. (3.2), we have

$$-ts/(3\mathfrak{h}^2) + u/\mathfrak{h} + A_1 = 0, \tag{3.3}$$

$$-tv/(3\mathfrak{h}^2) + w/\mathfrak{h} + B_1 = 0, \tag{3.4}$$

for some $s, u, v, w \in \mathbb{F}_p[a,b]$.

Now, we also have that r_1's second highest term is $3e_{p-2}x_0^{(3p-1)/2}$. Comparing the terms of $x_0^{(3p-1)/2}$ in Eq. (3.2), we have

$$0 = 3e_{p-2}c_0 + z/\mathfrak{h},$$

for some $z \in \mathbb{F}_p[a,b]$. So $c_0 = -z/(3e_{p-2}\mathfrak{h}) = -t/(3\mathfrak{h}^2)$. Hence $z\mathfrak{h} = te_{p-2}$. But since $\mathfrak{h}$ and e_{p-2} have no non-trivial common divisor by assumption, we must have $\mathfrak{h} \mid t$ in $\mathbb{F}_p[a,b]$. So $t = t_1\mathfrak{h}$ for some $t_1 \in \mathbb{F}_p[a,b]$.

Thus, Eqs. (3.3) and (3.4) then give us $A_1 = C_1/\mathfrak{h}, B_1 = D_1/\mathfrak{h}$ for some $C_1, D_1 \in \mathbb{F}_p[a,b]$. $\square$

Now, we want to show $(\mathfrak{h}, e_{p-2}) = 1$, where e_{p-2} is the coefficient of x_0^{p-2} in $f^{(p-1)/2}$. We start with the following lemma:

Lemma 3.2. *The variables a and b are not common divisors of $\mathfrak{h}$ and e_{p-2}.*

Proof. According to [Fin09, Lemma 2.2], we have

$$\begin{aligned} e_{p-2} &= \left(\frac{b}{a}\right)^{r+1} \sum_{i=s_1}^{s_2} \binom{r}{i} \binom{i}{3i-r-1} \left(\frac{a^3}{b^2}\right)^i \\ &= \sum_{i=s_1}^{s_2} \binom{r}{i} \binom{i}{3i-r-1} a^{3i-r-1} b^{r+1-2i}, \end{aligned}$$

where $r \stackrel{\text{def}}{=} (p-1)/2$, $s_1 \stackrel{\text{def}}{=} \lceil (r+1)/3 \rceil$, $s_2 \stackrel{\text{def}}{=} \lfloor (r+1)/2 \rfloor$.

So $\nu_a(e_{p-2}) = 3s_1 - r - 1$, $\nu_b(e_{p-2}) = r + 1 - 2s_2$. Considering the four possible residues of p modulo 12, we get

$$\nu_a(e_{p-2}) = \begin{cases} 2, & \text{if } p \equiv 1 \pmod 6, \\ 0, & \text{if } p \equiv 5 \pmod 6, \end{cases} \qquad \nu_b(e_{p-2}) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ 0, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

On the other hand, by [Li20, Lemma 5.17], we have

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

So, neither a nor b are common divisors of $\mathfrak{h}$ and e_{p-2}. □

It is easier to show that two polynomials in one variable are coprime than to show it for polynomials in two variables. So, we introduce

$$F(X) \stackrel{\text{def}}{=} \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} X^{i-r_1}, \tag{3.5}$$

$$F_1(X) \stackrel{\text{def}}{=} \sum_{i=s_1}^{s_2} \binom{r}{i} \binom{i}{3i-r-1} X^{i-s_1}, \tag{3.6}$$

where $r_1 \stackrel{\text{def}}{=} \lceil r/3 \rceil, r_2 \stackrel{\text{def}}{=} \lfloor r/2 \rfloor$, and remembering that $s_1 = \lceil (r+1)/3 \rceil$, $s_2 = \lfloor (r+1)/2 \rfloor$. (Note that F is defined in the same way as in [Fin09].) Then, we show it suffices to prove that $(F, F_1) = 1$ to get the desired result.

Lemma 3.3. *If $(F, F_1) = 1$, then e_{p-2} and $\mathfrak{h}$ have no non-trivial common factors.*

Proof. Assume $d \in \mathbb{F}_p[a,b] \setminus \mathbb{F}_p$ divides both e_{p-2} and $\mathfrak{h}$. Then $e_{p-2} = dg$ and $\mathfrak{h} = dh$ for some $g, h \in \mathbb{F}_p[a,b]$. Define $\bar{\mathfrak{h}}$ and $\bar{\mathfrak{h}}_1$ as in [FL21], i.e.,

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

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

Similarly, define

$$\begin{aligned}
\bar{e} &\stackrel{\text{def}}{=} \frac{e_{p-2}}{a^{3s_1-r-1}b^{r+1-2s_2}} \\
&= \sum_{i=s_1}^{s_2} \binom{r}{i}\binom{i}{3i-r-1} a^{3(i-s_1)}b^{2(s_2-i)} \in \mathbb{F}_p[a,b], \\
\bar{e}_1 &\stackrel{\text{def}}{=} \sum_{i=s_1}^{s_2} \binom{r}{i}\binom{i}{3i-r-1} u^{i-s_1}v^{s_2-i} \in \mathbb{F}_p[u,v].
\end{aligned}$$

Then $\bar{e}$ is homogeneous (with $\mathrm{wgt}(a) = 4$ and $\mathrm{wgt}(b) = 6$) and $a, b \nmid \bar{e}$. Since $a, b \nmid d$, we have $\bar{e} = dg_1$, and $\bar{\mathfrak{h}} = dh_1$, where $g_1 = g/(a^{3s_1-r-1}b^{r+1-2s_2})$ and $h_1 = h/(a^{3r_1-r}b^{r-2r_2}) \in \mathbb{F}_p[a,b]$.

We now show that $d, g_1, h_1 \in \mathbb{F}_p[a^3, b^2]$. We have $\bar{e}$ is homogeneous, so is d. Since $a, b \nmid d$ and $d \notin \mathbb{F}_p$, we have $d = c_1a^m + c_2b^n + abd_1$ for some $c_1, c_2 \in \mathbb{F}_p^\times$ and $d_1 \in \mathbb{F}_p[a,b]$, and with $4m = 6n$. Let a^ib^j be a monomial of d. Then $4i + 6j = 4m = 6n$, hence $3 \mid i$ and $2 \mid j$. So $d \in \mathbb{F}_p[a^3, b^2]$. Similarly, $g_1, h_1 \in \mathbb{F}_p[a^3, b^2]$.

So $d = d_2(a^3, b^2)$, $g_1 = g_2(a^3, b^2)$, $h_1 = h_2(a^3, b^2)$ for some $d_2, g_2, h_2 \in \mathbb{F}_p[u,v]$. Then $\bar{e}_1 = d_2g_2, \bar{\mathfrak{h}}_1 = d_2h_2$, and hence

$$\begin{aligned}
F_1(X) &= \bar{e}_1(X,1) = d_2(X,1)g_2(X,1), \\
F(X) &= \bar{\mathfrak{h}}_1(X,1) = d_2(X,1)h_2(X,1).
\end{aligned}$$

Therefore, since $(F, F_1) = 1$, we have that $d_2(X,1) \in \mathbb{F}_p^\times$. On the other hand, since $d \notin \mathbb{F}_p$ and $d = d_2(a^3, b^2)$, defining $\mathrm{wgt}(u) = \mathrm{wgt}(v) = 1$, we have that d_2 is homogeneous of positive weight. Also $v \nmid \bar{\mathfrak{h}}_1$, so $v \nmid d_2$, and thus d_2 has a monomial of the form u^m for some $m > 0$. Therefore, $d_2(X,1)$ cannot be constant, which is a contradiction. $\square$

Hence, now we must show that $(F, F_1) = 1$. Let us first study F_1. Our goal is to find a differential equation satisfied by F_1, but, following the ideas from [Fin09], we first find a differential equation for the related polynomial

$$\tilde{F}_1(X) \stackrel{\text{def}}{=} X^{s_1}F_1(X) = \sum_{i=s_1}^{s_2} \binom{r}{i}\binom{i}{3i-r-1} X^i.$$

Lemma 3.4. *We have:*

$$4X^2(4X+27)\tilde{F}_1'' + 16X^2\tilde{F}_1' + (15 - X)\tilde{F}_1 = 0.$$

One can easily verify that this equation holds simply by showing that the coefficient for every degree is zero.

From this simpler differential equation, we can obtain the one for F_1:

Lemma 3.5. *We have:*

$$X(4X+27)F_1''+(4(2s_1+1)X+54s_1)F_1'+\left(4s_1-\frac{29}{36}\right)F_1=0.$$

Proof. Since $\tilde{F}_1(X)=X^{s_1}F_1(X)$, taking derivatives both sides, we get equations for $\tilde{F}_1'$ and $\tilde{F}_1''$. Plugging these into the differential equation above, dividing both sides by $4X^{s_1+1}$, we get the desired differential equation. Here we used the fact that $s_1(s_1-1)=-5/36$ in $\mathbb{F}_p$, which can be shown by considering four cases where $p\equiv 1,5,7,11 \pmod{12}$. $\square$

Let $p=12m+4\delta+6\epsilon+1$, with $\epsilon,\delta\in\{0,1\}$. Thus, with our previous notation, we have that $s_1=r_1+(1-\delta)$ and $s_2=r_2+\epsilon$. We then have:

Lemma 3.6. *The polynomials F and F_1 satisfy*

$$\delta F+3XF'=(r-2r_1+2\delta-1)X^{1-\delta}F_1-2X^{2-\delta}F_1'. \tag{3.7}$$

Proof. First note that for $n,k\in\mathbb{Z}$ with $n\geq k\geq 1$, we have

$$\binom{n}{k}k=\binom{n}{k-1}(n-k+1) \tag{3.8}$$

By Eq. (3.5) and since $r=3r_1-\delta$, we have

$$\delta F+3XF'=\sum_{i=r_1}^{r_2}\binom{r}{i}\binom{i}{3i-r}(3i-r)X^{i-r_1}, \tag{3.9}$$

and by Eq. (3.6),

$$(r-2r_1+2\delta-1)X^{1-\delta}F_1-2X^{2-\delta}F_1'=\sum_{i=r_1+(1-\delta)}^{r_2+\epsilon}\binom{r}{i}\binom{i}{3i-r-1}(r-2i+1)X^{i-r_1}. \tag{3.10}$$

Now, by Eq. (3.8),

$$\binom{i}{3i-r}(3i-r)=\binom{i}{3i-r-1}(r-2i+1),$$

for $i=r_1+(1-\delta),\ldots,r_2$ since $i\geq 3i-r\geq 1$, $3r_1-r=\delta$, and $r-2r_2=\epsilon$. Moreover, if $\delta=0$, and hence $3r_1=r$, we have the term with $i=r_1$ in Eq. (3.9) is

$$\binom{r}{r_1}\binom{r_1}{0}0=0,$$

and if $\epsilon = 1$, and hence $r = 2r_2 + 1$, the term with $i = r_2 + \epsilon$ in Eq. (3.10) is

$$\binom{r}{r_2+1}\binom{r_2+1}{3r_2-r+2} 0 = 0.$$

These last three equations prove that the left sides of Eqs. (3.9) and (3.10) are equal, concluding the proof. □

Note that by [FL21, Lemma 6.3], we know F has no repeated roots. Moreover, we have that $F(0), F(-27/4) \neq 0$ by the definition of F and the comment following [Fin09, Lemma 3.1]. Finally, remember that by [Fin09, Proposition 4.2], we have that F satisfies the differential equation

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

Now, we can finally show that $(F, F_1) = 1$.

Theorem 3.7. *We have $(F, F_1) = 1$. Therefore, we have $A_1 = C_1/\mathfrak{h}$, $B_1 = D_1/\mathfrak{h}$ for some $C_1, D_1 \in \mathbb{F}_p[a,b]$.*

Proof. If $p = 7$, then $F_1 = F = 3$, so $(F, F_1) = 1$. We then assume $p \neq 7$. It suffices to show that F and F_1 have no common roots, and hence suppose $x_0 \in \bar{\mathbb{F}}_p$ is a common root. Then $x_0 \neq 0, -27/4$, and using the differential equations for F and F_1, we have

$$x_0 F_1''(x_0) = -\frac{(4(2s_1+1)x_0 + 54s_1)F_1'(x_0)}{4x_0+27}, \tag{3.11}$$

$$x_0 F''(x_0) = -\frac{(8(r_1+1)x_0 + 27(2r_1+1))F'(x_0)}{4x_0+27}. \tag{3.12}$$

Observing that

$$r_1 = \begin{cases} -\frac{1}{6}, & \text{if } \delta = 0, \\ \frac{1}{6}, & \text{if } \delta = 1, \end{cases}$$

we see that when $\delta = 0$, Eq. (3.7) becomes

$$3XF' = -\frac{7}{6}XF_1 - 2X^2F_1', \tag{3.13}$$

and when $\delta = 1$, it becomes

$$F + 3XF' = \frac{1}{6}F_1 - 2XF_1'. \tag{3.14}$$

Let us first look at the case when $\delta = 0$. Dividing Eq. (3.13) by X and taking derivatives, we obtain

$$3F'' = -\frac{19}{6}F_1' - 2XF_1''.$$

Therefore, evaluating these equations at $X = x_0$, we have

$$3F'(x_0) = -2x_0F_1'(x_0), \tag{3.15}$$

$$3F''(x_0) = -(19/6)F_1'(x_0) - 2x_0F_1''(x_0). \tag{3.16}$$

Then, using Eqs. (3.11) and (3.12), and noting that $s_1 = r_1 + (1-\delta) = r_1 + 1$, Eq. (3.16) gives

$$-3\frac{((8r_1+8)x_0 + 54r_1 + 27)F'(x_0)}{x_0(4x_0+27)} = -\frac{19}{6}F_1'(x_0) + 2\frac{((8r_1+12)x_0 + 54r_1 + 54)F_1'(x_0)}{4x_0+27}.$$

Using Eq. (3.15) we then get $(7/6)F_1'(x_0) = 0$. Since $p \neq 7$, we have that $F_1'(x_0) = 0$, and hence $F'(x_0) = 0$. This is a contradiction, since F has no repeated roots.

Now, for the case when $\delta = 1$, taking derivatives on Eq. (3.14), we get

$$3XF'' + 4F' = -\frac{11}{6}F_1' - 2XF_1''.$$

Evaluating the two equations above at $X = x_0$, we have

$$F_1'(x_0) = -\frac{3}{2}F'(x_0), \tag{3.17}$$

$$3x_0F''(x_0) + (5/4)F'(x_0) = -2x_0F_1''(x_0). \tag{3.18}$$

By Eqs. (3.11) and (3.12) and the fact $s_1 = r_1$ in this case, Eq. (3.18) gives

$$-3\frac{((8r_1+8)x_0 + (54r_1+27))F'(x_0)}{4x_0+27} + \frac{5}{4}F'(x_0) \ = 2\frac{((8r_1+4)x_0 + 54r_1)F_1'(x_0)}{4x_0+27}.$$

Using Eq. (3.17), we can simplify it, obtaining $(7/4)F'(x_0) = 0$. Again, since $p \neq 7$, we must have that $F_1'(x_0) = 0$, which, as before, yields a contradiction. $\square$

4. The improved bounds for the powers of a, b in the j-invariant construction

Let A_2 and B_2 be the third coordinates of the Weierstrass coefficients of the canonical lifting from the j-invariant construction. The goal of this section is to give improved bounds for the valuations $\nu_a(A_2)$, $\nu_a(B_2)$, $\nu_b(A_2)$, and $\nu_b(B_2)$.

	$p = 5$		$p = 7$	
	Actual	Bound	Actual	Bound
$\nu_a(A_2)$	-35	-61	-35	-98
$\nu_a(B_2)$	-60	-86	-84	-147
$\nu_b(A_2)$	-40	-100	-112	-211
$\nu_b(B_2)$	-15	-75	-63	-162

Table 4.1. Actual valuations versus bounds.

By [FL20, Theorem 12.3], we have

$$\nu_a(A_2) \geq \begin{cases} -2p^2, & \text{if } p \equiv 1 \pmod 6, \\ -2p^2 - 2p - 1, & \text{if } p \equiv 5 \pmod 6, \end{cases}$$

$$\nu_a(B_2) \geq \begin{cases} -3p^2, & \text{if } p \equiv 1 \pmod 6, \\ -3p^2 - 2p - 1, & \text{if } p \equiv 5 \pmod 6, \end{cases}$$

$$\nu_b(A_2) \geq \begin{cases} -4p^2, & \text{if } p \equiv 1 \pmod 4, \\ -4p^2 - 2p - 1, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

$$\nu_b(B_2) \geq \begin{cases} -3p^2, & \text{if } p \equiv 1 \pmod 4, \\ -3p^2 - 2p - 1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Table 12.1 of [FL20] gives the comparison of the bounds with the actual values for $p = 5, 7$. Table 4.1 records the relevant values, showing that the given bounds are still far from the actual valuations. Our goal in this section is to improve these bounds.

The improvement follows a similar method as the one from [FL20], but also using Theorem 2.2 (which is again simply [Fin12, Theorem 7.2]).

We start with valuations at a, for which we can determine the exact values at A_2 and B_2.

Theorem 4.1. *We have*

$$\nu_a(A_2) = 3p(2\lfloor (p-1)/6 \rfloor + 1) - 2p^2 = \begin{cases} -p^2 + 2p, & \textit{if } p \equiv 1 \pmod 6, \\ -p^2 - 2p, & \textit{if } p \equiv 5 \pmod 6, \end{cases}$$

$$\nu_a(B_2) = 3p(2\lfloor (p-1)/6 \rfloor + 1) - 3p^2 = \begin{cases} -2p^2 + 2p, & \textit{if } p \equiv 1 \pmod 6, \\ -2p^2 - 2p, & \textit{if } p \equiv 5 \pmod 6. \end{cases}$$

Proof. Remember in the j-invariant construction we have that

$$\begin{aligned} \boldsymbol{a} &= \boldsymbol{\lambda}^4 \cdot \frac{27\boldsymbol{j}}{4(1728-\boldsymbol{j})}, \\ \boldsymbol{b} &= \boldsymbol{\lambda}^2 \boldsymbol{a}, \end{aligned}$$

where $\boldsymbol{\lambda} = (\sqrt{b/a}, 0, 0, \ldots)$.

Let then:

$$1728 = (\alpha_0, \alpha_1, \alpha_2), \tag{4.1}$$

$$27/4 = (\beta_0, \beta_1, \beta_2), \tag{4.2}$$

$$1728 - \boldsymbol{j} = (u_0, u_1, u_2), \tag{4.3}$$

$$\frac{1}{1728-\boldsymbol{j}} = (v_0, v_1, v_2), \tag{4.4}$$

$$\frac{27}{4(1728-\boldsymbol{j})} = (w_0, w_1, w_2), \tag{4.5}$$

$$\frac{27\boldsymbol{j}}{4(1728-\boldsymbol{j})} = (z_0, z_1, z_2), \tag{4.6}$$

and R be the localization of $\mathbb{F}_p[a,b]$ at the prime ideal (a).

Since $\nu_a(j) = 3$,

$$\nu_a(J_1(j)) = \begin{cases} 2p+1, & \text{if } p \equiv 1 \pmod 6, \\ 2p-1, & \text{if } p \equiv 5 \pmod 6, \end{cases}$$

by [FL20, Theorem 13.1], and by Theorem 2.2 we have $\nu_a(J_2(j)) = 3p(2\lfloor (p-1)/6 \rfloor + 1)$, we obtain that $\boldsymbol{j} \in \boldsymbol{W}_3(R)$, and hence $1728 - \boldsymbol{j} \in \boldsymbol{W}_3(R)$. It is also clear that $\nu_a(u_0) = 0$.

Since then u_0 is a unit of R, we have that $1/(1728-\boldsymbol{j}) \in \boldsymbol{W}_3(R)$ and $\nu_a(v_0) = 0$. Similarly, we have that $27/(4(1728-\boldsymbol{j})) \in \boldsymbol{W}_3(R)$, which implies that $\nu_a(w_1), \nu_a(w_2) \geq 0$, and $\nu_a(w_0) = \nu_a(\beta_0) + \nu_a(v_0) = 0$.

Now, by Lemma 2.4, we have that z_2 equals $w_0^{p^2} J_2(j)$ plus terms of the form $j^\alpha J_1(j)^\beta w_0^{\gamma_0} w_1^{\gamma_1} w_2^{\gamma_2}$, where $\alpha + \beta p = p^2$, and hence $\beta \leq p$. Then, we have $\nu_a(w_0^{p^2} J_2(j)) = 3p(2\lfloor (p-1)/6 \rfloor + 1)$, and by Theorem 2.3,

$$\nu_a(j^\alpha J_1(j)^\beta w_0^{\gamma_0} w_1^{\gamma_1} w_2^{\gamma_2}) \geq 3\alpha + (2p-1)\beta = 3p^2 - (p+1)\beta \geq p(2p-1).$$

Since

$$3p(2\lfloor (p-1)/6 \rfloor + 1) \leq p((p-1)+3) = p(p+2) < p(2p-1)$$

for $p \geq 5$, we have $\nu_a(z_2) = \nu_a(J_2(j))$. So, $\nu_a(A_2) = \nu_a(J_2(j)) - 2p^2 = 3p(2\lfloor (p-1)/6 \rfloor + 1) - 2p^2$, and $\nu_a(B_2) = \nu_a(J_2(j)) - 3p^2 = 3p(2\lfloor (p-1)/6 \rfloor + 1) - 3p^2$.

The last equality of each equation can be shown by considering cases $p = 6k+1, 6k+5$. $\square$

We now turn to the valuations at b, for which we only get lower bounds, although better ones than previously known.

Theorem 4.2. *We have:*

$$\nu_b(A_2) \geq \begin{cases} -2p^2, & \text{if } p \equiv 1 \pmod 4, \\ -2p^2 - 2p, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

$$\nu_b(B_2) \geq \begin{cases} -p^2, & \text{if } p \equiv 1 \pmod 4, \\ -p^2 - 2p, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. We start with the case of $p \equiv 3 \pmod 4$. Since in this case we have, by Theorem 2.2, that

$$J_2(X) = \frac{F_2(X)}{(X-1728)^p S_p(X)^{2p+1}},$$

and $S_p(1728) \neq 0$, we get $\nu_b(J_2(j)) = -2p$. We will keep the notation from Eqs. (4.1) to (4.6).

Clearly $\nu_b(\alpha_0) = 0$ and $\nu_b(\alpha_1), \nu_b(\alpha_2) \geq 0$. Also, clearly we have $\nu_b(j) = 0$ and $\nu_b(u_0) = 2$, and by Theorem 2.3 we also have that $\nu_b(J_1(j)) \geq 0$ and $\nu_b(u_1) \geq p - 1$.

Moreover, u_2 equals $-J_2(j)$ plus terms of the form $j^\alpha J_1(j)^\beta \alpha_0^{\gamma_0} \alpha_1^{\gamma_1} \alpha_2^{\gamma_2}$. Since $\nu_b(-J_2(j)) = -2p$, and $\nu_b(j^\alpha J_1(j)^\beta \alpha_0^{\gamma_0} \alpha_1^{\gamma_1} \alpha_2^{\gamma_2}) \geq 0$, we have $\nu_b(u_2) = -2p$.

We now turn to $(1728 - \boldsymbol{j})^{-1}$. We clearly have that $\nu_b(v_0) = -2$ and $v_1 = -u_1/u_0^{2p}$, and hence $\nu_b(v_1) \geq -3p - 1$. Also, v_2 equals $u_0^{-p^2}$ times the sum of $u_2 v_0^{p^2}$ and terms of the form $v_0^\alpha v_1^\beta u_0^\gamma u_1^\delta$, where $\alpha + \beta p = \gamma + \delta p = p^2$. Hence $\beta, \delta \leq p$. We have $\nu_b(u_2 v_0^{p^2}) = -2p - 2p^2$, and

$$\begin{aligned} \nu_b(v_0^\alpha v_1^\beta u_0^\gamma u_1^\delta) &\geq -2\alpha + (-3p-1)\beta + 2\gamma + (p-1)\delta \\ &= -2p^2 + (-p-1)\beta + 2p^2 + (-p-1)\delta \\ &\geq -2p - 2p^2. \end{aligned}$$

So, $\nu_b(v_2) \geq -2p - 4p^2$.

Turning to $27/(4(1728-\boldsymbol{j}))$, we note that clearly $\nu_b(\beta_0)=0$, $\nu_b(\beta_1)$, $\nu_b(\beta_2)\geq 0$, $\nu_b(w_0)=\nu_b(\beta_0)+\nu_b(v_0)=-2$, $w_1=v_0^p\beta_1+\beta_0^p v_1$, and hence $\nu_b(w_1)\geq -3p-1$.

Also, w_2 equals $\beta_0^{p^2}v_2+\beta_2 v_0^{p^2}$ plus terms of the form $v_0^\alpha v_1^\beta \beta_0^\gamma \beta_1^\delta$ where $\alpha+\beta p=p^2$. From our work above we have $\nu_b(\beta_0^{p^2}v_2)\geq -2p-4p^2$, $\nu_b(\beta_2 v_0^{p^2})\geq -2p^2$, and

$$\begin{aligned}\nu_b(v_0^\alpha v_1^\beta \beta_0^\gamma \beta_1^\delta) &\geq -2\alpha+(-3p-1)\beta\\ &= -2p^2+(-p-1)\beta\\ &\geq -3p^2-p.\end{aligned}$$

So, $\nu_b(w_2)\geq -2p-4p^2$.

Finally, we turn to $27\boldsymbol{j}/(4(1728-\boldsymbol{j}))$. We have that z_2 equals $w_2 j^{p^2}+w_0^{p^2}J_2(j)$ plus terms of the form $w_0^\alpha w_1^\beta j^\gamma J_1(j)^\delta$, where $\alpha+\beta p=p^2$. We have $\nu_b(w_2 j^{p^2})\geq -2p-4p^2$, $\nu_b(w_0^{p^2}J_2(j))=-2p-2p^2$, and since $\nu_b(J_1(j))\geq 0$,

$$\nu_b(w_0^\alpha w_1^\beta j^\gamma J_1(j)^\delta)\geq -2\alpha+(-3p-1)\beta\geq -3p^2-p.$$

So, $\nu_b(z_2)\geq -2p-4p^2$. Hence, $\nu_b(A_2)=\nu_b(z_2)+2p^2\geq -2p-2p^2$, and $\nu_b(B_2)=\nu_b(z_2)+3p^2\geq -2p-p^2$.

We now look at the case when $p\equiv 1 \pmod 4$. Again, by Theorem 2.2, in this case we have

$$J_2(X)=\frac{F_2(X)}{S_p(X)^{2p+1}},$$

and since $S_p(1728)\neq 0$, we have $\nu_b(J_2(j))\geq 0$.

As before, we have $\nu_b(\alpha_0)=0$, $\nu_b(\alpha_1),\nu_b(\alpha_2)\geq 0$, $\nu_b(u_0)=2$. But now, by Theorem 2.3, $\nu_b(u_1)\geq p+1$. Also, $\nu_b(u_2)\geq 0$, since the valuations of 1728 and $\boldsymbol{j}$ are all non-negative.

We then clearly have that $\nu_b(v_0)=-2$ and $\nu_b(v_1)=\nu_b(-u_1/u_0^{2p})\geq -3p+1$. Also, v_2 equals $u_0^{-p^2}$ times the sum of $u_2 v_0^{p^2}$ and terms of the form $v_0^\alpha v_1^\beta u_0^\gamma u_1^\delta$. We have $\nu_b(u_2 v_0^{p^2})\geq -2p^2$, and

$$\begin{aligned}\nu_b(v_0^\alpha v_1^\beta u_0^\gamma u_1^\delta) &\geq -2\alpha+(-3p+1)\beta+2\gamma+(p+1)\delta\\ &= -2p^2+(-p+1)\beta+2p^2+(-p+1)\delta\\ &\geq -2p^2+2p.\end{aligned}$$

So, $\nu_b(v_2)\geq -4p^2$.

We also have $\nu_b(\beta_0) = 0$, $\nu_b(\beta_1), \nu_b(\beta_2) \geq 0$, $\nu_b(w_0) = -2$, and since $w_1 = v_0^p \beta_1 + \beta_0^p v_1$, we have $\nu_b(w_1) \geq -3p + 1$.

Also, w_2 equals $\beta_0^{p^2} v_2 + \beta_2 v_0^{p^2}$ plus terms of the form $v_0^\alpha v_1^\beta \beta_0^\gamma \beta_1^\delta$. We have $\nu_b(\beta_0^{p^2} v_2) \geq -4p^2$, $\nu_b(\beta_2 v_0^{p^2}) \geq -2p^2$, and

$$\begin{aligned} \nu_b(v_0^\alpha v_1^\beta \beta_0^\gamma \beta_1^\delta) &\geq -2\alpha + (-3p+1)\beta \\ &= -2p^2 + (-p+1)\beta \\ &\geq -3p^2 + p. \end{aligned}$$

So, $\nu_b(w_2) \geq -4p^2$.

Next, z_2 equals $w_2 j^{p^2} + w_0^{p^2} J_2(j)$ plus terms of the form $w_0^\alpha w_1^\beta j^\gamma J_1(j)^\delta$. Since $\nu_b(w_2 j^{p^2}) \geq -4p^2$, $\nu_b(w_0^{p^2} J_2(j)) \geq -2p^2$, and

$$\nu_b(w_0^\alpha w_1^\beta j^\gamma J_1(j)^\delta) \geq -2\alpha + (-3p+1)\beta \geq -3p^2 + p,$$

we have $\nu_b(z_2) \geq -4p^2$. Hence, $\nu_b(A_2) \geq -2p^2$, and $\nu_b(B_2) \geq -p^2$. □

Computations show that the bounds from the theorem are sharp for $p = 7, 11$, the cases when $p \equiv 3 \pmod 4$. On the other hand, the bounds are *not* sharp for $p = 5, 13, 17$, the cases when $p \equiv 1 \pmod 4$. That is due to the lack of information about $\nu_b(u_2)$ in this case. The computations for these concrete examples in this case actually give that $\nu_b(u_2) = 2p$, while in our proof we are only able to state that $\nu_b(u_2) \geq 0$.

On the other hand, we were able to show that $\nu_b(u_2) = -2p$ for the cases when $p \equiv 3 \pmod 4$, thus obtaining better bounds.

Acknowledgments. The computations mentioned were done with MAGMA or Sage.

References

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

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

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

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

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

[Fin20] L. R. A. Finotti. Weierstrass coefficients of the canonical lifting. *International Journal of Number Theory*, 16(02):397–422, 2020.

[FL20] L. R. A. Finotti and D. Li. Denominator of the weierstrass coefficients of the canonical lifting, 2020. Available at `sites.google.com/vols.utk.edu/delongli/home`.

[FL21] L. R. A. Finotti and D. Li. The discriminant in universal formulas for the canonical lifting. *Bulletin des Sciences Mathématiques*, 169:102981, 2021.

[Jac84] N. Jacobson. *Basic Algebra*, volume 2. W. H. Freeman and Company, second edition, 1984.

[Li20] Delong Li. *Denominators of the Weierstrass Coefficients of the Canonical Lifting*. PhD thesis, University of Tennessee at Knoxville, 2020.

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

[Ser79] J-P. Serre. *Local Fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.

Department of Mathematics, University of Tennessee, Knoxville, TN, 37996

Email address: `lfinotti@utk.edu`

URL: `www.math.utk.edu/~finotti`

Beijing Institute of Mathematical Sciences and Applications, Beijing, 101408

Email address: `delongli24@163.com`

URL: `sites.google.com/vols.utk.edu/delongli/home`