COORDINATES OF THE j-INVARIANT OF THE CANONICAL LIFTING

LUÍS R. A. FINOTTI

Abstract. Let $j_0 \mapsto (j_0, J_1(j_0), J_2(j_0), \ldots)$ be the map that takes the j-invariant of an ordinary elliptic curve in characteristic p to the j-invariant of its canonical lifting over the ring of Witt vectors. We have that $J_i \in \mathbb{F}_p(X)$, and in this paper we describe how to derive these rational functions from the modular polynomial in an efficient way and give more precise description of the numerators and denominators of the reduced forms of these functions. In particular, upper bounds are given for the order of their poles.

1. Introduction

Let $\Bbbk$ be a perfect field of characteristic $p > 0$ and $\boldsymbol{W}(\Bbbk)$ be the ring of Witt vectors over $\Bbbk$. Then, given an ordinary elliptic curve $E/\Bbbk$, there is a unique elliptic curve (up to isomorphism), say $\boldsymbol{E}/\boldsymbol{W}(\Bbbk)$, which reduces to E modulo p and for which we can lift the Frobenius. $\boldsymbol{E}$ is then called the *canonical lifting* of E. (See, for instance, [2] or [12].) Hence, given an ordinary j-invariant $j_0 \in \Bbbk$, the canonical lifting gives us a unique $\boldsymbol{j} \in \boldsymbol{W}(\Bbbk)$. Therefore, if $\Bbbk^{ord}$ denotes the set of ordinary values of j-invariants in $\Bbbk$, then we have functions $J_i : \Bbbk^{ord} \to \Bbbk$, for $i = 1, 2, 3, \ldots$, such that the j-invariant of the canonical lifting of an elliptic curve with j-invariant $j_0 \in \Bbbk^{ord}$ is $(j_0, J_1(j_0), J_2(j_0), \ldots)$.

B. Mazur asked about the nature of these functions J_i. Partial answers were given in [4], [6], and [7]. Before we can quote the main results of these references, we need a little more notation.

Let

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

where

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

is the *supersingular polynomial* (as in, for instance, [3]),

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

2000 *Mathematics Subject Classification.* Primary 11G07; Secondary 11Y99.

Key words and phrases. elliptic curves, canonical lifting, j-invariant, modular polynomial.

Hence, $S_p(X) \in \mathbb{F}_p[X]$, and $S_p(0), S_p(1728) \neq 0$. (See, for instance, [3].) Also, let

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

In [4], [6], and [7], the following results were proven:

Theorem 1.1. *We have $J_i(X) \in \mathbb{F}_p(X)$. More precisely, if $p \geq 5$, $J_i = F_i/G_i$, with $F_i, G_i \in \mathbb{F}_p[X]$, $(F_i, G_i) = 1$, G_i monic, and $r_i = (i-1)p^{i-1}$, then, for $i \in \{1,2,3\}$, we have:*

(1) $\deg F_i - \deg G_i = p^i - \iota$;
(2) $G_i = S_p(X)^{ip^{i-1}+(i-1)p^{i-2}} \cdot H_i$, *where* $H_1 = 1$, $H_2 = (X-1728)^{\epsilon r_2}$, *and* $H_3 = X^{\delta p^2} \cdot (X-1728)^t$ *for some* $t \in \{0, \dots, \epsilon r_3\}$.

Also, in the above references, explicit and "simplified" (in a sense to be made precise later) expressions for J_i based on the modular polynomial $\Phi_p(X,Y)$, for $i \in \{1,2,3\}$ are given. (In fact, the above theorem is derived from these expressions.) The main goals here are to extend the theorem above for $i > 3$ and give a general simplified expression for J_n. Although we need some more notation to give this expression, which is done in Section 3, we can state now the generalization of Theorem 1.1:

Theorem 1.2. *Let $p \geq 5$, $J_i = F_i/G_i$, with $F_i, G_i \in \mathbb{F}_p[X]$, $(F_i, G_i) = 1$, and G_i monic. Also, let $r_i = (i-1)p^{i-1}$, $s_i = ((i-3)p^i + ip^{i-1})/3$ and $s_i' = \max\{0, s_i\}$. Then, for* all *$i \in \mathbb{Z}_{>0}$ we have:*

(1) $\deg F_i - \deg G_i = p^i - \iota$;
(2) $G_i = S_p(X)^{ip^{i-1}+(i-1)p^{i-2}} \cdot H_i$, *where* $H_i \mid X^{\delta s_i'} \cdot (X-1728)^{\epsilon r_i}$.

It should be observed that, unlike for $i = 1, 2$, we don't have an exact formula for H_i. In fact, it is not hard to see that if $\delta = 1$ and $i > 3$, then we actually have that the pole of J_i at $X = 0$ of order strictly less than s_i. For poles at $X = 1728$, examples show that the orders of poles seem also to be always strictly less than r_i if $i > 2$ and $\epsilon = 1$. So, there still some room for improvement.

We now give a brief description of the following sections. In Section 2 we review the Greenberg transform and give a formula for it, as derived in [5]. (Quite a bit of notation is introduced in this section.) In Section 3 we apply the formula for the Greenberg transform to obtain the desired formula for J_n. In Section 4 we introduce some lemmas that will help with the proof of Theorem 1.2, while in Sections 5 and 6 we prove items 1 and 2, respectively, from the theorem.

2. The Greenberg Transform

The Greenberg transform is crucial to the proof of the main results. In this section we briefly review it. (See also [10] and [8].) We will assume throughout that $\mathbb{k}$ is a perfect field of characteristic p.

Definition 2.1. Let $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{W}(\mathbb{k})[\boldsymbol{x}, \boldsymbol{y}]$. If we replace $\boldsymbol{x}$ and $\boldsymbol{y}$ by $(x_0, x_1, \ldots)$ and $(y_0, y_1, \ldots)$, seen as Witt vectors of unknowns, and expand the resulting expression using sums and products of Witt vectors, we obtain a Witt vector $(f_0, f_1, \ldots)$, with $f_i \in \mathbb{k}[x_0, \ldots, x_i, y_0, \ldots, y_i]$. This resulting vector is called the *Greenberg transform* of $\boldsymbol{f}$ and will be denoted by $\mathscr{G}(\boldsymbol{f})$.

Moreover, if

$$\boldsymbol{C}/\boldsymbol{W}(\mathbb{k}) \ : \ \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) = \boldsymbol{0},$$

we define the *Greenberg transform* $\mathscr{G}(\boldsymbol{C})$ of $\boldsymbol{C}$ to be the (infinite dimensional) variety over $\mathbb{k}$ defined by the zeros of the coordinates of $\mathscr{G}(\boldsymbol{f})$.

It is clear from the definition that there is a bijection between $\boldsymbol{C}(\boldsymbol{W}(\mathbb{k}))$ and $\mathscr{G}(\boldsymbol{C})(\mathbb{k})$.

In [5] a formula for the Greenberg transform is given. Although rather involved, it will be our main tool. Before we can give this formula, quite a bit of notation is necessary.

We start with some notation regarding Witt vectors.

Definition 2.2.

1. We denote by π the *reduction modulo p map*, i.e., $\pi((a_0, a_1, \ldots)) = a_0$.
2. Let $a \in \mathbb{k}$. Then, the *Teichmüller lift* of a is the Witt vector $\tau(a) \stackrel{\text{def}}{=} (a, 0, 0, \ldots)$. (Hence, τ is a section of π and when restricted to $\mathbb{k}^\times$ yields a group homomorphism.)
3. Define $\tau(\mathbb{k}) \stackrel{\text{def}}{=} \{(a_0, 0, 0, \ldots) \in \boldsymbol{W}(\mathbb{k}) \ : \ a_0 \in \mathbb{k}\}$. (This is a multiplicative set. E.g., if $\mathbb{k} = \mathbb{F}_q$, than $\tau(\mathbb{k})$ is made of all $(q-1)$-th roots of unity and zero.)
4. Let $\boldsymbol{a} \in \boldsymbol{W}(\mathbb{k})$. Define $\xi_k(\boldsymbol{a})$, for $k \in \mathbb{Z}_{\geq 0}$, as the *unique* element of $\tau(\mathbb{k})$ such that $\boldsymbol{a} = \sum_{k=0}^{\infty} \xi_k(\boldsymbol{a}) p^k$. (This is well defined since $\boldsymbol{W}(\mathbb{k})$ is a strict p-ring and $\tau(\mathbb{k})$ is a complete set of representatives of $\mathbb{k} = \boldsymbol{W}(\mathbb{k})/(p)$ in $\boldsymbol{W}(\mathbb{k})$.)

With the notation above, we have

$$\boldsymbol{a} = \sum_{k=0}^{\infty} \xi_k(\boldsymbol{a}) p^k = (\pi(\xi_0(\boldsymbol{a})), \pi(\xi_1(\boldsymbol{a}))^p, \pi(\xi_2(\boldsymbol{a}))^{p^2}, \ldots) \tag{2.1}$$

and

$$(a_0, a_1, \ldots) = \sum_{k=0}^{\infty} \tau(a_k)^{1/p^k} p^k. \tag{2.2}$$

(Remember we are assuming that $\mathbb{k}$ is perfect.)

We shall also need some auxiliary recursively defined functions.

Definition 2.3. Let p be a prime. Define $\eta_0(X_1, \dots, X_r) \stackrel{\text{def}}{=} X_1 + \cdots + X_r \in \mathbb{Q}[X_1, \dots, X_r]$, and recursively for $k \geq 1$

$$\eta_k(X_1, \dots, X_r) \stackrel{\text{def}}{=} \frac{X_1^{p^k} + \cdots + X_r^{p^k}}{p^k} - \sum_{i=0}^{k-1} \frac{\eta_i(X_1, \dots, X_r)^{p^{k-i}}}{p^{k-i}}. \tag{2.3}$$

Also, define $\eta_k(X_1) = 0$ for $k \geq 1$.

By Corollary 5.7 from [5], we have that $\eta_i(X_1, \dots, X_r) \in \mathbb{Z}[X_1, \dots, X_r]$ for all i.

Definition 2.4. If $\boldsymbol{g} \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$ is given by $\boldsymbol{g} = \sum_{i,j} \boldsymbol{a}_{i,j} \boldsymbol{x}^i \boldsymbol{y}^j$, then we write

$$\xi_k(\boldsymbol{g}) \stackrel{\text{def}}{=} \sum_{i,j} \xi_k(\boldsymbol{a}_{i,j}) \boldsymbol{x}^i \boldsymbol{y}^j,$$

with ξ_k as in Definition 2.2. (Hence, $\boldsymbol{g} \equiv \sum_{k=0}^{r} \xi_k(\boldsymbol{g}) p^k \pmod{p^{r+1}}$.) Furthermore, define

$$\boldsymbol{g}^{(i,j)} \stackrel{\text{def}}{=} \frac{1}{i!j!} \frac{\partial^{i+j}}{\partial \boldsymbol{x}^i \partial \boldsymbol{y}^j} \boldsymbol{g} \quad \text{and} \quad \boldsymbol{g}_{i,j,k} \stackrel{\text{def}}{=} \xi_k(\boldsymbol{g}^{(i,j)}).$$

Definition 2.5. We define $D_{k,n}^{i,j}$ to be the coefficient of $\boldsymbol{t}^k$ in

$$(\boldsymbol{t}\boldsymbol{x}_1^{p^{n-1}} + \boldsymbol{t}^2 \boldsymbol{x}_2^{p^{n-2}} + \cdots + \boldsymbol{t}^n \boldsymbol{x}_n)^i (\boldsymbol{t}\boldsymbol{y}_1^{p^{n-1}} + \boldsymbol{t}^2 \boldsymbol{y}_2^{p^{n-2}} + \cdots + \boldsymbol{t}^n \boldsymbol{y}_n)^j.$$

(E.g., if $n \geq 2$, then $D_{4,n}^{1,2} = 2\boldsymbol{x}_1^{p^{n-1}} \boldsymbol{y}_1^{p^{n-1}} \boldsymbol{y}_2^{p^{n-2}} + \boldsymbol{x}_2^{p^{n-2}} \boldsymbol{y}_1^{2p^{n-1}}$.) Furthermore, we shall denote

$$D_{k,n,l}^{i,j} \stackrel{\text{def}}{=} \xi_l(D_{k,n}^{i,j}).$$

Note that if $k < r$ (and $r \geq i$), then $D_{k,n}^{i,r-i} = 0$ and if $k \neq 0$, then $D_{k,n}^{0,0} = 0$.

Definition 2.6. If $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ are finite vectors, we denote by $\boldsymbol{v}_1 \odot \boldsymbol{v}_2$ the concatenation of these vectors, i.e.,

$$(a_1, \dots, a_m) \odot (b_1, \dots, b_n) = (a_1, \dots, a_m, b_1, \dots, b_n).$$

Moreover, if f is a polynomial (possibly in many variables), we write $\operatorname{vec}(f)$ for the vector that contains the terms of f (after some choice of order for the monomials). It is important to observe that we are assuming that the terms are reduced, i.e., if $f = 1 + X + 2X$, then $\operatorname{vec}(f) = (1, 3X)$, not $(1, X, 2X)$.

Definition 2.7. Let $\boldsymbol{f} \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}_0, \boldsymbol{y}_0]$. Then, for a given $n \geq 0$, let

$$(\mathcal{G}_{n,1}, \dots, \mathcal{G}_{n,N_n}) \stackrel{\text{def}}{=} \bigodot_{r=0}^{n} \bigodot_{i=0}^{r} \bigodot_{j=r}^{n} \bigodot_{k=r}^{j} \operatorname{vec}\left((\boldsymbol{f}^{\sigma^n})_{i,r-i,n-j} (\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) D_{k,n,j-k}^{i,r-i} \right).$$

(The ordering of the concatenations is not important.) Also, recursively, if $n > 1$, define

$$\mathcal{G}_{n,N_n+i+1} \stackrel{\text{def}}{=} \eta_{n-i}(\mathcal{G}_{i,1}, \dots, \mathcal{G}_{i,N_i+i}),$$

for $i \in \{0, \ldots, (n-1)\}$. Then, define,

$$\boldsymbol{f}_n \stackrel{\text{def}}{=} \sum_{i=1}^{N_n+n} \mathcal{G}_{n,i},$$

and $\mathcal{G}_n \stackrel{\text{def}}{=} (\mathcal{G}_{n,1}, \ldots, \mathcal{G}_{n,N_n+n})$.

Then, with the notation above, Theorem 6.4 from [5] gives the desire formula for the Greenberg transform:

Theorem 2.8. *With the notation above, we have that $\mathscr{G}(\boldsymbol{f}) = (f_0, f_1, \ldots)$, where f_n is the reduction modulo p of*

$$\boldsymbol{f}_n = \sum_{i=1}^{N_n+n} \mathcal{G}_{n,i} = \sum_{r=0}^{n} \sum_{i=0}^{r} \sum_{j=r}^{n} \sum_{k=r}^{j} (\boldsymbol{f}^{\sigma^n})_{i,r-i,n-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) D_{k,n,j-k}^{i,r-i} + \sum_{i=0}^{n-1} \eta_{n-i}(\mathcal{G}_i). \tag{2.4}$$

3. A Simplified Formula for J_n

By Theorem 3 of [12], we have that if $(j_0, J_1, J_2, \ldots)$ is the j-invariant of the canonical lifting of the curve with j-invariant j_0, then

$$\Phi_p((j_0, J_1, J_2, \ldots), (j_0^p, J_1^p, J_2^p, \ldots)) = 0, \tag{3.1}$$

where $\Phi_p(X, Y)$ is the (classical) modular polynomial. Together with the formula for the Greenberg transform (Theorem 2.8 above), one can immediately deduce a formula for J_n (in terms of the modular polynomial). On the other hand, we need some improvements in this first immediate formula.

So, from now on we will let $\boldsymbol{f} = \Phi_p$. We will use the notation $\mathcal{G}_{n,i}$ and $\mathcal{G}_n$ associated with this particular choice of $\boldsymbol{f}$.

Definition 3.1. For a given $n \geq 0$, let $\mathcal{H}_n = (\mathcal{H}_{n,1}, \ldots, \mathcal{H}_{n,N_n}) \stackrel{\text{def}}{=} (\mathcal{G}_{n,1}, \ldots, \mathcal{G}_{n,N_n})$ and

$$\boldsymbol{h}_n = \sum_{i=1}^{N_n} \mathcal{H}_{n,i} = \sum_{r=0}^{n} \sum_{i=0}^{r} \sum_{j=r}^{n} \sum_{k=r}^{j} (\boldsymbol{f}^{\sigma^n})_{i,r-i,n-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) D_{k,n,j-k}^{i,r-i}.$$

Also, let h_n be the reduction modulo p of $\boldsymbol{h}_n$ and we shall use the over bar to denote further reductions modulo p, e.g., $\bar{\mathcal{H}}_n$ denotes the reduction modulo p of $\mathcal{H}_n$.

The following theorem gives the desired simplification.

Theorem 3.2. *Let $p \geq 3$ and*

$$\begin{aligned}\bar{\mathcal{J}}_{i,1}^{(l)} &\stackrel{\text{def}}{=} \eta_i(\bar{\mathcal{H}}_l)\\ \bar{\mathcal{J}}_{i,2}^{(l)} &\stackrel{\text{def}}{=} \eta_i(\eta_{l-1}(\bar{\mathcal{G}}_1), \dots, \eta_1(\bar{\mathcal{G}}_{l-1}))\\ \bar{\mathcal{J}}_{i,3}^{(l)} &\stackrel{\text{def}}{=} \eta_i(h_l, \eta_{l-1}(\bar{\mathcal{G}}_1) + \cdots + \eta_1(\bar{\mathcal{G}}_{l-1})).\end{aligned}$$

For $i > 1$, let for $j \in \{1, \dots, (i-1)\}$,

$$\bar{\mathcal{J}}_{i,3+j}^{(l)} \stackrel{\text{def}}{=} \eta_j(\bar{\mathcal{J}}_{i-j,1}^{(l)}, \dots, \bar{\mathcal{J}}_{i-j,i-j+2}^{(l)}).$$

Then, $\eta_i(\bar{\mathcal{G}}_l) \equiv \sum_{j=1}^{i+2} \bar{\mathcal{J}}_{i,j}^{(l)} \pmod{x_0^p - y_0}$. In particular, $\eta_i(\bar{\mathcal{G}}_1) \equiv \eta_i(\bar{\mathcal{H}}_1) \pmod{x_0^p - y_0}$ for all $i \geq 1$.

Note that the congruences above will actually yield equalities when we replace $x_i = J_i$ and $y_i = J_i^p$, as necessary when using Eq. (3.1).

This theorem is a consequence of the Proposition 5.4 from [5], which we state below:

Proposition 3.3. *Let $v = (a_1, \dots, a_m)$ and $w = (b_1, \dots, b_n)$. For any $i \geq 1$, let*

$$\mathcal{M}_{i,1} = \eta_i(v), \qquad \mathcal{M}_{i,2} = \eta_i(w),$$
$$\mathcal{M}_{i,3} = \eta_i(a_1 + \cdots + a_m, b_1 + \cdots + b_n),$$

and, recursively for $i > 1$, define

$$\mathcal{M}_{i,3+j} = \eta_j(\mathcal{M}_{i-j,1}, \dots, \mathcal{M}_{i-j,i-j+2})$$

for $j \in \{1, \dots, i-1\}$. Then,

$$\eta_i(v \odot w) = \sum_{j=1}^{i+2} \mathcal{M}_{i,j}.$$

We can now prove the Theorem:

Proof of Theorem 3.2. Firstly, by Lemma 5.1 from [7], since $p \geq 3$ we have that $\eta_i(\bar{\mathcal{G}}_0) \equiv 0 \pmod{x_0^p - y_0}$ for all $i \geq 1$.

Let $v = \bar{\mathcal{H}}_l$ and $w = (\eta_l(\bar{\mathcal{G}}_0), \dots, \eta_1(\bar{\mathcal{G}}_{l-1}))$. Then, we have that $\bar{\mathcal{G}}_l = v \odot w$.

By Proposition 3.3, it suffices to prove that $\bar{\mathcal{J}}_{j,k}^{(l)} \equiv \mathcal{M}_{j,k} \pmod{x_0^p - y_0}$ (with $\mathcal{M}_{j,k}$ from Proposition 3.3 with our v and w above). We prove this by induction on i.

Since $\eta_l(\bar{\mathcal{G}}_0) \equiv 0 \pmod{x_0^p - y_0}$, we have $\mathcal{M}_{i,j} \equiv \bar{\mathcal{J}}_{i,j}^{(l)}$ for $j \in \{1, 2, 3\}$ for any i. In particular, the statement immediately follows for $i = 1$.

Now, if $\bar{\mathcal{J}}_{j,k}^{(l)} \equiv \mathcal{M}_{j,k} \pmod{x_0^p - y_0}$ for $j < i$, then for $j \in \{1, \dots, (i-1)\}$ we have

$$\mathcal{M}_{i,3+j} = \eta_j(\mathcal{M}_{i-j,1}, \dots, \mathcal{M}_{i-j,i-j+2}) \equiv \eta_j(\bar{\mathcal{J}}_{i-j,1}^{(l)}, \dots, \bar{\mathcal{J}}_{i-j,i-j+2}^{(l)}) = \bar{\mathcal{J}}_{i,3+j}^{(l)} \pmod{x_0^p - y_0},$$

which finishes the proof. $\square$

We introduce some more notation.

Definition 3.4. We define:

(1) If $\boldsymbol{g}(\boldsymbol{x}_0, \boldsymbol{y}_0) \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}_0, \boldsymbol{y}_0]$, then we denote by $g_{i,j,k}$ the reduction modulo p of $\boldsymbol{g}_{i,j,k}$ (with the notation of Definition 2.4).

(2) Given a polynomial $f \in \Bbbk[x_0, , \ldots, x_n, y_0, \ldots, y_n]$, we shall write f' for $f(J_0, \ldots, J_n, J_0^p, \ldots, J_n^p)$. (E.g., $\bar{\mathcal{G}}'_{i,j}$ is the value of $\bar{\mathcal{G}}_{i,j}$ when x_t is replaced by J_t and y_t is replaced by J_t^p for all t.)

(3) We denote by $E_{k,n,l}^{i,j}$ the evaluation of the reduction modulo p of $D_{k,n,l}^{i,j}$ (as in Definition 2.5) when x_t is replaced by $J_t(X)$ and y_t is replaced by $J_t(X)^p$.

(4) Let $\bar{\mathcal{I}}_{i,j} \stackrel{\text{def}}{=} \eta_i(\bar{\mathcal{G}}'_j)$.

We can now give the formula for J_n.

Theorem 3.5. *Let $p \geq 3$, $\boldsymbol{f} = \Phi_p$, and*

$$
\begin{aligned}
I_n \stackrel{\text{def}}{=} f_{0,0,n}(X^{p^n}, X^{p^{n+1}}) + \sum_{j=1}^{n-1} f_{0,1,n-j}(X^{p^n}, X^{p^{n+1}}) J_j^{p^{n-j+1}} \\
\sum_{j=1}^{n-1} f_{1,0,n-j}(X^{p^n}, X^{p^{n+1}}) J_j^{p^{n-j}} - \sum_{k=2}^{n} E_{k,n,n-k}^{1,1} + \\
\sum_{r=2}^{n-1} \sum_{i=0}^{r} \sum_{j=r}^{n-1} \sum_{k=r}^{j} f_{i,r-i,n-j}(X^{p^n}, X^{p^{n+1}}) E_{k,n,j-k}^{i,r-i}. \quad (3.2)
\end{aligned}
$$

Then, we have

$$J_n^p = -\frac{1}{(X^{p^2} - X)^{p^n}} \left[I_n + \sum_{i=0}^{n-1} \bar{\mathcal{I}}_{n-i,i} \right]. \quad (3.3)$$

(Note that this formula is simplified if one uses Theorem 3.2 to compute $\sum_{i=0}^{n-1} \bar{\mathcal{I}}_{n-i,i}$.)

Proof. By Eq. (3.1), we just need to apply Theorem 2.8 to $\Phi_p((j_0, J_1, \ldots), (j_0^p, J_1^p, \ldots))$.

First, observer that since $\boldsymbol{f}$ has integral coefficients, we have that $\boldsymbol{f}^{\sigma^n} = \boldsymbol{f}$. Then, evaluating $\boldsymbol{f}_n$ (from Theorem 2.8) at $\boldsymbol{x} = (X, J_1(X), \ldots)$ and $\boldsymbol{y} = (X^p, J_1(X)^p, \ldots)$ and reducing modulo p, we obtain

$$\sum_{r=0}^{n} \sum_{i=0}^{r} \sum_{j=r}^{n} \sum_{k=r}^{j} f_{i,r-i,n-j}(X^{p^n}, X^{p^{n+1}}) E_{k,n,j-k}^{i,r-i} + \sum_{i=0}^{n-1} \bar{\mathcal{I}}_{n-i,i} = 0. \quad (3.4)$$

When $r = 0$, the first sum of (3.4) gives only the term $f_{0,0,n}(X^{p^n}, X^{p^{n+1}})$, since $D_{k,n,j-k}^{0,0} = 0$ if $k \neq 0$, or if $k = 0$ and $j \neq k$. So, the part of Eq. (3.4) from $r = 0$ is only $f_{0,0,n}(X^{p^n}, X^{p^{n+1}})$.

We now look at $r=1$. We have that $D^{0,1}_{k,n} = \boldsymbol{y}_k^{p^{n-k}}$ and $D^{1,0}_{k,n} = \boldsymbol{x}_k^{p^{n-k}}$. So, $D^{0,1}_{k,n,0} = \boldsymbol{y}_k^{p^{n-k}}$, $D^{1,0}_{k,n,0} = \boldsymbol{x}_k^{p^{n-k}}$, and $D^{0,1}_{k,n,j-k} = D^{1,0}_{k,n,j-k} = 0$ if $k<j$. So, the terms with $r=1$ from the first (nested) sum of Eq. (3.4) are

$$\sum_{j=1}^{n} f_{0,1,n-j}(X^{p^n}, X^{p^{n+1}}) J_j^{p^{n-j+1}} + \sum_{j=1}^{n} f_{1,0,n-j}(X^{p^n}, X^{p^{n+1}}) J_j^{p^{n-j}}. \tag{3.5}$$

For $j=n$ we get the terms involving J_n. By Kronecker's relation (i.e., $f(X,Y) = (X^p - Y)(X - Y^p)$), we get that $f_{0,1,0}(X^{p^n}, X^{p^{n+1}}) = (X^{p^2} - X)^{p^n}$ and $f_{1,0,0}(X^{p^n}, X^{p^{n+1}}) = 0$. So, Eq. (3.5) is equal to

$$(X^{p^2} - X)^{p^n} J_n^p + \sum_{j=1}^{n-1} f_{0,1,n-j}(X^{p^n}, X^{p^{n+1}}) J_j^{p^{n-j+1}} + \sum_{j=1}^{n-1} f_{1,0,n-j}(X^{p^n}, X^{p^{n+1}}) J_j^{p^{n-j}}. \tag{3.6}$$

We now look at $r=2$. First, observe that $f_{0,2,0} = f_{2,0,0} = 0$, and $f_{1,1,0} = -1$. So, the term with $r=2$ in the first sum of Eq. (3.4) is:

$$\sum_{i=0}^{2}\sum_{j=2}^{n-1}\sum_{k=2}^{j} f_{i,2-i,n-j}(X^{p^n}, X^{p^{n+1}}) E^{i,2-i}_{k,n,j-k} - \sum_{k=2}^{n} E^{1,1}_{k,n,n-k}. \tag{3.7}$$

Finally, for $r \geq 3$, we have that $f_{i,r-i,0} = 0$ for all r and i in their given ranges. Thus, the part with $r \geq 3$ of Eq. (3.4) is:

$$\sum_{r=3}^{n}\sum_{i=0}^{r}\sum_{j=r}^{n-1}\sum_{k=r}^{j} f_{i,r-i,n-j}(X^{p^n}, X^{p^{n+1}}) E^{i,r-i}_{k,n,j-k}. \tag{3.8}$$

The result now easily follows. □

It should be noted that, with the observation about the simplification in the statement, Theorem 3.5 is the generalization of the formulas for J_i for $i = 1, 2, 3$, given in [4], by Theorem 9.1 from [6], and by Theorem 5.5 from [7] respectively. As observed in this last reference, great gains are indeed obtained in computations when using the simplifications of Theorem 3.2. (On the other hand, note also that, with Theorem 1.2, one can also compute the J_n's using interpolation.)

4. Some Lemmas

In this section we will introduce some lemmas necessary for the proof of Theorem 1.2.

The proof of is done by looking at order of zeros and poles of J_n. Hence, we need to look at valuations of the terms that appear in Eq. (3.3). Clearly the most troublesome part is $\sum_{i=0}^{n-1} \bar{\jmath}_{n-i,i}$. The next two lemmas help us deal with those.

Lemma 4.1. *Let* v *be a valuation on* $\mathbb{F}_p(X)$ *such that* $\mathrm{v}(a) = 0$ *for all* $a \in \mathbb{F}_p^\times$*. Then, if* $v_0 < 0$ *and* $v \stackrel{\text{def}}{=} (a_1, \ldots, a_n) \in \mathbb{F}_p(X)^n$ *with* $\mathrm{v}(a_i) \geq v_0$ *for all* i*, we have that* $\mathrm{v}(\eta_j(v)) > p^j v_0$ *for* $j \geq 1$*.*

Proof. From definition of η_j, a simple induction gives that, for $j \geq 1$, the polynomial $\eta_j(X_1, \ldots, X_r)$ has degree on each variable X_i strictly less than p^j. The lemma then easily follows. □

Lemma 4.2. *Let* $p \geq 3$ *and* v *be a valuation on* $\mathbb{F}_p(X)$ *such that* $\mathrm{v}(a) = 0$ *for all* $a \in \mathbb{F}_p^\times$*. Then, if* $\mathrm{v}(\bar{\mathcal{H}}'_{l,j}) \geq p^l v_0$*, with* $v_0 < 0$*, for all* j*, then* $\mathrm{v}(\bar{\mathcal{I}}_{i,l}) > p^{l+i} v_0$ *for* $i \geq 1$*. (Remember,* $\bar{\mathcal{I}}_{i,l} = \eta_i(\bar{\mathcal{G}}'_l)$*.)*

Proof. By Theorem 3.2, we have that $\bar{\mathcal{I}}_{i,l} = \eta_i(\bar{\mathcal{G}}'_l) = \sum_{j=1}^{i+2} (\bar{\mathcal{J}}_{i,j}^{(l)})'$, it suffices to show that $\mathrm{v}((\bar{\mathcal{J}}_{i,j}^{(l)})') > p^{l+i} v_0$.

We first prove that if $\mathrm{v}((\bar{\mathcal{J}}_{t,j}^{(l)})') > p^{l+t} v_0$ for all $t < i$ (and hence $\mathrm{v}(\bar{\mathcal{I}}_{t,l}) > p^{l+t} v_0$), we also have, $\mathrm{v}((\bar{\mathcal{J}}_{i,j}^{(l)})') > p^{l+i} v_0$.

Indeed, by Lemma 4.1, we have that for $j \in \{1, \ldots, (i-1)\}$ that

$$\mathrm{v}((\bar{\mathcal{J}}_{i,3+j}^{(l)})') = \mathrm{v}(\eta_j((\bar{\mathcal{J}}_{i-j,1}^{(l)})', \ldots, (\bar{\mathcal{J}}_{i-j,i-j+2}^{(l)})')) > p^{l+i} v_0.$$

Moreover, we have $\mathrm{v}((\bar{\mathcal{J}}_{i,1}^{(l)})') = \mathrm{v}(\eta_i(\bar{\mathcal{H}}'_l)) > p^{l+i} v_0$ (by hypothesis),

$$\mathrm{v}((\bar{\mathcal{J}}_{i,2}^{(l)})') = \mathrm{v}(\eta_i(\eta_{l-1}(\bar{\mathcal{G}}'_1), \ldots, \eta_1(\bar{\mathcal{G}}'_{l-1})))) = \mathrm{v}(\eta_i(\bar{\mathcal{I}}_{l-1,1}, \ldots, \bar{\mathcal{I}}_{1,l-1})) > p^{l+i} v_0,$$

and since $h_l = \sum_j \bar{\mathcal{H}}_{l,i}$, we have

$$\mathrm{v}((\bar{\mathcal{J}}_{i,3}^{(l)})') = \mathrm{v}(\eta_i(h'_l, \bar{\mathcal{I}}_{l-1,1} + \cdots + \bar{\mathcal{I}}_{1,l-1})) > p^{l+i} v_0.$$

Thus, by induction, it suffices to prove that $\mathrm{v}((\bar{\mathcal{J}}_{1,j}^{(l)})') > p^{l+1} v_0$, i.e., the case $i = 1$. We prove this by induction on l.

For $l = 1$, we have $\mathrm{v}((\bar{\mathcal{J}}_{1,1}^{(1)})') = \mathrm{v}(\eta_1(\bar{\mathcal{H}}'_1)) > p^2 v_0$ by hypothesis and Lemma 4.1. Also, $(\bar{\mathcal{J}}_{1,2}^{(1)})' = (\bar{\mathcal{J}}_{1,3}^{(1)})' = 0$. Therefore, the statement is true for $l = 1$.

So, suppose now that $\mathrm{v}((\bar{\mathcal{J}}_{1,j}^{(k)})') \geq p^{k+1} v_0$ for all $k < l$. Then, $\mathrm{v}((\bar{\mathcal{J}}_{1,1}^{(l)})') = \mathrm{v}(\eta_l(\bar{\mathcal{H}}'_1)) > p^{l+1} v_0$ again by hypothesis and Lemma 4.1. Now, since $h_l = \sum_j \mathcal{H}_{l,i}$ and $\eta_i(\bar{\mathcal{G}}'_k) = \sum_{j=1}^{i+2} (\bar{\mathcal{J}}_{i,j}^{(k)})'$, we also have $\mathrm{v}((\bar{\mathcal{J}}_{1,j}^{(l)})') > p^{l+1} v_0$ for $j = 2, 3$, finishing the proof. □

Since we also need to look at degrees of the $f_{i,j,k}$'s (in Eq. (3.2)), we shall need the following lemma.

Lemma 4.3. *Let* $\boldsymbol{f} = \Phi_p$*. Then*

$$\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) = \boldsymbol{x}^{p+1} + \boldsymbol{y}^{p+1} - \boldsymbol{x}^p \boldsymbol{y}^p + \sum_{k=0}^{p-1} \boldsymbol{g}_k(\boldsymbol{x}) \boldsymbol{y}^k, \qquad \textit{where } \deg \boldsymbol{g}_i < p, \tag{4.1}$$

and

$$\deg \boldsymbol{f}_{i,j}(\boldsymbol{x}^{p^n}, \boldsymbol{x}^{p^{n+1}}) \leq p^{n+2} - (j-1)p^{n+1} - ip^n.$$

Proof. The first part is well known. For instance, one can use Theorem 5.3 of [11] together with Kronecker's congruence relation.

The second part follows from the first. We have:

$$\begin{aligned} \boldsymbol{f}_{i,j}(\boldsymbol{x}^{p^n}, \boldsymbol{x}^{p^{n+1}}) = \delta_{j,0}\binom{p+1}{i}\boldsymbol{x}^{p^{n+1}-(i-1)p^n} + \delta_{i,0}\binom{p+1}{j}\boldsymbol{x}^{p^{n+2}-(j-1)p^{n+1}} \\ - \binom{p}{i}\binom{p}{j}\boldsymbol{x}^{p^{n+2}-(j-1)p^{n+1}-ip^n} + \sum_{k=0}^{p-1-j}\binom{k+j}{j}\frac{\boldsymbol{g}_{k+j}^{(i)}(\boldsymbol{x}^{p^n})}{i!}\boldsymbol{x}^{kp^{n+1}}, \end{aligned}$$

where $\delta_{i,j}$ is the Kronecker delta function. The result then immediately follows. $\square$

We also have the following trivial lemma that we need for looking at valuations of terms in $E^{i,r-i}_{k,n,j-k}$:

Lemma 4.4. *We have*

$$D^{i,r-i}_{k,n} = \sum_{k_1=r}^{k}\left(\sum_{\substack{i_1+i_2+\cdots+i_n=i \\ i_1+2i_2+\cdots+ni_n=k_1}} \boldsymbol{x}_1^{p^{n-1}i_1}\boldsymbol{x}_2^{p^{n-2}i_2}\cdots\boldsymbol{x}_n^{i_n}\right)\left(\sum_{\substack{j_1+j_2+\cdots+j_n=r-i \\ j_1+2j_2+\cdots+nj_n=k-k_1}} \boldsymbol{y}_1^{p^{n-1}i_1}\boldsymbol{y}_2^{p^{n-2}i_2}\cdots\boldsymbol{y}_n^{i_n}\right).$$

Moreover, if $k < n$ or $i, (r-i) \neq 0$, then the terms in $\boldsymbol{x}_n$ and $\boldsymbol{y}_n$ can be omitted, i.e., we must have $i_n = j_n = 0$.

After possible reindexing, notice we may write (with I_n as in Eq. (3.2))

$$I_n = \sum_{j=3}^{N_n} \bar{\mathcal{H}}'_{n,j},$$

$\bar{\mathcal{H}}'_{n,1} = -X^{p^n}J_n^p$, and $\bar{\mathcal{H}}'_{n,2} = X^{p^{n+2}}J_n^p$. We shall keep this notation from now on.

We can now introduce the main lemma used in the proof of Theorem 1.2.

Lemma 4.5. *Let $p \geq 3$ and v be a valuation on $\mathbb{F}_p(X)$ such that $\mathrm{v}(a) = 0$ for all $a \in \mathbb{F}_p^\times$. Suppose that for given n_0, $n > n_0$, and sequence of real numbers $\{v_i\}_{i \geq n_0}$ the following conditions are satisfied:*

1. *If $k < n_0$ we have that $\mathrm{v}(\bar{\mathcal{H}}'_{k,i}) \geq 0$ for all i and $\mathrm{v}(\bar{\mathcal{H}}'_{n_0,i}) \geq 0$ for all $i \geq 3$.*
2. *$v_{n_0+1} < 0$ and $v_i < pv_{i-1}$ for any $i > n_0$.*
3. *$\mathrm{v}(\bar{\mathcal{H}}'_{l,t}) \geq v_l$ for $t \in \{3, \ldots, N_l\}$ if $n_0 < l \leq n$.*
4. *$\mathrm{v}(J_l) \geq (v_l - p^l\,\mathrm{v}(X^{p^2} - X))/p$ if $n_0 \leq l < n$.*
5. *$p^{n+e}\,\mathrm{v}(X) + p^{n-l}v_l - p^n\,\mathrm{v}(X^{p^2} - X) \geq v_n$ for $e = 0, 2$ if $n_0 \leq l < n$.*

Then, we have that $\mathrm{v}(J_n) \geq (v_n - p^n \mathrm{v}(X^{p^2} - X))/p$.

Moreover, if further there exists a unique $t_0 \in \{3, \ldots, N_n\}$ *such that* $\mathrm{v}(\bar{\mathcal{H}}'_{n,t_0}) = v_n$, *then* $\mathrm{v}(J_n) = (v_n - p^n \mathrm{v}(X^{p^2} - X))/p$.

Proof. By conditions 4 and 5, we have for $n_0 \leq l < n$ that

$$\mathrm{v}(X^{p^{l+e}} J_l^p) \geq p^{l+e} \mathrm{v}(X) + v_l - p^l \mathrm{v}(X^{p^2} - X)) \geq p^{l-n} v_n$$

for $e = 0, 2$. Since $v_n < 0$, condition 1 together with the previous argument gives us that $\mathrm{v}(\bar{\mathcal{H}}'_{l,t}) \geq p^{l-n} v_n$ for $t = 1, 2$ for *all* $l < n$. Since by condition 2 we also have $v_l > p^{l-n} v_n$, by conditions 1 and 3 and using Lemma 4.2, we have $\mathrm{v}(\bar{\mathcal{I}}_{n-i,i}) > v_n$ for $i \in \{0, \ldots, n-1\}$.

Now, Eq. (3.3) can be written as

$$-(X^{p^2} - X)^{p^n} J_n^p = \sum_{t=3}^{N_n} \bar{\mathcal{H}}'_{n,t} + \sum_{i=0}^{n-1} \bar{\mathcal{I}}_{n-i,i}.$$

By the argument above and condition 3 (with $l = n$), we have $\mathrm{v}(J_n) \geq (v_n - p^n \mathrm{v}(X^{p^2} - X))/p$.

The final observation on the statement also can easily be seen from the analysis above with the due restrictions. $\square$

5. Proof of Item 1 of Theorem 1.2

We are now ready to prove item 1 of Theorem 1.2. To simplify the exposition we introduce one extra simple lemma.

Lemma 5.1. *Let* $0 \leq i \leq r \leq n$ *and assume that:*

$$j_1 + \cdots + j_{n-1} = i \qquad \textit{and} \qquad j_1 + \cdots + j_{n-1} = r - i,$$

with $i_t, j_t \in \mathbb{Z}_{\geq 0}$. *Then, for* $r \geq 2$ *we have that*

$$\sum_{t=1}^{n-1} \frac{i_t}{p^t} + \frac{j_t}{p^{t-1}} > \frac{1}{p^{n-1}}.$$

Proof. We have:

$$\sum_{t=1}^{n-1} \frac{i_t}{p^t} + \frac{j_t}{p^{t-1}} \geq \sum_{t=1}^{n-1} \frac{i_t}{p^{n-1}} + \frac{j_t}{p^{n-2}} \geq \sum_{t=1}^{n-1} \frac{i_t}{p^{n-1}} + \frac{j_t}{p^{n-1}} = \frac{r}{p^{n-1}} > \frac{1}{p^{n-1}}.$$

$\square$

Let v_∞ be the valuation on $\mathbb{F}_p(X)$ given by the order of zero at infinity. Then, item 1 of Theorem 1.2, namely $\deg F_n - \deg G_n = p^n - \iota$, is equivalent to $\mathrm{v}_\infty(J_n) = -(p^n - \iota)$, which is what we shall prove below.

Let $v_n \stackrel{\text{def}}{=} -(p^{n+2}+p^{n+1}-\iota p)$. We will use induction on n to show that $\mathrm{v}_\infty(J_n) = -(p^n-\iota)$ *and* $\mathrm{v}(\bar{\mathcal{H}}'_{n,t}) \geq v_n$ for $t \in \{3, \dots, N_n\}$. For $n = 1$ the results hold, as observed in [1]. (Note that $\bar{\mathcal{H}}'_1 = \bar{\mathcal{G}}'_1 = \mathrm{vec}\left(f_{0,0,1}(X^p, X^{p^2})\right)$.)

So, suppose that $\mathrm{v}(\bar{\mathcal{H}}'_{l,t}) \geq v_l$ for $t \in \{3, \dots, N_l\}$ and $\mathrm{v}_\infty(J_l) = -(p^l - \iota)$ if $1 \leq l < n$. With these assumptions and with v_n as given, we are in the conditions of Lemma 4.5 with $n_0 = 1$.

Thus, by the lemma, we only need to verify the special case of condition 3, i.e., $\mathrm{v}_\infty(\bar{\mathcal{H}}'_{n,t}) \geq -(p^{n+2} + p^{n+1} - \iota p)$ for $t \in \{3, \dots, N_n\}$, and equality occurs for exactly one t.

By Lemmas 4.4 and 5.1 (and using the notation of the former), we have that if $r \geq 2$, then the valuation v_∞ of a non-zero summand of $E^{i,r-i}_{k,n,j-k}$, for $k < n$, or for $i, (r-i) \neq 0$, is

$$\begin{aligned} -\sum_{t=1}^{n-1} & i_t p^{n-t}(p^t - \iota) + j_t p^{n-t+1}(p^t - \iota) \\ &= -p^n \left[\sum_{t=1}^{n-1} i_t + p j_t\right] + \iota p^n \left[\sum_{t=1}^{n-1} \frac{i_t}{p^t} + \frac{j_t}{p^{t-1}}\right] \\ &= -(r-i)p^{n+1} - ip^n + \iota p^n \left[\sum_{t=1}^{n-1} \frac{i_t}{p^t} + \frac{j_t}{p^{t-1}}\right] \\ &> -(r-i)p^{n+1} - ip^n + \iota p. \end{aligned}$$

In particular, if $\bar{\mathcal{H}}'_{n,t}$ comes from $E^{1,1}_{k,n,n-k}$ (and hence $r = 2$, $i = (r-i) = 1$), we have that

$$\mathrm{v}_\infty(\bar{\mathcal{H}}'_{n,t}) > -p^{n+1} - p^n + \iota p.$$

Also, by Lemma 4.3, we have, the valuation of any non-zero term of $f_{i,r-i,n-j}(X^{p^n}, X^{p^{n+1}})$ is greater than or equal to $-(p^{n+2} - (r-i-1)p^{n+1} - ip^n)$. Hence, a term $\bar{\mathcal{H}}'_{n,t}$ from $f_{i,r-i,n-j}(X^{p^n}, X^{p^{n+1}})E^{i,r-i}_{k,n,j-k}$, with $r \geq 2$ and $k < n$ (as in Eq. (3.2)), is also such that

$$\mathrm{v}_\infty(\bar{\mathcal{H}}'_{n,t}) \geq -p^{n+1} - p^n + \iota p.$$

Finally, we also have:

- $\mathrm{v}_\infty(\bar{\mathcal{H}}'_{n,t}) \geq -p^{n+2}$, if $\bar{\mathcal{H}}'_{n,t}$ comes from $f_{0,0,n}(X^{p^n}, X^{p^{n+1}})$ (by Eq 4.1);
- $\mathrm{v}_\infty(\bar{\mathcal{H}}'_{n,t}) \geq -(p^{n+2} + p^{n+1} - \iota p^{n-j+1}) \geq -(p^{n+2} + p^{n+1} - \iota p^2)$, if $\bar{\mathcal{H}}'_{n,t}$ comes from $(f_{0,1,n-j}(X^{p^n}, X^{p^{n+1}})J_j^{p^{n-j+1}}$ with $j < n$;
- $\mathrm{v}_\infty(\bar{\mathcal{H}}'_{n,t}) \geq -(p^{n+2} + p^{n+1} - \iota p^{n-j}) \geq -(p^{n+2} + p^{n+1} - \iota p)$, if $\bar{\mathcal{H}}'_{n,t}$ comes from $f_{1,0,n-j}(X^{p^n}, X^{p^{n+1}})J_j^{p^{n-j}}$ with $j < n$.

Note that the last equality can only occur if $j = (n-1)$. The corresponding term comes from $f_{1,0,1}(X^{p^n}, X^{p^{n+1}})J^p_{n-1}$. But, by Eq. (4.1), we have that $\deg f_{1,0,1}(X^{p^n}, X^{p^{n+1}}) =$

$p^{n+2}+p^{n+1}-p^n$, and hence $\mathrm{v}_\infty(\bar{\mathcal{H}}'_{n,t}) = -(p^{n+2}+p^{n+1}-\iota p)$ for exactly one term (coming from $f_{1,0,1}(X^{p^n}, X^{p^{n+1}})J_j^p$), which finishes the proof.

6. Proof of Item 2 of Theorem 1.2

We will now prove the item 2 of Theorem 1.2. First observe that G_n cannot have a zero in any ordinary value, as J_n must be regular at that value. In particular, the cases when δ or ϵ is zero follows immediately. Thus, from this point on, we will only consider the cases when δ and ϵ are equal to one.

So, let v_0, v_{1728}, w be the orders of zero at 0, 1728, and a root of $S_p(X)$ respectively. Then, to prove item 2 of Theorem 1.2, we need to prove the following:

- $\mathrm{v}_0(J_n) \geq p^{n-2}(n(-p^2-p)/3+p^2)$ (when $\delta = 1$);
- $\mathrm{v}_{1728}(J_n) \geq p^{n-2}(-pn+p)$ (when $\epsilon = 1$);
- $\mathrm{w}(J_n) = p^{n-2}(n(-p-1)+1)$;

To deal with these three cases at once, we let v denote a valuation on $\mathbb{F}_p(X)$ such that $\mathrm{v}(a) = 0$ for all $a \in \mathbb{F}_p^\times$, $\mathrm{v}(X) \geq 0$, $\mathrm{v}(X^{p^2}-X) = 1$, and $\mathrm{v}(J_k) \geq p^{k-2}(\alpha k+\beta)$ for some $\alpha < 0$ and $\beta > 0$ independent of k.

We will again rely on Lemma 4.5, with $v_n \stackrel{\text{def}}{=} p^{n-1}(\alpha n+\beta)+p^n$ in this case. Since $\alpha < 0$, the condition 2 from the lemma is satisfied, with $n_0 = 3$ if $\mathrm{v} = \mathrm{v}_0$, with $n_0 = 2$ if $\mathrm{v} = \mathrm{v}_{1728}$, and with $n_0 = 1$ if $\mathrm{v} = \mathrm{w}$.

With the above choice of n_0, Theorem 1.1 shows that condition 1 is satisfied.

Condition 5 is equivalent to $p\,\mathrm{v}(X) - \alpha \geq p$, and therefore is satisfied for the three valuations above.

So, let v be one of the valuations above. We then shall prove by induction on n that $\mathrm{v}(J_n) \geq p^{n-2}(\alpha n+\beta)$, with equality in the case of $\mathrm{v} = \mathrm{w}$, *and* that for $n > n_0$ we have $\mathrm{v}(\bar{\mathcal{H}}'_{n,t}) \geq v_n$ for $t \in \{3, \ldots, N_n\}$, with equality for exactly one t in the case $\mathrm{v} = \mathrm{w}$.

If $n \leq n_0$ and $\mathrm{v} = \mathrm{v}_{1728}$ or $\mathrm{v} = \mathrm{w}$, then the result holds by Theorem 1.1. If $n \leq n_0$ and $\mathrm{v} = \mathrm{v}_0$, then the result holds for $n = 1$ by Theorem 1.2 from [6] (which just restates results from [9]), for $n = 2$ by Theorem 6.2 from [7], and for $n = 3$ by Theorem 1.1.

So, let $n > n_0$ and suppose that for all $l \in \{1, \ldots, (n-1)\}$ we have $\mathrm{v}(J_l) \geq -p^{l-2}(\alpha l+\beta)$, with equality if $\mathrm{v} = \mathrm{w}$, and if $n_0 < l < n$ we have $\mathrm{v}(\bar{\mathcal{H}}'_{l,t}) \geq v_l$ for $t \in \{3, \ldots, N_l\}$. Thus, condition 3 for $l < n$ and condition 4 of Lemma 4.5 are satisfied. Therefore, we only need to verify the case $l = n$ of condition 3, with special care when $\mathrm{v} = \mathrm{w}$.

By Lemma 4.4 (and using its notation), we have that the valuation v of a non-zero summand of $E^{i,r-i}_{k,n,j-k}$, with either $k<n$ or $i,(r-i)\neq 0$, is

$$\begin{aligned} p^{n-2}\sum_{t=1}^{n-1}(\alpha t i_t+\beta i_t)+p(\alpha t j_t+\beta j_t) \\ &= p^{n-2}[(\alpha k_1+\beta i)+p(\alpha(k-k_1)+\beta(r-i))] \\ &= p^{n-2}[\alpha pk+\beta pr-(p-1)\alpha k_1-(p-1)\beta i] \end{aligned}$$

Hence, if T is a term from $E^{i,r-i}_{k,n,j-k}$, then since $k_1\in\{i,\dots,k\}$ and $\alpha<0$, we have

$$\mathrm{v}(T)\geq p^{n-2}[\alpha pk+\beta pr-(p-1)(\alpha+\beta)i].$$

Since $i\in\{0,\dots,r\}$, we have

$$\mathrm{v}(T)\geq\begin{cases} p^{n-1}[\alpha k+\beta r], & \text{if } \alpha+\beta\leq 0;\\ p^{n-2}[\alpha pk+(\beta-(p-1)\alpha)r], & \text{if } \alpha+\beta>0.\end{cases}$$

If $k\in\{r,\dots,n-1\}$, then since $\alpha<0$ we have

$$\mathrm{v}(T)\geq\begin{cases} p^{n-1}[\alpha(n-1)+\beta r], & \text{if } \alpha+\beta\leq 0;\\ p^{n-2}[\alpha p(n-1)+(\beta-(p-1)\alpha)r], & \text{if } \alpha+\beta>0.\end{cases}$$

Finally, if $r\in\{2,\dots,n-1\}$, then, since $\alpha<0$ and $\beta>0$, we have

$$\mathrm{v}(T)\geq\begin{cases} p^{n-1}[\alpha(n-1)+2\beta], & \text{if } \alpha+\beta\leq 0;\\ p^{n-1}[\alpha(n-1)+\beta]+p^{n-2}[2(\alpha+\beta)-p(2\alpha+\beta)], & \text{if } \alpha+\beta>0.\end{cases}$$

Therefore, since $\mathrm{v}(X)\geq 0$, for any $\bar{\mathcal{H}}'_{n,t}$ coming from either

$$\sum_{r=2}^{n-1}\sum_{i=0}^{r}\sum_{j=r}^{n-1}\sum_{k=r}^{j} f_{i,r-i,n-j}(X^{p^n},X^{p^{n+1}})E^{i,r-i}_{k,n,j-k}$$

or $\sum_{k=2}^{n-1}E^{1,1}_{k,n,n-k}$, we have

$$\mathrm{v}(\bar{\mathcal{H}}'_{n,t})\geq\begin{cases} p^{n-1}[\alpha(n-1)+2\beta], & \text{if } \alpha+\beta\leq 0;\\ p^{n-1}[\alpha(n-1)+\beta]+p^{n-2}[2(\alpha+\beta)-p(2\alpha+\beta)], & \text{if } \alpha+\beta>0.\end{cases}$$

Moreover, a similar analysis gives that terms coming from $E^{1,1}_{n,n,0}$ have valuation greater than or equal to $p^{n-1}[\alpha(n-1)+\beta]+p^{n-2}[\alpha+\beta]$.

Also, clearly $\bar{\mathcal{H}}'_{n,t}$'s coming from $f_{0,0,n}(X^{p^n},X^{p^{n+1}})$ have nonnegative valuations. If it comes from $f_{0,1,n-j}(X^{p^n},X^{p^{n+1}})J_j^{p^{n-j+1}}$, for $j\in\{1,\dots,(n-1)\}$, then it has valuation greater than or equal to $p^{n-1}[\alpha j+\beta]\geq p^{n-1}[(n-1)\alpha+\beta]$. And if it comes from

$f_{1,0,n-j}(X^{p^n}, X^{p^{n+1}})J_j^{p^{n-j}}$, again for $j \in \{1, \dots, (n-1)\}$, then it has valuation greater than or equal to $p^{n-2}[\alpha j + \beta] \geq p^{n-2}[(n-1)\alpha + \beta]$.

We now need to deal with the particular valuations.

Case 1: Let $\mathrm{v} = \mathrm{v}_0$, i.e., $n_0 = 3$, $\alpha = -(p^2 + p)/3$ and $\beta = p^2$. Then, the analysis above gives for $p \geq 7$

$$\mathrm{v}(\bar{\mathcal{H}}'_{n,t}) \geq p^{n-1}[\alpha(n-1) + \beta] + p^{n-2}[2(\alpha + \beta) - p(2\alpha + \beta)]] \geq v_n$$

for $t \geq 3$. For $p = 5$, we have

$$\mathrm{v}(\bar{\mathcal{H}}'_{n,t}) \geq p^{n-1}[\alpha(n-1) + \beta] \geq v_n$$

for $t \geq 3$.

Case 2: Let $\mathrm{v} = \mathrm{v}_{1728}$, i.e., $n_0 = 2$, $\alpha = -p$ and $\beta = p$. Then, the analysis above gives

$$\mathrm{v}(\bar{\mathcal{H}}'_{n,t}) \geq p^{n-1}[\alpha(n-1) + \beta] + p^{n-2}[\alpha + \beta] \geq v_n$$

for $t \geq 3$.

Case 3: Let $\mathrm{v} = \mathrm{w}$, i.e., $n_0 = 1$, $\alpha = -(p+1)$ and $\beta = 1$. Then, the analysis above gives

$$\mathrm{v}(\bar{\mathcal{H}}'_{n,t}) \geq p^{n-1}[\alpha(n-1) + \beta] + p^{n-2}[\alpha + \beta] \geq v_n$$

for $t \geq 3$. Note that in this case, there is only one term of valuation exactly equal to v_n, namely, the term $J_1^{p^{n-1}} J_{n-1}^{p^2}$ from $E^{1,1}_{n,n,0}$, and by the induction hypothesis (with equality in the valuation of J_j in this case) gives that this term has valuation exactly equal to v_n.

The three cases above finish the proof.

References

[1] E. de Shalit. Kronecker's polynomial, supersingular elliptic curves, and p-adic periods of modular curves. In *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, volume 165 of *Contemp. Math.*, pages 135–148. Amer. Math. Soc., Providence, RI, 1994.

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

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

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

[5] L. R. A. Finotti. Computations with Witt vectors and the Greenberg transform. Submitted. Available at `http://www.math.utk.edu/~finotti/`, 2011.

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

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

[8] M. J. Greenberg. Schemata over local rings. *Ann. of Math. (2)*, 73:624–648, 1961.

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

[10] S. Lang. On quasi algebraic closure. *Ann. of Math. (2)*, 55:373–390, 1952.

[11] S. Lang. *Elliptic Functions*, volume 112 of *Garduate Texts in Mathematics*. Springer-Verlag, second edition, 1986.

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

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

E-mail address: `finotti@math.utk.edu`

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