NONEXISTENCE OF PSEUDO-CANONICAL LIFTINGS

LUÍS R. A. FINOTTI

Abstract. In this paper we show that pseudo-canonical liftings do not exist, by showing that if $j_0 \mapsto (j_0, J_1(j_0), J_2(j_0), \dots)$ is the map that gives canonical liftings for ordinary j_0, then J_2 has a pole at $j_0 = 1728$ if $p \equiv 3 \pmod 4$ and J_3 has a pole at $j_0 = 0$ if $p \equiv 5 \pmod 6$. Moreover, precise descriptions of J_2 and J_3 are given.

1. Introduction

Let $\Bbbk$ be a perfect field of characteristic $p > 0$, $\boldsymbol{W}(\Bbbk)$ be the ring of Witt vectors over $\Bbbk$, and $\boldsymbol{W}_n(\Bbbk)$ denote the ring of Witt vectors of length n, which in this case can be seen as the quotient of $\boldsymbol{W}(\Bbbk)$ modulo the principal ideal generated by p^n. 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, [Deu41] or [LST64].) 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 $i = 1, 2, 3, \dots$, such that the j-invariant of the canonical lifting of an elliptic curve with j-invariant $j_0 \in \Bbbk^{ord}$ is $(j_0, J_1(j_0), J_2(j_0), \dots)$.

B. Mazur asked about the nature of these functions J_i and J. Tate asked about the possibility of extending them to supersingular values.

We've proved that the functions J_i are rational functions over $\mathbb{F}_p$ in [Fin10]. Tate's question motivates the following definition:

Definition 1.1. Suppose that $j_0 \notin \Bbbk^{ord}$ and J_i is regular at j_0 for all $i \leq n$. Then, we call an elliptic curve over $\boldsymbol{W}(\Bbbk)$ whose j-invariant reduces to $(j_0, J_1(j_0), \dots, J_n(j_0))$ modulo p^{n+1} a *pseudo-canonical lifting modulo p^{n+1} (or over $\boldsymbol{W}_{n+1}(\Bbbk)$)* of the elliptic curve associated to j_0.

If J_i is regular for all i, we call the elliptic curve with j-invariant $(j_0, J_1(j_0), J_2(j_0), \dots)$ the *pseudo-canonical lifting* of the elliptic curve associated to j_0.

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

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

Hence, Tate asks about the existence of such pseudo-canonical liftings. One would not expect pseudo-canonical liftings to exist, as they would yield curves which although are not canonical liftings, as those do not exist in the supersingular case, are obtained by the same formulas. On the other hand, we've proved that pseudo-canonical liftings modulo p^2 and p^3 do exist for specific supersingular values. More precisely, we've studied J_1 and J_2 in detail in [Fin10] (using many results from [KZ98]) and [Fin11b] respectively, proving the following:

Theorem 1.2. *With the notation above and $p \geq 5$:*

(1) *$J_1(X)$ is* always *regular at $X = 0$ and $X = 1728$, even when those values are supersingular, and $(0, J_1(0)) \equiv 0 \pmod{p^2}$ and $(1728, J_1(1728)) \equiv 1728 \pmod{p^2}$.*
(2) *If $j_0 \notin \Bbbk^{ord} \cup \{0, 1728\}$, then J_1 has a simple pole at j_0.*
(3) *$J_2(X)$ is* always *regular at $X = 0$, even if 0 is supersingular, and $(0, J_1(0), J_2(0)) \equiv 0 \pmod{p^3}$.*
(4) *If $j_0 \notin \Bbbk^{ord} \cup \{0, 1728\}$, then J_2 has a pole of order $2p + 1$ at j_0.*

As one can see, this statement does not give any information modulo p^3 in the case of 1728 being supersingular. We will prove here the following theorem, which was stated as a conjecture in [Fin10], more precisely, item (1) of Conjecture 9.3.

Theorem 1.3. *If $1728 \notin \Bbbk^{ord}$ (i.e., if $p \equiv 3 \pmod 4$), then J_2 has a pole of order p at 1728.*

So, this would tell us 1728 never yields pseudo-canonical liftings, leaving 0 as the only possibility. On the other hand, we will also show here that 0 also fails. This again was a conjecture of [Fin10], more precisely, Conjecture 10.1. (In fact, we prove here that Conjecture 9.7 from [Fin11b], which is equivalent to item (2) of Conjecture 9.3 from the same reference, is equivalent to Conjecture 10.1, and therefore all conjectures of [Fin11b] are proved here.)

Theorem 1.4. *If $0 \notin \Bbbk^{ord}$ (i.e., if $p \equiv 5 \pmod 6$), then J_3 has a pole of order p^2 at 0.*

This gives a complete answer to Tate's question, showing that, as expected, no pseudo-canonical lifting exist, and the only possible ones modulo p^2 are given by 0 and 1728, and modulo p^3, only by 0.

We will heavily rely on results and techniques from the author's [Fin10] and [Fin11b], although we will restate most of the necessary results. It should also be observed that Kaneko and Zagier's [KZ98], from which many results from [Fin10] are derived, provided many of the necessary tools, although we may refer to [Fin10] instead, as the results are phrased in a more compatible way. Finally, we will also need results from [Fin11a], which will be the main tool to analyze the properties of J_3.

We now give a brief description of the next sections. In Section 2 we review the concept of the Greenberg transform of a polynomial and recall the formulas for those which were derived in [Fin11b] and [Fin11a]. In Section 3 we introduce some alternatives to the j-invariant which will help us deal with the pole of J_2 at 1728, similarly to what was done in [Fin10]. In Section 4 we use these invariants to prove Theorem 1.3. In Section 5 we give a formula for J_3, similar to the formula for J_2 given in [Fin11b], while in Section 6 we use this formula to prove Theorem 1.4. Finally, on Section 7 we give some more information on the formulas for J_2 and J_3.

2. The Greenberg Transform

In this section we briefly review the definition of the Greenberg transform. (See also [Lan52] and [Gre61].)

Definition 2.1. Let $\boldsymbol{f}(\boldsymbol{x},\boldsymbol{y}) \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x},\boldsymbol{y}]$. 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 $f_i \in \Bbbk[x_0, \ldots, x_i, y_0, \ldots, y_i]$. This resulting vector is called the *Greenberg transform* of $\boldsymbol{f}$ and will be denoted by $\mathscr{G}(\boldsymbol{f})$.

Moreover, if

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

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

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

We will need the formula for the second coordinate of the Greenberg transform of a polynomial. This is given by Theorem 6.1 from [Fin11b], restated below as Theorem 2.4. But before we can state it, we need some extra notation:

Definition 2.2. Let p be a prime. Define $\eta_0(X_1, \ldots, X_r) \stackrel{\text{def}}{=} X_1 + \cdots + X_r$, and recursively for $k \geq 1$

$$\eta_k(X_1, \ldots, X_r) \stackrel{\text{def}}{=} \frac{X_1^{p^k} + \cdots + X_r^{p^k}}{p^k} - \sum_{i=0}^{k-1} \frac{\eta_i(X_1, \ldots, X_r)^{p^{k-i}}}{p^{k-i}}. \tag{2.1}$$

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

If R is a ring of characteristic p and $v = (a_1, \ldots, a_r) \in R^r$, we define $\eta_k(v) = \eta_k(a_1, \ldots, a_r)$ as the evaluation of $\eta_k(X_1, \ldots, X_r)$ at v. (This makes sense as $\eta_k(X_1, \ldots, X_r) \in \mathbb{Z}[X_1, \ldots, X_r]$. See [Fin11a].)

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

Sometimes it will be useful to use the following notation:

Definition 2.3. Given $\boldsymbol{f} = \sum_{i,j} \boldsymbol{a}_{i,j}\boldsymbol{x}^i\boldsymbol{y}^j \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$ and a positive integer n, define

$$\boldsymbol{f}^{[p^n]} \stackrel{\text{def}}{=} \sum_{i,j} \boldsymbol{a}_{i,j}^{p^n}\boldsymbol{x}^{ip^n}\boldsymbol{y}^{jp^n}.$$

We also define $\eta_k(\boldsymbol{f})$ to be the reduction modulo p of

$$\eta_k(\boldsymbol{f}) = \eta_k(\mathrm{vec}\,(\boldsymbol{f})) = \frac{\boldsymbol{f}^{[p^k]} - \boldsymbol{f}^{p^k}}{p^k} - \frac{\eta_1(\mathrm{vec}\,(\boldsymbol{f}))^{p^{k-1}}}{p^{k-1}} - \cdots - \frac{\eta_{k-1}(\mathrm{vec}\,(\boldsymbol{f}))^p}{p}. \tag{2.2}$$

Then, if $\boldsymbol{f}$ reduces to f modulo p, we have that $\eta_k(f) = \eta_k(\boldsymbol{f})$.

With the notation above, we can give a formula for the third coordinate of the Greenberg transform of $\boldsymbol{f}$.

Theorem 2.4. *Let $\boldsymbol{f} \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$ be given by*

$$\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i,j} \boldsymbol{a}_{i,j}\boldsymbol{x}^i\boldsymbol{y}^j,$$

with partial derivatives with respect to $\boldsymbol{x}$ and $\boldsymbol{y}$

$$\boldsymbol{f}_{\boldsymbol{x}}(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i,j} \boldsymbol{b}_{i,j}\boldsymbol{x}^i\boldsymbol{y}^j \qquad \textit{and} \qquad \boldsymbol{f}_{\boldsymbol{y}}(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i,j} \boldsymbol{c}_{i,j}\boldsymbol{x}^i\boldsymbol{y}^j,$$

respectively. Also, let f be the reduction modulo p of $\boldsymbol{f}$ (and use subscripts x_0 and y_0 to denote its partial derivatives), and

$$\begin{aligned}
\boldsymbol{a}_{i,j} &\equiv (a_{i,j,0}, a_{i,j,1}, a_{i,j,2}) \pmod{p^3},\\
\boldsymbol{b}_{i,j} &\equiv (b_{i,j,0}, b_{i,j,1}, b_{i,j,2}) \pmod{p^3},\\
\boldsymbol{c}_{i,j} &\equiv (c_{i,j,0}, c_{i,j,1}, c_{i,j,2}) \pmod{p^3}.
\end{aligned}$$

Then, the third coordinate of the Greenberg transform of $\boldsymbol{f}$ is given by

$$\begin{aligned}
f_{x_0}^{p^2} x_2 + f_{y_0}^{p^2} y_2 &+ \left(\sum_{i,j} b_{i,j,1} x_0^{ip} y_0^{jp}\right)^p x_1^p + \left(\sum_{i,j} c_{i,j,1} x_0^{ip} y_0^{jp}\right)^p y_1^p \\
&+ (f_{x_0x_0}/2)^{p^2} x_1^{2p} + f_{x_0y_0}^{p^2} x_1^p y_1^p + (f_{y_0y_0}/2)^{p^2} y_1^{2p} + \sum_{i,j} a_{i,j,2} x_0^{ip^2} y_0^{jp^2} \\
&+ \eta_1(f_{x_0}^p x_1 + f_{y_0}^p y_1 + \sum_{i,j} a_{i,j,1} x_0^{ip} y_0^{jp}) \\
&+ \eta_1(f_{x_0}^p x_1 + f_{y_0}^p y_1 + \sum_{i,j} a_{i,j,1} x_0^{ip} y_0^{jp}, \eta_1(f)) + \eta_2(f). \quad (2.3)
\end{aligned}$$

We also need a formula for the fourth coordinate of the Greenberg transform. In [Fin11a] we give a general formula (Theorem 5.4). Since this general formula is too convoluted in the general setting, we will give here only the particular case of the fourth coordinate here. The formula is still quite involved, and we need to introduce some extra notation in addition to the notation from Theorem 2.4.

Let

$$\frac{1}{2}\boldsymbol{f}_{\boldsymbol{xx}}(\boldsymbol{x},\boldsymbol{y}) = \sum_{i,j} \boldsymbol{d}_{i,j} \boldsymbol{x}^i \boldsymbol{y}^j, \qquad \boldsymbol{f}_{\boldsymbol{xy}}(\boldsymbol{x},\boldsymbol{y}) = \sum_{i,j} \boldsymbol{e}_{i,j} \boldsymbol{x}^i \boldsymbol{y}^j, \qquad \frac{1}{2}\boldsymbol{f}_{\boldsymbol{yy}}(\boldsymbol{x},\boldsymbol{y}) = \sum_{i,j} \boldsymbol{f}_{i,j} \boldsymbol{x}^i \boldsymbol{y}^j,$$

and

$$\begin{aligned}
\boldsymbol{d}_{i,j} &\equiv (d_{i,j,0}, d_{i,j,1}) \pmod{p^2}, \\
\boldsymbol{e}_{i,j} &\equiv (e_{i,j,0}, e_{i,j,1}) \pmod{p^2}, \\
\boldsymbol{f}_{i,j} &\equiv (f_{i,j,0}, f_{i,j,1}) \pmod{p^2}.
\end{aligned}$$

Moreover, let $\mathcal{G}_1$ be the vector

$$\operatorname{vec}\left((f_x)^p x_1 + f_y^p y_1 + \sum_{i,j} a_{i,j,1} x_0^{ip} y_0^{jp}\right)$$

with $\eta_1(f)$ appended (at the last entry) to it, and $\mathcal{G}_2$ be

$$\begin{aligned}
\operatorname{vec}\Bigg(f_{x_0}^{p^2} x_2 + f_{y_0}^{p^2} y_2 &+ \left(\sum_{i,j} b_{i,j,1} x_0^{ip} y_0^{jp}\right)^p x_1^p + \left(\sum_{i,j} c_{i,j,1} x_0^{ip} y_0^{jp}\right)^p y_1^p \\
&+ (f_{x_0x_0}/2)^{p^2} x_1^{2p} + f_{x_0y_0}^{p^2} x_1^p y_1^p + (f_{y_0y_0}/2)^{p^2} y_1^{2p} + \sum_{i,j} a_{i,j,2} x_0^{ip^2} y_0^{jp^2} \Bigg)
\end{aligned}$$

with $\eta_1(\mathcal{G}_1)$ and $\eta_2(f)$ appended (at the last two entries) to it.

We then have:

Theorem 2.5. *With the notation above and $p \geq 3$, the fourth coordinate of the Greenberg transform of $\boldsymbol{f}$ is given by*

$$
\begin{aligned}
&\sum_{i,j} a_{i,j,3} x_0^{ip^3} y_0^{jp^3} + f_{x_0}^{p^3} x_3 + f_{y_0}^{p^3} y_3 + \\
&\qquad + \left(\sum_{i,j} b_{i,j,1}^{p^2} x_0^{ip^3} y_0^{jp^3} \right) x_2^p + \left(\sum_{i,j} c_{i,j,1}^{p^2} x_0^{ip^3} y_0^{jp^3} \right) y_2^p \\
&\qquad + \left(\sum_{i,j} b_{i,j,2}^{p} x_0^{ip^3} y_0^{jp^3} \right) x_1^{p^2} + \left(\sum_{i,j} c_{i,j,2}^{p} x_0^{ip^3} y_0^{jp^3} \right) y_1^{p^2} \\
&\qquad + (f_{x_0x_0})^{p^3} x_1^{p^2} x_2^p + f_{x_0y_0}^{p^3} (x_1^{p^2} y_2^p + x_2^p y_1^{p^2}) + (f_{y_0y_0})^{p^3} y_1^{p^2} y_2^p \\
&+ \left(\sum_{i,j} d_{i,j,1}^{p^2} x_0^{ip^3} y_0^{jp^3} \right) x_1^{2p^2} + \left(\sum_{i,j} e_{i,j,1}^{p^2} x_0^{ip^3} y_0^{jp^3} \right) x_1^{p^2} y_1^{p^2} + \left(\sum_{i,j} f_{i,j,1}^{p^2} x_0^{ip^3} y_0^{jp^3} \right) y_1^{2p^2} \\
&+ (f_{x_0x_0x_0}/6)^{p^3} x_1^{3p^2} + (f_{x_0x_0y_0}/2)^{p^3} x_1^{2p^2} y_1^{p^2} + (f_{x_0y_0y_0}/2)^{p^3} x_1^{p^2} y_1^{2p^2} + (f_{y_0y_0y_0}/6)^{p^3} y_1^{3p^2} \\
&\qquad\qquad + \eta_1(\mathcal{G}_2) + \eta_2(\mathcal{G}_1) + \eta_3(f). \qquad (2.4)
\end{aligned}
$$

3. Alternative Invariants

To prove Theorem 1.3 we will use a couple of different invariants.

Definition 3.1. If j is the j-invariant of an elliptic curve, we shall denote $\hat{\jmath} \stackrel{\text{def}}{=} j - 1728$. We may refer to this alternative invariant as the $\hat{\jmath}$-invariant of the elliptic curve.

Let also $\hat{\Phi}_p(X, Y) = \Phi_p(X + 1728, Y + 1728)$, where Φ_p is the (classical) modular polynomial. Hence, two curves with $\hat{\jmath}$-invariants $\hat{\jmath}_1$ and $\hat{\jmath}_2$ have an isogeny of degree p between them if, and only if, $\hat{\Phi}_p(\hat{\jmath}_1, \hat{\jmath}_2) = 0$.

Now, if $\hat{\jmath}_0$ is the $\hat{\jmath}$-invariant of an ordinary elliptic curve in characteristic p, then, as with the original j-invariant (see [Fin10]), the $\hat{\jmath}$-invariant of its canonical lifting is given by

$$\hat{\boldsymbol{\jmath}} = (\hat{\jmath}_0, \hat{J}_1(\hat{\jmath}_0), \hat{J}_2(\hat{\jmath}_0), \dots) = (j_0, J_1(j_0), J_2(j_0), \dots) - 1728, \qquad (3.1)$$

where $\hat{J}_i(X) \in \mathbb{F}_p(X)$ and $j_0 = \hat{\jmath}_0 + 1728$ is the usual j-invariant of the curve.

The other invariant that we need was studied in [Fin10].

Definition 3.2. We define the $\tilde{\hat{\jmath}}$ of an elliptic curve with $j \neq 0$ to be

$$\tilde{\hat{\jmath}} = \frac{4(1728 - j)}{27j} = -\frac{4\hat{\jmath}}{27(\hat{\jmath} + 1728)}. \qquad (3.2)$$

This other invariant also has its own corresponding rational functions giving the canonical lifting, say $\tilde{\hat{J}}_i(X)$, which can be obtained from the $\hat{J}_i(X)$ (or $J_i(X)$) using Eq. (3.2).

The first step in proving Theorem 1.3 is to obtain the proper formula for $\hat{J}_2$ from $\hat{\Phi}_p$, in the same way we've obtained a formula for J_2 from Φ_p in [Fin11b]. In fact, the computation is quite similar, as $\hat{\Phi}_p(X,Y) \equiv \Phi_p(X,Y) \pmod{p}$.

Applying Theorem 2.4, we obtain the following proposition, which is the analogue of Theorem 9.1 from [Fin11b].

Proposition 3.3. *Let*

$$\hat{\Phi}_p = \sum_{i,j} \hat{\boldsymbol{a}}_{i,j} X^i Y^j, \qquad (\hat{\Phi}_p)_X = \sum_{i,j} \hat{\boldsymbol{b}}_{i,j} X^i Y^j, \qquad \text{and} \qquad (\hat{\Phi}_p)_Y = \sum_{i,j} \hat{\boldsymbol{c}}_{i,j} X^i Y^j,$$

respectively, with $\hat{\boldsymbol{a}}_{i,j} = (\hat{a}_{i,j,0}, \hat{a}_{i,j,1}, \ldots)$, $\hat{\boldsymbol{b}}_{i,j} = (\hat{b}_{i,j,0}, \hat{b}_{i,j,1}, \ldots)$, $\hat{\boldsymbol{c}}_{i,j} = (\hat{c}_{i,j,0}, \hat{c}_{i,j,1}, \ldots)$. *Also, let*

$$\hat{g}_2(X_0, Y_0, Y_1) \stackrel{\text{def}}{=} \eta_1((Y_0^p - X_0)^p Y_1 + \sum_{i,j} \hat{a}_{i,j,1} X_0^{ip} Y_0^{jp}).$$

Then, $\hat{g}_2(X, X^p, \hat{J}_1(X)^p)$ *is a p-power and*

$$\hat{J}_2(X) = \frac{-1}{(X^{p^2} - X)^p} \left[\left(\sum_{i,j} \hat{b}_{i,j,1} X^{ip+jp^2} \right) \hat{J}_1(X) + \left(\sum_{i,j} \hat{c}_{i,j,1} X^{ip+jp^2} \right) \hat{J}_1(X)^p \right.$$
$$\left. - \hat{J}_1(X)^{p+1} + \sum_{i,j} \hat{a}_{i,j,2} X^{ip+jp^2} + \hat{g}_2(X, X^p, \hat{J}_1(X)^p)^{1/p} \right]. \quad (3.3)$$

Proof. By Theorem 3 of [LST64], we have that if $(j_0, J_1, \ldots)$ is the j-invariant of the canonical lifting of the curve with j-invariant j_0, then

$$\Phi_p((j_0, J_1, \ldots), (j_0^p, J_1^p, \ldots)) = 0. \quad (3.4)$$

So, if $\boldsymbol{j} = (j_0, J_1, J_2, \ldots)$ and $\hat{\boldsymbol{\jmath}} = (\hat{\jmath}_0, \hat{J}_1, \hat{J}_2, \ldots)$ are the j and $\hat{\jmath}$-invariants of the canonical lifting of the curves with j and $\hat{\jmath}$-invariants j_0 and $\hat{\jmath}_0$ respectively, then

$$\hat{\Phi}_p((\hat{\jmath}_0, \hat{J}_1, \hat{J}_2), (\hat{\jmath}^p, \hat{J}_1^p, \hat{J}_2^p)) \equiv \Phi_p((j_0, J_1, J_2), (j^p, J_1^p, J_2^p)) \equiv 0 \pmod{p^3},$$

and thus the proof is virtually the same as the proof of Theorem 9.1 from [Fin11b]. □

We shall keep the notation of Proposition 3.3 throughout the next section.

4. Pole of J_2 at 1728

We shall prove Theorem 1.3 in this section. We will need some preliminary results.

Lemma 4.1. *Let K be a field and* v *a valuation on K,* $\boldsymbol{u} = (u_0, u_1), \boldsymbol{v} = (v_0, v_1) \in \boldsymbol{W}_2(K)$ *with* $\mathrm{v}(u_0) = 0$, $\mathrm{v}(v_0) = 1$, *and* $\mathrm{v}(u_1), \mathrm{v}(v_1) \geq 0$. *If* $\boldsymbol{w} = (w_0, w_1) = \boldsymbol{u} \cdot \boldsymbol{v}$, *then* $\mathrm{v}(w_1) \geq \min\{\mathrm{v}(v_1), p\}$.

Proof. This is a simple application of the formulas for products of Witt vectors. Since

$$w_1 = u_0^p v_1 + u_1 v_0^p,$$

clearly the statement about $\mathrm{v}(w_1)$ holds. $\square$

Let $\mathrm{v}_0 = \mathrm{ord}_{X=0}$, the order of zero at $X = 0$. (We shall keep this notation.) We then have:

Lemma 4.2. *With the previous notation, we have* $\mathrm{v}_0(\hat{J}_1) \geq \min\{\mathrm{v}_0(\tilde{\tilde{J}}_i), p\}$, *and* $\mathrm{v}_0(\tilde{\tilde{J}}_1) \geq \min\{\mathrm{v}_0(\hat{J}_1), p\}$.

Proof. Let

$$\hat{X} \stackrel{\text{def}}{=} -1728 \frac{27X}{27X+4}, \qquad \tilde{\tilde{X}} \stackrel{\text{def}}{=} -\frac{4X}{27(X+1728)},$$

and

$$\hat{\boldsymbol{\jmath}}(X) = (X, \hat{J}_1(X)), \qquad \tilde{\tilde{\boldsymbol{\jmath}}}(X) = (X, \tilde{\tilde{J}}_1(X)).$$

Then, by Eq. (3.2), we have that

$$\hat{\boldsymbol{\jmath}}(X) = -\frac{1728 \cdot 27}{27\tilde{\tilde{\boldsymbol{\jmath}}}(\tilde{\tilde{X}}) + 4} \cdot \tilde{\tilde{\boldsymbol{\jmath}}}(\tilde{\tilde{X}}).$$

Let

$$-\frac{1728 \cdot 27}{27\tilde{\tilde{\boldsymbol{\jmath}}}(\tilde{\tilde{X}}) + 4} = (\alpha_0(X), \alpha_1(X)).$$

By Propositions 4.2 and 4.3 of [Fin10], we have that $\mathrm{v}_0(\tilde{\tilde{J}}_1(X)) \geq (p-1)/2$, and hence the left hand side of this equation is regular at $X = 0$. Moreover, it is different from zero when evaluated at $X = 0$ (or $\tilde{\tilde{X}} = 0$), and therefore we have that $\mathrm{v}_0(\alpha_0) = 0$, and $\mathrm{v}_0(\alpha_1) \geq 0$. We can then apply Lemma 4.1, and thus $\mathrm{v}_0(\hat{J}_1) \geq \min\{\mathrm{v}_0(\tilde{\tilde{J}}_1), p\}$, and thus $\mathrm{v}_0(\hat{J}_1) \geq (p-1)/2$.

We also have, again by Eq. (3.2), that

$$\tilde{\tilde{\boldsymbol{\jmath}}}(X) = -\frac{4}{27(\hat{\boldsymbol{\jmath}}(\hat{X}) + 1728)} \cdot \hat{\boldsymbol{\jmath}}(\hat{X}).$$

Let

$$-\frac{4}{27(\hat{\boldsymbol{\jmath}}(\hat{X}) + 1728)} = (\beta_0(X), \beta_1(X)).$$

Again, since $\mathrm{v}_0(\hat{J}_1) \geq (p-1)/2$, the left hand side of this equation is regular at $X = 0$, and different from zero when evaluated at $X = 0$ (or $\hat{X} = 0$), and hence $\mathrm{v}_0(\beta_0) = 0$, and $\mathrm{v}_0(\beta_1) \geq 0$. Lemma 4.1 then gives us that $\mathrm{v}_0(\tilde{\tilde{J}}_1) \geq \min\{\mathrm{v}_0(\hat{J}_1), p\}$. $\square$

Lemma 4.3. *The following are equivalent:*

(1) $J_2(X)$ *has a pole of order* p *at* $X = 1728$.
(2) $\hat{J}_2(X)$ *has a pole of order* p *at* $X = 0$.

(3) $\hat{a}_{0,0,2} \neq 0$.

Proof. The equivalence of the first two items is an immediate consequence of Eq. (3.1) and arithmetic of Witt vectors. More precisely, if $1728 = (\gamma_0, \gamma_1, \gamma_2)$, then

$$\hat{J}_1(X - 1728) = J_1(X) + \gamma_1 + \eta_1(X, \gamma_0).$$

Since, $\eta_1(X, Y)$ is a polynomial and J_1 is regular at $X = 1728$ (by Theorem 1.2), we have that $\hat{J}_1$ is regular at $X = 0$. In the same way,

$$\hat{J}_2(X - 1728) = J_2(X) + \gamma_2 + f(X, J_1, \gamma_0, \gamma_1)$$

for some polynomial f and hence $\gamma_2 + f(X, J_1, \gamma_0, \gamma_1)$ is regular at $X = 1728$. The equivalence of the first two items then follows immediately.

The equivalence of the last two items follows from Eq. (3.3). Indeed, as observed in the proof of Lemma 4.2, $\hat{J}_1(X)$ has a zero at $X = 0$. This also implies that $\hat{g}_2(X, X^p, \hat{J}_1(X)^p)^{1/p}$ has a zero at $X = 0$. Thus, Eq. (3.3) gives us that $\hat{J}_2(X)$ has a pole of order p at $X = 0$ if, and only if, $\hat{a}_{0,0,2} \neq 0$. $\square$

We shall prove then that $\hat{a}_{0,0,2} \neq 0$. To do this, we follow the same idea used in [Fin11b] to show that the corresponding $a_{0,0,2}$ for the usual modular polynomial Φ_p is zero.

Proposition 4.4. *If $\hat{a}_{0,0,2} = 0$, then $\mathrm{v}_0(\tilde{\tilde{J}}_1) \geq (p+1)/2$.*

Proof. We use square roots of $\hat{\jmath}$ to obtain a simplified polynomial $\hat{\Psi}_p$ such that $\hat{\Psi}_p(\hat{\jmath}_1^{1/2}, \hat{\jmath}_2^{1/2}) = 0$ if the elliptic curves associated to $\hat{\jmath}_1$ and $\hat{\jmath}_2$ have an isogeny of degree p. This is the analogue of the polynomial Ψ_p from [Fin11b] (which we will use again in Section 6), and satisfies the analogous property:

$$\hat{\Phi}_p(X^2, Y^2) = \hat{\Psi}_p(X, Y)\hat{\Psi}_p(X, -Y). \tag{4.1}$$

(This corresponds to Eq. (23) of [Elk98] for $\hat{\Phi}_p$.) This clearly implies that

$$\hat{\Phi}_p(X^2, 0) = \left(\hat{\Psi}_p(X, 0)\right)^2 \tag{4.2}$$

and hence $\hat{\boldsymbol{a}}_{0,0}$ is a square. By Kronecker's relation,

$$\hat{\Psi}_p(X, 0) \equiv X^{p+1} \pmod p \tag{4.3}$$

(as $\hat{\Phi}_p(X, 0) \equiv X^{p+1} \pmod p$). Then, Eq. (4.3) implies that all coefficients of $\hat{\Psi}_p(X, 0)$ are divisible by p, except for the coefficient of X^{p+1}. Thus, by Eq. (4.2), we have that $\mathrm{v}_p(\hat{\boldsymbol{a}}_{i,0}) \geq 2$ for all $i < (p+1)/2$, where v_p denotes the valuation at p.

Since $\hat{\boldsymbol{a}}_{0,0}$ is a square, if $\hat{a}_{0,0,2} = 0$, then $p^4 \mid \hat{\boldsymbol{a}}_{0,0}$, and thus $p^2 \mid \hat{\Psi}_p(0,0)$. This last condition implies that $p^2 \mid \hat{\boldsymbol{a}}_{(p+1)/2,0}$, and we then have that $a_{i,0,1} = 0$ for $i \in \{0, \ldots, (p+1)/2\}$.

Now, the same proof from [Fin10] that gives

$$J_1(X) \equiv -\frac{\Phi_p(X, X^p)}{p(X^{p^2} - X)} \pmod{p}$$

also gives the equivalent formula for $\hat{J}_1$, namely,

$$\hat{J}_1(X) \equiv -\frac{\hat{\Phi}_p(X, X^p)}{p(X^{p^2} - X)} \equiv -\frac{\sum \hat{a}_{i,j,1} X^{i+jp}}{X^{p^2} - X} \pmod{p}.$$

But, by the computation above, this implies that $\mathrm{v}_0(\hat{J}_1) \geq (p+1)/2$. And by Lemma 4.2, we have that $\mathrm{v}_0(\tilde{\hat{J}}_1) \geq (p+1)/2$. $\square$

We finally can prove Theorem 1.3.

Proof of Theorem 1.3. By Lemma 4.3, it suffices to prove that $\hat{a}_{0,0,2} \neq 0$. Assume that $\hat{a}_{0,0,2} = 0$. In the proof of Proposition 5.6 of [Fin10], it is shown if $\tilde{\hat{J}}_1(X)$ has a zero of order greater than or equal to $s+1$ at 0, then the t-th derivative of J_1 at $X = 1728$ is given by $J_1^{(t)}(1728) = -(t-1)!(-1728)^{1-t}$ for $1 \leq t \leq s$. Hence, by Proposition 4.4, we obtain that

$$\begin{aligned} J_1^{((p-1)/2)}(1728) &= -((p-3)/2)!\,(-1728)^{-(p-3)/2} \\ &= (-1)^{(p-1)/2}((p-3)/2)!\,1728^{(p+1)/2}. \end{aligned} \tag{4.4}$$

Now, since $p \equiv 3 \pmod 4$, we have that Eq. (38) from [KZ98] (or from Theorem 3.2(3) from [Fin10]) reduces to

$$\begin{aligned} J_1'(X) &= -X^{p-1} + X^r \frac{(X-1728)^{(p+1)/2}}{\mathrm{ss}_p(X)^2} \\ &= -X^{p-1} + (X-1728)^{(p-3)/2} \frac{X^r}{f(X)}, \end{aligned} \tag{4.5}$$

where

$$r \stackrel{\text{def}}{=} \begin{cases} (2p-2)/3, & \text{if } p \equiv 1 \pmod 6, \\ (2p+2)/3, & \text{if } p \equiv 5 \pmod 6, \end{cases}$$

and $f(1728) \neq 0$.

Now, since

$$\frac{d^{(p-3)/2}}{dX^{(p-3)/2}} \left(-X^{p-1}\right)\Big|_{X=1728} = (-1)^{(p-1)/2}((p-3)/2)!\,1728^{(p+1)/2},$$

while
$$\frac{d^{(p-3)/2}}{dX^{(p-3)/2}}\left((X-1728)^{(p-3)/2}\frac{X^r}{f(X)}\right)\bigg|_{X=1728}=\frac{1728^r}{f(1728)}\neq 0,$$
Eq. (4.5) implies that $J_1^{(p-1)/2}(1728)\neq(-1)^{(p-1)/2}((p-3)/2)!\,1728^{(p+1)/2}$, contradicting Eq. (4.4). Thus, we must have that $\hat{a}_{0,0,2}\neq 0$. □

5. Formula for J_3

We will now deduce the formula for J_3 from Eq. (2.4).

As with proof of the formula for J_2 from [Fin11b] (the analogous to Eq. (3.3) above), the main idea is again to use Eq. (3.4).

We will use the notation of Theorems 2.4 and 2.5 for $\boldsymbol{f}=\Phi_p$. So, in particular, $f=(x_0-y_0^p)(x_0^p-y_0)$ (by Kronecker's relation) and $f_{x_0}=x_0^p-y_0$. Thus, we can obtain J_3 by evaluating Eq. (2.4) at $((x_0,\ldots,x_3),(y_0,\ldots,y_3))=((j_0,J_1,J_2,J_3),(j_0^p,J_1^p,J_2^p,J_3^p))$. Thus, we can find an expression for J_3^p.

On the other hand, terms from Eq. (2.4) that are divisible by $(x_0^p-y_0)$ will vanish when evaluating, and hence can be discarded from the formula for J_3.

Since we will often lift to characteristic 0 and use Eq. (2.2), we should note that since $(\boldsymbol{x}^p-\boldsymbol{y})$ is primitive, we have that if $\boldsymbol{g}\in\mathbb{Z}[\boldsymbol{x},\boldsymbol{y}]$ and $\boldsymbol{g}=(\boldsymbol{x}^p-\boldsymbol{y})\boldsymbol{g}_1$, with $\boldsymbol{g}_1\in\mathbb{Q}[x_0,x_1,\ldots,y_0,y_1,\ldots]$, then in fact $\boldsymbol{g}_1$ has integral coefficients.

Lemma 5.1. *If $p\neq 2$, then $\eta_k(f)\equiv 0 \pmod{(x_0^p-y_0)}$ for all $k\geq 1$.*

Proof. We have that $\eta_k(f)=\eta_k(\boldsymbol{f}_1)$, where $\boldsymbol{f}_1=(\boldsymbol{x}-\boldsymbol{y}^p)(\boldsymbol{x}^p-\boldsymbol{y})$. Then, if $p\neq 2$, we have
$$\boldsymbol{f}_1^{[p^k]}=(\boldsymbol{x}^{p^k}-\boldsymbol{y}^{p^{k+1}})(\boldsymbol{x}^{p^{k+1}}-\boldsymbol{y}^{p^k})=(\boldsymbol{x}^p-\boldsymbol{y})\boldsymbol{f}_{1,k},$$
for some $\boldsymbol{f}_{1,k}\in\mathbb{Z}[\boldsymbol{x},\boldsymbol{y}]$. Thus,
$$\frac{\boldsymbol{f}_1^{[p^k]}-\boldsymbol{f}_1^{p^k}}{p^k}=(\boldsymbol{x}^p-\boldsymbol{y})\boldsymbol{f}_{2,k}.$$
Hence, with $k=1$ we have that $\eta_1(\boldsymbol{f}_1)\equiv 0 \pmod{(x_0^p-y_0)}$.

Inductively, we get
$$\frac{\boldsymbol{f}^{[p^k]}-\boldsymbol{f}^{p^k}}{p^k}-\frac{\eta_1(\boldsymbol{f})^{p^{k-1}}}{p^{k-1}}-\cdots-\frac{\eta_{k-1}(\boldsymbol{f})^p}{p}\equiv 0 \pmod{(\boldsymbol{x}^p-\boldsymbol{y})},$$
and hence $\eta_k(f)\equiv 0 \pmod{(x_0^p-y_0)}$. □

Lemma 5.2. *If $g_1\equiv 0 \pmod{(x_0^p-y_0)}$, then $\eta_k(g_1,g_2)\equiv 0 \pmod{(x_0^p-y_0)}$.*

Proof. Let $\boldsymbol{g}_1,\boldsymbol{g}_2\in\mathbb{Z}[\boldsymbol{x},\boldsymbol{y}]$ be liftings of g_1 and g_2. Since $g_1\equiv 0 \pmod{(x_0^p-y_0)}$, we can assume that $\boldsymbol{g}_1\equiv 0 \pmod{(\boldsymbol{x}^p-\boldsymbol{y})}$.

We clearly have that

$$\sum_{i=1}^{p^k-1} \frac{1}{p^n}\binom{p^k}{i} \boldsymbol{g}_1^i \boldsymbol{g}_2^{p^k-i} \equiv 0 \pmod{(\boldsymbol{x}^p - \boldsymbol{y})}$$

(in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$). If $k = 1$, then we obtain $\eta_1(g_1, g_2) = \eta_1(\boldsymbol{g}_1, \boldsymbol{g}_2) \equiv 0 \pmod{(x_0^p - y_0)}$.

Inductively, we obtain that $\eta_k(g_1, g_2) = \eta_k(\boldsymbol{g}_1, \boldsymbol{g}_2) \equiv 0 \pmod{(x_0^p - y_0)}$, as it is the reduction modulo p of

$$\sum_{i=1}^{p^k-1} \frac{1}{p^n}\binom{p^k}{i} \boldsymbol{g}_1^i \boldsymbol{g}_2^{p^k-i} - \frac{\eta_1(\boldsymbol{g}_1, \boldsymbol{g}_2)^{p^{k-1}}}{p^{k-1}} - \cdots - \frac{\eta_{k-1}(\boldsymbol{g}_1, \boldsymbol{g}_2)^p}{p} \equiv 0 \pmod{(\boldsymbol{x}^p - \boldsymbol{y})}.$$

□

The following Lemma gives particular cases of Proposition 4.4 from [Fin11a]:

Lemma 5.3. *Let*

$$\begin{aligned}
\mathcal{M}_{i,1} &\stackrel{\text{def}}{=} \eta_i(X_1, \ldots, X_n)\\
\mathcal{M}_{i,2} &\stackrel{\text{def}}{=} \eta_i(X_{n+1}, \ldots, X_{n+m})\\
\mathcal{M}_{i,3} &\stackrel{\text{def}}{=} \eta_i(X_1 + \cdots + X_n, X_{n+1} + \cdots + X_{n+m}).
\end{aligned}$$

Then, we have

$$\eta_1(X_1, \ldots, X_{n+m}) = \mathcal{M}_{1,1} + \mathcal{M}_{1,2} + \mathcal{M}_{1,3}.$$

and

$$\eta_2(X_1, \ldots, X_{n+m}) = \mathcal{M}_{2,1} + \mathcal{M}_{2,2} + \mathcal{M}_{2,3} + \eta_1(\mathcal{M}_{1,1}, \mathcal{M}_{1,2}, \mathcal{M}_{1,3}).$$

In particular, if $m = 1$, we get

$$\eta_1(X_1, \ldots, X_{n+1}) = \mathcal{M}_{1,1} + \mathcal{M}_{1,3}$$

and

$$\eta_2(X_1, \ldots, X_{n+1}) = \mathcal{M}_{2,1} + \mathcal{M}_{2,3} + \eta_1(\mathcal{M}_{1,1}, \mathcal{M}_{1,3}).$$

We then have:

Proposition 5.4. *Let $p \geq 3$ and*

$$\mathcal{H}_1 \stackrel{\text{def}}{=} \operatorname{vec}\left((f_x)^p x_1 + (f_y)^p y_1 + \sum_{i,j} a_{i,j,1} x_0^{ip} y_0^{ip} \right),$$

$$h = f_{x_0}^{p^2} x_2 + f_{y_0}^{p^2} y_2 + \left(\sum_{i,j} b_{i,j,1} x_0^{ip} y_0^{jp}\right)^p x_1^p + \left(\sum_{i,j} c_{i,j,1} x_0^{ip} y_0^{jp}\right)^p y_1^p$$
$$+ (f_{x_0 x_0}/2)^{p^2} x_1^{2p} + f_{x_0 y_0}^{p^2} x_1^p y_1^p + (f_{y_0 y_0}/2)^{p^2} y_1^{2p} + \sum_{i,j} a_{i,j,2} x_0^{ip^2} y_0^{jp^2},$$

and $\mathcal{H}_2 = \operatorname{vec}(h)$. *Then (still with the notation from Theorem 2.5),*

$$\eta_2(\mathcal{G}_1) \equiv \eta_2(\mathcal{H}_1) \pmod{(x_0^p - y_0)}$$

and

$$\eta_1(\mathcal{G}_2) \equiv \eta_1(\mathcal{H}_2) + \eta_1(h, \eta_1(\mathcal{H}_1)) \pmod{(x_0^p - y_0)}.$$

Proof. Let

$$h_1 = \sum_{t \in \mathcal{H}_1} t = (f_x)^p x_1 + f_y^p y_1 + \sum_{i,j} a_{i,j,1} x_0^{ip} y_0^{ip}.$$

By Lemma 5.3, we have

$$\eta_2(\mathcal{G}_1) = \eta_2(\mathcal{H}_1) + \eta_2\left(h_1, \eta_1(f)\right) + \eta_1\left(\eta_1(\mathcal{H}_1), \eta_1\left(h_1, \eta_1(f)\right)\right).$$

By Lemma 5.1, $\eta_1(f) \equiv 0 \pmod{(x_0^p - y_0)}$ and thus, by Lemma 5.2, we get the first desired congruence.

Also, again by Lemma 5.3,

$$\eta_1(\mathcal{G}_2) = \eta_1(\mathcal{H}_2) + \eta_1(\eta_1(\mathcal{G}_1), \eta_2(f)) + \eta_1\left(h, \eta_1(\mathcal{G}_1) + \eta_2(f)\right). \tag{5.1}$$

By Lemmas 5.1, 5.2, and 5.3, we get that

$$\eta_1(\mathcal{G}_1) = \eta_1(\mathcal{H}_1) + \eta_1\left(h_1, \eta_1(f)\right) \equiv \eta_1(\mathcal{H}_1) \pmod{(x_0^p - y_0)}$$

and

$$\eta_1(\eta_1(\mathcal{G}_1), \eta_2(f)) \equiv 0 \pmod{(x_0^p - y_0)}. \tag{5.2}$$

Moreover, since $\frac{1}{p}\binom{p}{i} \in \mathbb{Z}$ for $i \in \{1, \dots, p-1\}$, we get

$$\begin{aligned}
\eta_1(h, \eta_1(\mathcal{G}_1) + \eta_2(f)) &= \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} h^i (\eta_1(\mathcal{G}_1) + \eta_2(f))^{p-i} \\
&\equiv \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} h^i (\eta_1(\mathcal{H}_1))^{p-1} \qquad (5.3) \\
&= \eta_1(h, \eta_1(\mathcal{H}_1)) \pmod{(x_0^p - y_0)}.
\end{aligned}$$

Thus, Eqs. (5.1), (5.2), and (5.3) give the desired formula. □

Finally, we can give the simplified formula for J_3.

Theorem 5.5. *Let $p \geq 3$. With the notation above, we have that if $g_3(x_0, x_1, x_2, y_0, y_1, y_2) \stackrel{\text{def}}{=} \eta_2(\mathcal{H}_1) + \eta_1(\mathcal{H}_2) + \eta_1(h, \eta_1(\mathcal{H}_1))$, then $g_3(X, J_1(X), J_2(X), X^p, J_1(X)^p, J_2(X)^p)$ is a p-th power and*

$$
\begin{aligned}
J_3(X) = -\frac{1}{(X^{p^2}-X)^{p^2}} \Bigg[& \sum_{i,j} a_{i,j,3} X^{ip^2+jp^3} \\
& + \left(\sum_{i,j} b_{i,j,1} X^{ip^2+jp^3} \right) J_2 + \left(\sum_{i,j} c_{i,j,1} X^{ip^2+jp^3} \right) J_2^p \\
& + \left(\sum_{i,j} b_{i,j,2} X^{ip^2+jp^3} \right) J_1^p + \left(\sum_{i,j} c_{i,j,2} X^{ip^2+jp^3} \right) J_1^{p^2} \\
& - (J_1^p J_2^p + J_1^{p^2} J_2) + \left(\sum_{i,j} d_{i,j,1} X^{ip^2+jp^3} \right) J_1^{2p} \\
& + \left(\sum_{i,j} e_{i,j,1} X^{ip^2+jp^3} \right) J_1^{p+p^2} + \left(\sum_{i,j} f_{i,j,1} X^{ip^2+jp^3} \right) J_1^{2p^2} \\
& + g_3(X, J_1, J_2, X^p, J_1^p, J_2^p)^{1/p} \Bigg]
\end{aligned} \tag{5.4}
$$

Proof. Applying the formula for the Greenberg transform from Theorem 2.5 to $\Phi_p(\boldsymbol{x}, \boldsymbol{y})$ and evaluating at $(x_0, x_1, x_2, x_2, y_0, y_1, y_2, y_3) = (X, J_1, J_2, J_3, X^p, J_1^p, J_2^p, J_3^p)$ should give zero by Eq. (3.4).

We then obtain the desired formula applying Proposition 5.4 to simplify the terms involving the η_i's, solving for J_3^p, and taking p-th roots. Observe that since Φ_p has integral coefficients, we have that the coefficients of the sums above are in $\mathbb{F}_p$, and so invariant under p-th powers.

Finally, the fact that g_3 is a p-th power follows from the fact that $J_3(X) \in \mathbb{F}_p(X)$. [See [Fin10].] $\square$

We have computed J_3 before in [Fin11a] by using general methods to compute the Greenberg transform of a polynomial (by means of Theorem 2.5 above). The simplification given by Proposition 5.4 above gives significant improvements in memory usage. Table 5.1 below shows differences in times and memory usages with ("New") and without ("Old") using Proposition 5.4. The tests were performed using MAGMA (version 2.16-1) on a Dell Precision 690 server with two dual-core 64 bit 3.2 gigahertz Inter Xeon processors, 16 gigabytes of RAM, and 8 gigabytes of swap, running Fedora Core 11 (GNU/Linux) with kernel 2.6.30.

	Old		New	
Char.	time (sec.)	memory (MB)	time (sec.)	memory (MB)
7	7.300	40.97	5.089	33.22
11	421.090	1010.03	289.439	103.94
13	6542.590	4175.28	7496.840	356.16
17	−−	−−	45967.959	1982.28
19	−−	−−	267733.840	3650.62
23	−−	−−	1574171.979	13647.28

TABLE 5.1. Computations of J_3

6. Pole of J_3 at 0

In this section we prove Theorem 1.4. We shall keep the notation from the previous sections and assume $p \geq 5$.

Lemma 6.1. *Let $p \geq 5$. The function $g_3(X, J_1, J_2, X^p, J_1^p, J_2^p)$ has a zero at $X = 0$. Thus, we have that, with notation of Theorem 5.5, $J_3(X)$ has a pole at $X = 0$ of order p^2 if, and only if, $a_{0,0,3} \neq 0$.*

Proof. By Theorem 1.2, we have that J_1 and J_2 have zeros at $X = 0$. In particular, we have that $a_{0,0,k} = 0$ for $k \in \{0, 1, 2\}$. (See Proposition 9.4 from [Fin11b].) Thus, every entry of the vectors $\mathcal{H}_1$ and $\mathcal{H}_2$ when evaluated at $(X, J_1, J_2, X^p, J_1^p, J_2^p)$ are divisible by X. Clearly, also h evaluated at $(X, J_1, J_2, X^p, J_1^p, J_2^p)$ is divisible by X. Thus, this must be the case also for all $\eta_1(\mathcal{H}_2)$, $\eta_2(\mathcal{H}_1)$, and $\eta_1(h, \eta_1(\mathcal{H}_1))$, and hence for g_3. □

Thus, we need to show that if $p \equiv 5 \pmod 6$, then $a_{0,0,3} \neq 0$, i.e., $\mathrm{v}_p(\boldsymbol{a}_{0,0}) = 3$. It turns out that this is related to Conjecture 9.10 of [Fin11b], which is equivalent to the second item of Conjecture 9.3 in the same reference. More precisely, these conjectures state the following:

Theorem 6.2. *Let $p \geq 5$. We have that $J_2(X)$ has a zero of order (exactly) sp, where $s = (2\lfloor (p-1)/6 \rfloor + 1)$, at $X = 0$, or equivalently, that $\mathrm{v}_p(\boldsymbol{a}_{s+1,0}) = 2$.*

The equivalence of the two statements in the theorem above is proved in [Fin11b]. Before we can explicitly show the connection between Theorems 1.4 and 6.2, we need a little more notation.

Let $\Psi_p(X, Y)$ be as in [Fin11b], i.e., $\Psi_p(X, Y)$ is the polynomial proposed by Atkin such that $\Psi_p(j^{1/3}, (j')^{1/3}) = 0$ if the elliptic curves associated to j and j' have an isogeny of degree p. (See, for instance, [Elk98].) This polynomial also satisfies:

$$\Phi_p(X^3, Y^3) = \Psi_p(X, Y)\Psi_p(X, \omega Y)\Psi_p(X, \omega^2 Y), \tag{6.1}$$

where $\omega \stackrel{\text{def}}{=} \mathrm{e}^{2\pi \mathrm{i}/3}$. (This is Eq. (23) of [Elk98].) This clearly implies that

$$\Phi_p(X^3, 0) = (\Psi_p(X, 0))^3 \tag{6.2}$$

and, by Kronecker's relation,

$$\Psi_p(X, 0) \equiv X^{p+1} \pmod{p} \tag{6.3}$$

(as $\Phi_p(X, 0) \equiv X^{p+1} \pmod{p}$). Let's write

$$\Phi_p(X, 0) = \sum_{i=0}^{p+1} \boldsymbol{a}_i X^i \qquad \text{and} \qquad \Psi_p(X, 0) = \sum_{i=0}^{p+1} \boldsymbol{b}_i X^i.$$

(So, $\boldsymbol{a}_i = \boldsymbol{a}_{i,0}$.) Then, Eq. (6.3) implies that $p \mid \boldsymbol{b}_i$ for $i \in \{0, \ldots, p\}$ and $p \nmid \boldsymbol{b}_{p+1}$. Thus, by Eq. (6.2), we have that $\mathrm{v}_p(\boldsymbol{a}_{i,0}) \geq 3$ for all $i < (p + 1)/3$.

Proposition 6.3. *Let $p \geq 5$ and*

$$i_0 \stackrel{\text{def}}{=} \begin{cases} 2, & \text{if } p \equiv 1 \pmod{6}, \\ 0, & \text{if } p \equiv 5 \pmod{6}. \end{cases}$$

Then, with the notation above, we have that the following are equivalent:

(1) $\mathrm{v}_p(\boldsymbol{a}_{i_0}) = 3$*;*
(2) $\mathrm{v}_p(\boldsymbol{b}_{i_0}) = 1$*;*
(3) $\mathrm{v}_p(\boldsymbol{a}_{s+1}) = 2$*, where* $s \stackrel{\text{def}}{=} (2 \lfloor (p-1)/6 \rfloor + 1)$*.*

Proof. We have that if $p \equiv 1 \pmod{6}$, then $\boldsymbol{a}_0 = \boldsymbol{a}_1 = 0$. (See, for instance, Proposition 9.4 from [Fin11b].) Thus, by Eq. (6.2), we have also that $\boldsymbol{b}_0 = \boldsymbol{b}_1 = 0$.

Then, by Eq. (6.2) again, we have in general that $\boldsymbol{a}_{i_0} = \boldsymbol{b}_{i_0}^3$, and hence $\mathrm{v}_p(\boldsymbol{a}_{i_0}) = 3$ if, and only if, $\mathrm{v}_p(\boldsymbol{b}_{i_0}) = 1$.

Observe now that $3(s + 1) = p + 1 + 2i_0$. So, the coefficient on X^{p+1+2i_0} of the left hand side of Eq. (6.2) is $\boldsymbol{a}_{s+1}$, while on the left hand side is $\sum_{i+j+k=p+1+2i_0} \boldsymbol{b}_i\, \boldsymbol{b}_j\, \boldsymbol{b}_k$. In other words,

$$\boldsymbol{a}_{s+1} = 3\boldsymbol{b}_{i_0}^2 \boldsymbol{b}_{p+1} + \sum_{\substack{i+j+k=p+1+2i_0 \\ i,j,k \neq p+1}} \boldsymbol{b}_i\, \boldsymbol{b}_j\, \boldsymbol{b}_k.$$

Thus, by our remarks above on the valuations of the $\boldsymbol{b}_i$'s, we have that $\mathrm{v}_p(\boldsymbol{a}_{s+1}) = 2$ if, and only if, $\mathrm{v}_p(\boldsymbol{b}_{i_0}) = 1$. $\square$

The next proposition then proves Theorems 1.4 and 6.2.

Proposition 6.4. *With the previous notation (and still $p \geq 5$), we have that $\mathrm{v}_p(\boldsymbol{b}_{i_0}) = 1$, and hence $\mathrm{v}_p(\boldsymbol{a}_{s+1,0}) = 2$ and $\mathrm{v}_p(\boldsymbol{a}_{i_0,0}) = 3$.*

Proof. As observed in [Fin10], we have that J_1 is the reduction modulo p of

$$-\frac{\Phi_p(X, X^p)}{p(X^{p^2} - X)} = -\frac{1}{X^{p^2} - X}\left[\sum_{i=0}^{p-1} \frac{\boldsymbol{a}_{i,0}}{p} X^i + \frac{X^p}{p} \sum{}' \boldsymbol{a}_{i,j} X^{i+jp-p}\right],$$

where $\sum'$ is a sum over (i, j) such that either $j \neq 0$ or $i \geq p$. Moreover, by Theorem 3.2 from this reference, we have that J_1 has a zero of order exactly $r \stackrel{\text{def}}{=} \lfloor (2p + 1)/3 \rfloor$ at $X = 0$. Therefore, $\mathrm{v}_p(\boldsymbol{a}_{i,0}) \geq 2$, for $i \in \{0, \ldots, r\}$, and $\mathrm{v}_p(\boldsymbol{a}_{r+1,0}) = 1$. Using the notation above, the coefficient of $3r + 3 = 2p + 2 + i_0$ in the left hand side of Eq. (6.2) is $\boldsymbol{a}_{r+1}$, while on the right hand side is

$$\sum_{i+j+k=2p+2+i_0} \boldsymbol{b}_i\, \boldsymbol{b}_j\, \boldsymbol{b}_k = 3\boldsymbol{b}_{i_0} \boldsymbol{b}_{p+1}^2 + \sum{}^* \boldsymbol{b}_i\, \boldsymbol{b}_j\, \boldsymbol{b}_k,$$

where $\sum^*$ is the sum over (i, j, k) such that $i + j + k = 2p + 2 + i_0$ and at most one of them is equal to $(p + 1)$. Since $p \mid \boldsymbol{b}_i$ for $i \in \{0, \ldots, p\}$ and $p \nmid \boldsymbol{b}_{p+1}$, as observed above, we have that $p^2 \mid \sum^* \boldsymbol{b}_i\, \boldsymbol{b}_j\, \boldsymbol{b}_k$, and since $\mathrm{v}_p(\boldsymbol{a}_{r+1}) = 1$, we must have that $\mathrm{v}_p(\boldsymbol{b}_{i_0}) = 1$. □

7. Refinements on the Formulas for J_2 and J_3

With the results from the previous sections, we are able to give more precise descriptions of J_2 and J_3.

We need some 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, [Fin09]),

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

Hence, $S_p(X) \in \mathbb{F}_p[X]$, and $S_p(0), S_p(1728) \neq 0$. (See, for instance, [Fin09].) Also, let

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

With this notation, [Fin10] (heavily relying on results from [KZ98] and [dS94]) gives a very precise description of J_1:

Theorem 7.1. *Let* $p \geq 5$ *and*

$$J_1(X) = F_1(X)/G_1(X), \qquad \text{with } F_1, G_1 \in \mathbb{F}_p[X] \text{ and } (F_1, G_1) = 1.$$

Then,

(1) $\deg F_1 - \deg G_1 = p - \iota$.
(2) F_1 *(and hence* J_1*) has a zero at* 0 *of order (exactly)* $r \stackrel{\text{def}}{=} \lfloor (2p+1)/3 \rfloor$.
(3) *Assuming* G_1 *is monic, we have* $G_1(X) = S_p(X)$.
(4) $\deg F_1 = p - \iota + S_p(X)$. *(Note that* $\deg S_p(X) = \lfloor (p-1)/4 \rfloor - \lceil (p-1)/6 \rceil$. *See, for instance,* [Fin09].*)*

Now we can give the corresponding result for J_2:

Theorem 7.2. *Let* $p \geq 5$ *and*

$$J_2(X) = F_2(X)/G_2(X), \qquad \text{with } F_2, G_2 \in \mathbb{F}_p[X] \text{ and } (F_2, G_2) = 1.$$

Then,

(1) $\deg F_2 - \deg G_2 = p^2 - \iota$.
(2) F_2 *(and hence* J_2*) has a zero at* 0 *of order (exactly)* sp*, where* $s \stackrel{\text{def}}{=} (2 \lfloor (p-1)/6 \rfloor + 1)$.
(3) *Assuming* G_2 *is monic, we have* $G_2(X) = (X - 1728)^{\epsilon p} S_p(X)^{2p+1}$.
(4) $\deg F_2 = p^2 - \iota + (2p+1) \deg S_p(X) + p\epsilon$.

Proof. Most of these properties are given by Theorem 9.6 from [Fin10]. The missing ones are given by Theorem 6.2 above. □

We will now deal with J_3, although we will not be able to be as precise as Theorems 7.1 and 7.2 above. To deal with g_3 from Eq. (5.4), we need the following lemma:

Lemma 7.3. *Let* K *be a field of rational functions over* $\Bbbk$ *and* v *be a valuation on* K *such that* $\mathrm{v}(a) = 0$ *for all* $a \in \Bbbk^{\times}$. *Let* $(\alpha_1, \ldots, \alpha_n)$ *be a vector with coefficients in* K*, and assume that* $\min\{\mathrm{v}(\alpha_i) \,:\, i \in \{1, \ldots, n\}\} = v_0$. *Then,* $\mathrm{v}(\eta_k(\alpha_1, \ldots, \alpha_n)) \geq p^k v_0$.

Proof. By a simple induction, we see that $\eta_k(X_1, \ldots, X_n)$ is a homogeneous polynomial (with coefficients in $\mathbb{Z}$) of degree p^k. The lemma then immediately follows. □

Theorem 7.4. *Let* $p \geq 5$ *and*

$$J_3(X) = F_3(X)/G_3(X), \qquad \text{with } F_3, G_3 \in \mathbb{F}_p[X] \text{ and } (F_3, G_3) = 1.$$

Then,

(1) $\deg F_3 - \deg G_3 = p^3 - \iota$.

(2) *F_3 (and hence J_3) does not have a zero at $X = 0$ unless $p \equiv 1 \pmod 6$, but in this case it has a zero at 0 of order (exactly) p^2.*

(3) *Assuming G_3 is monic, we have $G_3(X) = X^{\delta p^2}(X - 1728)^{\epsilon i} S_p(X)^{3p^2+2p}$ for some $i \in \{0, \dots, 2p^2\}$.*

(4) *With i as above, $\deg F_3 = (p^3 - \iota) + \delta p^2 + \epsilon i + (3p^2 + 2p)\deg(S_p)$.*

Proof. This theorem follows directly from Eq. (5.4) and Lemma 7.3.

For the first item, we have that $\deg F_3 - \deg G_3$ is the order of pole at infinity of J_3. By Theorems 7.1 and 7.2, we have that J_1 and J_2 have poles of order $p - \iota$ and $p^2 - \iota$, respectively. Also, as seen [Fin10], we have that

$$\deg\left(\sum_{i,j} b_{i,j,1} X^{ip+jp^2}\right) = p^3 + p^2 - p \qquad \text{and} \qquad \deg\left(\sum_{i,j} c_{i,j,1} X^{ip+jp^2}\right) \leq p^3.$$

In a similar way, we have

$$\begin{aligned}
&\deg\left(\sum_{i,j} b_{i,j,1} X^{ip^2+jp^3}\right) = p^4 + p^3 - p^2, &&\deg\left(\sum_{i,j} c_{i,j,1} X^{ip^2+jp^3}\right) \leq p^4,\\
&\deg\left(\sum_{i,j} b_{i,j,2} X^{ip^2+jp^3}\right) \leq p^4 + p^3 - p^2, &&\deg\left(\sum_{i,j} d_{i,j,1} X^{ip^2+jp^3}\right) \leq p^4 + p^3 - 2p^2,\\
&\deg\left(\sum_{i,j} e_{i,j,1} X^{ip^2+jp^3}\right) \leq p^4 - p^2, &&\deg\left(\sum_{i,j} f_{i,j,1} X^{ip^2+jp^3}\right) \leq p^4 - p^3.
\end{aligned}$$

Now, applying Lemma 7.3 with v as the order of zero at infinity to the definition of g_3 gives that $g_3(X, \dots, J_2^p)^{1/p}$ has a pole of order at most $p^4 + p^3 - p$. Comparing with the order of poles of the other terms we obtain the desired result.

The first observation of the second item is an immediate consequence of Theorem 1.4. Now, in case $a_{0,0,3} = 0$, i.e., $p \equiv 1 \pmod 6$, we need to analyze the orders of zeros at 0 of the terms in Eq. (5.4).

So, suppose that $p \equiv 1 \pmod 6$ and let v_0 denote again the order of zero at $X = 0$. Then, from Theorems 7.1 and 7.2, we get $\mathrm{v}_0(J_1) = r$ and $\mathrm{v}_0(J_2) = sp$, where $r \stackrel{\text{def}}{=} \lfloor (2p+1)/3 \rfloor$ and $s \stackrel{\text{def}}{=} (2\lfloor (p-1)/6 \rfloor + 1)$. This is in fact a consequence of Proposition 9.4 from [Fin11b], which states that $\boldsymbol{a}_{0,0} = \boldsymbol{a}_{1,0} = 0$ (if $p \equiv 1 \pmod 6$), $\boldsymbol{a}_{i,0} \equiv 0 \pmod{p^2}$ for $i \in \{0, \dots, r\}$, and $\boldsymbol{a}_{i,0} \equiv 0 \pmod{p^3}$ for $i \in \{0, \dots, s\}$. Since in this case $r \geq 5$ and $s \geq 3$, this implies that $a_{0,0,n} = a_{1,0,n} = 0$ for all n, and that $a_{2,0,2}$, $b_{0,0,1}$, $b_{1,0,1}$, $b_{0,0,2}$, $b_{1,0,2}$, $d_{0,0,1}$ are all equal to zero.

So, all terms inside the brackets of Eq. (5.4), except possibly g_3, has order at zero at least $2p^2$. Among those, we see that only $\sum a_{i,j,3} X^{ip^3+jp^3}$ has order exactly $2p^2$ (by Proposition 6.4).

We also have $\mathrm{v}_0(g_3(X, J_1, J_2, X^p, J_1^p, J_2^p)^{1/p}) > 2p^2$, again by using its definition and Lemma 7.3, which finishes the proof of the second item.

For the third item, we need to find the order of poles at $X = 0$ for all $j_0 \notin \Bbbk^{ord}$, as no ordinary value can give a pole. If $0 \notin \Bbbk^{ord}$, we have seen J_3 has a pole of order p^2 at $X = 0$.

For $j_0 \notin \Bbbk^{ord}$ and $j_0 \neq 0, 1728$, i.e., for the zeros of S_p, we have that the term inside the brackets of Eq. (5.4) with highest order of pole is $J_1^p J_2^p$, having order of pole equal to $2p^2 + 2p$. This includes the pole of $g_3(X, J_1, J_2, X^p, J_1^p, J_2^p)^{1/p}$, which, by Lemma 7.3, is at most $2p^2+p$. Hence, J_3 must have a pole of order $3p^3+2p$ at those values, as $S_p \mid (X^{p^2} - X)$.

Finally, for $j_0 = 1728$, if $\epsilon \neq 0$, then only J_2 can introduce poles, and thus the pole inside the bracket of Eq. (5.4) is of order at most p^2 (again using Lemma 7.3), giving the desired bound.

Finally, the last item is a trivial consequence of first and the third.

□

Acknowledgement. The author would like to thank A. V. Sutherland for suggesting the use of Ψ_p, which was essential to the proofs presented here. Also, the author would like to thank S. Mulay, for very valuable discussions, and the *Centre de Recherches Mathématique*, for providing an stimulating and productive environment in which the main ideas of this paper were born.

References

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

[dS94] 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.

[Elk98] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21–76. Amer. Math. Soc., Providence, RI, 1998.

[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.

[Fin11a] L. R. A. Finotti. Computations with Witt vectors and the Greenberg transform. Submitted. Available at `http://www.math.utk.edu/~finotti/`, 2011.

[Fin11b] L. R. A. Finotti. Computations with Witt vectors of length 3. *J. Théor. Nombres Bordeaux*, 23(2):417–454, 2011.

[Gre61] M. J. Greenberg. Schemata over local rings. *Ann. of Math. (2)*, 73:624–648, 1961.

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

[Lan52] S. Lang. On quasi algebraic closure. *Ann. of Math. (2)*, 55:373–390, 1952.

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

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

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

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