LIFTING THE j-INVARIANT: QUESTIONS OF MAZUR AND TATE

LUÍS R. A. FINOTTI

Abstract. In this paper we analyze the j-invariant of the canonical lifting of an elliptic curve as a Witt vector. We show that its coordinates are rational functions on the j-invariant of the elliptic curve in characteristic p. In particular, we prove that the second coordinate is always regular at $j = 0$ and $j = 1728$, even when those correspond to supersingular values. A proof is given which yields a new proof for some results of Kaneko and Zagier about the modular polynomial.

1. Introduction

Let k be a perfect field of characteristic $p > 0$. We say that an elliptic curve E/k is *ordinary* if the p-torsion subgroup of E is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Associated to an ordinary elliptic curve E, there exists a unique (up to isomorphisms) elliptic curve $\boldsymbol{E}$ over $\boldsymbol{W}(k)$, called the *canonical lifting* of E, and a map $\tau : E(\bar{k}) \to \boldsymbol{E}(\boldsymbol{W}(\bar{k}))$, i.e., a *lift of points*, called the *elliptic Teichmüller lift*, characterized by the following properties:

(1) the reduction modulo p of $\boldsymbol{E}$ is E;
(2) if σ denotes the Frobenius of both k and $\boldsymbol{W}(k)$, then the canonical lifting of E^σ (the elliptic curve obtained by applying σ to the coefficients of the equation that defines E) is $\boldsymbol{E}^\sigma$;
(3) τ is an injective group homomorphism and a section of the reduction modulo p;
(4) let $\phi : E \to E^\sigma$ denote the p-th power Frobenius; then there exists a map $\boldsymbol{\phi} : \boldsymbol{E} \to \boldsymbol{E}^\sigma$, such that the diagram

$$\begin{array}{ccc} \boldsymbol{E}(\boldsymbol{W}(\bar{k})) & \xrightarrow{\boldsymbol{\phi}} & \boldsymbol{E}^\sigma(\boldsymbol{W}(\bar{k})) \\ {\scriptstyle\tau}\Big\uparrow & & \Big\uparrow{\scriptstyle\tau^\sigma} \\ E(\bar{k}) & \xrightarrow{\phi} & E^\sigma(\bar{k}) \end{array}$$

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

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

2000 *Mathematics Subject Classification.* Primary 11G07; Secondary 11F11.

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

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

The j-invariant of the canonical lifting $\boldsymbol{E}$, say $\boldsymbol{j}$, depends only on the j-invariant of E, say j_0. Hence, as a Witt vector, we have

$$\boldsymbol{j} = (j_0, j_1, j_2, \ldots),$$

and the j_i's can be seen as functions of j_0, say $j_n = J_n(j_0)$. B. Mazur asked J. Tate about the nature of these functions. Tate used some of the author's previous computations of canonical liftings of general elliptic curves of small fixed characteristic to explicitly compute these functions in a few cases. More precisely, he found that:

$$j_1 = J_1(j_0) = \begin{cases} 3j_0^3 + j_0^4, & \text{if } p = 5, \\ 3j_0^5 + 5j_0^6, & \text{if } p = 7. \end{cases}$$

(Remember that p denotes the characteristic of the base field.) At this point, Tate asked the author for some more computations. In particular, he was surprised that these functions were polynomials (over $\mathbb{F}_p$), as they are then defined for supersingular values of j_0, such as $j_0 = 0$ for $p = 5$ and $j_0 = -1$ for $p = 7$.

Hence, if all j_n's would turn out to be polynomial functions on j_0, i.e., if $J_i \in \mathbb{F}_p[X]$, then we could use the same functions J_n's to lift supersingular elliptic curves.

More generally, if the functions J_i's are all regular at some supersingular j_0, we shall call the elliptic curve over $\boldsymbol{W}(k)$ associated to the j-invariant $\boldsymbol{j} = (J_0(j_0), J_1(j_0), \ldots)$ a *pseudo-canonical liftings* of the curve associated to j_0. If the functions J_i's are regular for $i \leq n$, then we shall call a *pseudo-canonical liftings modulo* p^{n+1} any curve over $\boldsymbol{W}(k)$ having its j-invariant $\boldsymbol{j}$ congruent to $(J_0(j_0), J_1(j_0), \ldots, J_n(j_0), \ldots)$ modulo p^{n+1}. Tate asked when these pseudo-canonical liftings exist.

Some further computations have shown that in characteristic 5 we have:

$$\begin{multline} J_2(X) = 3X^5 + 2X^{10} + 2X^{13} + 4X^{14} + 4X^{15} + \\ 4X^{16} + X^{17} + 4X^{18} + X^{19} + X^{20} + 3X^{23} + X^{24}, \end{multline}$$

while in characteristic 7, we have:

$$\begin{aligned} J_2(X) = (3X^{21} &+ 6X^{28} + 3X^{33} + 5X^{34} + 4X^{35} + 2X^{36} + 3X^{37} \\ &+ 6X^{38} + 3X^{39} + 5X^{40} + 5X^{41} + 5X^{42} + 2X^{43} + 3X^{44} + 6X^{45} \\ &+ 3X^{46} + 5X^{47} + 5X^{48} + 3X^{49} + 3X^{54} + 5X^{55})/(1 + X^7). \end{aligned} \tag{1.1}$$

So, although for $p = 5$ we have that $J_2(X) \in \mathbb{F}_5[X]$, for $p = 7$ we have that $J_2(X) \in \mathbb{F}_7(X)$ and has a pole of order 7 at -1. This is a bit more consistent with what was expected, as $j_0 = -1$ is supersingular in characteristic 7.

So, one sees that indeed it was too much to expect that $J_n(X) \in \mathbb{F}_p[X]$, but we will show that $J_n(X) \in \mathbb{F}_p(X)$. This is a very superficial answer to Mazur's question, but one can easily get more specific information on J_1. As we shall see, de Shalit's [dS94] and Kaneko and Zagier's [KZ98], which study of the (classical) modular polynomial modulo p^2, easily gives us the following theorems:

Theorem 1.1. *With the notation above, we have that $J_1(X)$ is regular at $X = 0$ and $X = 1728$, even if those values are supersingular, and that $(0, J_1(0)) \equiv 0 \pmod{p^2}$ and $(1728, J_1(1728)) \equiv 1728 \pmod{p^2}$. In other words, $j_0 = 0$ and $j_0 = 1728$ yield pseudo-canonical liftings modulo p^2 whenever those values are supersingular, and these have j-invariants $\boldsymbol{j}$ such that $\boldsymbol{j} \equiv 0 \pmod{p^2}$ and $\boldsymbol{j} \equiv 1728 \pmod{p^2}$ respectively.*

Theorem 1.2. *If $j_0 \neq 0, 1728$ is supersingular, then J_1 has a pole at j_0. In other words, no value of j_0 other than 0 and 1728 can yield pseudo-canonical liftings.*

Before realizing how the above references give the desired answers (modulo p^2), the author came up with a different proof of Theorem 1.1. On the other hand, this proof can be used to obtain a few results from [KZ98], with a very different approach. While the orginal proofs use modular forms, and hence are more analytic in nature, the proof given here is more elementary and algebraic, relying almost exclusively on the existence of the canonical lifting.

2. Rationality of $J_i(X)$

The main goal of this section is to prove the following proposition:

Proposition 2.1. *For any $p \geq 5$, we have that $J_n(X) \in \mathbb{F}_p(X)$.*

We shall assume henceforth that the characteristic, still denoted by p, is greater than or equal to 5. To compute the general form of $J_i(X)$ for this fixed p, one can use the base field

$k_0 \stackrel{\text{def}}{=} \mathbb{F}_p(a_0, b_0)$, where a_0 and b_0 are algebraically independent transcendental elements, and compute the canonical lifting of

$$E/k_0 \ : \ y_0^2 = f(x_0) \stackrel{\text{def}}{=} x_0^3 + a_0 x_0 + b_0. \tag{2.1}$$

The curve E/k_0 is an ordinary elliptic curve, since its Hasse invariant, i.e., the coefficient of x_0^{p-1} in $f(x_0)^{(p-1)/2}$, say A, is non-zero in k_0. More explicitly, we have

$$A = \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} a_0^{3i-r} b_0^{r-2i}, \tag{2.2}$$

where $r \stackrel{\text{def}}{=} (p-1)/2$, $r_1 \stackrel{\text{def}}{=} \lceil (p-1)/6 \rceil$, and $r_2 \stackrel{\text{def}}{=} \lfloor (p-1)/4 \rfloor$.

So, let

$$\boldsymbol{E}/\boldsymbol{W}(\bar{k}_0) \ : \ \boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{a}\boldsymbol{x} + \boldsymbol{b}, \tag{2.3}$$

with $\boldsymbol{a} = (a_0, a_1, \ldots)$ and $\boldsymbol{b} = (b_0, b_1, \ldots)$, be the canonical lifting of E. We shall identify $\boldsymbol{E}$ with its *Greenberg transform* $G(\boldsymbol{E})$, which is the infinite dimensional scheme over k_0 defined by the equations that one obtains when comparing the coordinates (as Witt vectors) of Eq. (2.3) when $\boldsymbol{x}$ and $\boldsymbol{y}$ are replaced by Witt vectors of variables $(x_0, x_1, \ldots)$ and $(y_0, y_1, \ldots)$ respectively.

As seen in Section 1, associated with the canonical lifting $\boldsymbol{E}$ we have the elliptic Teichmüller. In [Fin02] it is shown that $\tau(x_0, y_0) = ((x_0, F_1, F_2, \ldots), (y_0, y_0 H_1, y_0 H_2, \ldots))$, where $F_i, H_i \in k_0[x_0]$. (Remember that τ is a section of the reduction modulo p.)

Lemma 2.2. *With the notation above, we have that $a_n, b_n \in k_0$ and $F_n, H_n \in k_0[x_0]$ for all $n \geq 0$, i.e., the canonical lifting $\boldsymbol{E}$ is defined over $\boldsymbol{W}(k_0)$ and the elliptic Teichmüller lift $\tau : E \to G(\boldsymbol{E})$ is defined over k_0.*

Proof. Applying Lemma 7.4 in [Fin06], we see that at the $(n+1)$-th equation of $G(\boldsymbol{E})$ we have:

$$2y_0^{p^n} y_n + \cdots = (3x_0^2 + a_0)^{p^n} x_n + a_n x_0^{p^n} + b_n + \cdots ,$$

where no omitted term involves x_n, y_n, a_n or b_n. Pulling this back via τ^* gives an equality modulo the ideal $I \stackrel{\text{def}}{=} (y_0^2 - (x_0^3 - a_0 x_0 + b_0))$. But since $\tau^*(y_i) = y_0 H_i$, with $H_i \in k_0[x_0]$, we have that this pullback gives us

$$2f(x_0)^{(p^n-1)/2} H_n + \cdots \equiv (3x_0^2 + a_0)^{p^n} F_n + a_n x_0^{p^n} + b_n + \cdots \pmod{I}.$$

(Remember that f is the cubic from Eq. (2.1).) Since the expression above can be simplified so that it does not involve y_0 (see the proof of Proposition 5.2 in [Fin04]), it must be an actual equality of polynomials in $k_0[x_0]$, i.e.,

$$2f(x_0)^{(p^n-1)/2}H_n + \cdots = (3x_0^2+a_0)^{p^n}F_n + a_n x_0^{p^n} + b_n + \cdots\ . \tag{2.4}$$

We now proceed by induction, assuming that $F_i, H_i \in k_0[x_0]$ and $a_i, b_i \in k_0$ for all $i < n$. From [Fin04], we know that

$$\frac{\mathrm{d}F_n}{\mathrm{d}x_0} = A^{-(p^n-1)/(p-1)}\, f(x_0)^{(p^n-1)/2} - x_0^{p^n-1} - \sum_{i=1}^{n-1} F_i^{(p^{n-i}-1)}\, \frac{\mathrm{d}F_i}{\mathrm{d}x_0}, \tag{2.5}$$

and from [Fin02], we know that

$$\deg_{x_0} F_n \leq N(n) \stackrel{\text{def}}{=} \frac{(n+2)p^n - np^{n-1}}{2}$$

and

$$\deg_{x_0} H_n \leq M(n) \stackrel{\text{def}}{=} \frac{(n+3)p^n - np^{n-1} - 3}{2}.$$

Hence, if

$$F_n = \sum_{i=0}^{N(n)} c_i\, x_0^i,$$

the terms $c_0, c_p, c_{2p}, \ldots, c_{N(n)}$ are unknown if $n > 1$, and for $n = 1$, the terms c_0 and c_p are unknown. But all other c_i's are clearly in k_0, by Eq. (2.5) and our induction hypothesis.

We shall also denote

$$H_n = \sum_{i=0}^{M(n)} d_i\, x_0^i.$$

So, by looking at Eq. (2.4) with the d_i's, a_n, b_n, and the c_i's singled out above as unknowns, we obtain a linear system on those variables with coefficients in k_0.

Also, by Proposition 5.1 of [Fin02], we have that

$$\tau = ((F_0, \ldots, F_n, \ldots), (y_0 H_0, \ldots, y_0 H_n, \ldots))$$

is the elliptic Teichmüller lift if, and only if, $\tau^*(\boldsymbol{x}/\boldsymbol{y})$ is regular at the point at infinity. This implies that $(n+1)$-th coordinate of its expansion, namely,

$$\left(\frac{1}{y_0}\right)^{p^n} F_n + \left(-\frac{x_0}{y_0^2}\right)^{p^n} y_0 H_n + \cdots\ ,$$

must be regular at the point at infinity. Note that the division of Witt vectors gives us that the denominators appearing above contain only powers of y_0. (In fact, it is not hard to prove that the largest power is $y_0^{2p^n}$.) To have this to be regular at the point at infinity, terms in the numerator (after collecting all terms by means of a common denominator) having order of poles higher than the order of the denominator must cancel out. Imposing such cancellations on the numerator gives us another linear system on the c_i's and d_i's with coefficient in k_0.

So, any solution of these two linear systems put together yields the canonical lifting (modulo isomorphism) and elliptic Teichmüller lift. (The first system guarantees that we have a well defined lift and the second guarantees that this lift is the elliptic Teichmüller lift.) We know that there is a solution over $\bar{k}_0$, since the elliptic curve is ordinary. But, since the system is linear and over k_0, there is also a solution over k_0. □

Before we can prove Proposition 2.1, we also need the following basic lemma:

Lemma 2.3. *Let k be a field and $g, h \in k[a_0, b_0]$, with g and h non-zero and relatively prime. If*

$$\frac{g(a_0X^2, b_0X^3)}{h(a_0X^2, b_0X^3)} = \frac{g(a_0, b_0)}{h(a_0, b_0)}$$

(in $k(a_0, b_0, X)$), then there is a positive integer s such that

$$g(a_0, b_0) = \sum_{\ell=0}^{s} \alpha_\ell \, a_0^{3\ell} b_0^{2(s-\ell)}, \qquad h(a_0, b_0) = \sum_{\ell=0}^{s} \beta_\ell \, a_0^{3\ell} b_0^{2(s-\ell)},$$

with $\alpha_\ell, \beta_\ell \in k$. (Hence, if a_0 has weight 2 and b_0 has weight 3, then g and h are homogeneous of degree $6s$.)

Proof. If we write

$$\begin{aligned} g(a_0X^2, b_0X^3) &= g_0(a_0, b_0) + g_1(a_0, b_0)X + g_2(a_0, b_0)X^2 + \cdots \\ h(a_0X^2, b_0X^3) &= h_0(a_0, b_0) + h_1(a_0, b_0)X + h_2(a_0, b_0)X^2 + \cdots , \end{aligned}$$

with $g_i, h_i \in k[a_0, b_0]$, then we must have that $g\, h_i = h\, g_i$ for all i. Since g and h are relatively prime, we must have that there is some $d_i \in k[a_0, b_0]$ such that $g_i = g\, d_i$ and $h_i = h\, d_i$. Thus, $g(a_0X^2, b_0X^3) = g(a_0, b_0)\, d(a_0, b_0, X)$ and $h(a_0X^2, b_0X^3) = h(a_0, b_0)\, d(a_0, b_0, X)$, where $d = \sum_i d_i X^i$.

Since $g(a_0, b_0)$ and $g(a_0X^2, b_0X^3)$ have the same number of monomials (in $k[a_0, b_0, X]$), we must have that $d(a_0, b_0, X)$ has a single monomial, say $d(a_0, b_0, X) = \lambda(a_0, b_0)X^r$. Since also $g(a_0, b_0)$ and $g(a_0X^2, b_0X^3)$ have the same degrees in a_0 and b_0, we must have that $\lambda \in k$.

If

$$g(a_0, b_0) = \sum_{i,j} \alpha_{i,j} \, a_0^i b_0^j$$

with $\alpha_{i,j} \in k$, then

$$(\lambda X^r)\left(\sum_{i,j} \alpha_{i,j}\, a_0^i b_0^j\right) = g(a_0X^2, b_0X^3) = \sum_{i,j} \alpha_{i,j}\, a_0^i b_0^j X^{2i+3j}$$

and hence $\lambda = 1$ and $2i + 3j = r$ for all i and j such that $\alpha_{i,j} \neq 0$. Similarly we obtain the analogous result for h.

Now, observe that since g and h are relatively prime, if $a_0 \mid g$, then $a_0 \nmid h$. So, we must always have that either g or h is not divisible by a_0, and hence one of these has a term with $i = 0$, and hence $3 \mid r$. The analogous argument for b_0 gives us that $2 \mid r$, and hence $6 \mid r$.

So, for each pair (i, j) appearing in a term of either g or h, we must have that $r \equiv 2i \equiv 0 \pmod 3$ and $r \equiv 3j \equiv 0 \pmod 2$, and hence $3 \mid i$ and $2 \mid j$. Thus, taking $s = r/6$ and remembering that $2i + 3j = 6s$, one obtains the desired formulas for g and h. □

Now we are ready to prove Proposition 2.1.

Proof of Proposition 2.1. Since $a_n, b_n \in k_0 = \mathbb{F}_p(a_0, b_0)$ for all n, i.e., $\boldsymbol{a} = (a_0, a_1, \dots), \boldsymbol{b} = (b_0, b_1, \dots) \in \boldsymbol{W}(\mathbb{F}_p(a_0, b_0))$, we have that

$$\boldsymbol{j} = 1728\frac{4\boldsymbol{a}^3}{4\boldsymbol{a}^3 + 27\boldsymbol{b}^2} = (j_0, j_1, \dots)$$

with $j_n \in \mathbb{F}_p(a_0, b_0)$. So, let $g, h \in \mathbb{F}_p[X, Y]$ relatively prime polynomials such that $j_n = g(a_0, b_0)/h(a_0, b_0)$. Now, since j_n depends only on $j_0 = 1728\,(4a_0^3/(4a_0^3 + b_0^2))$, for any $\lambda \in \bar{k}_0$ we must have

$$j_n = g(\lambda^2 a_0, \lambda^3 b_0)/h(\lambda^2 a_0, \lambda^3 b_0) = g(a_0, b_0)/h(a_0, b_0).$$

By Lemma 2.3, there is a positive integer s such that if

$$g(a_0, b_0) = \sum_{\ell=0}^{s} \alpha_\ell\, a_0^{3\ell} b_0^{2(s-\ell)}, \qquad h(a_0, b_0) = \sum_{\ell=0}^{s} \beta_\ell\, a_0^{3\ell} b_0^{2(s-\ell)},$$

Hence,

$$j_n = \frac{g(a_0, b_0)}{h(a_0, b_0)} = \frac{g(a_0, b_0)/b_0^{2s}}{h(a_0, b_0)/b_0^{2s}} = \frac{\sum_{\ell=0}^{s} \alpha_\ell\, (a_0^3/b_0^2)^\ell}{\sum_{\ell=0}^{s} \beta_\ell\, (a_0^3/b_0^2)^\ell}.$$

Since

$$\frac{a_0^3}{b_0^2} = \frac{27j_0}{4(1728 - j_0)},$$

we have that j_n is a rational function of j_0. □

3. Pseudo-Canonical Liftings Modulo p^2

We will need the following definition (from [Fin04]):

Definition 3.1. Let $g(x_0, y_0) \in k[x_0, y_0]$ and $\boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{W}_2(k)$ be the lift of g defined by applying the Teichmüller lift to the coefficients of g, i.e., if λ is a coefficient of some monomial of g, then the corresponding monomial of $\boldsymbol{g}$ has coefficient $(\lambda, 0)$. We define

$$\psi(g) \stackrel{\text{def}}{=} \psi(\boldsymbol{g}) \stackrel{\text{def}}{=} \text{reduction modulo } p \text{ of } \frac{\boldsymbol{g}^\sigma(\boldsymbol{x}^p, \boldsymbol{y}^p) - \boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y})^p}{p},$$

where σ denotes the Frobenius of Witt vectors.

Let $\Phi_p(X, Y) \in \mathbb{Z}[X, Y]$ denote the classical modular polynomial. Then, by Theorem 3 of [LST64], we have that

$$\Phi_p((J_0, J_1, \ldots), (J_0^p, J_1^p, \ldots)) = 0. \tag{3.1}$$

Since, by Kronecker's congruence relation we have that

$$\Phi_p(X, Y) \equiv (X - Y^p)(X^p - Y) \pmod{p},$$

Lemma 8.1 of [Fin04] gives us that the second coordinate of $\Phi_p((X_0, X_1), (Y_0, Y_1))$ when expanded as Witt vectors is

$$(X_0^p - Y_0)^p X_1 + (Y_0^p - X_0)^p Y_1 + \psi(\Phi_p) + \sum_{i,j} \beta_{i,j} X_0^{ip} Y_0^{pj}, \tag{3.2}$$

where

$$\Phi_p(X, Y) \equiv \sum_{i,j} (\alpha_{i,j}, \beta_{i,j}) X^i Y^j \pmod{p^2}.$$

Also, Kronecker's congruence relation tells us that

$$\psi(\Phi_p(X, Y)) = \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} X_0^i (X_0^p - Y_0)^i Y_0^{p-i} (Y_0^p - X_0)^{p-i},$$

and hence,

$$\psi(\Phi_p(X, Y))\big|_{(X_0, Y_0) = (j_0, j_0^p)} = 0.$$

Therefore, Eqs. (3.1) and (3.2) give

$$J_1 = -\frac{\sum_{i,j} \beta_{i,j}^{1/p} j_0^{i+pj}}{j_0^{p^2} - j_0}.$$

Now, since $p(a_0, a_1, \ldots) = (0, a_0^0, a_1^p, \ldots)$, we have that this numerator is exactly the reduction modulo p of $\Phi_p(X, X^p)/p$ evaluated at $X = j_0$. Kaneko and Zagier denoted

$$H_p(X) \stackrel{\text{def}}{=} \frac{\Phi_p(X, X^p)}{p}, \qquad \text{and} \qquad \varphi_p(X) \stackrel{\text{def}}{=} \frac{H_p(X)}{X^{p^2} - X},$$

(this H_p should not to be confused with our $H_n \in k[x_0]$ coming from the elliptic Teichmüller lift) and studied their properties in [KZ98]. (It should also be mentioned that Buium's theory of *differential modular forms* also yield H_p modulo p explicitly. See [Bui00] and [Hur01].) Note then, that $J_1(X)$ is simply the reduction modulo p of $-\varphi_p(X)$.

Let's denote

$$\mathrm{ss}_p(X) \stackrel{\text{def}}{=} \prod_{j_0 \text{ supersing.}} (X - j_0),$$

i.e., $\mathrm{ss}_p(X)$ is the *supersingular polynomial* (in characteristic p). Observe that $X = 0$ is a root of $\mathrm{ss}_p(X)$ if, and only if, $p \equiv 5 \pmod 6$ and $X = 1728$ is a root of $\mathrm{ss}_p(X)$ if, and only if, $p \equiv 3 \pmod 4$. (See, for instance, [Fin08].)

In [KZ98] we have:

Theorem 3.2 (de Shalit, Kaneko, Zagier)**.** *Let $\bar{H}_p(X)$ and $\bar{\varphi}_p(X)$ denote the reductions modulo p of $H_p(X)$ and $\varphi_p(X)$ respectively.*

(1) $\bar{H}_p(j_0) = 0$ *for* $j_0 = 0, 1728$ *and all* ordinary $j_0 \in \mathbb{F}_{p^2}$. *(This was originally proved by de Shalit in* [dS94]*, but was deduced again in* [KZ98]*.)*

(2) *If j_0 is supersingular, then*

$$\bar{H}_p(j_0) = -j_0^r (j_0 - 1728)^s / \mathrm{ss}_p'(j_0)^2,$$

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

$$s \stackrel{\text{def}}{=} \begin{cases} (p-1)/2, & \text{if } p \equiv 1 \pmod 4, \\ (p+1)/2, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Hence, if j_0 is supersingular and different from 0 *and* 1728*, we have that $\bar{\varphi}_p(X)$ has a pole at $X = j_0$.*

(3) *We have that*

$$\bar{\varphi}_p'(X) = X^{p-1} - X^r \, \frac{(X - 1728)^s}{\mathrm{ss}_p(X)^2},$$

with r and s defined as above. In particular, if

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

and

$$s' \stackrel{\text{def}}{=} \begin{cases} (p-1)/2, & \text{if } p \equiv 1 \pmod 4, \\ (p-3)/2, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

then $\operatorname{ord}_{X=0} \bar{\varphi}_p(X) = r'$ *and* $\bar{\varphi}_p^{(t)}(1728) = (t-1)!\,(-1728)^{(1-t)}$ *for* $1 \leq t \leq s'$.

As observed in [KZ98], this theorem allows us to compute $H_p(X)$, and hence also $J_1(X)$, explicitly.

Observe that Theorem 3.2 allows us to prove Theorem 1.1 almost completely. Since $X^{p^2} - X$ have simple zeros for $X = 0$ and $X = 1728$ and $\bar{H}_p(X)$ also has zeros at those values (by item 1), we have that $J_1(X)$ is regular at those values. Moreover, item 3 gives us that $(0, J_1(0)) = (0, 0)$. The only piece missing then is that $(1728, J_1(1782)) \equiv 1728 \pmod{p^2}$. But note also that item 2 proves Theorem 1.2.

It's also worth noticing that our observation that $J_1(X) = -\bar{\varphi}_p(X)$ can be used to prove the second part of item 1 immediately: since $J_1(j_0)$ must be regular at all ordinary values, if j_0 is ordinary and in $\mathbb{F}_{p^2}$, then we must have that $\bar{H}_p(j_0) = 0$.

The goal now is to give an alternative proof of Theorem 1.1 without using the modular polynomial. (This proof will also include the missing piece.) Then, the identification $J_1(X) = -\bar{\varphi}_p(X)$ will give alternative proofs of some of the facts in Theorem 3.2. More precisely, it will prove item 1 (which follows immediately from Theorem 1.1), $\operatorname{ord}_{X=0} \bar{\varphi}_p(X) \geq r'$, and the formula for $\bar{\varphi}_p^{(t)}(1728)$ from item 3.

4. Valuations and Alternative Invariants

As in the previous section, let $k_0 \stackrel{\text{def}}{=} \mathbb{F}_p(a_0, b_0)$, where $p \geq 5$ and a_0, b_0 are algebraically independent transcendental elements. To simplify our computation, it will be easier to avoid the usual j-invariant and use instead:

$$\tilde{j}_0 \stackrel{\text{def}}{=} \frac{a_0^3}{b_0^2} \qquad \text{and} \qquad \tilde{\tilde{j}}_0 \stackrel{\text{def}}{=} \frac{b_0^2}{a_0^3}.$$

Those are certainly invariant under isomorphisms of elliptic curves as long as $b_0 \neq 0$ (i.e., $j_0 \neq 1728$) for the former and $a_0 \neq 0$ (i.e., $j_0 \neq 0$) for the latter. We will also use the invariants $\tilde{\boldsymbol{j}}$ and $\tilde{\tilde{\boldsymbol{j}}}$, defined in the same way, for curves over $\boldsymbol{W}(k_0)$.

Then, clearly,

$$\tilde{j}_0 = \frac{27 j_0}{4(1728 - j_0)}, \qquad \text{and} \qquad \tilde{\tilde{j}}_0 = \frac{4(1728 - j_0)}{27 j_0}, \tag{4.1}$$

and

$$j_0 = 1728 \frac{4\tilde{j}_0}{4\tilde{j}_0 + 27} = 1728 \frac{4}{27\tilde{\tilde{j}}_0 + 4}, \tag{4.2}$$

and the analogous formulas hold for $\tilde{\boldsymbol{j}}$ and $\tilde{\tilde{\boldsymbol{j}}}$ in terms of $\boldsymbol{j}$. Hence, since products and sums of Witt vectors are given by polynomial formulas, Proposition 2.1 tells us that there are $\tilde{J}_i, \tilde{\tilde{J}}_i \in \mathbb{F}_p(X)$ such that

$$\tilde{\boldsymbol{j}} = (\tilde{J}_0(\tilde{j}_0), \tilde{J}_1(\tilde{j}_0), \tilde{J}_2(\tilde{j}_0), \ldots) \quad \text{and} \quad \tilde{\tilde{\boldsymbol{j}}} = (\tilde{\tilde{J}}_0(\tilde{\tilde{j}}_0), \tilde{\tilde{J}}_1(\tilde{\tilde{j}}_0), \tilde{\tilde{J}}_2(\tilde{\tilde{j}}_0), \ldots),$$

where $\tilde{\boldsymbol{j}}$ and $\tilde{\tilde{\boldsymbol{j}}}$ are the invariants associated to the canonical lifting of the curve with invariants $\tilde{j}_0$ and $\tilde{\tilde{j}}_0$. More precisely,

$$(\tilde{J}_0(\tilde{X}), \tilde{J}_1(\tilde{X}), \ldots) = \frac{27(J_0\left(1728\frac{4\tilde{X}}{4\tilde{X}+27}\right), J_1\left(1728\frac{4\tilde{X}}{4\tilde{X}+27}\right), \ldots)}{4\left(1728 - (J_0\left(1728\frac{4\tilde{X}}{4\tilde{X}+27}\right), J_1\left(1728\frac{4\tilde{X}}{4\tilde{X}+27}\right), \ldots)\right)} \tag{4.3}$$

and

$$(\tilde{\tilde{J}}_0(\tilde{\tilde{X}}), \tilde{\tilde{J}}_1(\tilde{\tilde{X}}), \ldots) = \frac{4\left(1728 - (J_0\left(1728\frac{4}{27\tilde{\tilde{X}}+4}\right), J_1\left(1728\frac{4}{27\tilde{\tilde{X}}+4}\right), \ldots)\right)}{27(J_0\left(1728\frac{4}{27\tilde{\tilde{X}}+4}\right), J_1\left(1728\frac{4}{27\tilde{\tilde{X}}+4}\right), \ldots)}. \tag{4.4}$$

We then have the following proposition:

Proposition 4.1. *The rational function $J_i(X)$ is regular at $X = 0$ (resp., at $X = 1728$) for all $i \leq n$ if, and only if, $\tilde{J}_i(\tilde{X})$ (resp., $\tilde{\tilde{J}}_i(\tilde{\tilde{X}})$) is regular at $\tilde{X} = 0$ (resp., $\tilde{\tilde{X}} = 0$) for all $i \leq n$. Moreover, we have that $\boldsymbol{j}(j_0) \equiv 0 \pmod{p^n}$ (resp., at $\boldsymbol{j}(j_0) \equiv 1728 \pmod{p^n}$) if, and only if, $\tilde{\boldsymbol{j}}(\tilde{j}_0) \equiv 0 \pmod{p^n}$ (resp., $\tilde{\tilde{\boldsymbol{j}}}(\tilde{\tilde{j}}_0) \equiv 0 \pmod{p^n}$).*

Proof. We first observe that for any ring R, an element $\boldsymbol{c} = (c_0, c_1, \ldots) \in \boldsymbol{W}(R)$ is invertible if, and only if, $c_0 \in R^{\times}$.

For $n = 0$, the question is trivial, as $J_0(X) = X$, $\tilde{J}_0(\tilde{X}) = \tilde{X}$, and $\tilde{J}_0(\tilde{\tilde{X}}) = \tilde{\tilde{X}}$.

Assume then that $J_i(X)$ is regular at $X = 0$ (resp., at $X = 1728$) for all $i \leq n$. We will work then in $\boldsymbol{W}_{n+1}(k_0)$, i.e., with Witt vectors of length $(n+1)$. Since $J_0(X) = X$, we have that $(1728 - (J_0(0), \ldots, J_n(0))) \neq 0$ (resp., $27\,(J_0(1728), \ldots, J_n(1728)) \neq 0$), as $0 \not\equiv 1728 \pmod{p}$. Hence the denominators of Eq. (4.3) (resp., Eq. (4.4)) when evaluated at $\tilde{X} = 0$ (resp., $\tilde{\tilde{X}} = 0$) are invertible in $\boldsymbol{W}(\mathbb{F}_p)$ (and in $\boldsymbol{W}_{n+1}(\mathbb{F}_p)$), by our remark in the beginning of the proof.

Hence, formulas (4.3) and (4.4) show that if the J_i's are regular at $X = 0$ (resp., $X = 1728$) for $i \leq n$, then $\tilde{J}_i$'s are regular at $\tilde{X} = 0$ (resp., $\tilde{\tilde{X}} = 0$) for $i \leq n$.

The converse is similar, using

$$(J_0(X), J_1(X), \ldots) = 1728 \frac{4\left(\tilde{J}_0\left(\frac{27X}{4(1728-X)}\right), \tilde{J}_1\left(\frac{27X}{4(1728-X)}\right), \ldots\right)}{4\left(\tilde{J}_0\left(\frac{27X}{4(1728-X)}\right), \tilde{J}_1\left(\frac{27X}{4(1728-X)}\right), \ldots\right) + 27} \tag{4.5}$$

$$= 1728 \frac{4}{27\left(\tilde{\tilde{J}}_0\left(\frac{4(1728-X)}{27X}\right), \tilde{\tilde{J}}_1\left(\frac{4(1728-X)}{27X}\right), \ldots\right) + 4} \tag{4.6}$$

instead of Eqs. (4.3) and (4.4).

The final statement follows immediately from the transition formulas. □

Proposition 4.1 then allows us to use the invariants $\tilde{\boldsymbol{j}}$ and $\tilde{\tilde{\boldsymbol{j}}}$ to prove Theorem 1.1, i.e., it suffices to prove that $\tilde{J}_1(0) = \tilde{\tilde{J}}_1(0) = 0$.

To further simplify our computations note that if $\boldsymbol{a} = (a_0, a_1)$ and $\boldsymbol{b} = (b_0, b_1)$ are the coefficients of the canonical lifting of the curve with coefficients a_0 and b_0, then we can assume that either $a_1 = 0$, if $a_0 \neq 0$, or $b_1 = 0$, if $b_0 \neq 0$. Indeed, it suffices to take the curve with coefficients $\boldsymbol{\lambda}^2\boldsymbol{a}$ and $\boldsymbol{\lambda}^3\boldsymbol{b}$ instead, where $\boldsymbol{\lambda} \stackrel{\text{def}}{=} (1, -a_1/(2a_0^p))$ for the former, and $\boldsymbol{\lambda} \stackrel{\text{def}}{=} (1, -b_1/(3b_0^p))$ for the latter.

So, over k_0 (where $a_0, b_0 \neq 0$), we can assume that the canonical lifting of the curve given by Eq. (2.1) is such that $\boldsymbol{a} = (a_0, a_1)$ and $\boldsymbol{b} = (b_0, 0)$. In this case, we have

$$\tilde{\boldsymbol{j}} = \frac{(a_0, a_1)^3}{(b_0, 0)^2} = \left(\frac{a_0^3}{b_0^2}, \frac{3a_0^{2p}a_1}{b_0^{2p}}\right). \tag{4.7}$$

Assuming that the canonical lifting has $\boldsymbol{a} = (a_0, 0)$ and $\boldsymbol{b} = (b_0, b_1)$, we get that

$$\tilde{\tilde{\boldsymbol{j}}} = \frac{(b_0, b_1)^2}{(a_0, 0)^3} = \left(\frac{b_0^2}{a_0^3}, \frac{2b_0^p b_1}{a_0^{3p}}\right). \tag{4.8}$$

Let now $v \stackrel{\text{def}}{=} \operatorname{ord}_{a_0=0}$ and $w \stackrel{\text{def}}{=} \operatorname{ord}_{b_0=0}$ denote the orders of zeros of elements of k_0 at $a_0 = 0$ (seeing k_0 as $(\mathbb{F}_p(b_0))(a_0)$) and $b_0 = 0$ (seeing k_0 as $(\mathbb{F}_p(a_0))(b_0)$) respectively. We have:

Proposition 4.2. *Let $v(a_1) = r$ in the case of $b_1 = 0$ and $w(b_1) = s$ in the case $a_1 = 0$. Then*

$$\operatorname{ord}_{\tilde{j}=0}(\tilde{J}_1) = \frac{2p + r}{3} \qquad \textit{and} \qquad \operatorname{ord}_{\tilde{\tilde{j}}=0}(\tilde{\tilde{J}}_1) = \frac{p + s}{2}.$$

Hence, by Proposition 4.1, to prove Theorem 1.1, it suffices to prove that $w(a_1) > -2p$ in Eq. (4.7) and that $v(b_1) > -p$ in Eq. (4.8).

Proof. Since $v(a_1) = r$, we can write $a_1 = a_0^r a_1'$, with $v(a_1') = 0$. Then,

$$\tilde{J}_1(\tilde{j}) = \frac{3a_0^{2p}a_1}{b_0^{2p}} = 3\tilde{j}^p a_0^{r-p} a_1'.$$

Then, clearly, $a_0^{r-p}a_1'$ is a rational function on $\tilde{j}$. Thus,

$$\mathrm{ord}_{\tilde{j}=0}(a_0^{r-p}a_1') = \frac{1}{3}v(a_0^{r-p}a_1') = \frac{r-p}{3}.$$

So, $\mathrm{ord}_{\tilde{j}=0}(\tilde{J}_1) = p + (r-p)/3 = (2p+r)/3 > 0$ if, and only if, $r > -2p$.

In the same way, if $w(b_1) = s$, and $b_1 = b_0^s b_1'$ with $w(b_1') = 0$, then

$$\tilde{\tilde{J}}_1(\tilde{\tilde{j}}) = \frac{2b_0^p b_1}{a_0^{3p}} = 2\tilde{\tilde{j}}^p b_0^{s-p} b_1'.$$

Then, clearly, $b_0^{s-p}b_1'$ is a rational function on $\tilde{\tilde{j}}$. Thus,

$$\mathrm{ord}_{\tilde{\tilde{j}}=0}(b_0^{s-p}b_1') = \frac{1}{2}w(b_0^{s-p}b_1') = \frac{s-p}{2}.$$

So, $\mathrm{ord}_{\tilde{\tilde{j}}=0}(\tilde{\tilde{J}}_1) = p + (s-p)/2 = (p+s)/2 > 0$ if, and only if, $s > -p$. $\square$

We shall prove a stronger result:

Proposition 4.3. *Let A denote the Hasse invariant of the curve* (2.1)*, $v_0 \overset{\text{def}}{=} v(A)$, and $w_0 \overset{\text{def}}{=} w(A)$. Then, $v(a_1) \geq -v_0$ and $w(b_1) \geq -w_0$.*

Most of the remaining of this paper will be dedicated to the proof of Proposition 4.3. Note that

$$v_0 = \begin{cases} 0, & \text{if } p \equiv 1 \pmod 6, \\ 1, & \text{if } p \equiv 5 \pmod 6, \end{cases} \quad \text{and} \quad w_0 = \begin{cases} 0, & \text{if } p \equiv 1 \pmod 4, \\ 1, & \text{if } p \equiv 3 \pmod 4, \end{cases} \tag{4.9}$$

as if we let $r \overset{\text{def}}{=} (p-1)/2$, $r_1 \overset{\text{def}}{=} \lceil r/3 \rceil$, and $r_2 \overset{\text{def}}{=} \lfloor r/2 \rfloor$, then, an easy computation (see [Fin08]) shows that

$$A = \sum_{i=r_1}^{r_2} \binom{r}{i} \binom{i}{3i-r} a_0^{3i-r} b_0^{r-2i}.$$

5. Proof of Proposition 4.3

Let $\boldsymbol{a} = (a_0, a_1)$, $\boldsymbol{b} = (b_0, b_1)$ be the coefficients of the canonical lifting $\boldsymbol{E}$ of the curve E, given by Eq. (2.1), and $\tau = ((x_0, F_1), (y_0, y_0 H_1))$, with $F_1, H_1 \in k_0[x_0]$, be the elliptic Teichmüller lift (modulo p^2).

Then, Lemma 8.1 of [Fin04] gives us that the pullback of second coordinate of the equation of $\boldsymbol{E}$ by τ is given by

$$2(x_0^3 + a_0x_0 + b_0)^{(p+1)/2}H_1 = (3x_0^2 + a_0)^pF_1 + a_1x_0^p + b_1 + \psi(f), \tag{5.1}$$

where ψ is the function given in Definition 3.1. Since by Eq. (2.5) we have

$$F_1' = A^{-1}(x_0^3 + a_0x_0 + b_0)^{(p-1)/2} - x_0^{p-1},$$

taking derivatives with respect to x_0 in Eq. (5.1) and dividing by $(x_0^3 + a_0x_0 + b_0)^{(p-1)/2}$, we obtain

$$\begin{multline}(3x_0^2 + a_0)H_1 + 2(x_0^3 + a_0x_0 + b_0)H_1' = \\ A^{-1}(3x_0^{2p} + a_0^p) - (x_0^3 + a_0x_0 + b_0)^{(p-1)/2}(3x_0^2 + a_0). \tag{5.2}\end{multline}$$

We will analyze these two equations to estimate the wanted valuations.

Let's denote

$$F_1 = \sum_{i=0}^{(3p-1)/2} c_i x_0^i \qquad \text{and} \qquad H_1 = \sum_{i=0}^{2p-2} d_i x_0^i.$$

(Note that since we know F_1', we know all c_i's except c_0 and c_p.) Hence, looking at the terms of degree $(r+2)$ in Eq. (5.2), we obtain

$$(2r+3)d_r + (2r+5)a_0d_{r+2} + (2r+6)b_0d_{r+3} = \cdots , \tag{5.3}$$

where the omitted terms in the right hand side do not contain d_i's.

From now on, let's fix the notation $v_0 \stackrel{\text{def}}{=} v(A)$, $w_0 \stackrel{\text{def}}{=} w(A)$.

Proposition 5.1. *Let* $(3p-1)/2 \leq r \leq 2p-2$.

1. Case $b_1 = 0$: *We have that* $v(d_r) > -v_0$ *if* $2p - r \not\equiv 2 \pmod 3$ *and* $v(d_r) = -v_0$ *otherwise.*
2. Case $a_1 = 0$: *We have that* $w(d_r) > -w_0$ *if* r *is odd and* $w(d_r) = -w_0$ *otherwise.*

Proof. We start by observing that the right hand side of Eq. (5.2) has a term of degree $2p$, namely $3A^{-1}x_0^{2p}$, but no terms of degrees between $2p$ and $(3p+3)/2$. So, the term of degree $2p$ gives us that $d_{2p-2} = -3A^{-1}$. For $(3p-1)/2 < r < 2p-2$, the omitted terms on Eq. (5.3) are then zero. We can then determine the valuations of d_i's inductively.

One can easily check the cases $r = 2p-2, 2p-3, 2p-4$ directly, using Eq. (5.2). So, we assume the statement to hold for all $i > r \geq 2p-5$.

If $b_1 = 0$ and $2p - r \not\equiv 2 \pmod 3$, then, by the induction hypothesis, $v((2r+5)a_0d_{r+2})$ and $v((2r+6)b_0d_{r+3})$ are greater than $-v_0$. Hence, by Eq. (5.3), so is $v(d_r)$.

If $b_1 = 0$ and $2p - r \equiv 2 \pmod 3$, then, by the induction hypothesis, $v((2r+5)a_0 d_{r+2}) > -v_0$ and $v((2r+6)b_0 d_{r+3}) = -v_0$. Then, Eq. (5.3) gives us $v(d_r) = -v_0$.

In the same way, if $a_1 = 0$ and r is odd, then, by the induction hypothesis, $w((2r+5)a_0 d_{r+2})$ and $w((2r+6)b_0 d_{r+3})$ are greater than $-w_0$. Hence, by Eq. (5.3), so is $w(d_r)$.

If $a_1 = 0$ and r is even, then, by the induction hypothesis, $w((2r+5)a_0 d_{r+2}) = -w_0$ and $w((2r+6)b_0 d_{r+3}) > -w_0$. Then, Eq. (5.3) gives us $w(d_r) = -w_0$. □

Observe that the proof actually gives us an algorithm to find d_r's for $(3p-1)/2 \leq r \leq 2p-2$. But, for $r = (3p-3)/2$ we encounter a difficulty, as $(2r+3) = 0$, and hence Eq. (5.3) does not give us $d_{(3p-3)/2}$. So, let's denote $v_1 \stackrel{\text{def}}{=} v(d_{(3p-3)/2})$, $w_1 \stackrel{\text{def}}{=} w(d_{(3p-3)/2})$, and let δ_1 be the *initial coefficient* of $d_{(3p-3)/2}$ with respect to w, i.e.,

$$d_{(3p-3)/2} = \delta_1 b_0^{w_1} + \cdots ,$$

where all omitted terms have valuation greater than w_1.

Proposition 5.2. *If $b_1 = 0$ (resp., $a_1 = 0$) and $v_1 \geq -v_0$ (resp., $w_1 \geq -w_0$), then $v(d_r) \geq -v_0$ (resp., $w(d_r) \geq -w_0$) for $(p-1)/2 \leq r \leq (3p-3)/2$.*

Proof. Clearly only the terms of degree 0 and $2p$ on the right hand side of Eq. (5.2) have possibly negative valuations for v (resp., w), and these have valuation exactly equal to $-v_0$ (resp., $-w_0$). Hence all omitted terms on the right hand side of Eq. (5.3) have valuations greater than or equal to $-v_0$ (resp., $-w_0$). Thus, using Proposition 5.1, one then can easily see that if $v_1 \geq -v_0$ (resp., $w_1 \geq -w_0$), then we can continue using Eq. (5.3), as in the proof of Proposition 5.1, to guarantee that $v(d_r) \geq -v_0$ (resp., $w(d_r) \geq -w_0$) for $(p-1)/2 \leq r \leq (3p-3)/2$. □

We want to show that indeed $v_1 \geq -v_0$ and $w_1 \geq -w_0$. We will proceed by assuming otherwise and deriving a contradiction. We first need the following proposition:

Proposition 5.3. *Let $(p-1)/2 \leq r \leq (3p-3)/2$.*

(1) Case $b_1 = 0$: *Assume that $v_1 < -v_0$. We have that $v(d_r) > v_1$ if $r \not\equiv 0 \pmod 3$ and $v(d_r) = v_1$ otherwise.*
(2) Case $a_1 = 0$: *Assume that $w_1 < -w_0$. We have that $w(d_r) > w_1$ if $r \not\equiv (3p-3)/2 \pmod 2$ and $w(d_r) = w_1$ otherwise. In the latter case, the initial coefficient of d_r is*
$$\left(\prod_{i=0}^{(3p-7-2r)/4} \frac{2i+1}{2i+2} \right) (-a_0)^{(3p-3-2r)/4} \delta_1.$$

Proof. We first observe that, by Proposition 5.1, we have that $v(d_r) \geq -v_0$ and $w(d_r) \geq -w_0$ for $r > (3p-3)/2$. Also, as observed above, for $(p-1)/2 \leq r \leq (3p-3)/2$, the omitted terms in the right hand side of Eq. (5.3) have all valuations greater than or equal to 0. (Note that if $v_1 < -v_0$, then $v_1 < 0$, and if $w_1 < -w_0$, then $w_1 < 0$.) We again determine the valuations inductively using Eq. (5.3).

One can easily check the cases $r = (3p-3)/2, (3p-5)/2, (3p-7)/2$ directly. So, we assume the statement to hold for $i > r \geq (3p-9)/2$.

If $b_1 = 0$ and $r \not\equiv 0 \pmod 3$, then, by the induction hypothesis, $v((2r+5)a_0 d_{r+2})$ and $v((2r+6)b_0 d_{r+3})$ are greater than v_1. Since the omitted terms also have valuation greater than v_1 (as they have positive valuation), Eq. (5.3) gives us that $v(d_r) > v_1$.

If $b_1 = 0$ and $r \equiv 0 \pmod 3$, then, by the induction hypothesis, $v((2r+5)a_0 d_{r+2}) > v_1$ and $v((2r+6)b_0 d_{r+3}) = v_1$. Then, since the omitted terms have valuation greater than v_1, Eq. (5.3) gives us $v(d_r) = v_1$.

In the same way, if $a_1 = 0$ and $r \not\equiv (3p-3)/2 \pmod 2$, then, by the induction hypothesis, $w((2r+5)a_0 d_{r+2})$ and $w((2r+6)b_0 d_{r+3})$ are greater than w_1, and so $w(d_r) > w_1$.

If $a_1 = 0$ and $r \equiv (3p-3)/2 \pmod 2$, then, by the induction hypothesis, $w((2r+5)a_0 d_{r+2}) = w_1$ and $w((2r+6)b_0 d_{r+3}) > w_1$. Then, Eq. (5.3) gives us

$$\begin{aligned} d_r &= -\frac{2r+5}{2r+3}\, a_0 \left[\left(\prod_{i=0}^{(3p-7-2r)/4-1} \frac{2i+1}{2i+2} \right) (-a_0)^{(3p-3-2r)/4-1} \delta_1 \, b_0^{w_1} + \cdots \right] \\ &= \left(\prod_{i=0}^{(3p-7-2r)/4} \frac{2i+1}{2i+2} \right) (-a_0)^{(3p-3-2r)/4} \delta_1 \, b_0^{w_1} + \cdots \end{aligned}$$

□

For $r = (p-3)/2$, formula (5.3) cannot determine d_r. So, we yet again, need to deal with a term of unknown valuation. Similarly as before, we define $v_2 \stackrel{\text{def}}{=} v(d_{(p-3)/2})$, $w_2 \stackrel{\text{def}}{=} w(d_{(p-3)/2})$.

Proposition 5.4. *If $b_1 = 0$ (resp., $a_1 = 0$) and $v_1, v_2 \geq -v_0$ (resp., $w_1, w_2 \geq -w_0$), then $v(d_r) \geq -v_0$ (resp., $w(d_r) \geq -w_0$) for all r.*

Proof. The proof follows the same idea as the proof of Proposition 5.2. □

We still want to show that the assumption that neither $v_1 < -v_0$ nor $w_1 < -w_0$ can occur. But now we have to deal with another unknown valuation. We will show that also $v_2 \geq -v_0$ and $w_2 \geq -w_0$. We need a new proposition to derive a contradiction in the many possible cases.

Proposition 5.5. *Let $0 \leq r \leq (p-3)/2$.*

(1) Case $b_1 = 0$:

(a) Subcase $v_1 < \min\{-v_0, v_2\}$: *If* $p \equiv 1 \pmod 6$, *then* $v(d_r) > v_1$ *if* $r \not\equiv (p-1)/2 \pmod 3$, *and* $v(d_r) = v_1$ *otherwise.*
If $p \equiv 5 \pmod 6$, *then* $v(d_r) > v_1$ *if* $r \not\equiv (p+1)/2 \pmod 3$, *and* $v(d_r) = v_1$ *otherwise.*

(b) Subcase $v_2 < \min\{-v_0, v_1\}$: *We have that* $v(d_r) > v_2$ *if* $r \not\equiv (p-3)/2 \pmod 3$, *and* $v(d_r) = v_2$ *otherwise.*

(c) Subcase $v_1 = v_2 < -v_0$: *If* $p \equiv 1 \pmod 6$, *then* $v(d_r) > v_1$ *if* $r \equiv (p+1)/2 \pmod 3$, *and* $v(d_r) = v_1$ *otherwise.*
If $p \equiv 5 \pmod 6$, *then* $v(d_r) > v_1$ *if* $r \equiv (p-1)/2 \pmod 3$, *and* $v(d_r) = v_1$ *otherwise.*

(2) Case $a_1 = 0$:

(a) Subcase $w_1 < \min\{-w_0, w_2\}$: *We have that* $w(d_r) > w_1$.

(b) Subcase $w_2 \leq \min\{-w_0 - 1, w_1\}$: *We have that* $w(d_r) > w_2$ *if* $r \equiv (p-1)/2 \pmod 2$, *and* $w(d_r) = w_2$ *otherwise.*

Proof. We again proceed by induction, and use Proposition 5.3 to check the cases when $r = (p-3)/2, (p-5)/2, (p-7)/2$ directly.

So, now assume $b_1 = 0$ and $v_1 \leq \min\{-v_0-1, v_2\}$. If $p \equiv 1 \pmod 6$, then for $r \equiv (p-1)/2 \pmod 3$, the induction hypothesis and Eq. (5.3) give us that $v(d_r) = v_1$.

In the same way, if $p \equiv 5 \pmod 6$, then for $r \equiv (p+1)/2 \pmod 3$ the induction hypothesis and Eq. (5.3) give us that $v(d_r) = v_1$.

If now we assume $b_1 = 0$ and $v_2 \leq \min\{-v_0 - 1, v_1\}$, then for $r \equiv (p-3)/2 \pmod 3$ the induction hypothesis and Eq. (5.3) give us that $v(d_r) = v_2$.

The case when $a_1 = 0$ and $w_1 < \min\{-w_0, w_2\}$ is straight forward, as the omitted terms in the right hand side of Eq. (5.3) have non-negative valuations.

Finally, the case when $a_1 = 0$ and $w_2 \leq \min\{-w_0-1, w_1\}$, if $r \equiv (p-1)/2 \pmod 2$, then the induction hypothesis gives us that $w((2r+5)a_0 d_{r+2}) > w_2$ and $w((2r+6)b_0 d_{r+3}) = w_2 + 1$. Thus, Eq. (5.3) guarantees that $w(d_r) > w_2$. If $r \equiv (p-3)/2 \pmod 2$, then the induction hypothesis and Eq. (5.3) give us that $w(d_r) = w_2$. □

To derive a contradiction from the assumptions that either $v_1 < -v_0$, $w_1 < -w_0$, $v_2 < -v_0$, or $w_2 < -w_0$, we need some extra equations.

Taking the terms of degrees 1 and 0 of Eq. (5.2), we have

$$3a_0 d_1 + 4b_0 d_2 = -\binom{p-1}{2} a_0^2 b_0^{(p-3)/2}, \tag{5.4}$$

$$a_0 d_0 + 2b_0 d_1 = A^{-1} a_0^p - a_0 b_0^{(p-1)/2}. \tag{5.5}$$

Now, let

$$(x_0^3 + a_0 x_0 + b_0)^{(p+1)/2} = \sum_{i=0}^{(3p+3)/2} \alpha_i \, x_0^i.$$

Then, taking the terms of degrees 0, p, $2p$, and $3p$ from Eq. (5.1), we have

$$2b_0^{(p+1)/2} d_0 = a_0^p c_0 + b_1, \tag{5.6}$$

$$2 \sum_{i=0}^{p} \alpha_i \, d_{p-i} = a_0^p c_p + a_1 + \text{terms from } \psi(f), \tag{5.7}$$

$$d_{(p-3)/2} + \sum_{i=2}^{(3p-1)/2} \alpha_i \, d_{2p-i} = \frac{3}{2} c_0 + \text{terms from } \psi(f), \tag{5.8}$$

$$d_{(3p-3)/2} + \sum_{i=p+2}^{(3p-1)/2} \alpha_i \, d_{3p-i} = \frac{3}{2} c_p. \tag{5.9}$$

Assume first that $b_1 = 0$ and $v_2 \leq \min\{-v_0 - 1, v_1\}$. If $(p-3)/2 \equiv 2 \pmod 3$, then Proposition 5.5 tells us that $v(d_2) = v_2$ and $v(d_1) > v_2$. On the other hand, by Eq. (5.4), we have that

$$v(d_2) \geq \min\{v(d_1) + 1, 2\} > v_2,$$

a contradiction.

If $(p-3)/2 \equiv 1 \pmod 3$, then Proposition 5.5 tells us that $v(d_1) = v_2$ and $v(d_0) > v_2$. On the other hand, by Eq. (5.5), we have that

$$v(d_1) \geq \min\{v(d_0) + 1, 1, p - v_0\} > v_2,$$

a contradiction.

So, assume now that $b_1 = 0$ and $v_1 < \min\{-v_0, v_2\}$. Note that, by Proposition 5.5, independently of the congruence class of p modulo 6, we have that $v(d_0) = v_1$. Eq. (5.6) then gives us that $v(d_0) = v(c_0) + p$, i.e., $v(c_0) = v_1 - p$. But this would imply that while Propositions 5.3 and 5.5 tells us that the left hand side of Eq. (5.8) has valuation greater than or equal to v_1, the right hand side has valuation strictly smaller than that, a contradiction.

So, assume now that $a_1 = 0$ and $w_2 \leq \min\{-w_0 - 1, w_1\}$. If $p \equiv 1 \pmod 4$, then by Proposition 5.5 we have that $w(d_2) > w_2$ and $w(d_1) = w_2$. Hence, the valuation of the left hand side of Eq. (5.4) is w_2, while the valuation of its right hand side is $(p-3)/2$, a contradiction.

If $p \equiv 3 \pmod 4$, then by Proposition 5.5 we have that $w(d_1) > w_2$ and $w(d_0) = w_2$. Hence, the valuation of the left hand side of Eq. (5.5) is w_2, while the valuation of its right hand side is $-w_0$, a contradiction.

Finally, assume that $a_1 = 0$ and $w_1 < \min\{-w_0, w_2\}$. Then, by Proposition 5.1, we have that $w(d_{3p-i}) \geq -w_0$ for $p+2 \leq i \leq (3p-1)/2$. Hence, Eq. (5.9) tells us that $w(c_p) = w_1$, and its initial coefficient is $2/3\,\delta_1$. Also, Eq. (5.7) gives us that

$$c_p = \frac{2}{a_0^p}\left[\left(\sum_{i=0}^{(p-1)/2} \alpha_i\, d_{p-i}\right) + \alpha_{(p+1)/2}\, d_{(p-1)/2} + \left(\sum_{i=(p+3)/2}^{p} \alpha_i\, d_{p-i}\right)\right]. \tag{5.10}$$

By Proposition 5.5, the terms inside the second parentheses in the equation above have valuations greater than w_1. Observe that $w(\alpha_i) > 0$ for $i = 0, \ldots, (p-1)/2$, and thus Proposition 5.3 tells us that the valuations of the terms inside the first parentheses also have valuations greater than w_1.

Observing that $w(\alpha_{(p+1)/2}) = 0$, and its initial coefficient is $a_0^{(p+1)/2}$, Proposition 5.3 gives us that the initial term of c_p is

$$(-1)^{(p-1)/2}\, 2 \left(\prod_{i=0}^{(p-3)/2} \frac{2i+1}{2i+2}\right) \delta_1.$$

But,

$$\begin{aligned}
\prod_{i=0}^{(p-3)/2} \frac{2i+1}{2i+2} &= \frac{1}{2}\cdot\frac{3}{4}\cdots\frac{p-4}{p-3}\cdot\frac{p-2}{p-1} \\
&= \frac{1}{p-1}\cdot\frac{3}{p-3}\cdots\frac{p-4}{4}\cdot\frac{p-2}{2} \\
&= (-1)^{(p-1)/2}.
\end{aligned}$$

Hence, the initial coefficient of c_p is $2\delta_1$. On the other hand, we had previously established that this initial term was $2/3\,\delta_1$, and hence we have a contradiction, as $\delta_1 \neq 0$ by definition.

Thus, we have established that, for all r, we have $v(d_r) \geq -v_0$ when $b_1 = 0$, and $w(d_r) \geq -w_0$ when $a_1 = 0$.

We now can prove Proposition 4.3.

Proof of Proposition 4.3. If $b_1 = 0$, then the Eq. (5.9) gives us that $v(c_p) \geq -v_0$, and then Eq. (5.7) gives us that $v(a_1) \geq -v_0$.

In the same way, if $a_1 = 0$, then the Eq. (5.8) gives us that $w(c_0) \geq -w_0$, and then Eq. (5.6) gives us that $w(b_1) \geq -w_0$. $\square$

This conclude the proof of Theorem 1.1. Note that by Proposition 4.2 we have that $\mathrm{ord}_{\tilde{j}_0=0}(\tilde{J}_1) = (2p+v(a_1))/3$ and $\mathrm{ord}_{\tilde{\tilde{j}}_0=0}(\tilde{\tilde{J}}_1) = (p+w(b_1))/2$. Since $v(a_1) \geq -v_0$ and $w(b_1) \geq -w_0$, Eq. (4.9) implies that

$$v(a_1) \geq \begin{cases} 1, & \text{if } p \equiv 1 \pmod 6, \\ -1, & \text{if } p \equiv 5 \pmod 6, \end{cases} \quad \text{and} \quad w(b_1) \geq \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Hence,

$$\mathrm{ord}_{\tilde{j}_0=0}(\tilde{J}_1) \geq \begin{cases} (2p+1)/3, & \text{if } p \equiv 1 \pmod 6, \\ (2p-1)/3, & \text{if } p \equiv 5 \pmod 6, \end{cases}$$

and

$$\mathrm{ord}_{\tilde{\tilde{j}}_0=0}(\tilde{\tilde{J}}_1) \geq \begin{cases} (p+1)/2, & \text{if } p \equiv 1 \pmod 4, \\ (p-1)/2, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

We can obtain then the analogue result for the usual invariant.

Proposition 5.6. *Let r' and s' be as in Theorem 3.2. Then,* $\mathrm{ord}_{j_0=0}(J_1) \geq r'$*,* $J_1(1728) = (1728-1728^p)/p$*, and* $J_1^{(t)}(1728) = -(t-1)!\,(-1728)^{1-t}$*, for* $1 \leq t \leq s'$*.*

Proof. This is a simple computation with Witt vectors. Let

$$4 = (\alpha_0, \alpha_1), \quad 27 = (\beta_0, \beta_1), \quad 1728 = (\gamma_0, \gamma_1),$$

and $F(X,Y) \stackrel{\text{def}}{=} \psi(X+Y)$ (with ψ as in Definition 3.1). (Note that $\alpha_0, \beta_0, \gamma_0 \neq 0$.) Then, the second coordinate of $1728(4\tilde{\boldsymbol{j}}/(4\tilde{\boldsymbol{j}}+27))$ is equal to

$$\gamma_0 \left(-\alpha_0 \tilde{J}_0^p \frac{\alpha_0 \tilde{J}_1 + \alpha_1 \tilde{J}_0^p + \beta_1 + F(\alpha_0 \tilde{J}_0, \beta_0)}{(\alpha_0 \tilde{J}_0^p + \beta_0)^p} + \frac{\alpha_0 \tilde{J}_1 + \alpha_1 \tilde{J}_0^p}{\alpha_0 \tilde{J}_0^p + \beta_0} \right) + \gamma_1 \frac{\alpha_0 \tilde{J}_0^p}{\alpha_0 \tilde{J}_0^p + \beta_0}. \tag{5.11}$$

Thus, by Eq. (4.5), if $\tilde{J}_1(\tilde{X})$ has a zero of order less than p at $\tilde{X}=0$, then $J_1(X)$ has a zero of the same order at $X=0$. If $\tilde{J}_1(\tilde{X})$ has a zero of order greater than or equal to p at $\tilde{X}=0$, then $J_1(X)$ has a zero of order greater than or equal to p at $X=0$. Thus Proposition 4.3 gives the desired lower bound for $\mathrm{ord}_{j_0=0}(J_1)$.

Now, by Eq. (4.6), we have that

$$\boldsymbol{j} - 1728 = 1728 \frac{27\tilde{\tilde{\boldsymbol{j}}}}{27\tilde{\tilde{\boldsymbol{j}}} + 4}.$$

Similarly to the computation above, one sees that the second coordinate of the right hand side of this equation is

$$\gamma_0 \left(-\beta_0 \tilde{J}_0^p \frac{\beta_0 \tilde{J}_1 + \beta_1 \tilde{J}_0^p + \alpha_1 + F(\beta_0 \tilde{J}_0, \alpha_0)}{(\beta_0 \tilde{J}_0^p + \alpha_0)^p} + \frac{\beta_0 \tilde{J}_1 + \beta_1 \tilde{J}_0^p}{\beta_0 \tilde{J}_0^p + \alpha_0} \right) + \gamma_1 \frac{\beta_0 \tilde{J}_0^p}{\beta_0 \tilde{J}_0^p + \alpha_0},$$

while the left hand side is

$$J_1(X) - \gamma_1 + \psi(X - \gamma_0).$$

Now, the order of the zero of the right hand side at $X = \gamma_0 = 1728$ is the same as the order of the zero at $\tilde{\tilde{X}} = 0$, and hence, by our estimates on $\mathrm{ord}_{\tilde{\tilde{j}}_0=0}(\tilde{\tilde{J}}_1)$ above, it is greater than or equal to s'.

Since

$$\psi(X - \gamma_0)|_{X=\gamma_0} = -\gamma_0^p \sum_{i=1}^{p-1} \left(\frac{1}{p} \binom{i}{p} \right) (-1)^i = 0,$$

we have that $J_1(\gamma_0) = \gamma_1 = (1728 - 1728^p)/p$.

Also, since the t-th derivative (with respect to X) of the right hand since is zero at $X = \gamma_0$ for $1 \leq t \leq s' - 1$, we have that $J_1^{(t)}(\gamma_0) = -(\psi(X - \gamma_0))^{(t)}\big|_{X=\gamma_0}$. But, for $1 \leq t \leq (p-1)$, we have

$$\begin{aligned} \psi(X - \gamma_0))^{(t)} &= (p-1)(p-2)\cdots(p-t+1)(X^{p-t} - (X-\gamma_0)^{p-t}) \\ &= (-1)^{t-1}(t-1)!\,(X^{p-t} - (X-\gamma_0)^{p-t}, \end{aligned}$$

which gives the desired formula for $J_1^{(t)}(1728)$. $\square$

Note that Proposition 5.6 is just a restatement of the second part of item 3 of Theorem 3.2, except that we only proved a lower bound for $\mathrm{ord}_{X=0}\,\bar{\varphi}_p(X)$.

6. Experimental Data and Further Questions

A question that naturally arises is what happens modulo p^3. For instance, is J_2 regular at $j_0 = 0$ and $j_0 = 1728$? Unfortunately the author's MAGMA program to compute the *general* formulas (i.e., over $\mathbb{F}_p(a_0, b_0)$ with a_0 and b_0 algebraically independent transcendental elements) of canonical liftings modulo p^3 seem to require a lot of computer power. Assuming there is no bug in the authors code (or in MAGMA), a computer with 16 gigabytes of memory cannot compute the general formula for the canonical lifting (and elliptic Teichmüller lift) modulo 17^3. The problem lies in the computation of the Greenberg transform of the elliptic curve, computed using the polynomial formulas for the sum and products of Witt vectors. So the data in this case is quite restricted, and so far we only have it for $p \leq 13$. On the other hand, as seen in Eq. (1.1), for $p = 7$ we have that $j_0 = 1728 = -1$ is a pole of J_2. Hence, in contrast with the case modulo p, we have $j_0 = 1728$ might not yield pseudo-canonical liftings modulo p^3. Also, the same holds for $p = 11$, i.e., $j_0 = 1728$ is a pole of J_2.

On the other hand, we have that $j_0 = 0$ is supersingular for $p = 5, 11$, but J_2 has zeros at that value (of orders 5 and 33 respectively). So, it seems that it could be the case that

$j_0 = 0$ still yield pseudo-canonical liftings modulo p^3. But even if that turns out to be the case, the failure of $j_0 = 1728$ makes one wonder if $j_0 = 0$ will also fail for large enough power of p.

More data would certainly be helpful, and the author is current working in improving his algorithms.

Acknowledgement. The author would like to thank F. Voloch for the invaluable discussions on the subject of this paper. Also, the computations mentioned were done with MAGMA and Sage.

References

[Bui00] A. Buium. Differential modular forms. *J. Reine Angew. Math.*, 520:95–167, 2000.

[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.

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

[Fin04] L. R. A. Finotti. Minimal degree liftings of hyperelliptic curves. *J. Math. Sci. Univ. Tokyo*, 11(1):1–47, 2004.

[Fin06] L. R. A. Finotti. Minimal degree liftings in characteristic 2. *J. Pure Appl. Algebra*, 207(3):631–673, 2006.

[Fin08] L. R. A. Finotti. A formula for the supersingular polynomial. To appear at the Acta Arithmetica. Available at `http://www.math.utk.edu/~finotti/`, 2008.

[Hur01] C. Hurlburt. Isogeny covariant differential modular forms modulo p. *Compositio Math.*, 128(1):17–34, 2001.

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

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

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

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

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

Email address: `finotti@math.utk.edu`