Liftings of Elliptic and Hyperelliptic Curves

Luís Finotti

University of Tennessee

AMS Joint Meeting Jan 10, 2013





Let \mathbb{k} be a *perfect* field of characteristic p > 0 and $W = \mathbf{W}(\mathbb{k})$ be the ring of Witt vectors over \mathbb{k} .





Let k be a *perfect* field of characteristic p > 0 and W = W(k) be the ring of Witt vectors over k.

Remember also that we have a Frobenius map, which we denote by σ on W, defined by

$$\sigma(a_0, a_1, \ldots) = (a_0^p, a_1^p, \ldots).$$





Let k be a *perfect* field of characteristic p > 0 and W = W(k) be the ring of Witt vectors over k.

Remember also that we have a Frobenius map, which we denote by σ on $W\mbox{,}$ defined by

$$\sigma(a_0, a_1, \ldots) = (a_0^p, a_1^p, \ldots).$$

So, if σ denotes the Frobenius in characteristic p (i.e., $\sigma(a)=a^p$), we have a *lifting of the Frobenius*.





Let \mathbbm{k} be a *perfect* field of characteristic p > 0 and $W = \mathbf{W}(\mathbbm{k})$ be the ring of Witt vectors over \mathbbm{k} .

Remember also that we have a Frobenius map, which we denote by σ on W, defined by

$$\boldsymbol{\sigma}(a_0,a_1,\ldots)=(a_0^p,a_1^p,\ldots).$$

So, if σ denotes the Frobenius in characteristic p (i.e., $\sigma(a)=a^p$), we have a *lifting of the Frobenius*. More precisely, if $\pi:W\to \mathbb{k}$ is the reduction modulo p, we have the following diagram on multiplicative groups:

$$W^{\times} \xrightarrow{\sigma} W^{\times}$$

$$\downarrow^{\pi}$$

$$\mathbb{k}^{\times} \xrightarrow{\sigma} \mathbb{k}^{\times}$$





Witt Vectors (cont.)

Moreover, the *Teichmüller lift* $\tau: a \mapsto (a,0,0,\ldots)$ (a *group homomorphism*) yields the following diagram:

$$W^{\times} \xrightarrow{\sigma} W^{\times}$$

$$\pi \left(\begin{array}{c} \tau \\ \tau \end{array} \right) \tau \qquad \tau \left(\begin{array}{c} \tau \\ \tau \end{array} \right) \pi$$

$$\mathbb{R}^{\times} \xrightarrow{\sigma} \mathbb{R}^{\times}$$





Witt Vectors (cont.)

Moreover, the *Teichmüller lift* $\tau: a \mapsto (a,0,0,\ldots)$ (a *group homomorphism*) yields the following diagram:

$$W^{\times} \xrightarrow{\sigma} W^{\times}$$

$$\pi \left(\begin{array}{ccc} \tau & \tau & \tau \\ \tau & \tau & \tau \end{array} \right) \pi$$

$$\mathbb{R}^{\times} \xrightarrow{\sigma} \mathbb{R}^{\times}$$

Question

Can we also lift the Frobenius for curves over k?





More precisely, given a curve C/\mathbb{k} and if $\phi:C\to C^\sigma$ is the Frobenius map, is there a lifting C/W for which we can lift the Frobenius:

$$C(\mathbf{W}(\bar{\mathbb{k}})) \xrightarrow{\phi} C^{\sigma}(\mathbf{W}(\bar{\mathbb{k}}))$$

$$\downarrow^{\pi} \qquad \qquad \downarrow^{\pi}$$

$$C(\bar{\mathbb{k}}) \xrightarrow{\phi} C^{\sigma}(\bar{\mathbb{k}})$$





More precisely, given a curve C/\mathbb{k} and if $\phi:C\to C^{\sigma}$ is the Frobenius map, is there a lifting C/W for which we can lift the Frobenius:

$$C(W(\bar{\mathbb{k}})) \xrightarrow{\phi} C^{\sigma}(W(\bar{\mathbb{k}}))$$

$$\downarrow^{\pi} \qquad \qquad \downarrow^{\pi}$$

$$C(\bar{\mathbb{k}}) \xrightarrow{\phi} C^{\sigma}(\bar{\mathbb{k}})$$

Answer: Yes, for *ordinary* elliptic curves and Abelian varieties (Deuring and Serre-Tate),



More precisely, given a curve C/\mathbb{k} and if $\phi:C\to C^{\sigma}$ is the Frobenius map, is there a lifting C/W for which we can lift the Frobenius:

$$C(\mathbf{W}(\bar{\mathbb{k}})) \xrightarrow{\phi} C^{\sigma}(\mathbf{W}(\bar{\mathbb{k}}))$$

$$\downarrow^{\pi} \qquad \qquad \downarrow^{\pi}$$

$$C(\bar{\mathbb{k}}) \xrightarrow{\phi} C^{\sigma}(\bar{\mathbb{k}})$$

Answer: Yes, for *ordinary* elliptic curves and Abelian varieties (Deuring and Serre-Tate), but no for higher genus curves (Raynaud).





More precisely, given a curve C/\mathbb{k} and if $\phi:C\to C^{\sigma}$ is the Frobenius map, is there a lifting C/W for which we can lift the Frobenius:

$$C(\mathbf{W}(\bar{\mathbb{k}})) \xrightarrow{\phi} C^{\sigma}(\mathbf{W}(\bar{\mathbb{k}}))$$

$$\downarrow^{\pi} \qquad \qquad \downarrow^{\pi}$$

$$C(\bar{\mathbb{k}}) \xrightarrow{\phi} C^{\sigma}(\bar{\mathbb{k}})$$

Answer: Yes, for *ordinary* elliptic curves and Abelian varieties (Deuring and Serre-Tate), but no for higher genus curves (Raynaud). In the case of elliptic curves we also have a *Teichmüller lift*.





More precisely, given a curve C/\mathbb{k} and if $\phi:C\to C^{\sigma}$ is the Frobenius map, is there a lifting C/W for which we can lift the Frobenius:

$$C(\mathbf{W}(\bar{\mathbb{k}})) \xrightarrow{\phi} C^{\sigma}(\mathbf{W}(\bar{\mathbb{k}}))$$

$$\downarrow^{\pi} \qquad \qquad \downarrow^{\pi}$$

$$C(\bar{\mathbb{k}}) \xrightarrow{\phi} C^{\sigma}(\bar{\mathbb{k}})$$

Answer: Yes, for *ordinary* elliptic curves and Abelian varieties (Deuring and Serre-Tate), but no for higher genus curves (Raynaud). In the case of elliptic curves we also have a *Teichmüller lift*.

Also, Mochizuki showed that one can lift the Frobenius for some curves of genus $g \geq 2$ if we allow singularities (at (p-1)(g-1) points).





An elliptic curve (given by $y^2=x^3+ax+b$) over a field \mathbbm{k} of characteristic p>3 is *ordinary* if $E[p]\cong \mathbb{Z}/p$.





An elliptic curve (given by $y^2=x^3+ax+b$) over a field \mathbbm{k} of characteristic p>3 is *ordinary* if $E[p]\cong \mathbb{Z}/p$. (Or, equivalently, if the coefficient of x^{p-1} in $(x^3+ax+b)^{(p-1)/2}$ is non-zero.)





An elliptic curve (given by $y^2=x^3+ax+b$) over a field k of characteristic p>3 is *ordinary* if $E[p]\cong \mathbb{Z}/p$. (Or, equivalently, if the coefficient of x^{p-1} in $(x^3+ax+b)^{(p-1)/2}$ is non-zero.) Otherwise, the elliptic curve is said to be *supersingular*.



AMS Joint Meet. - 01/10/13

An elliptic curve (given by $y^2=x^3+ax+b$) over a field \mathbbm{k} of characteristic p>3 is *ordinary* if $E[p]\cong \mathbbm{Z}/p$. (Or, equivalently, if the coefficient of x^{p-1} in $(x^3+ax+b)^{(p-1)/2}$ is non-zero.) Otherwise, the elliptic curve is said to be *supersingular*.

Note: Only finitely many elliptic curves (up to isomorphism) are supersingular.



An elliptic curve (given by $y^2=x^3+ax+b$) over a field \mathbbm{k} of characteristic p>3 is *ordinary* if $E[p]\cong \mathbbm{Z}/p$. (Or, equivalently, if the coefficient of x^{p-1} in $(x^3+ax+b)^{(p-1)/2}$ is non-zero.) Otherwise, the elliptic curve is said to be *supersingular*.

Note: Only finitely many elliptic curves (up to isomorphism) are supersingular.

We can lift the Frobenius for ordinary elliptic curves, i.e., if \mathbbm{k} is a perfect field with $\operatorname{char}(\mathbbm{k})=p$ and $E/\mathbbm{k}:y_0^2=x_0^3+a_0x_0+b_0$, then there exists ${\boldsymbol a}=(a_0,a_1,\ldots),{\boldsymbol b}=(b_0,b_1,\ldots)\in W$ such that ${\boldsymbol E}/W:{\boldsymbol y}^2={\boldsymbol x}^3+a{\boldsymbol x}+{\boldsymbol b}$ has a lifting of the Frobenius:

$$E(\mathbf{W}(\bar{\mathbb{k}})) \xrightarrow{\phi} E^{\sigma}(\mathbf{W}(\bar{\mathbb{k}}))$$

$$\downarrow^{\pi} \qquad \qquad \downarrow^{\pi}$$

$$E(\bar{\mathbb{k}}) \xrightarrow{\phi} E^{\sigma}(\bar{\mathbb{k}})$$





Moreover, the curve ${\pmb E}$ above is unique up to isomorphism and it is called the *canonical lifting of* E.





Moreover, the curve E above is unique up to isomorphism and it is called the *canonical lifting of* E.

As with Witt vectors, we also have a section of the reduction modulo p, the so called *elliptic Teichmüller lift* τ :

$$E(\mathbf{W}(\bar{\mathbb{k}})) \xrightarrow{\phi} E^{\sigma}(\mathbf{W}(\bar{\mathbb{k}}))$$

$$\downarrow^{\tau} \qquad \qquad \downarrow^{\tau} \qquad \uparrow^{\tau} \qquad \qquad \downarrow^{\tau} \qquad \downarrow^{\tau^{\sigma}}$$

$$E(\bar{\mathbb{k}}) \xrightarrow{\phi} E^{\sigma}(\bar{\mathbb{k}})$$





Moreover, the curve E above is unique up to isomorphism and it is called the *canonical lifting of* E.

As with Witt vectors, we also have a section of the reduction modulo p, the so called *elliptic Teichmüller lift* τ :

Also, au is a group homomorphism



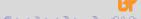
Moreover, the curve E above is unique up to isomorphism and it is called the *canonical lifting of* E.

As with Witt vectors, we also have a section of the reduction modulo p, the so called *elliptic Teichmüller lift* τ :

Also, τ is a group homomorphism, and one can show that:

$$\tau(x_0, y_0) = ((F_0, F_1, F_2, \ldots), (y_0, y_0 G_1, y_0 G_2, \ldots)),$$

where $F_i, G_i \in \mathbb{k}[x_0]$.



AMS Joint Meet. - 01/10/13

Voloch and Walker used canonical liftings and the elliptic Teichmüller lift to create error-correcting codes.





Voloch and Walker used canonical liftings and the elliptic Teichmüller lift to create error-correcting codes. The bounds for the parameters (which measure "how good" the resulting codes are likely to be) depend on the degrees of F_i 's and G_i 's,





Voloch and Walker used canonical liftings and the elliptic Teichmüller lift to create error-correcting codes. The bounds for the parameters (which measure "how good" the resulting codes are likely to be) depend on the degrees of F_i 's and G_i 's, with lower degrees giving better bounds.





Voloch and Walker used canonical liftings and the elliptic Teichmüller lift to create error-correcting codes. The bounds for the parameters (which measure "how good" the resulting codes are likely to be) depend on the degrees of F_i 's and G_i 's, with lower degrees giving better bounds. They showed that F_1 and G_1 had minimal degrees, making the canonical lifting the natural choice.





Voloch and Walker used canonical liftings and the elliptic Teichmüller lift to create error-correcting codes. The bounds for the parameters (which measure "how good" the resulting codes are likely to be) depend on the degrees of F_i 's and G_i 's, with lower degrees giving better bounds. They showed that F_1 and G_1 had minimal degrees, making the canonical lifting the natural choice.

On the other hand, F_i and G_i for $i \geq 2$ are **not** minimal.





Voloch and Walker used canonical liftings and the elliptic Teichmüller lift to create error-correcting codes. The bounds for the parameters (which measure "how good" the resulting codes are likely to be) depend on the degrees of F_i 's and G_i 's, with lower degrees giving better bounds. They showed that F_1 and G_1 had minimal degrees, making the canonical lifting the natural choice.

On the other hand, F_i and G_i for $i \geq 2$ are **not** minimal.

One should note that, one can construct codes with more general liftings of curves in a very similar way.





Error Correcting Codes (cont.)

With elliptic curves, we have:

Theorem

Let E/\mathbb{k} as above and $\tilde{E}/W_3(\mathbb{k})$ be a lifting for which we have a lifting of points $\nu: E(\bar{\mathbb{k}}) \to \tilde{E}/W_3(\bar{\mathbb{k}})$ having "minimal degrees". Then \tilde{E} is the canonical lifting of E (modulo p^3)



Error Correcting Codes (cont.)

With elliptic curves, we have:

Theorem

Let E/\Bbbk as above and $\tilde{E}/W_3(\Bbbk)$ be a lifting for which we have a lifting of points $\nu: E(\bar{\Bbbk}) \to \tilde{E}/W_3(\bar{\Bbbk})$ having "minimal degrees". Then \tilde{E} is the canonical lifting of E (modulo p^3) and we have a lifting of the Frobenius on the affine part of E so that the following diagram commutes:

$$\tilde{E}(W_{3}(\bar{\mathbb{k}})) \xrightarrow{\tilde{\phi}} \tilde{E}^{\sigma}(W_{3}(\bar{\mathbb{k}}))$$

$$\pi \left(\begin{array}{c} \\ \\ \\ \\ \end{array} \right) \nu \qquad \pi \left(\begin{array}{c} \\ \\ \\ \end{array} \right) \nu^{\sigma}$$

$$E(\bar{\mathbb{k}}) \xrightarrow{\phi} E^{\sigma}(\bar{\mathbb{k}})$$





Error Correcting Codes (cont.)

With elliptic curves, we have:

Theorem

Let E/\Bbbk as above and $\tilde{E}/W_3(\Bbbk)$ be a lifting for which we have a lifting of points $\nu: E(\bar{\Bbbk}) \to \tilde{E}/W_3(\bar{\Bbbk})$ having "minimal degrees". Then \tilde{E} is the canonical lifting of E (modulo p^3) and we have a lifting of the Frobenius on the affine part of E so that the following diagram commutes:

$$\tilde{E}(W_{3}(\bar{\mathbb{k}})) \xrightarrow{\tilde{\phi}} \tilde{E}^{\sigma}(W_{3}(\bar{\mathbb{k}}))$$

$$\pi \left(\begin{array}{c} \\ \\ \\ \\ \end{array} \right) \nu \qquad \pi \left(\begin{array}{c} \\ \\ \\ \end{array} \right) \nu^{\sigma}$$

$$E(\bar{\mathbb{k}}) \xrightarrow{\phi} E^{\sigma}(\bar{\mathbb{k}})$$

Moreover, any supersingular elliptic curve will yield larger degrees.



Therefore, the notions of *ordinary elliptic curve* and its *canonical lifting* (at least modulo p^3) can be defined strictly from the point of view of minimal degree liftings:





Therefore, the notions of *ordinary elliptic curve* and its *canonical lifting* (at least modulo p^3) can be defined strictly from the point of view of minimal degree liftings:

■ *E* is ordinary if there is a lifting satisfying the lower bound on the degrees of the lifting map;





Therefore, the notions of *ordinary elliptic curve* and its *canonical lifting* (at least modulo p^3) can be defined strictly from the point of view of minimal degree liftings:

- *E* is ordinary if there is a lifting satisfying the lower bound on the degrees of the lifting map;
- $m{E}$ is the canonical lifting of E if there is a lifting map satisfying the lower bound.





Therefore, the notions of *ordinary elliptic curve* and its *canonical lifting* (at least modulo p^3) can be defined strictly from the point of view of minimal degree liftings:

- *E* is ordinary if there is a lifting satisfying the lower bound on the degrees of the lifting map;
- $m{E}$ is the canonical lifting of E if there is a lifting map satisfying the lower bound.

On the other hand, in this way, these notions can be generalized to higher genus curves, and in a very similar way, one can obtain very similar results for *hyperelliptic* curves!





Mochizuki Liftings

For genus 2 curves (and so hyperelliptic) in characteristic 3, one can have a Mochizuki lifting of the Frobenius if one removes (some) 2 points from the curve.





Mochizuki Liftings

For genus 2 curves (and so hyperelliptic) in characteristic 3, one can have a Mochizuki lifting of the Frobenius if one removes (some) 2 points from the curve. These two points are invariant by the hyperelliptic involution and thus can be put at "infinity".





Mochizuki Liftings

For genus 2 curves (and so hyperelliptic) in characteristic 3, one can have a Mochizuki lifting of the Frobenius if one removes (some) 2 points from the curve. These two points are invariant by the hyperelliptic involution and thus can be put at "infinity".

We then have:

Theorem (F.-Mochizuki)

The notions of "ordinary" and "canonical lifting" (modulo p^2) from minimal degree lifting coincide with the ones coming from Mochizuki's theory.





Mochizuki Liftings

For genus 2 curves (and so hyperelliptic) in characteristic 3, one can have a Mochizuki lifting of the Frobenius if one removes (some) 2 points from the curve. These two points are invariant by the hyperelliptic involution and thus can be put at "infinity".

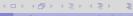
We then have:

Theorem (F.-Mochizuki)

The notions of "ordinary" and "canonical lifting" (modulo p^2) from minimal degree lifting coincide with the ones coming from Mochizuki's theory.

Thus, we were able to give a concrete example of a family of Mochizuki liftings.

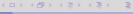




The J_n Functions

We now return to ordinary elliptic curves and their canonical liftings.





The J_n Functions

We now return to ordinary elliptic curves and their canonical liftings.

If \mathbb{k}^{ord} denotes the set of ordinary j-invariants in \mathbb{k} , we have functions $J_i: \mathbb{k}^{ord} \to \mathbb{k}$ such that $(j_0, J_1(j_0), J_2(j_0), \ldots)$ is the j-invariant of the canonical lifting of the curve with j-invariant $j_0 \in \mathbb{k}^{ord}$.



The J_n Functions

We now return to ordinary elliptic curves and their canonical liftings.

If \mathbb{k}^{ord} denotes the set of ordinary j-invariants in \mathbb{k} , we have functions $J_i: \mathbb{k}^{ord} \to \mathbb{k}$ such that $(j_0, J_1(j_0), J_2(j_0), \ldots)$ is the j-invariant of the canonical lifting of the curve with j-invariant $j_0 \in \mathbb{k}^{ord}$.

Mazur's Question (to John Tate)

What kind of functions are these J_n ? Can one say anything about them?

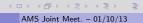




Examples:

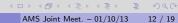
$$p = 5$$
 $I_1 = 3j_0^3 + j_0^4$;





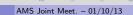
Examples:





Examples:

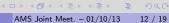
Question: Can these functions all be polynomials?



Examples:

Question: Can these functions all be polynomials?





Examples:

$$p=5$$

- p=5 $J_1=3j_0^3+j_0^4$;
 - $J_2 =$

$$3j_0^5 + 2j_0^{10} + 2j_0^{13} + 4j_0^{14} + 4j_0^{15} + 4j_0^{16} + j_0^{17} + 4j_0^{18} + j_0^{19} + j_0^{20} + 3j_0^{23} + j_0^{24}.$$

Question: Can these functions all be polynomials?

$$o = 7$$

- p = 7 $J_1 = 3i_0^5 + 5i_0^6$:
 - $J_2 =$





Examples:

$$p = 5 \qquad \mathbf{I}_1 = 3j_0^3 + j_0^4;$$

$$\mathbf{I}_2 = 3j_0^5 + 2j_0^{10} + 2j_0^{13} + 4j_0^{14} + 4j_0^{15} + 4j_0^{16} + j_0^{17} + 4j_0^{18} + j_0^{19} + j_0^{20} + 3j_0^{23} + j_0^{24}.$$

Question: Can these functions all be polynomials?

$$\begin{array}{ll} p=7 & \bullet & J_1=3j_0^5+5j_0^6;\\ \bullet & J_2=\\ & (3j_0^{21}+6j_0^{28}+3j_0^{33}+5j_0^{34}+4j_0^{35}+2j_0^{36}+3j_0^{37}+6j_0^{38}+3j_0^{39}+5j_0^{40}+5j_0^{41}+\\ & 5j_0^{42}+2j_0^{43}+3j_0^{44}+6j_0^{45}+3j_0^{46}+5j_0^{47}+5j_0^{48}+3j_0^{49}+3j_0^{54}+5j_0^{55})/(1+j_0^7). \end{array}$$

Note: If $j_0 = -1$, then E is supersingular, i.e., no canonical lifting.

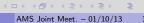




(Superficial) Answer to Mazur's Question

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





(Superficial) Answer to Mazur's Question

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

Tate's Question

Is there a supersingular value of j_0 (for some fixed characteristic p) for which all functions J_n are regular at j_0 . (E.g., $j_0=0$ for p=5 for J_1 and J_2 ?)





(Superficial) Answer to Mazur's Question

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

Tate's Question

Is there a supersingular value of j_0 (for some fixed characteristic p) for which all functions J_n are regular at j_0 . (E.g., $j_0=0$ for p=5 for J_1 and J_2 ?)

This lead us to define:

Definition

The elliptic curve over $W(\mathbb{k})$ given by $j \stackrel{\text{def}}{=} (j_0, J_1(j_0), J_2(j_0), \ldots)$ for such a supersingular j_0 is a pseudo-canonical lifting of the elliptic curve given by j_0 .

(Superficial) Answer to Mazur's Question

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

Tate's Question

Is there a supersingular value of j_0 (for some fixed characteristic p) for which all functions J_n are regular at j_0 . (E.g., $j_0=0$ for p=5 for J_1 and J_2 ?)

This lead us to define:

Definition

The elliptic curve over $W(\mathbb{R})$ given by $\mathbf{j} \stackrel{\text{def}}{=} (j_0, J_1(j_0), J_2(j_0), \ldots)$ for such a supersingular j_0 is a pseudo-canonical lifting of the elliptic curve given by j_0 . Tate's question: do they exist at all?

Theorem

Let $j_0 \notin \mathbb{k}^{ord}$ and $p \geq 5$. Then:





Theorem

Let $j_0 \notin \mathbb{k}^{ord}$ and $p \geq 5$. Then:

1 J_1 is regular at j_0 if, and only if, j_0 is either 0 or 1728.





Theorem

Let $j_0 \notin \mathbb{k}^{ord}$ and $p \geq 5$. Then:

- 1 J_1 is regular at j_0 if, and only if, j_0 is either 0 or 1728.
- 2 J_2 is regular at j_0 if, and only if, j_0 is 0.





Theorem

Let $j_0 \notin \mathbb{k}^{ord}$ and $p \geq 5$. Then:

- 1 J_1 is regular at j_0 if, and only if, j_0 is either 0 or 1728.
- 2 J_2 is regular at j_0 if, and only if, j_0 is 0.
- **3** For $n \geq 3$, we have that J_n is never regular at j_0 .





Theorem

Let $j_0 \notin \mathbb{R}^{ord}$ and $p \geq 5$. Then:

- 1 J_1 is regular at j_0 if, and only if, j_0 is either 0 or 1728.
- 2 J_2 is regular at j_0 if, and only if, j_0 is 0.
- **3** For $n \geq 3$, we have that J_n is never regular at j_0 .

For p=2,3 (in which case only $j_0=0$ is supersingular), we have that J_i is regular at 0 if, and only if, $i \le 11$ for p = 2





Theorem

Let $j_0 \notin \mathbb{R}^{ord}$ and $p \geq 5$. Then:

- 1 J_1 is regular at j_0 if, and only if, j_0 is either 0 or 1728.
- 2 J_2 is regular at j_0 if, and only if, j_0 is 0.
- **3** For $n \geq 3$, we have that J_n is never regular at j_0 .

For p=2,3 (in which case only $j_0=0$ is supersingular), we have that J_i is regular at 0 if, and only if, $i \le 11$ for p = 2 or $i \le 5$ for p = 3.





Theorem

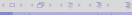
Let $j_0 \notin \mathbb{k}^{ord}$ and $p \geq 5$. Then:

- 1 J_1 is regular at j_0 if, and only if, j_0 is either 0 or 1728.
- 2 J_2 is regular at j_0 if, and only if, j_0 is 0.
- **3** For $n \geq 3$, we have that J_n is never regular at j_0 .

For p=2,3 (in which case only $j_0=0$ is supersingular), we have that J_i is regular at 0 if, and only if, $i \le 11$ for p=2 or $i \le 5$ for p=3.

So, (unrestricted) pseudo-canonical liftings don't exits.



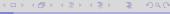


We need some notation: let

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

(the supersingular polynomial)





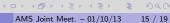
We need some notation: let

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

(the *supersingular polynomial*) and

$$S_p(X) \stackrel{\mathrm{def}}{=} \prod_{\substack{j \text{ supers.} \\ j \neq 0,1728}} (X-j).$$





We need some notation: let

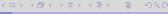
$$\operatorname{ss}_p(X) \stackrel{\text{def}}{=} \prod_{j \text{ supers.}} (X - j)$$

(the supersingular polynomial) and

$$S_p(X) \stackrel{\mathrm{def}}{=} \prod_{\substack{j \text{ supers.} \\ j \neq 0,1728}} (X-j).$$

One then has that $\mathrm{ss}_p(X), S_p(X) \in \mathbb{F}_p[X]$, and $S_p(0), S_p(1728) \neq 0$.





We need some notation: let

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

(the supersingular polynomial) and

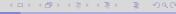
$$S_p(X) \stackrel{\mathrm{def}}{=} \prod_{\substack{j \text{ supers.} \\ j \neq 0,1728}} (X - j).$$

One then has that $\mathrm{ss}_p(X), S_p(X) \in \mathbb{F}_p[X]$, and $S_p(0), S_p(1728) \neq 0$. Also, let

$$\iota = \begin{cases} 8, & \text{if } p = 2; \\ 3, & \text{if } p = 3; \\ 2, & \text{if } p = 31; \\ 1, & \text{otherwise.} \end{cases}$$



15 / 19

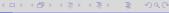


Then, we have:

Theorem

Let $J_i = F_i/G_i$, with $F_i, G_i \in \mathbb{F}_p[X]$, $(F_i, G_i) = 1$, and G_i monic.





Then, we have:

Theorem





Then, we have:

Theorem





Then, we have:

Theorem

- 2 if $p \ge 5$, then $G_i = S_p(X)^{ip^{i-1} + (i-1)p^{i-2}} \cdot H_i$, where $H_i \mid X^{s_i'} \cdot (X 1728)^{r_i}$;



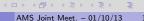


Then, we have:

Theorem

- 2 if $p \geq 5$, then $G_i = S_p(X)^{ip^{i-1} + (i-1)p^{i-2}} \cdot H_i$, where $H_i \mid X^{s_i'} \cdot (X 1728)^{r_i}$;
- $\mathbf{3}$ if p=2,3, then $G_i=X^{t_i}$, where $t_i\leq p^i$.





Then, we have:

Theorem

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

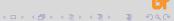
- 2 if $p \ge 5$, then $G_i = S_p(X)^{ip^{i-1} + (i-1)p^{i-2}} \cdot H_i$, where $H_i \mid X^{s_i'} \cdot (X 1728)^{r_i}$;
- $\mathbf{3}$ if p=2,3, then $G_i=X^{t_i}$, where $t_i\leq p^i$.

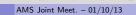
Also, there is a formula for $J_i(X)$ (which can be simplified if $p \geq 3$) obtained from the *classical modular polynomial*.





Assume from now $p \geq 5$.





Assume from now $p\geq 5$. Another perspective: if E/\mathbb{k} , ordinary, is given by $y_0^2=x_0^3+a_0x_0+b_0$, and E/W is its canonical lifting and (after some "choice") is given by $y^2=x^3+ax+b$, then





Assume from now $p\geq 5$. Another perspective: if E/\mathbb{k} , ordinary, is given by $y_0^2=x_0^3+a_0x_0+b_0$, and E/W is its canonical lifting and (after some "choice") is given by $\boldsymbol{y}^2=\boldsymbol{x}^3+\boldsymbol{a}\boldsymbol{x}+\boldsymbol{b}$, then

$$a = (A_0, A_1, A_2, \ldots),$$

 $b = (B_0, B_1, B_2, \ldots),$

where $A_i, B_i \in \mathbb{k}(a_0, b_0)$.





Assume from now $p\geq 5$. Another perspective: if E/\mathbb{k} , ordinary, is given by $y_0^2=x_0^3+a_0x_0+b_0$, and E/W is its canonical lifting and (after some "choice") is given by $\boldsymbol{y}^2=\boldsymbol{x}^3+\boldsymbol{a}\boldsymbol{x}+\boldsymbol{b}$, then

$$a = (A_0, A_1, A_2, \ldots),$$

 $b = (B_0, B_1, B_2, \ldots),$

where $A_i, B_i \in \mathbb{k}(a_0, b_0)$. In fact, if \mathcal{H} is the *Hasse invariant* of E (i.e., the coefficient of x_0^{p-1} is $(x_0^3 + a_0x_0 + b_0)^{(p-1)/2}$), then A_i, B_i possibly have poles only at the zeros of \mathcal{H}





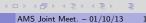
Assume from now $p\geq 5$. Another perspective: if E/\mathbb{k} , ordinary, is given by $y_0^2=x_0^3+a_0x_0+b_0$, and E/W is its canonical lifting and (after some "choice") is given by $\boldsymbol{y}^2=\boldsymbol{x}^3+\boldsymbol{a}\boldsymbol{x}+\boldsymbol{b}$, then

$$a = (A_0, A_1, A_2, \ldots),$$

 $b = (B_0, B_1, B_2, \ldots),$

where $A_i, B_i \in \mathbb{k}(a_0, b_0)$. In fact, if \mathcal{H} is the *Hasse invariant* of E (i.e., the coefficient of x_0^{p-1} is $(x_0^3 + a_0x_0 + b_0)^{(p-1)/2}$), then A_i, B_i possibly have poles only at the zeros of \mathcal{H} (or $\Delta = 4a_0^3 + 27b_0^2$).





Assume from now $p\geq 5$. Another perspective: if E/\mathbb{k} , ordinary, is given by $y_0^2=x_0^3+a_0x_0+b_0$, and E/W is its canonical lifting and (after some "choice") is given by $\boldsymbol{y}^2=\boldsymbol{x}^3+\boldsymbol{a}\boldsymbol{x}+\boldsymbol{b}$, then

$$a = (A_0, A_1, A_2, \ldots),$$

 $b = (B_0, B_1, B_2, \ldots),$

where $A_i, B_i \in \mathbb{k}(a_0, b_0)$. In fact, if \mathcal{H} is the *Hasse invariant* of E (i.e., the coefficient of x_0^{p-1} is $(x_0^3 + a_0x_0 + b_0)^{(p-1)/2}$), then A_i, B_i possibly have poles only at the zeros of \mathcal{H} (or $\Delta = 4a_0^3 + 27b_0^2$).

Question

What are the weights of the A_i 's and B_i 's?



Assume from now $p\geq 5$. Another perspective: if E/\mathbb{k} , ordinary, is given by $y_0^2=x_0^3+a_0x_0+b_0$, and E/W is its canonical lifting and (after some "choice") is given by $\boldsymbol{y}^2=\boldsymbol{x}^3+\boldsymbol{a}\boldsymbol{x}+\boldsymbol{b}$, then

$$a = (A_0, A_1, A_2, \ldots),$$

 $b = (B_0, B_1, B_2, \ldots),$

where $A_i, B_i \in \mathbb{k}(a_0, b_0)$. In fact, if \mathcal{H} is the *Hasse invariant* of E (i.e., the coefficient of x_0^{p-1} is $(x_0^3 + a_0x_0 + b_0)^{(p-1)/2}$), then A_i, B_i possibly have poles only at the zeros of \mathcal{H} (or $\Delta = 4a_0^3 + 27b_0^2$).

Question

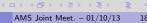
What are the weights of the A_i 's and B_i 's? What are the order of the poles?



Conjecture

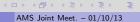
1 A_i has weight $4p^i$.





- **1** A_i has weight $4p^i$.
- **2** B_i has weight $6p^i$.





- **1** A_i has weight $4p^i$.
- **2** B_i has weight $6p^i$.
- ${f 3}$ A_i and B_i have poles of order at most (i-1)p+1 at the zeros of ${\cal H}.$



- **1** A_i has weight $4p^i$.
- **2** B_i has weight $6p^i$.
- **3** A_i and B_i have poles of order at most (i-1)p+1 at the zeros of \mathcal{H} . (At least for $i \leq 2$. Not enough data yet.)





- **1** A_i has weight $4p^i$.
- **2** B_i has weight $6p^i$.
- 3 A_i and B_i have poles of order at most (i-1)p+1 at the zeros of \mathcal{H} . (At least for $i\leq 2$. Not enough data yet.)
- 4 A_i and B_i have no zeros at zeros of Δ .





Conjecture

- **1** A_i has weight $4p^i$.
- **2** B_i has weight $6p^i$.
- 3 A_i and B_i have poles of order at most (i-1)p+1 at the zeros of $\mathcal{H}.$ (At least for $i\leq 2$. Not enough data yet.)
- 4 A_i and B_i have no zeros at zeros of Δ .

So, if true, the isomorphism $(a_0,b_0) \leftrightarrow (\lambda_0^4 a_0,\lambda_0^6 b_0)$ corresponds to the isomorphism $(a,b) \leftrightarrow (\lambda^4 a,\lambda^6 b)$, where $\lambda = \tau(\lambda_0) = (\lambda_0,0,0,\ldots)$.





Thank you!





Thank you!

And sorry for going over...



