RESEARCH STATEMENT

LUÍS R. A. FINOTTI

1. Introduction

My research has been focused on liftings (from characteristic $p > 0$ to characteristic 0) of algebraic curves, mostly canonical lifting of elliptic curves, although I have also dealt with some particular liftings of hyperelliptic curves (called *minimal degree liftings*) which had properties of particular interest to coding theory.

Apart from being of independent interest, canonical liftings have been used in many applications, such as counting rational points in ordinary elliptic curves, as in Satoh's [Sat00], counting torsion points of curves of genus $g \geq 2$, as in Poonen's [Poo01] and Voloch's [Vol97], and coding theory, as in Voloch/Walker's [VW00].

My recent work has been on questions of Mazur and Tate about the j-invariant of the canonical lifting. These problems, and the results so far, are described in Section 2. Also, while working on it, I also found necessary to improve computations with Witt vectors in order to obtain data for conjectures. Some of these improvements are discussed in Section 3.

I briefly discuss my current research and some of the topics I might work on in the future in Section 4 .

All my papers, as well as some of the routines used in the computations mentioned below, can be found on my web page `http://www.math.utk.edu/~finotti/` in the section *Research*.

2. Lifting the j-invariant

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. Then, the *canonical lifting* of an *ordinary* elliptic curve $E/\Bbbk$ is the unique elliptic curve (up to isomorphism) over $\boldsymbol{W}(\Bbbk)$, say $\boldsymbol{E}/\boldsymbol{W}(\Bbbk)$, which reduces to E modulo p and for which we can lift the Frobenius. (See, for instance, [Deu41] or [LST64], where the concept is generalized to Abelian varieties.)

Hence, given an ordinary j-invariant $j_0 \in \Bbbk$, the canonical lifting gives us a unique $\boldsymbol{j} \in \boldsymbol{W}(\Bbbk)$. Therefore, if $\Bbbk^{ord}$ denotes the set of ordinary values of j-invariants in $\Bbbk$, then we have functions $J_i : \Bbbk^{ord} \to \Bbbk$, for $i = 1, 2, 3, \ldots$, such that the j-invariant of the canonical lifting of an elliptic curve with j-invariant $j_0 \in \Bbbk^{ord}$ is $(j_0, J_1(j_0), J_2(j_0), \ldots)$.

B. Mazur asked J. Tate about the nature of these functions J_i in 2000 or 2001. Tate then used some of my formulas for canonical liftings to compute some explicit examples. (These formulas are available at `http://www.math.utk.edu/~finotti/can_lifts/`.) He computed $J_1(j_0)$ for $p = 5, 7$ (for an arbitrary j_0) and observed that these were polynomial functions in j_0. At this point he wrote me asking if I could compute more examples, and if it could be the case that these functions were always polynomial. This would be surprising, as the J_n would then be regular at supersingular values (for which the canonical lifting does not exist). But, my computations showed that this was not always the case, e.g., J_1 for $p = 13$ or J_2 for $p = 7$ have denominators.

But Tate's question motivates the following definition:

Definition 2.1. 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 $(j_0, J_1(j_0), \ldots, J_n(j_0))$ 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 $(j_0, J_1(j_0), J_2(j_0), \ldots)$ the *pseudo-canonical lifting* of the elliptic curve associated to j_0.

Hence, Tate asked 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, computations had shown the existence of such pseudo-canonical liftings modulo p^2 and p^3.

Here are the main results I have obtained so far. With respect to Tate's question:

Theorem 2.2. *Let $j_0 \notin \Bbbk^{ord}$. Then:*

(1) *j_0 yields a pseudo-canonical lifting modulo p^2 if, and only if, j_0 is either* 0 *or* 1728*. In this case, the corresponding pseudo-canonical lifting has j-invariant congruent to* 0 *or* 1728 *modulo p^2 respectively. (See* [Fin10b]*.)*

(2) *j_0 yields a pseudo-canonical lifting modulo p^3 if, and only if, j_0 is* 0*. In this case, the corresponding pseudo-canonical lifting has j-invariant congruent to* 0 *modulo p^3. (See* [Fin10a] *and* [Fin11b]*.)*

(3) *j_0 never yields a pseudo-canonical lifting modulo p^n for $n \geq 4$. (See* [Fin11b]*.)*

Therefore, all questions about pseud-canonical liftings have been completely answered and, in particular, there are no (unrestricted) pseudo-canonical liftings.

Before the results with regards with Mazur's questions can be stated, 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*,

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

(I give an explicit and relatively simple formula for $\mathrm{ss}_p(X)$ in [Fin09]. The formula itself is basically due to Deuring, who stopped one step short of giving it explicitly. Oddly enough, this formula does not seem to appear in the most common references about the supersingular polynomial, such as Kaneko and Zagier's [KZ98] or Brillhart and Morton's [BM04].) Hence, $S_p(X) \in \mathbb{F}_p[X]$, and $S_p(0), S_p(1728) \neq 0$. Also, let

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

Then, in [Fin10b], [Fin10a], and [Fin11b], the following is proved:

Theorem 2.3. *We have that $J_i \in \mathbb{F}_p(X)$. Moreover, let $p \geq 5$ and $J_i = F_i/G_i$, with $F_i, G_i \in \mathbb{F}_p[X]$, $(F_i, G_i) = 1$, and G_i monic. Then, for $i = 1, 2, 3$:*

1. $\deg F_i - \deg G_i = p^i - \iota$*;*
2. *if J_i is* regular *at $X = 0$, then F_i (and so J_i) has a zero of order $r_i p^{i-1}$ at $X = 0$, where $r_1 \stackrel{\text{def}}{=} \lfloor (2p+1)/3 \rfloor$, $r_2 \stackrel{\text{def}}{=} 2\lfloor (p-1)/6 \rfloor + 1$, and $r_3 = 1$;*
3. *$G_i = S_p(X)^{ip^{i-1}+(i-1)p^{i-2}} \cdot H_i$, where $H_1 = 1$, $H_2 = (X-1728)^{\epsilon p}$, $H_3 = X^{\delta p^2}(X-1728)^{\epsilon k}$, for some $k \in \{0, \dots, 2p^2\}$.*

It should be observed that the results above for J_1 follow from Kaneko and Zagier's [KZ98], although their results were phrased in terms of the modular polynomial rather than J_1. In [Fin10b] I give a *non-modular* proof of the results (although some results from [KZ98] are stronger), using only the existence of the canonical lifting (and an algorithm that computes it without using the modular polynomial).

One of the main tools to prove Theorems 2.2 and 2.3 was a formula for the *Greenberg transform* (see Section 3 for the definition and some details), done in [Fin10b] and [Fin11a], which allowed us to give somewhat explicit formulas for J_i for $i = 2, 3$.

3. Computations with Witt Vectors

Computations with Witt vectors can be quite demanding, as the polynomials that define the sum and product of Witt vectors are themselves often enormous. In some cases one can perform computations efficiently by identifying the ring of Witt vectors with a well known ring. This is the case, for example, for Witt vectors over finite fields, in which case the ring of Witt vectors is canonically isomorphic to an unramified extension of p-adic integers $\mathbb{Z}_p$.

Unfortunately, in most other cases we lack this canonical isomorphism and need to resort to the defining polynomial equations to perform operations.

Remember that the sum and product of Witt vectors are given by *integral* polynomials S_i and P_i which are defined recursively by

$$S_n = (X_n + Y_n) + \frac{1}{p}(X_{n-1}^p + Y_{n-1}^p - S_{n-1}^p) + \cdots + \frac{1}{p^n}(X_0^{p^n} + Y_0^{p^n} - S_0^{p^n}) \tag{3.1}$$

and

$$\begin{aligned} P_n &= \frac{1}{p^n}\Big[(X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) - \\ &\qquad \Big(P_0^{p^n} + \cdots + p^{n-1}P_{n-1}^p\Big)\Big] \\ &= (X_0^{p^n} Y_n + X_1^{p^{n-1}} Y_{n-1}^p + \cdots + X_n Y_0^{p^n}) \\ &\quad + \frac{1}{p}(X_0^{p^n} Y_{n-1}^p + \cdots + X_{n-1}^p Y_0^{p^n}) \\ &\quad \vdots \\ &\quad + \frac{1}{p^n}(X_0^{p^n} Y_0^{p^n}) - \frac{1}{p^n}P_0^{p^n} - \cdots - \frac{1}{p}P_{n-1}^p \\ &\quad + p\left(X_1^{p^{n-1}} Y_n + X_2^{p^{n-2}}(Y_{n-1}^p + pY_n) + \ldots\right). \end{aligned} \tag{3.2}$$

Thus, we have that if $\boldsymbol{a} = (a_0, a_1, \ldots)$ and $\boldsymbol{b} = (b_0, b_1, \ldots)$, then

$$\boldsymbol{a} + \boldsymbol{b} \overset{\text{def}}{=} (S_0(a_0, b_0), S_1(a_0, a_1, b_0, b_1), \ldots)$$

and

$$\boldsymbol{a} \cdot \boldsymbol{b} \overset{\text{def}}{=} (P_0(a_0, b_0), P_1(a_0, a_1, b_0, b_1), \ldots).$$

One should observe that simply computing S_2 can take a lot of time and memory. For instance, for $p = 31$ the polynomial S_2 has 152994 monomials!

To actually compute and get information on the functions J_i, I needed we to compute the *Greenberg transform* of the modular polynomial $\Phi_p(X, Y)$. More explicitly:

Definition 3.1. Let $\boldsymbol{f}(\boldsymbol{x},\boldsymbol{y}) \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x},\boldsymbol{y}]$. If $\boldsymbol{x}_0 = (x_0, x_1, \ldots), \boldsymbol{y}_0 = (y_0, y_1, \ldots) \in \boldsymbol{W}(\Bbbk[x_0, y_0, x_1, y_1, \ldots])$, then $\boldsymbol{f}(\boldsymbol{x}_0, \boldsymbol{y}_0) = (f_0, f_1, \ldots) \in \boldsymbol{W}(\Bbbk[x_0, y_0, x_1, y_1, \ldots])$ (in fact, $f_n \in \Bbbk[x_0, \ldots, x_n, y_0, \ldots, y_n]$) is 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 zeros of the coordinates f_n of $\mathscr{G}(\boldsymbol{f})$.

So, to compute the Greenberg transform of a polynomial, we perform the sums and products of Witt vectors over polynomial rings. These computations get quite involved. So, to obtain some concrete examples of J_2 (to be able to make some conjectures on what happens in that case), it was necessary to develop more efficient ways to compute with Witt vectors of length 3. (This was done in [Fin10a].) Later, to deal with J_3, I was able to generalize the methods to arbitrary length in [Fin11a]. In particular, in these references formulas for the third and n-th coordinate of the Greenberg transform, respectively, are given. This was crucial not only to optimize computations, but also to prove Theorems 2.2 and 2.3.

The formula for the n-th coordinate of the Greenberg transform is quite involved and use some auxiliary functions η_i:

Definition 3.2. Let p be a prime. Define $\eta_0(X_1, \ldots, X_r) \overset{\text{def}}{=} X_1 + \cdots + X_r \in \mathbb{Q}[X_1, \ldots, X_r]$, and recursively for $k \geq 1$

$$\eta_k(X_1, \ldots, X_r) \overset{\text{def}}{=} \frac{X_1^{p^k} + \cdots + X_r^{p^k}}{p^k} - \sum_{i=0}^{k-1} \frac{\eta_i(X_1, \ldots, X_r)^{p^{k-i}}}{p^{k-i}}. \tag{3.3}$$

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

The η_i's are in fact integral polynomials and can be used instead of the S_i's and P_i's in order to make computations with Witt vectors, yielding considerable improvements.

As an example (from [Fin11a]) of the improvements obtained, we can look at the computation of J_3. In principle, we would need to compute the Greenberg transform of the modular polynomial $\Phi_p(X, Y)$. Using the *usual* sum and product and products of Witt vectors, we could only compute J_3 for $p = 5$. For $p = 7$ over 24 gigabytes of memory (all that I have available) was required. Using the new methods mentioned above (with the η_i's), the same computer could compute J_3 for $p = 7$ in 7.3 seconds and using only 40.97 megabytes of memory! This method also allowed me to compute J_3 for $p \leq 13$.

Moreover, using the formula for the Greenberg transform, one can identify terms which will vanish in the process of computing J_3 (which was done in [Fin11b]), giving further

	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 3.1. Computations of J_3

improvements and allowing us to compute J_3 for $p \leq 23$. (Observe that with the information from 2.3 one can compute J_3 by interpolation. But these computations were done before the theorem was proved. Besides, the goal here is to show improvements on computations with Witt vectors.) Table 3.1 shows the times and memory usages for these last two methods.

Here is another application of these new methods from [Fin11a]. The 24 gigabytes of memory I had available were not enough to compute S_4 for $p = 11$, even when using my newer methods. (Note that S_4 is just the fifth coordinate of the Greenberg transform of $\boldsymbol{x} + \boldsymbol{y}$.) On the other hand, my new methods actually allows us to add Witt vectors using the η_i's, and so we do not need S_4 anymore. In fact, in [Fin11a] gives two different methods: one that precompute and stores the necessary η_i's and another which evaluates the η_i's on the fly.

Then we can, for instance, add two vectors in $\boldsymbol{W}_6(\mathbb{F}_{11^{10}})$ (which would require S_5 for $p = 11$ before) in about a second (on average), after we spend approximately 3.61 hours to compute the $\bar{\eta}_i(X, Y)$ for $i \in \{1, 2, 3, 4, 5\}$. (Although this might seem as long time, it takes the same computer 7.20 hours to compute S_3 with the improved methods and we cannot even compute S_4 with the memory available!) Using the second algorithm, which does not precompute the $\eta_i' s$, we need only 5.750 seconds to precompute other necessary data, but then it takes us about 26 seconds on average to add two Witt vectors in $\boldsymbol{W}_6(\mathbb{F}_{11^{10}})$. So, in this case, this second algorithm would certainly be more efficient if we ones does not need too many additions. (Of course, there are better ways to perform computation with Witt vectors over finite fields, but the goal here was merely compare the general methods. One could perform the computations above over, say, polynomial rings, but the times would be considerably greater.)

4. Current and Future Research

4.1. **More on J_n.**

I've been currently working on generalize some parts of Theorem 2.3. More precisely, I am working on proving the following conjecture:

Conjecture 4.1. *Let $p \geq 5$ and $J_i = F_i/G_i$, with $F_i, G_i \in \mathbb{F}_p[X]$, $(F_i, G_i) = 1$, and G_i monic. Then, for* all *$i \in \mathbb{Z}_{>0}$ we have:*

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

Using the formula for the Greenberg transform, I believe I have found simplifications on the formula for J_n (similar to the ones on J_3 that yielded great improvements on its computation) and with that I believe I was able to prove item 1 above. (This was done very recently, so I am still hesitant to claim it has been proved until I have all details properly written.) I also believe that $G_i = S_p(X)^{ip^{i-1}+(i-1)p^{i-2}} \cdot H_i$, where $H_i \mid X^{\delta k_1} \cdot (X-1728)^{\epsilon k_2}$, for some k_1 and k_2, should follow from a similar analysis, but I have not worked it out yet. On the other hand, the bounds for k_1 and k_2 that would give item 2 of the conjecture might require a little more work.

I hope to finish this project and submit it for publication by the end of the summer. The preprint will be available in my web page (`http://www.math.utk.edu/~finotti/`) as soon as it is finished.

Finally, it would also be interesting to study the J_n's through a *modular* perspective, similarly to what Kaneko and Zagier did with J_1 in [KZ98], but I have not started working on this yet.

4.2. **Canonical Liftings of Genus 2.** It would be interesting to see if one can perform explicit computations of canonical liftings of Abelian varieties of higher dimensions. One could in principle have as initial goal the case Jacobians of curves of genus two, for which some information is already known. (If so, can one lift the Igusa invariants as done with j-invariants? At least modulo p^2? Could one apply it to coding theory, as done by Voloch and Walker for elliptic curves?)

Also, there is no actual canonical lifting (in the sense of lifting the Frobenius) for curves of genus 2 (in characteristic $p > 0$), but one can compute the canonical lifting of its *Jacobian*, which is itself a Jacobian of a genus 2 curve (in characteristic 0), which we might call the "canonical lifting" of the original curve. J.-F. Mestre has some (unpublished) work on the subject with curves over field of characteristic 2. (It seems that his main interest was counting points, which has applications in cryptography, and the case of characteristic 2 is then the most relevant.) I would be interested in verifying if these "canonical liftings" have any relation with minimal degree liftings (as in [Fin04] and [Fin06]), as do canonical liftings of elliptic curves or Mochizuki liftings of genus 2 curves. Also, is it possible to generalize Mestre's methods to other characteristics?

4.3. **Mochizuki Lifts.** I would also like to take a deeper look at connections between Mochizuki lifts and minimal degree lifts. Mochizuki's theory is very extensive and quite sophisticated, making this a long term project.

A question more suitable for a more immediate project was posed by Mochizuki: one can try to verify if the concepts of ordinariness and Mochizuki-ordinariness also coincide for elliptic curves in characteristic 2, as they do for curves of genus 2 in characteristic 3, as shown in [Fin04].

References

[BM04] J. Brillhart and P. Morton. Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial. *J. Number Theory*, 106(1):79–111, 2004.

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

[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.

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

[Fin10a] L. R. A. Finotti. Computations with Witt vectors of length 3. To appear at the "Journal de Théorie des Nombres de Bordeaux". Available at `http://www.math.utk.edu/~finotti/`, 2010.

[Fin10b] 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. Non-existance of pseudo-canonical liftings. To appear at the "International Journal Number Theory". Available at `http://www.math.utk.edu/~finotti/`, 2011.

[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.

[Vol97] J. F. Voloch. Torsion points of $y^2 = x^6 + 1$. *unpublished manuscript*, 1997. available at `http://www.ma.utexas.edu/users/voloch/oldpreprint.html`.

[VW00] J. F. Voloch and J. L. Walker. Euclidean weights of codes from elliptic curves over rings. *Trans. Amer. Math. Soc.*, 352(11):5063–5076, 2000.