

Computations with Witt Vectors and Lifting the j -Invariant

Luís Finotti

University of Tennessee

CRM – April 22, 2010



p -Adic Integers

Let:

- p be a prime, $r \in \mathbb{Z}_{>0}$, and $q \stackrel{\text{def}}{=} p^r$
- \mathbb{Q}_q be the unramified extension of \mathbb{Q}_p of degree r ;
- \mathbb{Z}_q be the ring of integers of \mathbb{Q}_q .

Then \mathbb{Z}_q is a p -adic ring (or **strict p -ring**) with residue field \mathbb{F}_q .

Question

Given a **perfect** field \mathbb{k} of characteristic p , is there a p -adic ring $R_{\mathbb{k}}$ with residue field \mathbb{k} ?

Yes! Witt gave an explicit construction of such ring!

Constructing $W(\mathbb{F}_q)$

Let μ_m denote the m -th roots of unity. We have:

- $\mu_{q-1} \subseteq \mathbb{Z}_q$ (Hensel's Lemma).
- $\{0\} \cup \mu_{q-1}$ is a complete set of representatives of \mathbb{F}_q in \mathbb{Z}_q .
- $a \in \mathbb{Z}_q$ has a unique representation of the form $a = \sum_{i=0}^{\infty} a_i p^i$ with $a_i \in \{0\} \cup \mu_{q-1}$.

We can then identify a with $(\bar{a}_0, \bar{a}_1, \bar{a}_2, \dots)$. But how do we add and multiply these elements now? We have

$$(\bar{a}_0, \bar{a}_1, \bar{a}_2, \dots) + (\bar{b}_0, \bar{b}_1, \bar{b}_2, \dots) = (S_0(\bar{a}_0, \bar{b}_0), S_1(\bar{a}_0, \bar{a}_1, \bar{b}_0, \bar{b}_1), \dots),$$

where $S_n \in \mathbb{Z}[X_0, X_1^{1/p}, \dots, X_n^{1/p^n}, Y_0, Y_1^{1/p}, \dots, Y_n^{1/p^n}]$. The product is similar.

Constructing $W(\mathbb{F}_q)$ (cont.)

Better idea: to identify $a = \sum a_i p^i$ with $(\bar{a}_0, \bar{a}_1^p, \bar{a}_2^{p^2}, \dots)$. Then:

$$\begin{aligned}(\bar{a}_0, \bar{a}_1, \bar{a}_2, \dots) + (\bar{b}_0, \bar{b}_1, \bar{b}_2, \dots) &= (S_0(\bar{a}_0, \bar{b}_0), S_1(\bar{a}_0, \bar{a}_1, \bar{b}_0, \bar{b}_1), \dots), \\(\bar{a}_0, \bar{a}_1, \bar{a}_2, \dots) \cdot (\bar{b}_0, \bar{b}_1, \bar{b}_2, \dots) &= (P_0(\bar{a}_0, \bar{b}_0), P_1(\bar{a}_0, \bar{a}_1, \bar{b}_0, \bar{b}_1), \dots),\end{aligned}$$

where $S_n, P_n \in \mathbb{Z}[X_0, X_1, \dots, X_n, Y_0, Y_1, \dots, Y_n]$. (S_n and P_n depend only on p .)

Hence, we have an isomorphism of ring \mathbb{F}_q^∞ with sum and product defined by polynomial equations above and \mathbb{Z}_q .

The Ring $\mathbf{W}(\mathbb{k})$

Given a **perfect field** \mathbb{k} of characteristic p , this construction makes \mathbb{k}^∞ a p -adic ring with residue field \mathbb{k} (with $p = (0, 1, 0, \dots)$), the **ring of Witt vectors** over \mathbb{k} , denoted by $\mathbf{W}(\mathbb{k})$.

As we can see from the power series identification, we have that

$\mathbf{W}_n(\mathbb{k}) \stackrel{\text{def}}{=} \mathbf{W}(\mathbb{k})/(p^n)$ is the truncation of vectors to the n -th coordinate, and hence we call this quotient **ring the ring of Witt vectors of length n** .

The p -th power Frobenius σ of \mathbb{k} lifts to $\mathbf{W}(\mathbb{k})$ by $\sigma(a_0, a_1, \dots) = (\sigma(a_0), \sigma(a_1), \dots) = (a_0^p, a_1^p, \dots)$.



Computing in $\mathbf{W}(\mathbb{k})$

To compute with $\mathbf{W}_n(\mathbb{k})$, need S_i, P_i for $i \in \{0, \dots, (n-1)\}$.

Problem: These polynomials are huge! E.g., for $p = 31$, S_2 has 152,994 monomials!

Thus, if $\mathbb{k} = \mathbb{F}_q$, one should make computations in \mathbb{Z}_q .

But, depending on \mathbb{k} , we cannot see $\mathbf{W}(\mathbb{k})$ as a known local ring, and so we might need to use S_n and P_n for sums and products.

The Polynomials S_n and P_n .

S_n and P_n are given recursively:

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

and

$$\begin{aligned} P_n &= (X_0^{p^n} Y_n + X_1^{p^{n-1}} Y_{n-1}^p + \cdots + X_n Y_0^{p^n}) \\ &\quad + \frac{1}{p}(X_0^{p^n} Y_{n-1}^p + \cdots + X_{n-1}^p Y_0^{p^n}) \\ &\quad \vdots \\ &\quad + \frac{1}{p^n}(X_0^{p^n} Y_0^{p^n}) - \frac{1}{p^n} P_0^{p^n} - \cdots - \frac{1}{p} P_{n-1}^p \\ &\quad + p(\cdots). \end{aligned}$$

We cannot plug in coordinates on these formulas! Have to expand and simplify!



Canonical Liftings

Let E/\mathbb{k} (\mathbb{k} as above) be an **ordinary** elliptic curve. (I.e., $E[p] \neq 0$.) Then there exists a **unique** elliptic curve $E/W(\mathbb{k})$ for which we can **lift the Frobenius** $\phi : E \rightarrow E^\sigma$:

$$\begin{array}{ccc}
 E(W(\mathbb{k})) & \xrightarrow{\phi} & E^\sigma(W(\mathbb{k})) \\
 \pi \downarrow & & \downarrow \pi \\
 E(\mathbb{k}) & \xrightarrow{\phi} & E^\sigma(\mathbb{k})
 \end{array}$$

Definition

E is the **canonical lifting** of E .

Canonical liftings are often used in point counting (e.g., **Satoh's algorithm**).



The Elliptic Teichmüller Lift

The map $\tau : \mathbb{k} \rightarrow \mathbf{W}(\mathbb{k})$ defined by $\tau(a_0) = (a_0, 0, 0, \dots)$ is section of the reduction modulo p which induced a homomorphism of the multiplicative groups, which commutes with the Frobenius. It is called the **Teichmüller lift**.

We have the analogue for elliptic curves:

$$\begin{array}{ccc}
 E(\mathbf{W}(\mathbb{k})) & \xrightarrow{\phi} & E^\sigma(\mathbf{W}(\mathbb{k})) \\
 \tau \uparrow & & \uparrow \tau^\sigma \\
 E(\mathbb{k}) & \xrightarrow{\phi} & E^\sigma(\mathbb{k})
 \end{array}$$

This is called the **elliptic Teichmüller lift**.

One can use it to compute the canonical lifting **without using the modular polynomial**, and it has been used to construct **error correcting codes**.



Greenberg Transform

Let $\mathbf{f} \in \mathbf{W}(\mathbb{k})[\mathbf{x}, \mathbf{y}]$. By letting $\mathbf{x} = (x_0, x_1, \dots)$ and $\mathbf{y} = (y_0, y_1, \dots)$ (seen as Witt vectors) and expanding, we have $\mathbf{f}(\mathbf{x}, \mathbf{y}) = (f_0, f_1, f_2, \dots)$. We call $\mathcal{G}(\mathbf{f}) \stackrel{\text{def}}{=} (f_0, f_1, \dots)$ the **Greenberg transform** of \mathbf{f} .

Examples

$$\mathcal{G}(\mathbf{x} + \mathbf{y}) = (S_0, S_1, S_2, \dots)$$

$$\mathcal{G}(\mathbf{x} \cdot \mathbf{y}) = (P_0, P_1, P_2, \dots).$$

If $\mathbf{C}/\mathbf{W}(\mathbb{k}) : \mathbf{f}(\mathbf{x}, \mathbf{y}) = \mathbf{0}$, then the **Greenberg transform** of \mathbf{C} is the (infinite dimensional) variety given by the zeros of the coordinates of $\mathcal{G}(\mathbf{f})$. This gives a bijection between $\mathbf{C}(\mathbf{W}(\mathbb{k}))$ and $\mathcal{G}(\mathbf{C})(\mathbb{k})$.



An Example of a Greenberg Transform

Let $E/W(\mathbb{F}_5) : \mathbf{y}^2 = \mathbf{x}^3 + \mathbf{1}$. Then, the first three equations of the Greenberg Transform are:

$$\textcircled{1} \quad y_0^2 = x_0^3 + 1;$$

$$\textcircled{2} \quad 2y_0^5 y_1 = 4x_0^{12} + 3x_0^{10} x_1 + 3x_0^9 + 3x_0^6 + 4x_0^3;$$

$$\textcircled{3} \quad 4y_0^{25} y_1^5 + 2y_0^{25} y_2 + y_1^{10} = 4x_0^{72} + 3x_0^{69} + 3x_0^{66} + 4x_0^{63} + 2x_0^{58} x_1 + 3x_0^{57} + 3x_0^{56} x_1^2 + x_0^{55} x_1 + x_0^{54} x_1^3 + 2x_0^{54} + 3x_0^{53} x_1^2 + x_0^{52} x_1^4 + 4x_0^{52} x_1 + 4x_0^{51} x_1^3 + 2x_0^{50} x_1^5 + 4x_0^{50} x_1^2 + 3x_0^{50} x_2 + 2x_0^{49} x_1^4 + 3x_0^{49} x_1 + 3x_0^{48} x_1^3 + x_0^{48} + 2x_0^{46} x_1^4 + 4x_0^{44} x_1^2 + x_0^{43} x_1^4 + 4x_0^{43} x_1 + 3x_0^{42} x_1^3 + 4x_0^{41} x_1^2 + 4x_0^{40} x_1 + 4x_0^{39} x_1^3 + 4x_0^{39} + 4x_0^{37} x_1 + x_0^{36} x_1^3 + 4x_0^{36} + 4x_0^{35} x_1^2 + 3x_0^{32} x_1^2 + 3x_0^{31} x_1 + 3x_0^{29} x_1^2 + 4x_0^{28} x_1 + x_0^{27} + 3x_0^{25} x_1^{10} + x_0^{25} x_1 + 2x_0^{22} x_1 + 2x_0^{21} + 3x_0^{18} + 4x_0^{12} + 3x_0^9 + 3x_0^6 + 4x_0^3$$

Lifting the j -Invariant

$E/\mathbb{k} : y_0^2 = f(x_0) \stackrel{\text{def}}{=} x_0^3 + a_0x_0 + b_0$ (assumed to be **ordinary**) has j -invariant

$$j_0 \stackrel{\text{def}}{=} 1728 \frac{4a_0^3}{4a_0^3 + 27b_0^2}.$$

Let $\mathbf{j} = (j_0, j_1, \dots)$ be the j -invariant of the canonical lifting \mathbf{E} . Clearly j_n 's are functions of j_0 only. Say, $j_n = J_n(j_0)$.

Mazur's Question (to John Tate)

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

First Computations

Examples:

$$p = 5 \quad \bullet \quad J_1 = 3j_0^3 + j_0^4;$$

$$\bullet \quad J_2 = 3j_0^5 + 2j_0^{10} + 2j_0^{13} + 4j_0^{14} + 4j_0^{15} + 4j_0^{16} + j_0^{17} + 4j_0^{18} + j_0^{19} + j_0^{20} + 3j_0^{23} + j_0^{24}.$$

Question: Can these functions all be polynomials?

$$p = 7 \quad \bullet \quad J_1 = 3j_0^5 + 5j_0^6;$$

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

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

Pseudo-Canonical Liftings

(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 ?)

Definition

The elliptic curve over $\mathbf{W}(\mathbb{k})$ given by $j \stackrel{\text{def}}{=} (j_0, J_1(j_0), J_2(j_0), \dots)$ for such a supersingular j_0 is a **pseudo-canonical lifting** of the elliptic curve given by j_0 . **Tate's question:** are there any?

The Answer Module p^2

Theorem

- 1 $J_1(X)$ is *always* regular at $X = 0$ and $X = 1728$.
- 2 $(0, J_1(0)) \equiv 0 \pmod{p^2}$ and $(1728, J_1(1728)) \equiv 1728 \pmod{p^2}$.
- 3 If $j_0 \neq 0, 1728$ is supersingular, then J_1 has a (simple) pole at j_0 .

Hence:

- **Only** $j_0 = 0$ and $j_0 = 1728$ can yield pseudo-canonical liftings modulo p^2 , and they **always** do (when they are supersingular values).
- In those cases the pseudo-canonical lifting has its j_0 -invariant, say \mathbf{j} , such that $\mathbf{j} \equiv 0 \pmod{p^2}$ and $\mathbf{j} \equiv 1728 \pmod{p^2}$ respectively.

The 2nd Coordinate of the GT

Definition

Given $f = \sum_{i,j} a_{i,j} x^i y^j \in \mathbf{W}(\mathbb{k})[x, y]$, define

$$f^{(p^n)} \stackrel{\text{def}}{=} \sum_{i,j} a_{i,j}^{p^n} x^{ip^n} y^{jp^n},$$

Note: This is **not a homomorphism!**

Definition

Let $g(x_0, y_0) \in \mathbb{k}[x_0, y_0]$ and $\mathbf{g}(x, y) \in \mathbf{W}_2(\mathbb{k})$ the **Teichmüller lift** of g , i.e., the coefficient a goes to $(a, 0, 0, \dots)$. We define

$$\eta_1(g) \stackrel{\text{def}}{=} \eta_1(\mathbf{g}) \stackrel{\text{def}}{=} \pi \left(\frac{\mathbf{g}^{(p)} - \mathbf{g}^p}{p} \right).$$

The 2nd Coordinate of the GT (cont.)

Proposition

Let

$$g(x, y) = \sum_{i,j} a_{i,j} x^i y^j \in \mathbf{W}_2(\mathbb{k})[x, y],$$

with $\mathbf{a}_{i,j} = (a_{i,j,0}, a_{i,j,1})$. Then, the second coordinate of $\mathcal{G}(g)$ is given by

$$x_1 \left(\frac{\partial g}{\partial x_0} \right)^p + y_1 \left(\frac{\partial g}{\partial y_0} \right)^p + \eta_1(g) + \sum_{i,j} a_{i,j,1} x_0^{pi} y_0^{pj}.$$

Canonical Lifting and Frobenius

Now, if \mathbf{E} is the canonical lifting of E (in characteristic p), and if $\mathbf{j} = (j_0, j_1, \dots)$ is the j -invariant of \mathbf{E} , then

$$\Phi_p(\mathbf{j}, \mathbf{j}^\sigma) = \Phi_p((j_0, j_1, \dots), (j_0^p, j_1^p, \dots)) = 0.$$

The second coordinate of $\Phi_p((j_0, j_1), (j_0^p, j_1^p)) = 0$ is then

$$(j_0^{p^2} - j_0)^p j_1^p + \sum_{i,j} \beta_{i,j} j_0^{ip+jp^2} = 0,$$

where

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


Formula for J_1

Hence, since $\Phi_p(X, Y) \in \mathbb{Z}[X, Y]$ and $\alpha^p = \alpha$ in $\mathbb{Z}/p\mathbb{Z}$, we have

$$J_1(X_0) = -\frac{H_p(X_0)}{X_0^{p^2} - X_0},$$

where $H_p(X_0) \stackrel{\text{def}}{=} \pi(\Phi_p(X, X^p)/p)$.

(Note the denominators!)

Kaneko and Zagier's results on H_p proves the **Modulo p^2 case** . Their proof use **modular forms**, and is hence *analytic* in nature. I gave an alternative (elementary) proof which proves some of their results. (No modular polynomial, using the elliptic Teichmüller (and Greenberg transform) instead.)

Computation of $J_2(X)$

To compute $J_2(X)$, one can find the canonical lifting (modulo p^2) for a **generic** elliptic curve. Part of my old algorithm is to compute the GT, which gets quite complicated. The usual computation of sums of Witt vectors demand a lot of memory. The computation of the GT (by the old methods) for $p = 17$ used **24 gigabytes** (16 of RAM and 8 of swap) before it crashed **still unfinished!**

Hence, there was not much data to form a conjecture about $J_2(X)$. I had only p from 5 to 13. On the old hand:

- 1 $J_2(0) = 0$ for these p 's, and $j_0 = 0$ is supersingular for $p = 5, 11$.
- 2 $J_2(j_0)$ has a **pole** at $j_0 = 1728$ for $p = 7, 11$, and $j_0 = 1728$ is supersingular for those p 's.

Computing J_n

Previous method not the best. (Don't need the elliptic Teichmüller.) We can use the modular polynomial. [▶ go](#) The Proposition [▶ go](#) on the second coordinate of the GT was crucial. (And helps the other algorithm too!)

With this generalization one can try to generalize the proof I gave (elementary) for J_1 . (But it is very messy!)

A geometrical proof would be much more interesting. (Or analytical, as done by Kaneko and Zagier.)



Results for J_2

With our formula for the Greenberg transform, we can compute J_n explicitly from $\Phi_p(X, X^p)$ **without having to use sums and products of Witt vectors**. (So far, only did $n = 2$.)

Theorem

If $J_2 = F(X)/G(X)$, with $\gcd(F, G) = 1$, then:

- ① $\deg F - \deg G = p^2 - 1$ (or $p^2 - 2$ if $p = 31$);
- ② if 0 or 1728 is a zero of G , then it is a zero of order p ;
- ③ every other supersingular value is a zero of order $2p + 1$ of G ;
- ④ we have some precise upper bound for $\deg F$.

Conjectures for J_2 (cont.)

We could then compute many examples of J_2 (for $p \leq 37$) and we then conjecture:

Conjecture

If $J_2 = F(X)/G(X)$, with $\gcd(F, G) = 1$, then:

- ① $G(0) \neq 0$, even if $j_0 = 0$ is supersingular;
- ② if 1728 is supersingular, then it is a zero of G (or order p);
- ③ F has a zero of order $(2\lfloor(p-1)/6\rfloor + 1)p$ at 0.

In particular, if 0 is supersingular, $\mathbf{j} = (0, 0, 0)$ gives the pseudo-canonical lifting of $j_0 = 0$ over $\mathbf{W}_3(\mathbb{k})$ and no other supersingular value (possibly including 1728) has a pseudo-canonical lifting over $\mathbf{W}_3(\mathbb{k})$.

Related Conjecture

Items one and three from previous conjecture are equivalent to:

Conjecture

Let $p \geq 5$, v_p denote the valuation at p , $\Phi_p(X, Y) = \sum a_{i,j} X^i Y^j$ be the modular polynomial, and $s = (2\lfloor (p-1)/6 \rfloor + 1)$. Then:

- ① $v_p(a_{i,0}) \geq 3$ for $i \in 0, \dots, s$;
- ② $v_p(a_{s+1,0}) = 2$.

The conjecture above has been verified for $p \leq 353$.

We know:

- ① $v_p(a_{i,0}) \geq 2$ for $i \in \{0, \dots, \lfloor (2p+1)/3 \rfloor\}$,
- ② if $p \equiv 1 \pmod{6}$, then $a_{0,0} = a_{1,0} = 0$.

Conjecture for J_3

I haven't implemented the new formulas for the GT yet. So, data is scarce. (Only $p = 5$ has been computed.) But based on the valuations of the coefficients of the modular polynomial (and some heuristic arguments), we have:

Conjecture

If 0 is supersingular, then $J_3(X)$ has a pole of order p^2 at $X = 0$.

More data soon.

General Idea

We want to:

- 1 avoid computing and storing the (huge) S_n and P_n ;
- 2 avoid expanding powers;
- 3 perform computations (almost) entirely in characteristic p .

For example: if $\eta_1(X_0, Y_0) = (X_0^p + Y_0^p - (X_0 + Y_0)^p)/p$ can be stored as a function $\eta_1(X_0, Y_0) = \sum_{i=1}^{p-1} \left(\frac{1}{p} \binom{p}{i}\right) X_0^i Y_0^{p-i}$. And

$$S_1 = X_1 + Y_1 + \eta_1(X_0, Y_0).$$

For the second item, if we want to evaluate the polynomial function $(X_0 + Y_0)^n$, it is better to not expand the powers. The polynomials S_n and P_n have “hidden powers” that are not easily spotted.



Length 3 (the “Good Case”)

All of those can be accomplished nicely for length 3. For greater length some polynomial functions *much* simpler than S_n and P_n need to be computed and stored. (More on this soon.)

Performance Improvements

The following table shows the times and memory needed to compute the polynomials S_1 and S_2 for different characteristics p , using the **original** recursion (in $\mathbb{Z}/p^3\mathbb{Z}$) and using the **new** computations in characteristic p (and formula for the GT) in MAGMA.

char.	$t_{\text{orig.}}$ (sec)	t_{new} (sec)	$m_{\text{orig.}}$ (MB)	m_{new} (MB)
23	5.589	0.590	26.06	11.96
31	56.100	1.389	68.72	18.38
41	638.029	4.259	210.56	57.80
53	8560.129	14.160	545.75	81.75

Note that with the new method one does not need to compute S_1 and S_2 to compute sums and products of Witt vectors.

Computation over \mathbb{F}_q

Remember that we don't want to use Witt vectors to work with $\mathbf{W}(\mathbb{F}_q)$, but for comparison, here is some average times to sum two Witt vectors of length 3 in MAGMA.

Field	evaluating S_1 and S_2	recursive method
$\mathbb{F}_{11^{15}}$	0.017 sec.	0.004 sec.
\mathbb{F}_{13^7}	0.125 sec.	0.014 sec.
$\mathbb{F}_{23^{10}}$	0.709 sec.	0.058 sec.
\mathbb{F}_{43^4}	3.475 sec.	0.847 sec.
\mathbb{F}_{53^4}	8.489 sec.	2.428 sec.
\mathbb{F}_{61^4}	15.413 sec.	5.055 sec.
$\mathbb{F}_{101^{20}}$	2027.190 sec.	85.779 sec.

The times for the old method **do not** take into account the time to compute S_1 and S_2 .



GT of Quadratic Polynomial

The following table shows the times and memory needed to compute the GT of

$$\mathbf{x}^2 + (a_0, a_1, a_2)\mathbf{x} + (b_0, b_1, b_2)$$

char.	t_{old}	t_{new}	t_{GT}	m_{old}	m_{new}	m_{GT}
7	0.420	0.410	0.360	11.57	11.28	10.31
11	9.730	4.570	1.909	130.62	107.69	36.38
13	39.929	20.800	7.730	520.12	383.88	94.28
17	758.480	262.910	74.620	4647.69	3032.72	529.75
19	--	988.269	187.659	--	7208.94	1124.44
23	--	--	1086.250	--	--	4185.97

For $p = 23$, the third coordinate of the GT has nine variables, namely the x_i 's, a_i 's, and b_i 's, and has 65,553,940 terms.

GT of Cubic Polynomial

The following table shows the times and memory needed to compute the GT of

$$\mathbf{x}^3 + (a_0, a_1, a_2)\mathbf{x}^2 + (b_0, b_1, b_2)\mathbf{x} + (c_0, c_1, c_2),$$

char.	t_{old}	t_{new}	t_{GT}	m_{old}	m_{new}	m_{GT}
5	0.420	0.410	0.370	11.53	13.6	10.62
7	5.490	4.150	1.810	94.12	90.50	44.44
11	2517.389	987.440	240.849	8380.22	7209.50	2110.59
13	--	--	2579.769	--	--	10516.19

The third coordinate for $p = 7, 11, 13$ is a polynomial in 12 variables with 533,574, 31,216,093, and 153,065,983 monomials!



Auxiliary Polynomials

We need the functions:

Definition

Define, recursively, for $k \geq 1$

$$\eta_k(X_1, \dots, X_r) \stackrel{\text{def}}{=} \frac{X_1^{p^k} + \dots + X_r^{p^k} - (X_1 + \dots + X_r)^{p^k}}{p^k} \\ - \frac{\eta_1(X_1, \dots, X_r)^{p^{k-1}}}{p^{k-1}} - \dots - \frac{\eta_{k-1}(X_1, \dots, X_r)^p}{p}.$$

Proposition

We have that $\eta_k(X_0, Y_0) = S_k(X_0, 0, \dots, 0, Y_0, 0, \dots, 0)$ and $\eta_k(X_0, \dots, X_r)$ has integral coefficients.

Auxiliary Polynomials (cont.)

The functions $\eta_k(X_0, Y_0)$ (only two variables) are needed to compute with $\mathcal{W}_{k+1}(\mathbb{k})$. For $k \geq 3$, we must compute and store them. (Simpler than S_k . E.g., for $p = 31$, η_2 has 920 terms while S_2 has 152,994.)

In fact, by using the recursive definition only need η_{k-1} . (For $p = 31$, η_1 has 30 monomials.)

We also need $\eta_k(X_1, \dots, X_r)$, but it can be computed recursively from the two variables version. (In a few slides.)

Computing in Characteristic p

Also, η_k can be computed (almost) entirely in characteristic p , but the implementation is complicated. (I haven't tried yet.) It is not clear that it will be much faster than computing them in $\mathbb{Z}/p^{k+1}\mathbb{Z}$ unless we find a **non-wasteful** method.

Example: Computing S_3 for $p = 11$ with the usual recursion takes 130.56 hours, while with the new method (not optimized yet) takes 7.20 hours. (So, hard to make many tests.)



Extending the Entries

To compute $\eta_k(X_1, \dots, X_r)$ from $\eta_k(X_0, Y_0)$:

Proposition

For any $k \geq 1$, let

$$\begin{aligned} \mathcal{N}_{k,1} &= \eta_k(X_1, \dots, X_n), & \mathcal{N}_{k,2} &= \eta_k(X_{n+1}, \dots, X_{n+m}), \\ \mathcal{N}_{k,3} &= \eta_k(X_1 + \dots + X_n, X_{n+1} + \dots + X_{n+m}) \\ \text{for } k > 1, j \in \{1, \dots, k-1\}, & \mathcal{N}_{k,3+j} &= \eta_j(\mathcal{N}_{k-j,1}, \dots, \mathcal{N}_{k-j,k-j+2}). \end{aligned}$$

Then,

$$\eta_k(X_1, \dots, X_{n+m}) = \sum_{j=1}^{k+2} \mathcal{N}_{k,j}.$$

Computing η_k in Characteristic p

Let $a_{i,j,k} \stackrel{\text{def}}{=} \frac{1}{p^j} \binom{p^k}{ip^{k-j}} = \sum_{r=0}^{\infty} a_{i,j,k,r} p^r$ (with the good representatives), and $b_{i,j,k} = a_{i,j,k,k-j}$. Let $\mathcal{M}_{k,i}$ for $i \in \{1, \dots, N_k\}$ be the monomials of

$$\sum_{j=1}^k \sum_{\substack{i=1 \\ p \nmid i}}^{p^j-1} b_{i,j,k} \mathbf{x}^{ip^{k-j}} \mathbf{y}^{p^k - ip^{k-j}}$$

and for $i \in \{1, \dots, k-1\}$ let $\mathcal{M}_{k,N_k+l} \stackrel{\text{def}}{=} \eta_l(\mathcal{M}_{k-l,1}, \dots, \mathcal{M}_{k-l,N_k+k-1})$. Then,

$$\begin{aligned} \eta_k(\mathbf{x}, \mathbf{y}) \equiv \sum_{i=1}^{N_k+k-1} \mathcal{M}_{k,i} &= \sum_{j=1}^k \sum_{\substack{i=1 \\ p \nmid i}}^{p^j-1} b_{i,j,k} \mathbf{x}^{ip^{k-j}} \mathbf{y}^{p^k - ip^{k-j}} \\ &+ \sum_{l=1}^{k-1} \eta_l(\mathcal{M}_{k-l,1}, \dots, \mathcal{M}_{k-l,N_k+k-1}) \pmod{p}. \end{aligned}$$

The Greenberg Transform

Theorem

Let $\mathbf{f}(x, y) \in \mathbf{W}(\mathbb{k})[x, y]$, and let \mathbf{f}_n be defined recursively by

$$\mathbf{f}_0^{p^n} + p\mathbf{f}_1^{p^{n-1}} + \cdots + p^n \mathbf{f}_n = \mathbf{f}^{\sigma^n}(x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n, y_0^{p^n} + py_1^{p^{n-1}} + \cdots + p^n y_n)$$

Then, $\mathcal{G}(\mathbf{f}) = (f_0, f_1, \dots)$ where f_i is the reduction modulo p of \mathbf{f}_i .

The Greenberg Transform

We need some notation. Let $\mathbf{g} \stackrel{\text{def}}{=} \sum_{i,j} \mathbf{a}_{i,j} \mathbf{x}^i \mathbf{y}^j \in \mathbf{W}(\mathbb{k})[\mathbf{x}, \mathbf{y}]$.

- ① Write $\mathbf{a}_{i,j} = \sum_{k=0}^{\infty} \mathbf{a}_{i,j,k} p^k$ (with the proper repres. $\mathbf{a}_{i,j,k}$).
- ② Define $\mu_k(\mathbf{g}) \stackrel{\text{def}}{=} \sum_{i,j} \mathbf{a}_{i,j,k} \mathbf{x}^i \mathbf{y}^j$. (Hence, $\mathbf{g} = \sum_{k=0}^{\infty} \mu_k(\mathbf{g}) p^k$.)
- ③ Define $\mathbf{g}^{(i,j)} \stackrel{\text{def}}{=} \frac{1}{i!j!} \frac{\partial^{i+j}}{\partial^i \partial^j} \mathbf{g}$, and $\mathbf{g}_{i,j,k} \stackrel{\text{def}}{=} \mu_k(\mathbf{g}^{(i,j)})$.
- ④ Define $D_{k,n}^{i,j}$ to be the coefficient of \mathbf{t}^k in

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

$$(\text{E.g., } D_{4,n}^{1,2} = 2 \mathbf{x}_1^{p^{n-1}} \mathbf{y}_1^{p^{n-1}} \mathbf{y}_2^{p^{n-2}} + \mathbf{x}_2^{p^{n-2}} \mathbf{y}_1^{2p^{n-1}}.)$$

- ⑤ Finally, $D_{k,n,l}^{i,j} \stackrel{\text{def}}{=} \mu_l(D_{k,n}^{i,j})$.

The Greenberg Transform (cont.)

Let $\mathbf{f} \in \mathbf{W}(\mathbb{k})[\mathbf{x}, \mathbf{y}]$.

- ① For $l \geq 0$, let $\{\mathcal{G}_{l,1}, \dots, \mathcal{G}_{l,N_l}\}$ be the monomials of $(\mathbf{f}^{\sigma^l})_{i,r-i,l-j}(\mathbf{x}_0^{p^l}, \mathbf{y}_0^{p^l}) D_{k,l,j-k}^{i,r-i}$, for $0 \leq i \leq r \leq j, k \leq l$.
- ② If $l > 1$, $\mathcal{G}_{l,N_l+i+1} \stackrel{\text{def}}{=} \eta_{l-i}(\mathcal{G}_{i,1}, \dots, \mathcal{G}_{i,N_i+i})$, for $i \in \{0, \dots, (l-1)\}$.
- ③ Let

$$\mathbf{f}_l \stackrel{\text{def}}{=} \sum_{i=1}^{N_l+l} \mathcal{G}_{l,i} = \sum_{r=0}^l \sum_{i=0}^r \sum_{j=r}^l \sum_{k=r}^j (\mathbf{f}^{\sigma^l})_{i,r-i,l-j}(\mathbf{x}_0^{p^l}, \mathbf{y}_0^{p^l}) D_{k,l,j-k}^{i,r-i} + \sum_{i=0}^{l-1} \eta_{l-i}(\mathcal{G}_{i,1}, \dots, \mathcal{G}_{i,N_i+i})$$

Theorem

We have that $\mathcal{G}(\mathbf{f}) = (f_0, f_1, \dots)$, where f_i is the reduction modulo p of \mathbf{f}_i .

The Third Coordinate

Let $\mathbf{f}(x, y) = \sum_{i,j} a_{i,j} x^i y^j$, $f_x(x, y) = \sum_{i,j} b_{i,j} x^i y^j$, and $f_y(x, y) = \sum_{i,j} c_{i,j} x^i y^j$. Then, the third coordinate of the Greenberg transform of \mathbf{f} is given by

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



S_n and P_n

Example

Let $\mathcal{S}_{k,1} \stackrel{\text{def}}{=} \mathbf{x}_k$, $\mathcal{S}_{k,2} \stackrel{\text{def}}{=} \mathbf{y}_k$, and for $i \in \{2, \dots, k+2\}$,

$$\mathcal{S}_{k,i} \stackrel{\text{def}}{=} \eta_{k-i-2}(\mathcal{S}_{i-2,1}, \dots, \mathcal{S}_{i-2,i})$$

Then, $S_n \equiv \sum_{i=1}^{n+2} \mathcal{S}_{n,i} = \mathbf{x}_n + \mathbf{y}_n + \sum_{i=0}^{n-1} \eta_{n-i}(\mathcal{S}_{i,1}, \dots, \mathcal{S}_{i,i+2}) \pmod{p}$.

Example

For $i \in \{1, \dots, k+1\}$, let $\mathcal{P}_{k,i} \stackrel{\text{def}}{=} \mathbf{x}_i^{p^{k-i}} \mathbf{y}_{k-i}^{p^i}$, and for $i \in \{k+2, \dots, 2k\}$,

$$\mathcal{P}_{k,i} \stackrel{\text{def}}{=} \eta_{2k+1-i}(\mathcal{P}_{i-k-1,1}, \dots, \mathcal{P}_{i-k-1,2i-2k-2}).$$

Then, $P_n \equiv \sum_{i=1}^{2n} \mathcal{P}_{n,i} = \sum_{i=0}^n \mathbf{x}_i^{p^{k-i}} \mathbf{y}_{k-i}^{p^i} + \sum_{i=0}^{n-1} \eta_{n-i}(\mathcal{P}_{i,1}, \dots, \mathcal{P}_{i,2i}) \pmod{p}$.

Thank you!

