FORMAL COMPLETION OF THE JACOBIANS OF PLANE CURVES AND HIGHER REAL K-THEORIES

V. GORBOUNOV AND M. MAHOWALD

Abstract. In this note we will study the formal completion of the Jacobian of a certain class of curves over p-adic rings. These curves generalize the Legendre family of elliptic curves. As an immediate application, we will describe the representation which is crucial for calculating the initial term of the spectral sequence, converging to the homotopy groups of the higher real K-theories EO_n.

1. Introduction

Let G_n be a maximal finite subgroup of the Morava stabilizer group $\mathbb{S}_n$. Hopkins and Miller define EO_n to be the homotopy fixed point spectrum of the action of G_n on $\mathbb{E}_n$, which extends the action of $\mathbb{S}_n$ on the ring E_n. The later is defined using the deformation theory of formal groups [7]. We call this representation the Lubin-Tate representation. These spectra come equipped with a spectral sequences for calculating its homotopy groups:

$$H^*(G_n, E_n)^{\mathrm{Gal}} \Rightarrow \pi_* EO_n.$$

EO_2 agrees with the usual elliptic cohomology when 6 is inverted [6]. In this paper we will study a formal group which can be used to define EO_n for $n = p - 1$, and describe the Lubin-Tate representation of G_n. It was suggested to the authors by Mike Hopkins that a universal lift of a formal group of height n over $\mathbb{F}_p$ should come as a summand in the formal completion of the Jacobian of a certain curve with p marked points. There is an action of G_n on such a curve, which can be expressed in terms of permutations of the marked points. This leads to a precise description of the Lubin-Tate action of G_n on the spectrum $\mathbb{E}_n$. The authors wish to thank Mike Hopkins for useful comments during the preparation of this paper.

2. Overview of the Honda theory

We recall briefly the Honda classification of formal groups from [4]. Let K be a discrete valuation field. Denote by $\mathfrak{o}$, $\mathfrak{p}$ and $\mathfrak{o}_{\mathfrak{p}}$ the ring of integers of K, the maximal ideal of $\mathfrak{o}$, and the completion of $\mathfrak{o}$ with respect to $\mathfrak{p}$ respectively. We assume that the residue class field is of characteristic $p > 0$. Suppose also that there is an endomorphism σ of K and a power q of p such that $a^\sigma = a^q$ modulo $\mathfrak{p}$ for any $a \in \mathfrak{v}$.

Let F be an n-dimensional abelian formal group over $\mathfrak{v}$ and $f = (f_1, \dots, f_n)$ denote its logarithm. Define an action of the twisted power series ring $M_n(\mathfrak{v}_\mathfrak{p})[[T]]^\sigma$ on the vector space of n-dimensional vectors over the ring $K[[x_1, \dots, x_n]]$ by

$$(u * f)(x) = \Sigma_{\eta=0}^{\infty} C_\eta f^{\sigma^\eta}(x^{q^\eta}),$$

where $u = \Sigma_\eta C_\eta T^\eta$. An element u in the twisted power series ring $M_n(\mathfrak{v}_\mathfrak{p})[[T]]^\sigma$ is said to be special for F if $u \cong \pi I_n$ modulo degree 1 and $(u * f)(x) = 0$ modulo $\mathfrak{p}$, where π is a uniformizer for $\mathfrak{p}$ and I_n is the $n \times n$ identity matrix. The following theorem is proved in [4]

Theorem 2.1. *Suppose that K is a discrete totally unramified valuation field (in addition to the conditions stated above), then the strict isomorphism classes of formal group laws over $\mathfrak{v}$ correspond bijectively to left associate classes of elements $u \in M_n(\mathfrak{v}_\mathfrak{p})[[T]]^\sigma$ of the form $u \cong \pi I_n$ modulo degree 1.*

We intend to study the formal completion of the Jacobian of a certain class of curves. Let us state the connection, established in [3], between the formal completion of the Jacobian of a curve and the space of holomorphic differentials on it. Let Γ be a curve of genus $n > 0$ over K. Denote by J the Jacobian of Γ, and by Λ the canonical map $\Gamma \to \Lambda$. Let $\omega_1, \dots, \omega_n$ be a base of holomorphic differentials on Γ, each defined over K. Choose a local parameter $z \in K(\Gamma)$ at some point P, and denote by $\omega_i(z)$ the expansion of ω_i at P. There are $\psi_i(z) \in K[[z]]$, $1 \le i \le n$, such that $\psi_i(0) = 0$ and $\omega_i(z) = d\psi_i(z)$. Let $y = (y_1, \dots, y_n) \subset K(J)$ be a system of local parameters at the origin of J and let $\nu_1, \dots, \nu_n$ be the invariant differentials on J such that

$$\nu_i \circ \Lambda = \omega_i \ \ (1 \le i \le n).$$

Let S_1 be the set of primes at which at least one the above algebro-geometric objects has a bad reduction. Let S_0 be the set of ramified primes of K.

Proposition 2.2. ([3], Theorem 1) *There is a finite set S of primes of K satisfying the following conditions:*

- *S contains $S_0 \cup S_1$.*
- *If $\mathfrak{p} \notin S$ and u is a special element of $M_n(\mathfrak{v}_\mathfrak{p})[[T]]^\sigma$ which kills $\psi(z)$ modulo $\mathfrak{p}$, then u also kills the logarithm of F mod $\mathfrak{p}$, so that F is of type u as a formal group over $\mathfrak{v}_\mathfrak{p}$.*

Remark 2.3. *As it was pointed out in* [1] (20.3.11) *the Honda classification result applies in the following situation: A is a ring of characteristic zero that is also a $\mathbb{Z}_{(p)}$-algebra, $K = A \otimes \mathbb{Q}$, $\sigma : K \to K$, such that $\sigma(a) = a^p \, modpA$ for all $a \in A$. Note that the ring $A = \mathbb{Z}_p[[u_1, \dots, u_n]]$ is of that type.*

3. Motivating example: points on elliptic curves and Lubin Tate representation

In this section we will use the properties of the Legendre curve to describe the Lubin-Tate representation of G_2 for $p = 3$. We can handle the case $p = 2$ in a similar fashion. The general strategy here will be to work with lifts of elliptic curves to the appropriate moduli space rather than with lifts of formal groups.

We choose to describe the action of G_2 on the moduli space, E_2, of the formal completion of the elliptic curve

$$y^2 = x^3 - x \tag{3.1}$$

The fromal completion is a formal group of height two, therefore the group of its automorphisms over a suitable extension of $\mathbb{F}_3$ is isomorphic to $\mathbb{S}_2$. We will present a convenient model for the moduli space of lifts of (3.1) to Artinian rings.

The Legendre curve is a plane curve defined by the equation

$$y^2 = x(x-1)(x-\lambda)$$

over the ring $e = \mathbb{Z}[\frac{1}{2}, \lambda]$. Denote this curve by C_2 and rewrite its equation as

$$y^2 = x(x-1)(x-u_1+1). \tag{3.2}$$

Complete e with respect to the ideal $(3, \lambda+1)$ and denote the completion E_2^0. The formal completion F_{C_2} of (3.2) is a Lubin-Tate lift of the formal completion of (3.1). Indeed, as a simple computation shows, the formal completion of C_2 is a series in two variables

$$F(z_1, z_2) = z_1 + z_2 + u_1(z_1^2 z_2 + z_1 z_2^2) \mod (z_1, z_2)^4$$

The pair (E_2^0, F_{C_2}) is the model of Lubin-Tate lift we will use.

Now we are ready to describe the Lubin-Tate representation of G_2. For that we consider G_2 as the group of automorphisms of the elliptic curve (3.1) over the field $\mathbb{F}_9$. This representation of G_2 is given by the substitutions

$$\begin{array}{lll} \mathbf{s_1}: & x = x' & y = y' \\ \mathbf{s_2}: & x = -x' & y = -iy' \end{array}$$

where $i^4 = 1$.

Proposition 3.3. *There are six automorphisms of the moduli space E_2^0 which preserve the isomorphism class of the curve C_2.*

Proof. This is a standard fact in elliptic curve theory, (cf [9]). In particular, if one adds to the moduli space e a forth root of unity i, then it admits six automorphisms which preserve the isomorphism class of C_2. Because this example illustrates our latter work, we will outline the proof. We have three marked points on our curve with x coordinates $\{0, 1, \lambda\}$. Any automorphism g of the moduli space takes the triple $\{0, 1, \lambda\}$ to an unordered triple $\{0, 1, g(\lambda)\}$. Let

$$x' = w^2 x + r$$
$$y' = w^3 y$$

be an isomorphism between g^*C and C. It, in its turn, takes the triple $\{0, 1, \lambda\}$ to an unordered triple $\{r, w^2+r, w^2\lambda+r\}$. There are six way to match these two unordered triples, which produce the following values for λ:

$$\{\lambda,\ \ 1-\lambda,\ \ \frac{1}{\lambda},\ \ \frac{\lambda-1}{\lambda},\ \ \frac{1}{1-\lambda},\ \ \frac{\lambda}{\lambda-1}\}$$

□

All we need now is to replace λ with $u_1 - 1$ and take into account the g fixes elements of the base ring $W(\mathbb{F}_9)$. Here are possible values for $g(u_1)$:

$$\left\{u_1,\ \ 3-u_1,\ \ \frac{u_1}{u_1-1},\ \ \frac{2u_1-3}{u_1-1},\ \ \frac{u_1-3}{u_1-2},\ \ \frac{2u_1-3}{u_1-2}\right\}$$

Remark 3.4. *By definition, $g(u) = \frac{u}{w}$. The appropriate values of w are easy to calculate. For the substitutions 3.3 they are*

$$\sqrt{-\frac{1}{\lambda}},\quad \sqrt{\frac{1}{\lambda}}$$

.

Remark 3.5. *The fact that we found only six automorphisms of the moduli space E_2^0 means that the center of the group $\mathbb{Z}/3 \rtimes \mathbb{Z}/4$ acts trivially on it. It always happens this way as is proved in* [5].

4. The generalized Legendre family

Fix a prime number p. Then a maximal finite subgroup of $\mathbb{S}_n$, G_{p-1}, is isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}/(p-1)^2$ [2]. The important points in the example with the Legendre curve C_2 are:

i) C_2 is a 2-cover of the projective line with three marked points on it. The reduction of this curve modulo the ideal $(\lambda + 1)$ has G_2 as a subgroup of its group of automorphisms via 3.3.

ii) The formal completion of the Jacobian of C_2 is a universal Lubin-Tate lift of a formal group of height two.

We would like to realize universal Lubin-Tate lifts of formal groups of other heights in a similar "algebraic" fashion. In particular, we would like to obtain them as summands in the formal completion of the Jacobian of curves. The work of Manin [8] suggests considering curves of the form

$$y^{p^a-1} = x^p - x,$$

defined over $\mathbb{F}_p$. He showed in [8] that, at least up to isogeny, the formal completion of the Jacobians of such a curve contains one dimensional summands, whose heights divide $a(p-1)$. Here we will study the case when $a = 1$.

Definition 4.1. *We will call a plane curve C_p over $E^0_{p-1} \cong \mathbb{Z}_p[[u_1, \dots, u_{p-2}]]$ defined by the following equation:*

$$y^{p-1} = x^p + u_1 x^{p-1} + \ldots + u_{p-2}x^2 + (-1 - \Sigma_{i=1}^{p-2} u_i)x \tag{4.2}$$

the generalized Legendre curve. Denote $-1 - \Sigma_{i=1}^{p-2} u_i$ by b.

If we factor out the ideal $I = (p, u_1, \dots u_{p-2})$, then the reduction of the curve C_p will be a curve $\bar{C}_p$ over $\mathbb{F}_p$ defined by the equation

$$y^{p-1} = x^p - x$$

The roots of the right hand side are $0, 1, 2, \dots p-1 \bmod p$.

Remark 4.3. *Hensel's lemma implies that all the roots of the polynomial in the right hand side of 4.2 are in E^0_{p-1}, so the curve C_p may be defined by the following equation:*

$$y^{p-1} = x(x-1)(x-e_1)\cdot \ldots \cdot (x-e_{p-2})$$

where $e_i = i + 1 \bmod I$.

As we see from the above remark C_p is a $p-1$ covering of the projective line with p marked points on it. Over the ring $\mathbb{F}_{p^{p-1}}$ the group of automorphisms of $\bar{C}_p$ contains G_{p-1}. Indeed, $\mathbb{Z}/p$ and $\mathbb{Z}/(p-1)^2$ act on the curve $\bar{C}_p$ via a substitutions:

$$x = x' + 1, \quad y = y', \qquad x = \zeta^{p-1}x', \quad y = \zeta^p y', \tag{4.4}$$

where $\zeta^{(p-1)^2} = 1$.

Proposition 4.5. *For all primes p the curves C_p and $\bar{C}_p$ are non-singular curves of genus $m = (p-1)(p-2)/2$. The following differentials*

$$\omega_{ij} = \frac{x^i dx}{y^j}, \quad 0 \le i \le j-1 \le p-3$$

form a basis of the space of holomorphic differentials.

Proof. Direct computation shows that the curves C_p and $\bar{C}_p$ are non-singular. To calculate the genus note that

$$div(x) = (p-1)P_0 - (p-1)P_\infty$$

$$div(y) = P_0 + P_1 + P_{e_1} + \ldots + P_{e_{p-2}} - pP_\infty$$

$$div(dx) = (p-2)P_0 + (p-2)P_1 + (p-2)P_{e_1} + \ldots + (p-2)P_{e_{p-2}} - pP_\infty$$

So the above differentials are indeed holomorphic. A standard argument shows that these form a basis for the space of holomorphic differentials. The Riemann-Roch theorem implies the proposition. □

Corollary 4.6. *The order of the zero at infinity of ω_{ij} is equal to $p(j-1)-(p-1)i$. If we choose $z = \frac{x}{y}$ as a local parameter at infinity than the expansion of ω_{ij} is a power series in z congruent to $j-1$ modulo $p-1$.*

5. The splitting of the formal completion of the Jacobian

Denote by $\psi_{ij}(z)$ the formal anti-derivative of the formal expansion of ω_{ij}. We will prove that in our case the prime number p belongs to the set S from 2.2. In other words we will show that the formal completion of $J(C_p)$ is defined by a special element for a vector $\psi = (\psi_{ij}(z))$, and we will study the properties of this special element. Recall that $m = (p-1)(p-2)/2$.

Theorem 5.1. *For all prime numbers p:*
i *The formal completion F of $J(C_p)$ is a formal group law over $\mathbb{Z}_p[[u_1, \ldots, u_{p-2}]]$.*
ii *If a special element u of $M_m(\mathbb{Z}_p[[u_1, \ldots, u_{p-2}]])[[T]]]^\sigma$ kills the vector (ψ_{ij}) mod p, then it also kills the logarithm of F modulo p, so that F is of type u as a formal group over $\mathbb{Z}_p[[u_1, \ldots, u_{p-2}]]$.*

Proof. **i**. We can use the general theory of reduction of algebraic varieties [10]. In our case the statement follows from the fact that the curve C_p is non-singular and its reduction is non-singular. In the terminology of [10] it means that the objects we deal with are I-simple. Note also that in our case F is killed by a special element according to 2.3.

ii. The proof repeats word for word the proof of Theorem 1 from [3], if we show that the following version of Lemma 1 from [3] holds in our case.

Lemma 5.2. *Let $\psi = (\psi_{ij})$ be as above. Then, if u and v are special elements of $M_m(\mathbb{Z}_p[[u_1, \dots, u_{p-2}]])[[T]]^\sigma$ such that $u * \psi = v * \psi = 0$ mod p, there is a unit of $M_m(\mathbb{Z}_p[[u_1, \dots, u_{p-2}]])[[T]]^\sigma$ such that $v = tu$.*

Proof.

$$u = pI_m + \Sigma_{k=1}^{\infty} C_k T^k, \quad v = pI_m + \Sigma_{k=1}^{\infty} D_k T^k$$

$C_k,\ D_k \in M_k(\mathbb{Z}_p[[u_1, \dots, u_{p-2}]])$. We will show that if $C_k = D_k$, $0 \leq k \leq l-1$ with some $l \geq 1$, then $C_l = D_l$ modulo p. We have

$$\Sigma_{k=l}^{\infty} (C_k - D_k) T^k \equiv 0 \mod p$$

It follows from 4.6 by direct computation that all the entries of $C_l - D_l$ are divisible by p. Put now

$$t_l = I_m - \frac{1}{p}(C_l - D_l) T^l$$

t_l is a unit in $M_m(\mathbb{Z}_p[[u_1, \dots, u_{p-2}]])[[T]]^\sigma$ and $t_l u = v$ modulo degree $l+1$. In this way we can find units $t_1, \dots, t_l$ successively for each $l > 0$ so that $t_l \dots t_1 u = v$ modulo degree $l+1$ and $t_l \dots t_1$ converges as l approaches infinity. The limit of $t_l \dots t_1$ clearly satisfies the requirement of our lemma. $\square$

$\square$

Theorem 5.3. *For all prime numbers p, F splits into $p-2$ summands of dimensions $1, 2, \dots p-2$ respectively. The differential $y^{-1}dx$ corresponds to a summand of F of dimension one. Denote this summand by F_{C_p}. The height of the reduction of F_{C_p} modulo the ideal I is $p-1$.*

Proof. Let u be a special element for the vector $\psi = (\psi_{ij}(z))$. To prove the splitting we will show that there is a special element for $(\psi_{i,j}(z))$, which is made out of blocks of dimensions $1, 2, \dots, p-2$. Let $u = pI_m + \Sigma_{k=1}^{\infty} C_k T^k$ be a special element which kills ψ modulo p. The coordinates of the vector ψ are naturally split into $p-2$ groups, according to the order of the zero at infinity of ω_{ij} modulo $p-1$. Recall that the order of zero at infinity of ω_{ij} is equal to $j-1$. Denote these subsets Ω_k, $k = 1, \dots, p-2$, then $\psi_{ij} \in \Omega_j$, and is a formal series in powers of z congruent to j modulo $p-1$. We can assume that the coordinates of $\psi = (\psi_{ij})$ are arranged in such a way that j is increasing. Using the definition of the operation $*$ and the fact that $p = 1$ modulo $p-1$, we see that each component r of the vector $u * \psi$ is a sum of $p-2$ power series r_j such that r_j is a power series of powers of z congruent to j mod $p-1$. Since $u*\psi = 0$ mod p we get that each $r_j = 0$ mod p. The above shows that the element $u' = pI_m + \Sigma_{k=1}^{\infty} C'_k T^k$ where each C'_k is a block submatrix of C_k with the blocks of dimensions $1, \dots, p-2$ along the the diagonal, kills vector $(\psi_{ij}(z))$ modulo p. This together with 2.2 proves the splitting.

¿From the Honda theory [4] of special elements it follows that the formal expansion of the differential $y^{-1}dx$ is the invariant differential of the one dimensional summand in the above splitting. Denote by $F^0_{C_p}$ the reduction of F_{C_p} modulo the ideal $I_0 = (u_1, \dots, u_{p-2})$. So now $F^0_{C_p}$ is a formal group over Z_p. Its differential is given by the formula

$$\omega = \frac{(1-p)dz}{1+(p-1)zw^{p-2}} \tag{5.4}$$

where the series $w(z)$ obeys the following functional equation:

$$w = z^p - zw^{p-1}$$

This shows that w is a series in powers of z congruent to p modulo $(p-1)^2$ and, therefore, ω is a series in powers of z congruent to zero modulo $(p-1)^2$. This implies that the extension of degree $p-1$ of Z_p, obtained by adding the $(p-1)^2$ root of unity acts as endomorphisms of $F^0_{C_p}$. Hence, according to [11], $p-1$ divides the height of $F^0_{C_p}$. Then, according to [8], page 71 (4.7), the reduction of $F^0_{C_p}$ modulo p must contain an indecomposable summand of dimension $k(p-1)-1$, for some natural number k. But as we saw above the maximal dimension of an indecomposable summand of F can be $p-2$, therefore $k=1$, and the height of $F^0_{C_p}$ is equal to $p-1$. ☐

6. Lubin-Tate representation of G_{p-1}

Denote by E_{p-1} the ring $W(\mathbb{F}_{p^{p-1}}) \otimes_{\mathbb{Z}_p} E^0_{p-1}[u^{-1}, u]$. In order to obtain formulas for the Lubin-Tate representation of G_{p-1} we will use the curve C_p in the same way we used C_2 in section three.

Set $e_0 = 1$ and $e_{p-1} = 0$ and denote by $[m]$ the reduction of the integer m mod p. With this notations we have $e_i \equiv [i+1]$ mod I, $0 \le i \le p-1$. G_{p-1} is generated by two elements of order p and $(p-1)^2$ respectively. Let $1 < k < p$ be a generator of $\mathbb{F}_p^{\times}$.

A general form of a transformation C_p, which reduces to an automorphism of order p of $\bar{C}_p$ is:

$$x' = v_i^{p-1}x + r_i$$

$$y' = v_i^p y$$

where $r_i = i$, $1 \leq i \leq p-1$, and $v_i \equiv 1 \mod I$, and a general form of a lift an automorphism of $\bar{C}_p$ of order $(p-1)^2$ is

$$x' = v^{p-1}x$$

$$y' = v^p y$$

where $v \equiv \zeta \mod I$, $\zeta^{(p-1)^2} = 1$. We can always assume that $\zeta^{p-1} = k^{-1}$.

Proposition 6.1. *There are automorphisms $\tilde{a}_i$, $i = 1, \dots, p-1$, and $\tilde{b}$ of the space E_{p-1}, and transformations a_i and b of the form described above, such that*

$$\tilde{a}_i^*(C_p) = a_i(C_p), \quad \tilde{b}^*(C_p) = b(C_p)$$

Here $\tilde{a}_i^*(C_p)$, and $\tilde{b}^*(C_p)$ denote the inverse images of C_p under $\tilde{a}$ and $\tilde{b}$ respectively.

Proof. It is enough to look at the images of the marked points $(0,0), (1,0), (e_1, 0), \dots, (e_{p-2}, 0)$ of C_p. If we match the images of these points under a_i and $\tilde{a}_i$, and b and $\tilde{b}$ in the following way:

$$\begin{array}{ll} 0 = v_i^{p-1} e_{[-1-i]} + r_i & 1 = v^{p-1} e_{[k-1]} \\ 1 = v_i^{p-1} e_{[-i]} + r_i & \tilde{b}(e_j) = v^{p-1} e_{[(j+1)k-1]} \\ \tilde{a}_i(e_j) = v_i^{p-1} e_{[j-i]} + r_i & \end{array}$$

$1 \leq j \leq p-2$, we can solve the resulting equations for $\tilde{a}_i$ and $\tilde{b}$. In terms of the roots $e_1, \dots, e_{p-2}$ these automorphisms are given by the formulas:

$$\tilde{a}_i(e_j) = \frac{e_{[j-i]} - e_{[-i-1]}}{e_{[-i]} - e_{[-1-i]}} \qquad \tilde{b}(e_j) = \frac{e_{[(j+1)i-1]}}{e_{[k-1]}}$$

$$\tilde{a}_i(u) = (e_{[-i]} - e_{[-1-i]})^{\frac{1}{p-1}} u \quad \tilde{b}(u) = (e_{[k-1]})^{\frac{1}{p-1}} u$$

□

Remark 6.2. *The series $(1+x)^{\frac{1}{p-1}}$ exists in $\mathbb{Z}_p[[x]]$.*

Denote by a_i^F and b^F the expansions of a_i and b in terms of the local parameter z. Then the one dimensional summand F_{C_p} has the following property.

Corollary 6.3.

$$\tilde{a}_i^*(F_{C_p}) = a_i^F(F_{C_p}), \quad \tilde{b}^*(F_{C_p}) = b^F(F_{C_p})$$

Remark 6.4. *Let $\gamma : F_{C_p} \to G$ be an isomorphism of formal group laws, then*

$$\tilde{a}_i^*(G) = \tilde{a}_i^*(\gamma) \circ a_F \circ \gamma^{-1}(G), \quad \tilde{b}^*(G) = \tilde{b}^*(\gamma) \circ b_F \circ \gamma^{-1}(G)$$

.

For the purposes of computations with the above formulas let us state the following proposition.

Proposition 6.5.

$$e_j = j + 1 + a_1 u_1 + \ldots + a_{p-2} u_{p-2}$$

modulo degree 2, where $a_i = (j+1)^{p-i} - (j+1)$ modulo p.

7. On the properties of the one dimensional summand

The purpose of this section is to prove the theorem

Theorem 7.1. *Formal group law F_{C_p} is a universal Lubin-Tate lift of the formal group of height $p-1$ over $\mathbb{F}_p$.*

In this section $log(F)$ always denotes the logarithm of a formal group law $F(x,y)$.

Since our base ring is a $Z_{(p)}$-algebra, F_{C_p} is strictly isomorphic to a p-typical formal group law, which we denote by G_{C_p} again. We also denote by $G_{\bar{C}_p}$ and by $G^0_{C_p}$ the reductions of F_{C_p} modulo the ideals I and I_0 respectively.

Remark 7.2. *According to* [1], *(16.4.14), $log(G_{C_p})$ is obtained from $log(F_{C_p})$ by crossing out the terms $m_i z^i$ with $i \neq p^k$. This, together with 5.3, implies that*

$$log(G^0_{C_p}) = z + \frac{a}{p} z^{p^{p-1}}$$

modulo degree $p^{p-1} + 1$, $a \in \mathbb{Z}_p$, $a \neq 0$ mod p.

Proposition 7.3. *There is an automorphism α of $G_{\bar{C}_p}(x,y)$ of order p such that $\alpha(z) = z + z^p$ modulo degree $p+1$.*

Proof. $G_{\bar{C}_p}$ and $F_{\bar{C}_p}$ are equal modulo degree $p+1$, as it follows from 5.4. $F_{\bar{C}_p}$ has an automorphism of order p with the desired property. Take, for example, a_1^F from 6.1 and reduce it modulo I. This implies the statement of the proposition. ☐

The theorem 7.1 follows from the following proposition.

Proposition 7.4.

$$log(G_{C_p}) = z + \Sigma_{i=1}^{p-2} \frac{t_i}{p} u_i z^{p^i} + t z^{p^{p-1}} \tag{7.5}$$

$t_i \in \mathbb{Z}_p^\times$, modulo I_0^2.

Proof. According to the above remark the logarithm of G_{C_p} can be obtained in the following way: choosing a local parameter z as in 4.6 we obtain the following formula for the expansion of the differential $\frac{dx}{y}$ on the curve C_p:

$$\omega = \frac{(1-p)dz}{1 - (\Sigma_{i=1}^{p-2} i u_i z^{p-i} w^{i-1} + (p-1) b z w^{p-2})}$$

where w satisfies the equation

$$w = z^p + \Sigma_{i=1}^{p-2} u_i z^{p-i} w^i + bzw^{p-1}$$

Integrate it and cross out the terms $m_i z^i$ with i not equal to a power of p. This is the logarithm of G_{C_p}. We claim that 7.5 holds for some $t_i \in \mathbb{Q}_p$, modulo I_0^2. This follows from the following facts:
a. In the series $w(z)$ and $\frac{1}{\omega(z)}$, reduced modulo I_0, the powers of z are congruent to p and zero modulo $(p-1)^2$ respectively.
b. In the series $w(z)$ the coefficient of z^k is equal to u_i modulo degree two iff $k = p - i + pi$ or zero modulo $(p-1)^2$.
c. In the series $\omega(z)$ the coefficient of z^k is equal to u_i modulo degree two iff k is congruent to $pi - i$ or zero modulo $(p-1)^2$.
d. $p^{p-1} - 1 = 0 \bmod (p-1)^2$, $p^i - 1 = pi - p \bmod (p-1)^2$ Now we will prove that $t_i \in \mathbb{Z}_p^\times$. Examining the above formula for the expansion of the differential $\frac{dx}{y}$, we easily see that it is true for $i = 1$. Suppose we have proved the proposition for $j < i$. F_{C_p} is isomorphic to G_{C_p} by construction. 6.4 implies that there is a lift α' of α such that

$$\tilde{a}_1^*(G_{C_p}) = \alpha'(G_{C_p})$$

That implies that

$$\tilde{a}_1(\frac{t_i}{p} u_i) = \frac{t_i}{p} u_i + \frac{t_{i-1}}{p} u_{i-1} + n_i u_i + n_{i-1} u_{i-1} + n,$$

modulo I_0^2, and modulo $u_1, \ldots, u_{i-2}$, and $n_i, n_{i-1}, n \in \mathbb{Z}_p$. On the other hand, the formulas 6.1 tell that

$$\tilde{a}_1(u_i) = u_i + c_{i-1} u_{i-1}$$

$c_{i-1} \in \mathbb{Z}_p^\times$, modulo $p, u_1 \ldots, u_{i-2}$, and I_0^2. This implies that t_i must be a unit.

□

References

[1] M. Hazewinkel, Formal groups and applications, *Academic Press*, (1978).
[2] T. Hewett, Finite subgroups of the Morava stabilizer algebra, *Preprint.*
[3] T. Honda, On the formal structure of the Jacobian variety of the Fermat curve over a p-adic integer ring, *Symp. Math. INDAM* **11** (1973), 271-284.
[4] T. Honda, On the theory of commutative formal groups, *J. Math. Soc. Japan*, **22** (1970), 213-246.
[5] M. J. Hopkins, B. H. Gross, The rigid analytic period mapping, Lubin-Tate space, and stable homotopy theory, *Bull. Amer. Math. Soc.*, v 30, No **1**, (1994), 76-86.
[6] H. Miller, AMS Summer Research Institute, Seattle, 1996.
[7] J. Lubin, J. Tate, Formal moduli for one parameter formal Lie groups, *Bull. Soc. Math. France* **94** (1966), 49-60.
[8] Yu. I. Manin, The theory of commutative formal groups over fields of finite characteristic, *Russian Math. Surveys*, **18**, (1963), 1-81.
[9] J. H. Silverman, The Arithmetic of Elliptic Curves, *Springer Graduate Texts in Mathematics*, **106**, 1986.
[10] G. Shimura and Y. Taniyama, Complex multiplication of abelian varieties and its application to number theory, *Publ. Math. Soc. Japan*, **6**, 1960.
[11] W. C. Waterman, The height of formal A-modules, *Proc of AMS*, **46**, No 3, (1974), 332-333.

University of Kentucky, Lexington KY

Northwestern University, Evanston IL 60208