

TOWARD HIGHER CHROMATIC ANALOGS OF ELLIPTIC COHOMOLOGY II

DOUGLAS C. RAVENEL

(communicated by Name of Editor)

Abstract

Let p be a prime and f a positive integer, greater than 1 if $p = 2$. We construct liftings of the Artin-Schreier curve $C(p, f)$ in characteristic p defined by the equation $y^e = x - x^p$ (where $e = p^f - 1$) to a curve $\tilde{C}(p, f)$ over a certain polynomial ring R' in characteristic 0 which shares the following property with $C(p, f)$. Over a certain quotient of R' , the formal completion of the Jacobian $J(\tilde{C}(p, f))$ has a 1-dimensional formal summand of height $(p - 1)f$.

Along the way we show how Honda's theory of commutative formal group laws can be extended to more general rings and prove a conjecture of his about the Fermat curve.

Contents

1	Introduction	1
2	Some arithmetic results	14
3	Deformations of the Artin-Schreier curve	25

1. Introduction

This paper is a sequel to [Rav07]. The main result there was the following.

Theorem 1.1. Let p be a prime and f a positive integer, greater than one if $p = 2$. Let $C(p, f)$ be the Artin-Schreier curve over \mathbf{F}_p defined by the affine equation

$$y^e = x^p - x \quad \text{where } e = p^f - 1.$$

(Assume that $(p, f) \neq (2, 1)$.) Then its Jacobian $J(C(p, f))$ has a 1-dimensional formal summand of height $h = (p - 1)f$.

The author acknowledges support from NSF grants DMS-9802516 and DMS-0404651

Received Month Day, Year, revised Month Day, Year; published on Month Day, Year.

2000 Mathematics Subject Classification: Primary: 55N34; Secondary: 14H40, 14H50, 14L05, 55N22.

Key words and phrases: formal group law, elliptic cohomology, algebraic curve.

This article is available at <http://intlpress.com/HHA/v10/n1/a?>

Copyright © 2008, International Press. Permission to copy for private use granted.

In this paper we will work instead with the curve defined by

$$y^e = x - x^p$$

in order to simplify certain signs.

When the Jacobian of an algebraic curve over a ring R has a 1-dimensional formal summand as above, it defines a 1-dimensional formal group law over R , and hence by Quillen's theorem a homomorphism $\varphi : MU_* \rightarrow R$ (called a genus), where MU_* is the complex cobordism ring. One can then ask if the functor from spaces or spectra to R -modules defined by

$$X \mapsto MU_*(X) \otimes_{MU_*} R$$

(using the MU_* -module structure on R defined by φ) is a generalized homology theory. This boils down to asking if the functor has suitable exactness properties. The Landweber Exact Functor theorem spells out explicit algebraic conditions on φ which which characterize this exactness. Landweber's conditions are *not* satisfied in the example above, and it would be desirable to have a curve for which they are. Here is such an example.

Conjecture 1.2. Let $L(p, f)$ be the curve over over $L = \mathbf{Z}_p[u_1, \dots, u_{h-1}]$ defined by

$$y^e = x - x^p + \sum_{i=0}^{h-2} u_{i+1} x^{p-1-[i/f]} y^{p^{f-1}-p^{i-[i/f]f}}.$$

Then its Jacobian has a formal 1-dimensional subgroup isomorphic to the Lubin-Tate lifting of the formal group law above, and the resulting genus is Landweber exact.

We can think $L(p, f)$ as a family of curves over \mathbf{Z}_p parametrized by the affine scheme $\text{Spec}(L)$ in which the curve at the origin is an integral lifting of the Artin-Schreier curve. The methods of the present paper only allow us to make the necessary calculations over the ring $L/(u_1 \cdots u_{h-1})^2$. This means we only get the formal splitting over an infinitesimal neighborhood of the origin.

In this paper we will also study the *deformed Artin-Schreier curve* $\tilde{C}(p, f)$ defined by the equation

$$y^e = x - x^p + \sum_{s=1}^p \epsilon_s x^{p-s} \quad \text{where } \epsilon_s = \sum_{0 \leq t < se/pq} a_{se-pqt} y^{qt} \quad (1.3)$$

with $q = p - 1$. It is defined over the ring

$$R = \mathbf{Z}_p[a_\nu : \nu \in N]$$

where

$$N = \{se - pqt : 1 \leq s \leq p, 0 \leq t < se/pq\}. \quad (1.4)$$

Note that the ring L of 1.2 is a quotient of this R . We will see below that the Jacobian of this curve over R does *not* have a suitable 1-dimensional formal summand. In order

to get such a splitting it is necessary to pass to a quotient of R by making some of the a_ν decomposable. The resulting ring is

$$R' = \mathbf{Z}_p[a_\nu : \nu \in N'] \quad (1.5)$$

with

$$\begin{aligned} N' = & \{se + p^i - 1 : 0 \leq s \leq p-1, 1 \leq i \leq f\} \\ & \cup \begin{cases} \{se - pqt : 2 \leq s \leq p, t_0 \leq t < se/pq\} & \text{for } p > 2 \\ \{2t : 1 \leq t < 2^{f-1} - 1\} & \text{for } p = 2 \end{cases} \\ & \text{where } t_0 = (p^{f-1} + 1)/q. \end{aligned} \quad (1.6)$$

We wish to thank the referee for finding some gaps in an earlier version of this paper which motivated us to make some improvements, namely spelling out the generality of Honda's formal group law theory and to proving Lemma 1.19. This in turn led us to Theorem 1.22, in which we prove a conjecture of Honda about the Fermat curve.

Some results from Honda's theory of commutative formal group laws

We will restate some of the results in [Hon70].

Hypothesis 1.7. R is an algebra over \mathbf{Z}_p or $\mathbf{Z}_{(p)}$ (for a fixed prime p) that is free as a module over its ground ring. Let

$$K = R \otimes \mathbf{Q} = p^{-1}R \quad \text{and} \quad k = R/(\pi)$$

where π generates a maximal principal ideal containing p . Moreover R has an endomorphism σ (denoted by $a \mapsto a^\sigma$) inducing the p^j th power map in k for some $j > 0$, which extends to K by linearity.

Honda indicates (on page 220) that R (which he denotes by \mathfrak{o}) is the ring of integers in a discrete valuation field K , but *his proofs of the results we are quoting do not make use of any properties of R other than those stated above.*

We need more generality than he states, for example the case where R is a finitely generated polynomial algebra over \mathbf{Z}_p . In our case K and k need not be fields or even integral domains. We are claiming that he has proved his theorems in more generality than he indicates. This is admittedly an awkward assertion since the only way the skeptical reader can verify it is to read Honda's paper carefully. However there is no point in repeating all of Honda's proofs verbatim here.

Let $K_\sigma[[T]]$ and $R_\sigma[[T]]$ denote noncommutative power series rings in a variable T over K and R subject to the rule $T\alpha = \alpha^\sigma T$ for α in K or R . Let $\mathfrak{B}_{m,n}$ and $\mathfrak{A}_{m,n}$ denote the modules of $m \times n$ matrices over $K_\sigma[[T]]$ and $R_\sigma[[T]]$, with $\mathfrak{B}_n = \mathfrak{B}_{n,n}$ and $\mathfrak{A}_n = \mathfrak{A}_{n,n}$, the rings of $n \times n$ matrices over $K_\sigma[[T]]$ and $R_\sigma[[T]]$. We will denote the $n \times n$ identity matrix by I_n .

$K[[x]]_0^n$ and $R[[x]]_0^n$ will denote the set of n -dimensional column vectors of power series (in a set of variables x) over K and R with trivial constant terms. We omit the superscript when $n = 1$.

For a multi-index $I = (i_1, \dots, i_g)$ of nonnegative integers, let $pI = (pi_1, \dots, pi_g)$, $|I| = i_1 + \dots + i_g$ and $x^I = x_1^{i_1} \cdots x_g^{i_g}$. Thus an element $f(x) \in K[[x]]_0$ has the form

$$f(x) = \sum_{|I|>0} f_I x^I \quad \text{with } f_I \in K,$$

and we define

$$T * f = \sum_{|I|>0} f_I^\sigma x^{p^j I}. \quad (1.8)$$

In this way $K[[x]]_0$ and $R[[x]]_0$ become modules over $K_\sigma[[T]]$ and $R_\sigma[[T]]$. In a similar way, $\mathfrak{B}_{m,n}$ and $\mathfrak{A}_{m,n}$ act by left multiplication on $K[[x]]_0^n$ and $R[[x]]_0^n$.

Definition 1.9. Two power series $f, g \in K[[x]]$ (in any number of variables) over K are **congruent** ($f \equiv g$) if their coefficients differ by elements in R , i.e., if $f - g \in R[[x]]$.

Definition 1.10. An element $H \in \mathfrak{B}_n$ is a **Honda matrix** if $H \equiv I_n$ modulo T and $\pi H \in \mathfrak{A}_n$. Given an invertible matrix $P \in M_n(R)$, an element $f \in K[[x]]_0^n$ is of **type** $(P; H)$ if $f(x) \equiv Px$ modulo $(x)^2$ and $H * f$ as defined in (1.8) is congruent (as defined above) to 0. When $P = I_n$, we say f has **type** H .

Honda [**Hon70**, page 221] calls πH (which he typically denotes by u) a *special element* in \mathfrak{A}_n . He proves the following results without using his stronger hypotheses on K and R .

Theorem 1.11. [**Hon70**, Theorem 2] Assume K and R satisfy 1.7. Let P be an invertible matrix in $M_n(R)$ and let $H \in \mathfrak{B}_n$ be a Honda matrix. If $f \in K[[x]]_0^n$ is of type $(P; H)$, then

$$F(x, y) = f^{-1}(f(x) + f(y))$$

is a formal group law over R . If $Q \in M_n(R)$ is another invertible matrix and $g \in K[[x]]_0^n$ is of type $(Q; H)$, then the formal group law $G(x, y) = g^{-1}(g(x) + g(y))$ is isomorphic to F . If $P = Q$, then F and G are strictly isomorphic.

Here is a simple example where $n = 1$, $P = Q = I_1$, $R = \mathbf{Z}_{(p)}$ and the component of the 1×1 matrix H is $1 - T/p$. Then let

$$f(x) = \sum_{i>0} \frac{x^i}{i} \quad \text{and} \quad g(x) = \sum_{j \geq 0} \frac{x^{p^j}}{p^j}.$$

F is the multiplicative formal group law, and G is its p -typical isomorph. Then we have

$$\left(1 - \frac{T}{p}\right) * f = \sum_{i>0} \frac{x^i}{i} - \sum_{i>0} \frac{x^{pi}}{pi} = \sum_{\substack{i>0 \\ p \nmid i}} \frac{x^i}{i} \in \mathbf{Z}_{(p)}[[x]]$$

while

$$\left(1 - \frac{T}{p}\right) * g = \sum_{j \geq 0} \frac{x^{p^j}}{p^j} - \sum_{j \geq 0} \frac{x^{p^{j+1}}}{p^{j+1}} = x \in \mathbf{Z}_{(p)}[[x]],$$

so f and g both have type H and are thus strictly isomorphic over $\mathbf{Z}_{(p)}$.

Theorem 1.12. [**Hon70**, Theorem 3] Assume K and R satisfy 1.7. Let $H_1 \in \mathfrak{A}_n$ and $H_2 \in \mathfrak{A}_m$ be Honda matrices. Let $f \in K[[x]]_0^n$ and $g \in K[[x]]_0^m$ have types H_1 and H_2 respectively. Let $F(x, y) = f^{-1}(f(x) + f(y))$ and $G(x, y) = g^{-1}(g(x) + g(y))$. Then $g^{-1} \circ (Cf)$ for $C \in M_{m,n}(R)$ is an element of $\text{Hom}_R(F, G)$ iff there exists $M \in \mathfrak{A}_{m,n}$ with $H_2C = MH_1$.

Moreover, $\text{Hom}_R(F, G)$ is canonically isomorphic to $M_{m,n}(R) \cap H_2^{-1}\mathfrak{A}_{m,n}H_1$.

In [**Hon70**, Prop. 1.6] Honda shows that $\text{Hom}_K(F, G)$ is isomorphic to $M_{m,n}(K)$.

Theorems 1.11 and 1.12 are in [**Hon70**, §2]. The next two results are from his §3 where an additional hypothesis is needed.

Hypothesis 1.13. Let K, R and σ be as in 1.7 with $j = 1$ and $\pi = p$.

Hence we are now assuming that the prime p is unramified in R , so a Honda matrix has the form

$$H = I_n + \sum_{\nu > 0} \frac{A_\nu T^\nu}{p} \quad \text{with } A_\nu \in M_n(R).$$

Theorem 1.14. [**Hon70**, Prop. 3.3] Let F be an n -dimensional formal group law over R (satisfying 1.13) with logarithm f . Then there is a Honda matrix H such that f is of type H .

Definition 1.15. Two Honda matrices $H_1, H_2 \in \mathfrak{B}_n$ are **left associate** if there is a matrix $U \in \mathfrak{A}_n$ with $H_2 = UH_1$.

Note that the matrix U above is invertible since it is congruent to I_n modulo T .

It is often possible to simplify a Honda matrix by p -adic completion. For example when $R = \mathbf{Z}_{(p)}$, a Honda matrix of the form

$$H = I_n + \sum_{\nu > 0} \frac{A_\nu T^\nu}{p} \quad \text{with } A_1 \text{ invertible and } A_\nu \in M_n(R)$$

is left associate to one of the form

$$H_\mu = I_n + \frac{A_1^{(\mu)} T}{p} + p^{\mu-1} \sum_{\nu \geq 2} A_\nu^{(\mu)} T^\nu \quad \text{with } A_\nu^{(\mu)} \in M_n(R)$$

for each integer $\mu > 0$, with the sequence $\{A_1^{(\mu)}\}$ converging p -adically as μ increases. Hence H is left associate over \mathbf{Z}_p to a Honda matrix of the form

$$H' = 1 + \frac{A_1' T}{p}.$$

In this paper we will study certain formal group laws defined over a $\mathbf{Z}_{(p)}$ -algebra R and then construct Honda matrices for them defined over $R \otimes \mathbf{Z}_p$.

Theorem 1.16. [**Hon70**, Theorem 4] For R as in 1.13, every n -dimensional formal group law over R is obtained from a Honda matrix by the method of Theorem 1.11. The strict isomorphism classes of such formal group laws correspond bijectively to the left associate classes of Honda matrices in \mathfrak{B}_n .

Let $M \subset R$ be a complete set of representatives of the elements of k . Then the strict isomorphism classes of such formal group laws correspond bijectively to the set of Honda matrices H such that the coefficients of T^ν for $\nu > 0$ in ρH lie in M .

With this in mind we make the following definition.

Definition 1.17. Let K , R and σ be as in 1.13, and let $f \in K[[x]]_0^n$ be a vector of n power series over K in some number of variables. Then f is a **Honda vector of type H** if there is a Honda matrix H with $H * f \equiv 0$ and any two Honda matrices with this property are left associate.

Hence Theorem 1.16 says that the logarithm of a formal group law over R is a Honda vector.

Honda's method for studying the formal completion of a Jacobian

Let J be an abelian variety of dimension g over a torsion free ring R . Let $\{y_1, \dots, y_g\}$ be a coordinate system centered at the identity. Then the holomorphic (or equivalently, invariant) 1-forms of J form a free R -module of rank g and they have power series expansions in the y_i about the origin. This module has a unique basis of the form $\{\omega_1, \dots, \omega_g\}$ so that

$$\omega_i = \sum_{j=1}^g \varphi_{i,j}(y_1, \dots, y_g) dy_j \equiv dy_i \pmod{(y_1, \dots, y_g)} \quad (1.18)$$

These differential forms are known to be exact, so there are power series $f_i(y_1, \dots, y_g)$ over $K = R \otimes \mathbf{Q}$ with

$$f_i \equiv y_i \pmod{(y_1, \dots, y_g)^2} \quad \text{and} \quad \omega_i = df_i.$$

These g power series in g variables constitute the logarithm of the g -dimensional formal group law F associated with J . More precisely,

$$F(x, y) = f^{-1}(f(x) + f(y))$$

where x and y denote the sets of g variables (x_1, \dots, x_g) and (y_1, \dots, y_g) , and $f = {}^t(f_1, \dots, f_g)$ is a vector of g power series in g variables. It is invertible since its Jacobian (in the sense of multivariable calculus) at the origin is the identity matrix. Hence if R satisfies 1.13, Theorem 1.16 says that f is a Honda vector (1.17).

Now suppose that J is the Jacobian (in the sense of algebraic geometry) $J(C)$ of a curve C over R of genus g . Then there is a canonical map $\Lambda : C \rightarrow J$ inducing an isomorphism between the R -module (which is free of rank g) of holomorphic 1-forms (also called differentials of the first kind) on $J(C)$ with those on C ; see [Mil86]. If $\{\eta_1, \dots, \eta_g\}$ is a basis of the latter, we can choose a basis $\{\omega_1, \dots, \omega_g\}$ of the former so that $\omega_i \circ \Lambda = \eta_i$ for each i . The η_i are also known to be exact and at any point on the curve they have power series expansions in terms of a local parameter x . Let $\psi_i = \int_0^x \omega_i$, so $\Psi = {}^t(\psi_1, \psi_2, \dots) \in K[[x]]_0^g$.

It turns out that Ψ is a Honda vector with the same type as f , but contrary to what we claimed in [Rav07], *Honda did not prove this in full generality in [Hon73]*. In Theorem 1 of that paper (which we will restate and reprove below as Theorem

1.23) he showed that if Ψ is a Honda vector, then it has the same type as f . In Lemma 1 (which we will generalize below in Lemma 1.19) he showed that Ψ is a Honda vector under certain hypotheses (spelled out below) which are too restrictive for our purposes.

He was interested in the Fermat curve defined by the affine equation $x^N + y^N = 1$ for $N > 2$. He determined the vector Ψ in that case and observed that it satisfied the hypotheses of his Lemma 1 for almost all primes. He conjectured but did not prove that it is a Honda vector at all primes not dividing N , the primes at which the curve has good reduction. Modulo this conjecture, he determined the formal structure of the curve's Jacobian for all such primes. We will verify his conjecture below in Theorem 1.22.

Here is our generalization of [**Hon73**, Lemma 1].

Lemma 1.19. For K, R and σ as in 1.13, let $f \in K[[x]]_0^n$ (for a single variable x) with

$$f_i(x) = \sum_{\alpha \geq \alpha_i} a_\alpha^{(i)} x^\alpha \quad \text{for } 1 \leq i \leq n.$$

Assume that there is a Honda matrix H with $H * f \in R[[x]]_0^n$ and that the following conditions are satisfied.

- (a) For each i , $\alpha_i a_{\alpha_i}^{(i)}$ is a unit in R .
- (b) $0 < \alpha_1 < \cdots < \alpha_n$.
- (c) $\alpha a_\alpha^{(i)} \in R$ for $1 \leq i \leq n$ and $\alpha > 0$.
- (d) If α_i is divisible by p , then there is an $i' < i$ with $p\alpha_{i'} = \alpha_i$.

Then f is a Honda vector.

Note that (c) is satisfied whenever the derivative of f has coefficients in R .

Honda's hypotheses were the following.

- (a) For each i , $a_{\alpha_i}^{(i)}$ is a unit in R .
- (b) $0 < \alpha_1 < \cdots < \alpha_n < q\alpha_1$, where q is the power of p used in the definition of σ .
- (c) $a_\alpha^{(i)} \in R$ for $1 \leq i \leq n$ and $\alpha \leq \alpha_n$.

Note that when K is a number field, any vector of the form shown in 1.19 satisfies Honda's hypotheses for all but a finite number of primes.

Proof. We can assume without loss of generality that f satisfies a fifth condition, namely

- (e) The coefficient $a_{\alpha_j}^{(i)}$ vanishes for $i \neq j$, and $a_{\alpha_i}^{(i)} = 1/\alpha_i$.

A vector f satisfying (a)-(c) can be converted to one satisfying (e) by left multiplication by an invertible upper triangular matrix $P \in M_n(R)$. Then PHP^{-1} is a Honda matrix satisfying $PHP^{-1} * Pf = PH * f \equiv 0$.

We are trying to show that any two Honda matrices sending f to $R[[x]]_0^n$ are left associate. It suffices to show this is true if we replace f by its image induced by the

K -linear projection of $K[[x]]_0^n$ onto the free K -module on the set

$$\{x^{\alpha_i} : 1 \leq i \leq n\}.$$

In other words we can replace f by the vector ${}^t(x^{\alpha_1}/\alpha_1, \dots, x^{\alpha_n}/\alpha_n)$, which depends only on the leading exponent set

$$E = \{\alpha_1, \dots, \alpha_n\}.$$

(This does not mean that the Honda matrices are determined by E . For example when $E = \{1\}$, f we could be the logarithm of any 1-dimensional formal group law.)

Let

$$H_1 = I_n + \sum_{\nu > 0} C_\nu T^\nu / p \quad \text{and} \quad H_2 = I_n + \sum_{\nu > 0} D_\nu T^\nu / p$$

with $H_1 * f, H_2 * f \equiv 0$ and $C_\nu, D_\nu \in M_n(R)$.

We claim

$$C_\nu = D_\nu \text{ for } 0 < \nu < \mu \quad \text{implies} \quad C_\mu \equiv D_\mu \pmod{p}. \quad (1.20)$$

Let

$$H_1 - H_2 = \sum_{\nu \geq \mu} B_\nu T^\nu / p \quad \text{with } B_\nu = C_\nu - D_\nu \in M_n(R).$$

We will denote the entries of B_ν by $b_{i,j}^{(\nu)}$.

We will illustrate what happens next in the case $E = \{1, p\}$. There we have

$$\begin{aligned} & (H_1 - H_2) * f / p \\ &= (B_\mu T^\mu + B_{\mu+1} T^{\mu+1} + \dots) * f / p \\ &= (B_\mu + B_{\mu+1} T + \dots) * \begin{bmatrix} x^{p^\mu} / p \\ x^{p^{\mu+1}} / p^2 \end{bmatrix} \\ &= \begin{bmatrix} b_{1,1}^{(\mu)} x^{p^\mu} / p + (b_{1,2}^{(\mu)} + p b_{1,1}^{(\mu+1)}) x^{p^{\mu+1}} / p^2 \\ b_{2,1}^{(\mu)} x^{p^\mu} / p + (b_{2,2}^{(\mu)} + p b_{2,1}^{(\mu+1)}) x^{p^{\mu+1}} / p^2 \end{bmatrix}. \end{aligned}$$

Here we are only considering terms with exponents lying in $p^\mu E = \{p^\mu, p^{\mu+1}\}$. The integrality of this, i.e., the fact that it lies in $R[[x]]_0^2$, implies that $B_\mu \equiv 0 \pmod{p}$ as desired.

More generally, let $g = (H_1 - H_2) * f$ and only consider the monomials with exponents lying in $p^\mu E$. Then we have

$$g_i = \sum_{j=1}^n \frac{g_{i,j} x^{p^\mu \alpha_j}}{p \alpha_j} \quad \text{with } g_{i,j} \in R, \quad (1.21)$$

and we will show that $g_{i,j} \equiv b_{i,j}^{(\mu)} \pmod{p}$, so the integrality of g implies that $C_\mu \equiv D_\mu \pmod{p}$. In order to do this it is convenient to use α_i as an index rather than i . Thus

we replace (1.21) by

$$\tilde{g}_s = \sum_{t \in E} \frac{\tilde{g}_{s,t} x^{p^\mu t}}{pt} \quad \text{for } s \in E$$

where $\tilde{g}_{\alpha_i, \alpha_j} = g_{i,j}$. We define $\tilde{b}_{s,t}^{(\nu)}$ similarly. Then for $s \in E$ we have

$$\begin{aligned} \tilde{g}_s &= \sum_{\substack{t \in E \\ \nu \geq 0}} \tilde{b}_{s,t}^{(\mu+\nu)} \frac{x^{p^{\mu+\nu} t}}{pt} \\ &= \sum_{\substack{t'/p^\nu \in E \\ \nu \geq 0}} \tilde{b}_{s,t'/p^\nu}^{(\mu+\nu)} \frac{p^\nu x^{p^\mu t'}}{pt'} \quad \text{where } t' = p^\nu t \\ \text{so } \tilde{g}_{s,t} &= \sum_{t/p^\nu \in E} p^\nu \tilde{b}_{s,t/p^\nu}^{(\mu+\nu)} \equiv \tilde{b}_{s,t}^{(\mu)} \pmod{p}. \end{aligned}$$

Note that if $t \in E$ and t/p^ν is an integer, then t/p^ν is also in E by our hypothesis (d). This gives the desired congruence for $g_{i,j}$, thereby proving (1.20).

Now we will use Honda's method to show that if H_1 and H_3 are Honda matrices with $H_1 * f, H_3 * f \equiv 0$, then they are left associate. We will construct a sequence of Honda matrices $\{H_3^{(\mu)}\}$ left associate with H_3 converging to H_1 by induction on μ . We start the induction with $H_3^{(0)} = H_3$. Suppose we have a Honda matrix $H_3^{(\mu-1)}$ that is left associate with H_3 and congruent to H_1 modulo T^μ . We will use (1.20) with $H_2 = H_3^{(\mu-1)}$. It says that $C_\mu \equiv D_\mu \pmod{p}$, so we can define

$$\begin{aligned} H_3^{(\mu)} &= (I_n + (C_\mu - D_\mu)T^\mu/p) H_3^{(\mu-1)} \\ &= (I_n + (C_\mu - D_\mu)T^\mu/p) \\ &\quad (I_n + C_1T/p + \cdots + C_{\mu-1}T^{\mu-1}/p + D_\mu T^\mu/p + \cdots) \\ &= I_n + C_1T/p + \cdots + C_\mu T^{\mu-1}/p + \cdots \end{aligned}$$

$H_3^{(\mu)}$ is left associate with $H_3^{(\mu-1)}$ and hence with H_3 since $I_n + (C_\mu - D_\mu)T^\mu/p \in \mathfrak{A}_n$. This completes the inductive step. \square

Now we will apply this lemma to the Fermat curve of degree N studied by Honda in [Hon73] and prove the conjecture stated there after Theorem 3.

Theorem 1.22. Let C be the affine plane curve over $\mathbf{Z}_{(p)}$ defined by the equation $x^N + y^N = 1$ where $N > 2$ is not divisible by p . Using x as a local parameter at the point $(0, 1)$, the power series expansions for the integrals of the first kind form a Honda vector.

Honda noted that for a given N , the power series expansions form a Honda vector for all sufficiently large primes, and conjectured that they do so for all primes not dividing N .

Proof. As explained in [Hon73, §3], the space of differentials of the first kind is spanned by

$$\eta(i, j) = x^{i-1}y^{-j}dx = x^{i-1}(1-x^N)^{-j/N}dx$$

for $0 < i < j < N$. In order to get differentials with distinct leading exponents, we need a change of basis. Let

$$z = y^{-1} - 1 = (1-x^N)^{-1/N} - 1 = \frac{x^N}{N} + \dots$$

and replace $\eta(i, j)$ by

$$\begin{aligned} \eta_{i,j} &= x^{i-1}(1-x^N)^{-(i+1)/N}z^{j-i-1}dx \\ &= \left(\frac{x^{i-1+(j-i-1)N}}{N^{j-i-1}} + \dots \right) dx \end{aligned}$$

Integrating these gives a collection of power series with leading exponent set

$$\begin{aligned} E &= \{i + N(j - i - 1) : 0 < i < j < N\} \\ &= \{i + Ns : 1 \leq i \leq N - 2, 0 \leq s \leq N - i - 2\}. \end{aligned}$$

We claim this satisfies the hypotheses of Lemma 1.19.

The only hard part of this is verifying (d). Let $i = pi_1 + i_0$, $s = ps_1 + s_0$ and $N = pN_1 + N_0$ with $0 \leq i_0, s_0, N_0 < p$. Our assumption that p does not divide N means that $N_0 > 0$, but we do not need that condition to verify (d). Now suppose $pr \in E$ for a positive integer r with

$$\begin{aligned} pr &= i + sN \quad \text{with } i > 0 \text{ and } i + s \leq N - 2 \\ &= pi_1 + i_0 + (ps_1 + s_0)(pN_1 + N_0) \\ &= p(s_1N + s_0N_1 + i_1) + i_0 + s_0N_0. \end{aligned}$$

This means $i_0 + s_0N_0$ is divisible by p , so let $t = (i_0 + s_0N_0)/p$, which satisfies $0 \leq t < p$ since

$$i_0 + s_0N_0 \leq p - 1 + (p - 1)^2 = p^2 - p.$$

We want to show that $r \in E$. We have

$$r = s_1N + s_0N_1 + i_1 + t = s_1N + i'.$$

To show that $r \in E$, it suffices to verify that $i' > 0$ and $i' + s_1 \leq N - 2$. For the lower bound on i' we have

$$pi' = ps_0N_1 + pi_1 + i_0 + s_0N_0 = s_0N + i > 0$$

since $i > 0$. For the upper bound on $s_1 + i'$ we have

$$\begin{aligned} ps_1 + pi' &= ps_1 + s_0N + i \\ &= s + s_0(N - 1) + i \\ &\leq s_0(N - 1) + N - 2 \quad \text{since } i + s \leq N - 2 \\ &\leq pN - p - 1 < p(N - 1) \quad \text{since } s_0 \leq p - 1, \end{aligned}$$

so $s_1 + i' \leq N - 2$ and $r \in E$. □

Now here is Honda's result [**Hon73**, Theorem 1] linking integrals of the first kind on an algebraic curve to the formal completion of its Jacobian.

Theorem 1.23. For K, R and σ as in 1.13, let C be an algebraic curve of genus g over R and let $\Psi \in K[[x]]_0^g$ be a vector of power series expansions of its integrals of the first kind in terms of a local parameter x at a point $P \in C$. Then if Ψ is a Honda vector of type H , then the same is true of the logarithm of the formal completion $\widehat{J}(C)$ of the Jacobian $J(C)$.

Proof. Following Honda, we use the canonical map $\Lambda : C \rightarrow J(C)$ sending P to the identity element of $J(C)$. Let $\eta_i = d\psi_i$. Let $y = (y_1, \dots, y_g)$ be a system of local parameters at the origin of $J(C)$ and let ω_i be invariant differentials on $J(C)$ such that $\eta_i = \omega_i \circ \Lambda$. Then we have

$$\omega_i = \sum_{j=1}^g \varphi_{i,j}(y_1, \dots, y_g) dy_j$$

with $\varphi_{i,j} \in K[[y_1, \dots, y_g]]$. These differentials are known to be exact, so there power series $\Phi_i(y) \in K[[y_1, \dots, y_g]]$ with $\omega_i = d\Phi_i$ and $\Phi_i(0) = 0$. Since the $y_j \circ \Lambda$ are functions in $R(C)$, there is a g -tuple $\xi = {}^t(\xi_1, \dots, \xi_g)$ of algebraic functions in $R[[x]]$ such that $y \circ \Lambda = \xi \circ x$. Then $\omega = d\Phi(y)$ implies $\eta = d(\Phi(\xi(y)))$, so $\Phi \circ \xi = \Psi$.

Let $A \in M_g(R)$ be the invertible matrix such that

$$\Phi(y) \equiv Ay \quad \text{mod } (y_1, \dots, y_g)^2$$

replacing the local parameters y by Ay , we may assume that $A = I_g$, so $\Phi(y)$ is the logarithm of $\widehat{J}(C)$. Hence there is Honda matrix $H \in \mathfrak{B}_g$ with $H * \Phi \in R[[y]]_0^g$. Then $H * \Psi = H * (\Phi \circ \xi)$ and it follows from [**Hon70**, Lemma 2.3] that

$$H * (\Phi \circ \xi) \equiv (H * \Phi) \circ \xi.$$

so $H * \Psi \equiv 0$. Conversely if there is another Honda matrix H' with $H' * \Psi \equiv 0$, then $H' = UH$ for some $U \in \mathfrak{A}_g$ since Ψ is a Honda vector. This means that Φ and Ψ are Honda vectors of the same type. \square

A concrete example: $(p, f) = (3, 2)$

We will illustrate this calculation in more detail for the lifting of the curve $C(3, 2)$ to \mathbf{Z}_3 defined by the affine equation

$$y^8 = x - x^3.$$

It has genus 7 and we are looking for a 1-dimensional formal summand of height 4 in its Jacobian. The vector Ψ is

$$\Psi = (\psi_1, \psi_2, \psi_3, \psi_4, \psi_5, \psi_9, \psi_{10});$$

where

$$\psi_r = \sum_{i \geq 0} \binom{3i + [(r+1)/8]}{i} \frac{y^{16i+r}}{16i+r}$$

and $E = \{1, 2, 3, 4, 5, 9, 10\}$.

The form of ψ_r implies that $T^n \psi_r$ is congruent (modulo power series with p -local integer coefficients) to a multiple of $\psi_{r'}$ only if

$$r \equiv 3^n r' \pmod{16},$$

i.e., only if the indices r and r' , regarded as elements in $\mathbf{Z}/(16)$, lie in the same orbit under iterated multiplication by 3. Thus if we denote the entries of the Honda matrix by $h_{s,t}$ with $s, t \in E$, it follows that $h_{s,t}$ is nonzero only if s and t lie in the same orbit. The relevant orbits are

$$\{1, 3, 9, 11\}, \{2, 6\}, \{4, 12\}, \{5, 15, 13, 7\}, \text{ and } \{10, 14\}.$$

The intersection of E with the first of these has three elements, while each of the others intersects E in a singleton. This means that H has a block decomposition into four 1-dimensional summands and one 3-dimensional summand. It turns out that the height of each summand is equal to the cardinality of the corresponding orbit.

In particular

$$\psi_5 = \sum_{i \geq 0} \binom{3i}{i} \frac{y^{16i+5}}{16i+5}$$

is an eigenseries corresponding to the desired 1-dimensional formal summand of height 4. A binomial coefficient exercise reveals that the i th coefficient of this power series is a 3-local integer unless $16i+5$ is divisible by 3^4 , i.e., unless i has the form $81j+25$, so modulo p -local integer terms we have

$$\begin{aligned} \psi_5 &\equiv \sum_{j \geq 0} \binom{3(81j+25)}{81j+25} \frac{y^{16(81j+25)+5}}{16(81j+25)+5} \\ &\equiv \sum_{i \geq 0} \binom{243i+75}{81i+25} \frac{y^{3^4(16i+5)}}{3^4(16i+5)}, \end{aligned}$$

$$\text{and } \frac{T^4}{3} * \psi_5 \equiv \sum_{i \geq 0} \binom{3i}{i} \frac{y^{3^4(16i+5)}}{3(16i+5)}.$$

Thus if there is a 3-adic unit u such that

$$\left(1 - \frac{uT^4}{3}\right) * \psi_5 \equiv 0,$$

it must be such that

$$\binom{3^5 i + 75}{3^4 i + 25} \frac{1}{3^4(16i+5)} - u \binom{3i}{i} \frac{1}{3(16i+5)} \in \mathbf{Z}_3 \quad (1.24)$$

for every nonnegative integer i . This suggests setting

$$u = \lim_{t \rightarrow -5/16} \frac{\binom{3^5 t + 75}{3^4 t + 25}}{3^3 \binom{3t}{t}},$$

where the limit is taken 3-adically, assuming that the indicated function of t is 3-adically continuous and unit valued. In Theorem 2.7 below we will show that the

function has these properties, the limit can be expressed in terms of the 3-adic Gamma function (first defined by Morita [Mor75]), and that the resulting value of u satisfies the congruences required by (1.24).

In the general case there is always an orbit of cardinality h whose intersection with E is a singleton, namely the orbit of $\ell = p^f - p^{f-1} - 1$, which we will denote by L . This was proved in [Rav07, Lemma 3.13]. The corresponding series is

$$\psi_\ell = \sum_{i \geq 0} \binom{p^i}{i} \frac{y^{mi+\ell}}{mi+\ell}.$$

In Theorem 2.10 we will show there is a p -adic unit u (denoted there by $\tau(h)$) such that

$$\left(1 - \frac{uT^h}{p}\right) * \psi_\ell \equiv 0.$$

It follows that the corresponding 1-dimensional formal summand is isomorphic to one whose logarithm is

$$\sum_{n \geq 0} \frac{u^n x^{p^{hn}}}{p^n};$$

this has height h as claimed.

Deformations of the Artin-Schreier curve

Let

$$\varepsilon = \sum_{0 \leq s < p} \varepsilon_s \tilde{x}^s, \quad \text{where} \quad \varepsilon_s = \sum_{0 \leq t < (p-s)e/pq} a_{pe-se-pqt} y^{qt}.$$

Let $\tilde{F}(\tilde{x}, y) = u^m \tilde{x} - \tilde{x}^p + \varepsilon - y^e$ and consider the curve defined by the equation

$$\tilde{F}(\tilde{x}, y) = 0. \tag{1.25}$$

We will refer to it as the *deformed Artin-Schreier curve*. This curve is defined over the ring

$$R = \mathbf{Z}_p[[a_\nu : \nu \in N]][u, u^{-1}]$$

where N is as in (1.4). For reasons that will be explained below, we will also want to consider the quotient ring R' of (1.5). The cardinality (for any prime) of N' (the indexing set of polynomial generators of R' given in (1.6)) is

$$\#N' = \binom{p}{2} \binom{p^{f-1} - 1}{p-1} + pf = \frac{p^f + p(2f-1)}{2}.$$

For topological purposes we define a grading on the rings $R[\tilde{x}, y]$ and $R[x, y]$ by

$$|u| = 2, |\tilde{x}| = |x| = 2e, |y| = 2p, \text{ and } |a_\nu| = 2\nu$$

so

$$|\varepsilon_s| = 2(p-s)e, |\varepsilon| = 2e \text{ and } |\tilde{F}(\tilde{x}, y)| = 2e.$$

The Honda operator T multiplies this grading by p , sending u and a_ν to their p th powers.

Let \overline{R} and \overline{R}' denoted the ungraded quotients of R and R' obtained by setting u equal to 1. From now on all calculations will be understood to be in $\overline{R}/(a_\nu)^2$ or $\overline{R}'/(a_\nu)^2$. This means that $T(a_\nu) = 0$, where T is Honda's p th power operator.

We will show that over the quotient ring $\overline{R}'/(a_\nu)^2$ the Jacobian of our curve has a 1-dimensional formal summand, and the resulting formal group law can be canonically lifted to R' itself. The Honda eigenseries for this splitting is θ' defined below in Theorem 3.8.

In §2 we will collect some arithmetic lemmas that we need to prove our theorems.

In §3 we will use our arithmetic results to analyze the holomorphic 1-forms on the deformed Artin-Schreier curve.

2. Some arithmetic results

Some power series formulas

Lemma 2.1. The power series solution to $x - x^p = z$ (where $p > 1$ need not be a prime) which vanishes when $z = 0$ satisfies

$$x^j = z^j \sum_{i \geq 0} c_{i,j} z^{iq},$$

where $q = p - 1$ and

$$c_{i,j} = \frac{j}{pi + j} \binom{pi + j}{i}$$

(and $c_{0,0}=1$), which is always an integer.

We will prove this below.

More generally we define integers $c_{i,j,k}$ for $k \geq 0$ by

$$\left(\frac{d}{dz}\right)^k x^{j+k} = (j+k)z^j \sum_{i \geq 0} c_{i,j,k} z^{qi}.$$

In particular we have

$$c_{i,j,0} = c_{i,j},$$

$$c_{i,j,1} = \binom{pi + j}{i},$$

$$\text{and } c_{i,j,2} = (pi + j + 1) \binom{pi + j}{i} = (i + 1) \binom{pi + j + 1}{i + 1}.$$

Let $w = 1 - px^q$. Then we have

$$\begin{aligned} \frac{dx^{j+1}}{dz} &= \frac{(j+1)x^j}{w} \\ \frac{x^j}{w} &= z^j \sum_{i \geq 0} c_{i,j,1} z^{qi} \end{aligned} \tag{2.2}$$

and

$$\begin{aligned} \frac{1}{j+s+1} \left(\frac{d}{dz} \right)^2 x^{j+s+1} &= (j+s) \frac{x^{j+s-1}}{w^2} + pq \frac{x^{j+s+p-2}}{w^3} \\ (j+s) \frac{x^{j+s-1}}{w^2} + pq \frac{x^{j+s+p-2}}{w^3} &= z^{j+s-1} \sum_{i \geq 0} c_{i,j+s-1} z^{qi}. \end{aligned} \quad (2.3)$$

To study the Artin-Schreier curve defined by

$$F(x, y) = x - x^p - y^e = 0,$$

we substitute $z = y^e$. Then (2.2) and (2.3) give

$$\frac{x^j}{w} = y^{ej} \sum_{i \geq 0} c_{i,j,1} y^{mi} \quad (2.4)$$

and

$$(j+s) \frac{x^{j+s-1}}{w^2} + pq \frac{x^{j+s+p-2}}{w^3} = y^{(j+s-1)e} \sum_{i \geq 0} c_{i,j+s-1,2} y^{mi}, \quad (2.5)$$

where $m = qe$.

Hence we can define holomorphic 1-forms

$$\eta_{j,k} = \frac{x^j y^k dy}{F_x} = \frac{x^j y^k dy}{w} = y^{je+k} \sum_{i \geq 0} c_{i,j,1} y^{mi} dy$$

for $ej + pk < q(e-1)$. These integrate to

$$\psi_{ej+k+1} = \sum_{i \geq 0} \binom{pi+j}{i} \frac{y^{mi+ej+k+1}}{mi+ej+k+1}. \quad (2.6)$$

Proof. Clearly we have

$$x^j = z^j \sum_{i \geq 0} f_{i,j} z^{iq}.$$

for some integers $f_{i,j}$. We will show that $f_{i,j} = c_{i,j}$ by induction on i , and for each i by induction on j . To start the induction, note that $f_{0,j} = c_{0,j} = 1$ for all $j \geq 0$ and $f_{i,0} = c_{i,0} = 0$ for all $i > 0$.

Take the defining equation

$$x - x^p = z.$$

Multiplying both sides by x^{j-1} gives

$$x^j - x^{j+p-1} = zx^{j-1},$$

which implies that

$$f_{i,j} = f_{i,j-1} + f_{i-1,j+p-1}.$$

We can assume inductively that $f_{i,j-1}$ and $f_{i-1,j+p-1}$ have the expected values. Then we have

$$\begin{aligned} (pi + j - 1)f_{i,j} &= (pi + j - 1)(c_{i,j-1} + c_{i-1,j+p-1}) \\ &= (j - 1) \binom{pi + j - 1}{i} + (j + p - 1) \binom{pi + j - 1}{i - 1} \\ &= (j - 1) \left[\binom{pi + j - 1}{i} + \binom{pi + j - 1}{i - 1} \right] + p \binom{pi + j - 1}{i - 1} \\ &= (j - 1) \binom{pi + j}{i} + \frac{pi}{(pi + j)} \binom{pi + j}{i} \\ &= \frac{(j - 1)(pi + j) + pi}{(pi + j)} \binom{pi + j}{i} \\ &= \frac{j(pi + j - 1)}{(pi + j)} \binom{pi + j}{i} \\ &= (pi + j - 1)c_{i,j}. \end{aligned}$$

□

Lemma 2.1 can also be derived from the Lagrange inversion formula, originally published in 1770, and cited in Whittaker–Watson [**WW62**, page 133]. It says that for $\zeta = a + t\phi(\zeta)$,

$$f(\zeta) = f(a) + \sum_{n=1}^{\infty} \frac{t^n}{n!} \frac{d^{n-1}}{da^{n-1}} (f'(a)\phi(a)^n)$$

for analytic functions ϕ and f , with $|t\phi(z)| < |z - a|$.

Consider the case $t = 1$, $\zeta = x$, $a = z$, $\phi(x) = x^p$ and $f(x) = x^j$. Then the equation reads $x = a + x^p$ and the series is

$$\begin{aligned}
x^j &= z^j + \sum_{n=1}^{\infty} \frac{j}{n!} \frac{d^{n-1}}{dz^{n-1}} (z^{pn+j-1}) \\
&= z^j + \sum_{n=1}^{\infty} \frac{j}{n!} \frac{d^n}{dz^n} \left(\frac{z^{pn+j}}{pn+j} \right) \\
&= \sum_{n=0}^{\infty} \frac{j}{n!} \frac{d^n}{dz^n} \left(\frac{z^{pn+j}}{pn+j} \right) \\
&= \sum_{n=0}^{\infty} \frac{j}{pn+j} \binom{pn+j}{n} z^{qn+j}.
\end{aligned}$$

The arithmetic function $\Phi_{n,a,b}$

In order to state our next result, we need the p -adic Gamma function of Morita [Mor75], defined on positive integers n by

$$\Gamma_p(n+1) = (-1)^{n+1} \prod_{\substack{1 \leq j \leq n \\ p \nmid j}} j = \frac{(-1)^{n+1} n!}{[n/p]! p^{[n/p]}}.$$

It is known to extend uniquely to a continuous function from the p -adic integers to the p -adic units. Details can be found in [Rob00, VII.1].

Theorem 2.7. Given integers $n > 0$, and $a, b \geq 0$ satisfying $b < p$ and $qa + b < p^n$, for a nonnegative integer t let

$$\Phi_{n,a,b}(t) = \binom{p(p^n t + a) + b}{p^n t + a} / p^{\alpha'(a,b)} \binom{pt}{t},$$

for nonnegative integers t , where $\alpha'(a,b) = (\alpha(qa + b) - b)/q$, and $\alpha(x)$ is the sum of the digits in the p -adic expansion of x , denoted in [Rob00] by $S_p(x)$. It extends uniquely to a continuous function from the p -adic integers to the p -adic units and has the following properties:

(i)

$$\Phi_{1,0,0}(t) = -\frac{\Gamma_p(1 + p^2 t)}{\Gamma_p(1 + pt)\Gamma_p(1 + qpt)}.$$

(ii)

$$\Phi_{n,0,0}(t) = \prod_{i=0}^{n-1} \Phi_{1,0,0}(p^i t).$$

(iii)

$$\frac{\Phi_{n,a,b}(t)}{\Phi_{n,0,0}(t)} = \frac{\prod_{i_1=1}^{pa+b} (p^{n+1}t + i_1)}{p^{\alpha'(a,b)} \prod_{i_2=1}^{qa+b} (qp^n t + i_2) \prod_{i_3=1}^a (p^n t + i_3)},$$

which is a unit for all t .

(iv) If $t' \equiv t''$ modulo p^k , then $\Phi_{n,a,b}(t') \equiv \Phi_{n,a,b}(t'')$ modulo p^{k+1} .

Proof. Unit valued continuity will follow from (i)-(iii). For (i) we have

$$\begin{aligned} \Phi_{1,0,0}(t) &= \binom{p^2t}{pt} \bigg/ \binom{pt}{t} = \frac{(p^2t)!t!(qt)!}{(pt)!(pqt)!(pt)!} \\ &= \prod_{\substack{i_1=1 \\ p \nmid i_1}}^{p^2t} i_1 \bigg/ \prod_{\substack{i_2=1 \\ p \nmid i_2}}^{pqt} i_2 \prod_{\substack{i_3=1 \\ p \nmid i_3}}^{pt} i_3 \\ &= \frac{\Gamma_p(1+p^2t)}{\Gamma_p(1+pt)\Gamma_p(1+pqt)}. \end{aligned}$$

(ii) follows directly from the definition of Φ , as does the formula in (iii). To see that the ratio of (iii) is a unit, note that the p -adic valuation v of $\binom{pa+b}{a}$ satisfies

$$\begin{aligned} qv &= \alpha(a) + \alpha(qa+b) - \alpha(pa+b) \\ &= \alpha(a) + \alpha(qa+b) - \alpha(a) - b \\ &= \alpha(qa+b) - b \end{aligned}$$

$$\text{so } v = \alpha'(a, b),$$

and the ratio

$$\frac{\prod_{i_1=1}^{pa+b} (p^{n+1}t + i_1)}{\prod_{i_2=1}^{qa+b} (qp^nt + i_2) \prod_{i_3=1}^a (p^nt + i_3)}$$

is a unit multiple of

$$\frac{\prod_{i_1=1}^{pa+b} i_1}{\prod_{i_2=1}^{qa+b} i_2 \prod_{i_3=1}^a i_3} = \frac{(pa+b)!}{(qa+b)!a!} = \binom{pa+b}{a}.$$

For (iv), we first reduce to the case $(n, a, b) = (1, 0, 0)$. Let $g(t)$ be the ratio of (iii). A simple calculation using logarithmic differentiation shows that

$$\begin{aligned} g'(t) &= p^n g(t) \left(p \sum_{i=1}^{pa+b} \frac{1}{p^{n+1}t + i} - q \sum_{i=1}^{qa+b} \frac{1}{qp^nt + i} - \sum_{i=1}^a \frac{1}{p^nt + i} \right) \\ &\equiv p^n g(t) \left(p \sum_{j=1}^a \frac{1}{p^{n+1}t + pj} - q \sum_{i=1}^{qa+b} \frac{1}{qp^nt + i} - \sum_{i=1}^a \frac{1}{p^nt + i} \right) \\ &\quad \text{mod } p\mathbf{Z}_{(p)} \\ &\equiv -qp^n g(t) \sum_{i=1}^{qa+b} \frac{1}{qp^nt + i} \equiv 0; \end{aligned}$$

in the last step we use the hypothesis that $qa+b < p^n$. It follows that if $t' \equiv t''$ modulo p^k , then $g(t') \equiv g(t'')$ modulo p^{k+1} , provided that the Mean Value Theorem holds. For this we refer to [Rob00, V.3.2] and note that the power series expansion of $g(t)$ is “restricted,” meaning that its coefficients tend to zero p -adically.

Thus we have reduced (iv) to the case $a = b = 0$. Reduction to the case $n = 1$ follows from (ii). It is known ([Rob00, VII.1.2(3)]) that for $p > 2$, $x \equiv y$ modulo p^k

implies $\Gamma_p(x) \equiv \Gamma_p(y)$ modulo p^k , so it implies that $\Gamma_p(px) \equiv \Gamma_p(py)$ modulo p^{k+1} and the same congruence holds for $\Phi_{1,0,0}$.

For $p = 2$, Γ_p satisfies a similar congruence except when $k = 2$. Thus we have to worry about $\Phi_{1,0,0}$ in the case $k = 1$. We have

$$\Phi_{1,0,0}(t) = -\frac{\Gamma_2(1+4t)}{\Gamma_2(1+2t)^2}.$$

Thus for two values of t differing by a multiple of 2, the numerators are congruent modulo 4 while the denominators (being squares of odd integers) are congruent modulo 8, so the two values of Φ are congruent modulo 4 as required. \square

Some power series congruences

Fix a prime p and a positive integer f , with $f > 1$ if $p = 2$. The following notation will be used in the rest of this section, along with the notion of congruence defined in 1.9.

$$\left\{ \begin{array}{l} e = p^f - 1 \\ m = qe \\ h = qf \\ \psi_{ej+k+1} = \sum_{i \geq 0} \binom{pi+j}{i} \frac{y^{mi+ej+k+1}}{mi+ej+k+1} \\ \text{for } 0 \leq k < e \\ \text{and } 0 \leq j < q \end{array} \right. \quad \begin{array}{l} q = p - 1 \\ \ell = e - p^{f-1} \end{array} \quad (2.8)$$

Our next lemma is a description of the orbit of $\ell \in \mathbf{Z}/m$ under multiplication by p (where $\ell = p^f - p^{f-1} - 1$), which we denote by L . It has $h = (p-1)f$ elements. We want to define integers $\lambda(r)$ between 0 and m so that $\lambda(r)$ is congruent to $p^r \ell$. Since p^f is congruent to 1 modulo e , it follows that the congruence class of $\lambda(r)$ modulo e depends only on the congruence of r modulo f .

Note that

$$\begin{aligned} p\ell &= p^{f+1} - p^f - p = pe - p^f = (p-1)e - 1 \equiv -1 \pmod{m} \\ \text{so } \lambda(0) &= \ell \equiv -1/p \\ \text{and } \lambda(r) &\equiv -p^{r-1}. \end{aligned}$$

We denote the mod f reduction of $r - 1$ by r_0 , so we can write $\lambda(r) = \kappa(r)e - p^{r_0}$ for a suitable $\kappa(r)$.

We will illustrate this for the case $(p, f) = (5, 4)$, for which $h = 16$, $e = 624$, $m = 2496$, and $\ell = 499$. The values of $\lambda(r)$ can be read down and from left to right in the following table, in which the values of r_0 and $\kappa(r)$ are indicated in the top row and leftmost column respectively.

	0	1	2	3
1				$e - p^3 = 499$
4	$4e - 1 = 2495$	$4e - p = 2491$	$4e - p^2 = 2471$	$4e - p^3 = 2371$
3	$3e - 1 = 1871$	$3e - p = 1867$	$3e - p^2 = 1847$	$3e - p^3 = 1747$
2	$2e - 1 = 1247$	$2e - p = 1243$	$2e - p^2 = 1223$	$2e - p^3 = 1123$
1	$e - 1 = 623$	$e - p = 619$	$e - p^2 = 599$	

Lemma 2.9. Let $\lambda(0) = \ell$ and for $1 \leq r \leq h$, let

$$\lambda(r) = e - p^{r_0} + \kappa(r)e,$$

where $r_0 = r - 1 - f[(r - 1)/f]$ and $\kappa(r) = p - 2 - [(r - 1)/f]$. (Note that $\lambda(h) = \lambda(0)$.) Then $p^r \ell \equiv \lambda(r)$ modulo m , and the orbit of $\ell \in \mathbf{Z}/m$ is

$$L = \{(j + 1)e - p^k : 0 \leq j < p - 1, 0 \leq k < f\}.$$

Proof. Modulo m we have

$$\begin{aligned} p\ell &= p(e - p^{f-1}) \equiv e - p^f = -1, \\ \text{so } p^r \ell &\equiv -p^{r-1} \quad \text{for } r > 0. \end{aligned}$$

Let \bar{x} denote $x - m[x/m]$, the mod m reduction of x . Modulo m we have

$$\begin{aligned} p^{r-1} &\equiv p^{r_0 + f[(r-1)/f]} \equiv p^{r_0} (1 + e)^{[(r-1)/f]} \\ &\equiv p^{r_0} (1 + [(r-1)/f]e) \quad \text{since } e^2 \equiv 0 \\ &\equiv p^{r_0} + [(r-1)/f]e \quad \text{since } pe \equiv e \\ \text{so } -p^{r-1} &\equiv -p^{r_0} - [(r-1)/f]e \\ &\equiv e - p^{r_0} + (p - 2 - [(r-1)/f])e \\ &\equiv e - p^{r_0} + \kappa(r)e = \lambda(r). \end{aligned}$$

□

Our next result concerns a congruence relating $\psi_{\lambda(r)}$ and $T^r * \psi_\ell/p$; recall that $\lambda(r)$ is congruent to $p^r \ell$ modulo m .

Before stating it we will illustrate with the case $(p, f) = (3, 2)$ (for which $m = 16$ and $\ell = 5$) and $r = 2$. We have

$$\begin{aligned} \psi_\ell &= \psi_5 = \sum_{i \geq 0} \binom{3i}{i} \frac{y^{16i+5}}{16i+5} \\ T^2 * \psi_5 &= \sum_{i \geq 0} \binom{3i}{i} \frac{y^{144i+45}}{16i+5} \end{aligned}$$

and

$$\begin{aligned}
\psi_{\lambda(2)} = \psi_{13} &= \sum_{i \geq 0} \binom{3i+1}{i} \frac{y^{16i+13}}{16i+13} \\
&\equiv \sum_{i \geq 0} \binom{9i+7}{3i+2} \frac{y^{48i+45}}{48i+45} \\
&= \sum_{i \geq 0} \frac{(9i+7)(9i+6)}{(3i+2)(3i+1)} \binom{9i+5}{3i} \frac{y^{48i+45}}{3(16i+15)} \\
&= \sum_{i \geq 0} \frac{9i+7}{3i+1} \binom{9i+5}{3i} \frac{y^{48i+45}}{16i+15} \\
&\equiv \sum_{i \geq 0} \frac{27i+7}{9i+1} \binom{27i+5}{9i} \frac{y^{144i+45}}{3(16i+5)} \\
&= \sum_{i \geq 0} \frac{(27i+7)(27i+6)}{(9i+1)(9i+2)} \binom{27i+5}{9i} \frac{y^{144i+45}}{9(16i+5)} \\
&\equiv \sum_{i \geq 0} \binom{27i+7}{9i+2} \frac{y^{144i+45}}{9(16i+5)}.
\end{aligned}$$

For each i , the coefficients in $T^2 * \psi_5$ and $3\psi_{13}$ have the same 3-adic valuation, so the ratio between them is a 3-adic unit. We want a single 3-adic unit $\tau(2)$ that does the job for each i , i.e., such that

$$\psi_{13} \equiv \frac{\tau(2)T * \psi_5}{3}.$$

This means that $\tau(2)$ must satisfy

$$\binom{3i}{i} \tau(2) \equiv \frac{1}{3} \binom{27i+7}{9i+2} \pmod{3(16i+5)}.$$

The obvious choice is

$$\tau(2) = \lim_{i \rightarrow -5/16} \frac{\binom{27i+7}{9i+2}}{\binom{3i}{i}} = \Phi_{2,2,1}(-5/16),$$

which satisfies the required congruence by Theorem 2.7(iv).

Theorem 2.10. With notation as above, we have

$$\psi_{\lambda(r)} \equiv \frac{\tau(r)T^r}{p} * \psi_\ell,$$

where

$$\tau(r) = \Phi_{r,\iota(r),\kappa(r)}(-\ell/m) \quad \text{with} \quad \iota(r) = [p^{r-1}(m-1)/m].$$

In particular the i th coefficient of $\psi_{\lambda(r)}$ is a p -local integer unless

$$i \equiv \iota(r) \pmod{p^r}, \tag{2.11}$$

e.g. the i th coefficient of $\psi_\ell = \psi_{\lambda(h)}$ is integral unless $i \equiv \iota(h)$ modulo p^h .

Proof. We have

$$\psi_{\lambda(r)} = \sum_{i \geq 0} \binom{pi + \kappa(r)}{i} \frac{y^{mi + \lambda(r)}}{mi + \lambda(r)}.$$

We need to show that the i th coefficient is a p -local integer unless (2.11) holds. Again let \bar{x} denote $x - m[x/m]$, the mod m reduction of x . (2.11) implies

$$\begin{aligned} mi &\equiv p^{r-1}(m-1) - \overline{p^{r-1}(m-1)} \pmod{p^r} \\ &= p^{r-1}(m-1) - \overline{-p^{r-1}} \\ &= p^{r-1}(m-1) - \lambda(r) \\ mi + \lambda(r) &= p^{r-1}(m-1) \\ &\equiv 0 \quad \text{since } m \equiv 1 \pmod{p} \end{aligned}$$

Hence it implies that the denominator of the i th coefficient of $\psi_{\lambda(r)}$ is divisible by p^r .

If $i - \iota(r)$ is a unit multiple of p^t for some $t < s$, then so is $mi + \lambda(r)$. We need to show that the binomial coefficient is divisible by p^t in this case. Recall that its p -adic valuation is

$$\alpha'(i, \kappa(r)) = (\alpha(qi + \kappa(r)) - \kappa(r))/q.$$

We claim that

$$\iota(r) = \sum_{k=0}^{r-2} \left[\frac{k + pf - r + 1}{f} \right] p^k; \quad (2.12)$$

we will verify this at the end of the proof.

It follows that

$$\begin{aligned} q\iota(r) &= \sum_{k=0}^{r-2} \left[\frac{pf + k - r + 1}{f} \right] p^{k+1} - \left[\frac{pf + k - r + 1}{f} \right] p^k \\ &= \sum_{k=1}^{r-1} \left[\frac{pf + k - r}{f} \right] p^k - \sum_{k=0}^{r-2} \left[\frac{pf + k - r + 1}{f} \right] p^k \\ &= \sum_{k=0}^{r-1} \left(\left[\frac{k - r}{f} \right] - \left[\frac{k - r + 1}{f} \right] \right) p^k + p^r - \left[\frac{pf - r}{f} \right] \\ &= -\frac{p^{r+f-1} - p^{r_0}}{p^f - 1} + p^r - 1 - \kappa(r) \end{aligned}$$

so

$$\begin{aligned} q\iota(r) + \kappa(r) &= p^r - 1 - \frac{p^{r+f-1} - p^{r_0}}{p^f - 1} \\ &= \sum_{k=0}^{r-1} a_k p^k \\ &\text{where } a_k = \begin{cases} p-2 & \text{if } k \equiv s-1 \pmod{f} \\ p-1 & \text{otherwise.} \end{cases} \end{aligned}$$

Thus if $i = \iota(r)$ modulo p^t for $t < s$,

$$\begin{aligned} \alpha(qi + \kappa(r)) &\geq \sum_{k=0}^{t-1} a_k \geq qt - [t/f] \\ \alpha'(i, \kappa(r)) &= \frac{\alpha(qi + \kappa(r)) - \kappa(r)}{q} \geq \frac{qt - [t/f] - \kappa(r)}{q} \\ &= \frac{qt - [t/f] - (p-2 - [(r-1)/f])}{q} \\ &= \frac{qt + [(r-1)/f] - [t/f] - q + 1}{q} \\ &\geq t \quad \text{since it is an integer,} \end{aligned}$$

and we have the desired integrality condition.

This means that

$$\begin{aligned} \psi_{\lambda(r)} &\equiv \sum_{i \geq 0} \binom{p(p^r i + \iota(r)) + \kappa(r)}{p^r i + \iota(r)} \frac{y^{m(p^r i + \iota(r)) + \lambda(r)}}{m(p^r i + \iota(r)) + \lambda(r)} \\ &= \sum_{i \geq 0} \binom{p(p^r i + \iota(r)) + \kappa(r)}{p^r i + \iota(r)} \frac{y^{p^r(mi+\ell)}}{p^r(mi+\ell)} \\ \text{and } T^r * \psi_\ell &= \sum_{i \geq 0} \binom{pi}{i} \frac{y^{p^r(mi+\ell)}}{mi+\ell} \end{aligned}$$

Thus to verify the congruence of the theorem, we need to compare the coefficients of these two series and show that

$$p^{1-r} \binom{p(p^r i + \iota(r)) + \kappa(r)}{p^r i + \iota(r)} \equiv \Phi_{r, \iota(r), \kappa(r)}(-\ell/m) \binom{pi}{i} \pmod{p^{k+1}}$$

when i is congruent to $-\ell/m$ modulo p^k . This is implied by

$$\binom{p(p^r i + \iota(r)) + \kappa(r)}{p^r i + \iota(r)} \Big/ p^{r-1} \binom{pi}{i} \equiv \Phi_{r, \iota(r), \kappa(r)}(-\ell/m).$$

The left hand side is $\Phi_{r, \iota(r), \kappa(r)}(i)$ since $\alpha'(\iota(r), \kappa(r)) = r - 1$, so this is the congruence of Theorem 2.7 .

We still need to prove (2.12). For future reference, recall the identity

$$\left[-\frac{x}{f} \right] = \left[\frac{f-1-x}{f} \right]. \quad (2.13)$$

We have

$$\begin{aligned} \frac{1}{m} &= \frac{1}{(p-1)(p^f-1)} = \frac{1}{p^{f+1}(1-p^{-1})(1-p^{-f})} \\ &= \sum_{k \geq 0} \left[\frac{k+f}{f} \right] p^{-k-f-1} \quad \text{in the standard topology} \\ &= \sum_{k \geq f+1} \left[\frac{k-1}{f} \right] p^{-k} = \sum_{k \geq 1} \left[\frac{k-1}{f} \right] p^{-k} \\ \frac{m-1}{m} &= 1 - \frac{1}{m} = 1 - \sum_{k \geq 1} \left[\frac{k-1}{f} \right] p^{-k} = \sum_{k \geq 1} \left(p-1 - \left[\frac{k-1}{f} \right] \right) p^{-k} \\ &= \sum_{k \geq 1} \left(p-1 + \left[\frac{f-k}{f} \right] \right) p^{-k} \quad \text{by (2.13)} \\ &= \sum_{k \geq 1} \left(\left[\frac{pf-k}{f} \right] \right) p^{-k}, \end{aligned}$$

so

$$\begin{aligned} \iota(r) &= \left[\frac{p^{r-1}(m-1)}{m} \right] = \left[\sum_{k \geq 1} \left(\left[\frac{pf-k}{f} \right] \right) p^{r-1-k} \right] \\ &= \sum_{k=1}^{r-1} \left(\left[\frac{pf-k}{f} \right] \right) p^{r-1-k} = \sum_{k=0}^{r-2} \left(\left[\frac{pf-r+1+k}{f} \right] \right) p^k \end{aligned}$$

as claimed. \square

Lemma 2.14. Let $0 \leq s < p$ and let λ be a positive integer. Then

$$\sum_{i \geq 0} c_{i,s-1,2} \frac{y^{mi+\lambda}}{mi+\lambda} \equiv \frac{es-\lambda}{e} \sum_{i \geq 0} \binom{pi+s}{i} \frac{y^{mi+\lambda}}{mi+\lambda}.$$

If $se < \lambda \leq (s+1)e$, then the sum on the right is ψ_λ .

Proof. Recall that

$$c_{i,s-1,2} = (pi+s) \binom{pi+s-1}{i} = (qi+s) \binom{pi+s}{i},$$

so

$$\sum_{i \geq 0} c_{i,s-1,2} \frac{y^{mi+\lambda}}{mi+\lambda} = \sum_{i \geq 0} (qi+s) \binom{pi+s}{i} \frac{y^{mi+\lambda}}{mi+\lambda}.$$

We will subtract the power series

$$\frac{1}{e} \sum_{i \geq 0} \binom{pi + s}{i} y^{mi + \lambda},$$

which has p -local integer coefficients. Since

$$\frac{qi + s}{mi + \lambda} - \frac{1}{e} = \frac{es - \lambda}{e(mi + \lambda)},$$

we get the desired congruence. The relation to ψ_λ follows from the definition of the latter. \square

3. Deformations of the Artin-Schreier curve

The notation of 1.9 and (2.8) is still in force in this section.

Holomorphic 1-forms on the deformed Artin-Schreier curve

Lemma 3.1. Let $y^\epsilon = x - x^p = \tilde{x} - \tilde{x}^p + \epsilon$ as in (1.3). Then

$$\tilde{x} \equiv x - \frac{\epsilon}{w} \pmod{(a_\nu)^2},$$

where $w = 1 - px^q$.

Proof. It is clear that $\tilde{x} \equiv x$ modulo (ϵ) , so suppose

$$\tilde{x} \equiv x + \epsilon x_1 \pmod{(a_\nu)^2}$$

for some x_1 . Then modulo $(a_\nu)^2$ we have

$$\begin{aligned} \tilde{x}^p &\equiv x^p + p\epsilon x^q x_1 \\ \tilde{x} - \tilde{x}^p + \epsilon &\equiv x + \epsilon x_1 - (x^p + p\epsilon x^q x_1) + \epsilon \\ &\equiv x - x^p + \epsilon(1 + x_1(1 - px^q)) \\ &\equiv x - x^p + \epsilon(1 + x_1 w) \end{aligned}$$

so

$$0 = (\tilde{x} - \tilde{x}^p + \epsilon) - (x - x^p) \equiv \epsilon(1 + x_1 w)$$

and

$$x_1 \equiv -1/w \pmod{(a_\nu)}$$

and the result follows. \square

We will denote $1 - p\tilde{x}^q$ by \tilde{w} . We have

$$\begin{aligned}\tilde{w} &= 1 - p \left(x - \frac{\varepsilon}{w} \right)^q = w + \frac{pqx^{p-2}\varepsilon}{w} \\ \varepsilon' &= \frac{\partial \varepsilon}{\partial \tilde{x}} = \sum_{0 < s < p} s \varepsilon_s \tilde{x}^{s-1} \\ \tilde{F}_{\tilde{x}} &= \frac{\partial \tilde{F}(\tilde{x}, y)}{\partial \tilde{x}} = \tilde{w} + \varepsilon' = w + \frac{pqx^{p-2}\varepsilon}{w} + \varepsilon' \\ &= w \left(1 + pq \frac{x^{p-2}\varepsilon}{w^2} + \frac{\varepsilon'}{w} \right) \\ \frac{dy}{\tilde{F}_{\tilde{x}}} &= \frac{dy}{w} \left(1 - pq \frac{x^{p-2}\varepsilon}{w^2} - \frac{\varepsilon'}{w} \right).\end{aligned}$$

Hence the holomorphic 1-forms are

$$\begin{aligned}\tilde{\eta}_{j,k} &= \frac{\tilde{x}^j y^k dy}{\tilde{F}_{\tilde{x}}} \\ &= \left(x^j - \frac{jx^{j-1}\varepsilon}{w} \right) y^k \left(\frac{1}{w} - \frac{\varepsilon'}{w^2} - pq \frac{x^{p-2}\varepsilon}{w^3} \right) dy \\ &= y^k \left(\frac{x^j}{w} - \frac{jx^{j-1}\varepsilon + x^j \varepsilon'}{w^2} - \frac{pqx^{j+p-2}\varepsilon}{w^3} \right) dy \\ &= \frac{x^j y^k dy}{w} - \sum_{0 \leq s < p} \varepsilon_s \left(\frac{jx^{s+j-1} + sx^{j+s-1}}{w^2} + \frac{pqx^{j+s+p-2}}{w^3} \right) dy \\ &= \sum_{i \geq 0} c_{i,j,1} y^{mi+ej+k} dy - \sum_{0 \leq s < p} \varepsilon_s \sum_{i \geq 0} c_{i,j+s-1,2} y^{mi+(j+s-1)e+k} dy\end{aligned}$$

by (2.4) and (2.5)

for $ej + pk < q(e-1)$. Using the definition of ε_s , this gives

$$\begin{aligned}\tilde{\eta}_{j,k} &= \left(\sum_{i \geq 0} c_{i,j,1} y^{mi+ej+k} \right. \\ &\quad \left. - \sum_{s=0}^{p-1} \sum_{t=0}^{t_1} a_{pe-se-pqt} \sum_{i \geq 0} c_{i,j+s-1,2} y^{mi+n(j,k,s,t)} \right) dy.\end{aligned}$$

where $t_1 = [(pe - se - 1)/pq]$ and $n(j, k, s, t) = (j + s - 1)e + k + qt + 1$.

These integrate to

$$\begin{aligned}\tilde{\psi}_{ej+k+1} &= \sum_{i \geq 0} c_{i,j,1} \frac{y^{mi+ej+k+1}}{mi+ej+k+1} \\ &\quad - \sum_{s=0}^{p-1} \sum_{t=0}^{t_1} a_{pe-se-pqt} \sum_{i \geq 0} c_{i,j+s-1,2} \frac{y^{mi+n(j,k,s,t)}}{mi+n(j,k,s,t)}.\end{aligned}$$

Let

$$\begin{aligned} \tilde{\psi}_{ej+k+1,s,t} &= -a_{pe-se-pqt} \sum_{i \geq 0} c_{i,j+s-1,2} \frac{y^{mi+n(j,k,s,t)}}{mi+n(j,k,s,t)}. \\ \text{so } \tilde{\psi}_{ej+k+1} &= \psi_{ej+k+1} + \sum_{s=0}^{p-1} \sum_{t=0}^{t_1} \tilde{\psi}_{ej+k+1,s,t}. \end{aligned}$$

with ψ_{ej+k+1} as in Theorem (2.8).

We want to use this to compute $\tilde{\psi}_\ell$ (where $\ell = p^f - p^{f-1} - 1$ as before), for which we have

$$\begin{aligned} (j, k) &= (0, e - p^{f-1} - 1) \\ n(j, k, s, t) &= (s-1)e + e - p^{f-1} - 1 + qt + 1 = se + qt - p^{f-1} \end{aligned}$$

It follows that

$$\begin{aligned} \tilde{\psi}_{\ell,s,t} &\equiv -a_{pe-se-pqt} \sum_{i \geq 0} c_{i,s-1,2} \frac{y^{mi+se+qt-p^{f-1}}}{mi+se+qt-p^{f-1}} \\ &\equiv \left(\frac{qt-p^{f-1}}{e} \right) a_{pe-se-pqt} \sum_{i \geq 0} \binom{pi+s}{i} \frac{y^{mi+se+qt-p^{f-1}}}{mi+se+qt-p^{f-1}} \\ &\quad \text{by Lemma 2.14} \\ &= \begin{cases} \left(\frac{qt-p^{f-1}}{e} \right) a_{pe-se-pqt} \psi_{se+qt-p^{f-1}} & \text{if } t \geq (p^{f-1} + 1)/q \\ 0 & \text{if } p = 2 \text{ and } t = 2^{f-1}. \end{cases} \end{aligned} \quad (3.2)$$

Illustration for the case $(p, f) = (2, 3)$

The case $(p, f) = (2, 3)$ is the simplest example that illustrates the need to pass from R to R' . In this case, over \overline{R} we have

$$\begin{aligned} \tilde{F}(\tilde{x}, y) &= \tilde{x} - \tilde{x}^2 - y^7 + \varepsilon_0 + \varepsilon_1 \tilde{x} \\ &= \tilde{x} - \tilde{x}^2 - y^7 + \sum_{t=0}^6 a_{14-2t} y^t + \tilde{x} \sum_{t=0}^3 a_{7-2t} y^t. \end{aligned}$$

The genus is three and we have

$$\begin{aligned}\tilde{\psi}_3 &= \psi_3 + \sum_{s=0}^1 \sum_{t=0}^{6-3s} \tilde{\psi}_{3,s,t} \\ \text{where } \tilde{\psi}_{3,s,t} &= -a_{14-7s-2t} \sum_{i \geq 0} c_{i,s-1,2} \frac{y^{7i+7s+t-4}}{7i+7s+t-4} \\ &\equiv \left(\frac{t-4}{7}\right) a_{14-7s-2t} \sum_{i \geq 0} \binom{2i+s}{i} \frac{y^{7i+7s+t-4}}{7i+7s+t-4} \\ &\quad \text{by Lemma 2.14} \\ \text{so } \tilde{\psi}_{3,0,t} &\equiv \left(\frac{t-4}{7}\right) a_{14-2t} \sum_{i \geq 0} \binom{2i}{i} \frac{y^{7i+t-4}}{7i+t-4} \\ &\equiv \left(\frac{t-4}{7}\right) a_{14-2t} \sum_{i \geq 0} \binom{2i+2}{i+1} \frac{y^{7i+t+3}}{7i+t+3} \\ &\equiv 2 \left(\frac{t-4}{7}\right) a_{14-2t} \sum_{i \geq 0} \binom{2i+1}{i} \frac{y^{7i+t+3}}{7i+t+3}\end{aligned}$$

Thus we have

$$\begin{aligned}\tilde{\psi}_3 &\equiv \psi_3 + \sum_{t=0}^6 \left(\frac{t-4}{7}\right) (2a_{14-2t} + a_{7-2t}) \sum_{i \geq 0} \binom{2i+1}{i} \frac{y^{7i+t+3}}{7i+t+3} \\ &\quad \text{where } a_k = 0 \text{ for } k < 0 \\ &\equiv \psi_3 + \sum_{t=0}^3 \left(\frac{t-4}{7}\right) (2a_{14-2t} + a_{7-2t}) \sum_{i \geq 0} \binom{2i+1}{i} \frac{y^{7i+t+3}}{7i+t+3} \\ &\quad + \sum_{t=5}^6 2 \left(\frac{t-4}{7}\right) a_{14-2t} \sum_{i \geq 0} \binom{2i+1}{i} \frac{y^{7i+t+3}}{7i+t+3}.\end{aligned}$$

The second sum is

$$\begin{aligned}\sum_{t=5}^6 2 \left(\frac{t-4}{7}\right) a_{14-2t} \sum_{i \geq 0} \binom{2i+1}{i} \frac{y^{7i+t+3}}{7i+t+3} \\ \equiv \sum_{t=5}^6 2 \left(\frac{t-4}{7}\right) a_{14-2t} \psi_{t-4} = \sum_{\lambda=1}^2 \frac{2\lambda}{7} a_{6-2\lambda} \psi_\lambda\end{aligned}$$

Thus we define

$$\begin{aligned}\theta &= \tilde{\psi}_3 - \sum_{\lambda=1}^2 \frac{2\lambda}{7} a_{6-2\lambda} \psi_\lambda \\ &\equiv \psi_3 + \sum_{t=0}^3 \left(\frac{t-4}{7}\right) (2a_{14-2t} + a_{7-2t}) \sum_{i \geq 0} \binom{2i+1}{i} \frac{y^{7i+t+3}}{7i+t+3}\end{aligned} \tag{3.3}$$

For the original Artin-Schreier curve, Theorem 2.10 gives

$$\psi_3 \equiv \frac{\tau(3)T^3}{2} * \psi_3$$

where $\tau(3) = \Phi_{3,3,0}(-3/7)$, a 2-adic unit defined in Theorem 2.7. We would like to have a similar congruence for θ , namely

$$\theta \equiv \frac{1}{2} \sum_{r=1}^3 v_r T^r * \theta \quad (3.4)$$

for suitable values of v_r . Since θ is congruent to ψ_3 modulo (a_ν) , we can rewrite the desired congruence as

$$\begin{aligned} \theta &\equiv \frac{1}{2} \sum_{r=1}^3 v_r T^r * \psi_3 \equiv \frac{1}{2} \sum_{r=1}^3 v_r T^r * \sum_{i \geq 0} \binom{2i}{i} \frac{y^{7i+3}}{7i+3} \\ &\equiv \frac{1}{2} \sum_{r=1}^3 v_r \sum_{i \geq 0} \binom{2i}{i} \frac{y^{r(7i+3)}}{7i+3} \end{aligned}$$

This expression has powers of y with exponents congruent to 3, 5, and 6 modulo 7. On the other hand, the series θ of (3.3) has exponents congruent to 3, 4, 5, and 6. Thus *we must eliminate the terms in (3.3) with exponents congruent to 4 modulo 7, i.e., the ones with $t = 1$* . We do this by passing to the ring $R' = R/(a_5, a_{12})$. Note that in this case, N and N' as defined in (1.4) and (1.6) are

$$\begin{aligned} N &= \{14, 12, 10, 8, 6, 4, 2\} \cup \{7, 5, 3, 1\} \\ N' &= \{14, 10, 8, 6, 4, 2\} \cup \{7, 3, 1\} = N \setminus \{12, 5\}. \end{aligned}$$

The image of θ is \overline{R}' is

$$\begin{aligned} \theta' &\equiv \psi_3 + \sum_{t=0,2,3} \binom{t-4}{7} (2a_{14-2t} + a_{7-2t}) \sum_{i \geq 0} \binom{2i+1}{i} \frac{y^{7i+t+3}}{7i+t+3} \\ &\equiv \psi_3 + \sum_{\lambda=3,5,6} \binom{\lambda-7}{7} (2a_{20-2\lambda} + a_{13-2\lambda}) \sum_{i \geq 0} \binom{2i+1}{i} \frac{y^{7i+\lambda}}{7i+\lambda} \end{aligned}$$

Thus we need to show that for each λ ,

$$\binom{\lambda-7}{7} \sum_{i \geq 0} \binom{2i+1}{i} \frac{y^{7i+\lambda}}{7i+\lambda}$$

is congruent to a multiple of $T^r(\psi_3)/2$ for the appropriate r .

The case of general (p, f)

Lemma 3.5. Let $t_0 = (p^{f-1} + 1)/q$. (It is not an integer for $p > 3$.) Then for $t \geq t_0$, the exponent class of $\psi_{\ell,s,t}$ (i.e., $se + qt - p^{f-1} \in \mathbf{Z}/m$) is in the set

$$E = \{ej + k + 1 : j, k \geq 0, ej + pk < m - p\},$$

Proof. Since the genus is $q(e-1)/2$, $2g-1 = m-p$, and the set of exponents appearing in the $\tilde{\psi}_{\ell,s,t}$ is

$$S = \{se + qt - p^{f-1} : s, t \geq 0, es + pqt < pe\}$$

The inequality here implies that $qt < e$, so the (s, t) th element in S can be the (j, k) th element in E only if we set $j = s$ and $k = qt - p^{f-1} - 1$, which is nonnegative by our assumption on t . Then

$$ej + pk = es + pqt - p^f - p < pe - p^f - p = m - p - 1,$$

so we do indeed get an element in E . \square

Lemma 3.6. Let $0 \leq t < t_0$ if $p > 2$ or $0 \leq t < t_0 - 1 = 2^{f-1}$ if $p = 2$, $0 \leq s < p$, and $\lambda = se + qt - p^{f-1}$. Note that $\lambda < 0$ when $s = 0$. Then

$$\tilde{\psi}_{\ell,s,t} \equiv \begin{cases} p \left(\frac{m+p\lambda}{m} \right) a_{pe-pqt} \psi_{m+\lambda} & \text{if } s = 0 \\ \left(\frac{p\lambda - ms}{m} \right) a_{(p-s)e-pqt} \psi_{\lambda} & \text{if } s > 0. \end{cases}$$

and for $p = 2$, $\tilde{\psi}_{\ell,0,2^{f-1}} \equiv 0$.

Proof. The value of $\tilde{\psi}_{\ell,0,2^{f-1}}$ for $p = 2$ is from (3.2). For the other cases we have

$$\tilde{\psi}_{\ell,s,t} = \left(\frac{\lambda - se}{e} \right) a_{pe-se-pqt} \sum_{i \geq 0} \binom{pi+s}{qi+s} \binom{pi+s-1}{i} \frac{y^{mi+\lambda}}{mi+\lambda}$$

Let $i_0 = -\lambda/m$. Then

$$\begin{aligned} \frac{pi_0+s}{qi_0+s} &= \frac{ms-p\lambda}{ms-q\lambda} = \frac{ms-p\lambda}{q(es-\lambda)} \\ \frac{pi+s}{qi+s} - \frac{pi_0+s}{qi_0+s} &= \frac{(i-i_0)s}{(qi+s)(qi_0+s)} = \frac{(mi+\lambda)s}{(qi+s)q(es-\lambda)} \end{aligned}$$

so

$$\begin{aligned} \tilde{\psi}_{\ell,s,t} &= \left(\frac{\lambda - se}{e} \right) a_{pe-se-pqt} \\ &\quad \sum_{i \geq 0} \left(\frac{ms-p\lambda}{q(es-\lambda)} + \frac{(mi+\lambda)s}{(qi+s)q(es-\lambda)} \right) \binom{pi+s-1}{i} \frac{y^{mi+\lambda}}{mi+\lambda} \\ &= \left(\frac{p\lambda - ms}{m} \right) a_{pe-se-pqt} \sum_{i \geq 0} \binom{pi+s-1}{i} \frac{y^{mi+\lambda}}{mi+\lambda} \\ &\quad - \frac{a_{pe-se-pqt}}{m} \sum_{i \geq 0} \left(\frac{s}{pi+s} \right) \binom{pi+s-1}{i} y^{mi+\lambda} \\ &\equiv \left(\frac{p\lambda - ms}{m} \right) a_{pe-se-pqt} \sum_{i \geq 0} \binom{pi+s-1}{i} \frac{y^{mi+\lambda}}{mi+\lambda}. \end{aligned}$$

For $s > 0$ the sum is ψ_λ . For $s = 0$ (which means that $\lambda < 0$) we have

$$\begin{aligned}\tilde{\psi}_{\ell,0,t} &\equiv \left(\frac{p\lambda}{m}\right) a_{pe-pqt} \sum_{i \geq 0} \binom{pi-1}{i} \frac{y^{mi+\lambda}}{mi+\lambda} \\ &\equiv \left(\frac{p\lambda}{m}\right) a_{pe-pqt} \sum_{i \geq 0} \binom{pi+p-1}{i+1} \frac{y^{mi+m+\lambda}}{mi+m+\lambda} \\ &\equiv \left(\frac{p\lambda}{m}\right) a_{pe-pqt} \sum_{i \geq 0} \binom{pi+p-1}{i+1} \binom{pi+p-2}{i} \frac{y^{mi+m+\lambda}}{mi+m+\lambda}\end{aligned}$$

Let $i_1 = -1 - \lambda/m$. Then

$$\begin{aligned}\frac{pi_1+q}{i_1+1} &= \frac{p+p\lambda/m-q}{\lambda/m} = \frac{m+p\lambda}{l} \\ \frac{pi+q}{i+1} - \frac{pi_1+q}{i_1+1} &= \frac{i-i_1}{(i+1)(i_1+1)} = \frac{i-i_1}{(i+1)(-\lambda/m)} \\ &= \frac{-m(i-i_1)}{(i+1)\tau} = -\frac{mi+m+\lambda}{(i+1)\lambda}\end{aligned}$$

so

$$\begin{aligned}\tilde{\psi}_{\ell,0,t} &\equiv \left(\frac{p\lambda}{m}\right) a_{pe-pqt} \sum_{i \geq 0} \left(\frac{m+p\lambda}{\lambda} - \frac{mi+m+\lambda}{(i+1)\lambda}\right) \binom{pi+p-2}{i} \frac{y^{mi+m+\lambda}}{mi+m+\lambda} \\ &= p \left(\frac{m+p\lambda}{m}\right) a_{pe-pqt} \psi_{m+\lambda} \\ &\quad - p \left(\frac{a_{pe-pqt}}{m}\right) \sum_{i \geq 0} \binom{1}{i+1} \binom{pi+p-2}{i} y^{mi+m+\lambda} \\ &= p \left(\frac{m+p\lambda}{m}\right) a_{pe-pqt} \psi_{m+\lambda} \\ &\quad - p \left(\frac{a_{pe-pqt}}{m}\right) \sum_{i \geq 0} \binom{1}{pi+p-1} \binom{pi+p-1}{i+1} y^{mi+m+\lambda} \\ &\equiv p \left(\frac{m+p\lambda}{m}\right) a_{pe-pqt} \psi_{m+\lambda}\end{aligned}$$

□

Lemma 3.7. Let

$$\theta = \tilde{\psi}_\ell - \sum_{s=0}^{p-1} \sum_{t_0 \leq t \leq t_1} \tilde{\psi}_{\ell,s,t} = \psi_\ell + \sum_{s=0}^{p-1} \sum_{0 \leq t < t_0} \tilde{\psi}_{\ell,s,t},$$

where as before $t_0 = (p^{f-1} + 1)/q$ and $t_1 = [(pe - se - 1)/pq]$. Then

$$\theta = \begin{cases} \psi_\ell + \sum_{0 \leq t < t_0} \left(\frac{m + pqt - p^f}{m} \right) (pa_{pe-pqt} + a_{e-pqt}) \psi_{m+qt-p^{f-1}} \\ \quad + \sum_{1 \leq s \leq p-2} \sum_{0 \leq t < t_0} \left(\frac{se + pqt - p^f}{m} \right) a_{(p-s)e-pqt} \psi_{se+qt-p^{f-1}} & \text{for } p > 2 \\ \psi_\ell + \sum_{0 \leq t < 2^{f-1}} \left(\frac{2t-1}{2^f-1} \right) (2a_{2e-2t} + a_{e-2t}) \psi_{t+2^{f-1}-1} & \text{for } p = 2. \end{cases}$$

Proof. We use the values of $\tilde{\psi}_{\ell,s,t}$ given by Lemma 3.6. For $0 < s < q$, the values given here are the same, and we have

$$\begin{aligned} \tilde{\psi}_{\ell,0,t} &= p \left(\frac{m + p\lambda}{m} \right) a_{pe-pqt} \psi_{m+\lambda} \\ &\quad \text{where } \lambda = qt - p^{f-1}, \text{ so } m + p\lambda = m + pqt - p^f \\ &= p \left(\frac{m + pqt - p^f}{m} \right) a_{pe-pqt} \psi_{m+qt-p^{f-1}} \end{aligned}$$

and

$$\begin{aligned} \tilde{\psi}_{\ell,q,t} &= \left(\frac{p\lambda - qm}{m} \right) a_{e-pqt} \psi_\lambda \\ &\quad \text{where } \lambda = m + qt - p^{f-1}, \text{ so } p\lambda - qm = m + pqt - p^f \\ &= \left(\frac{m + pqt - p^f}{m} \right) a_{e-pqt} \psi_{m+qt-p^{f-1}}, \end{aligned}$$

so

$$\tilde{\psi}_{\ell,0,t} + \tilde{\psi}_{\ell,q,t} = \left(\frac{m + pqt - p^f}{m} \right) (pa_{pe-pqt} + a_{e-pqt}) \psi_{m+qt-p^{f-1}}.$$

The result follows. \square

We have $se + qt - p^{f-1} \in L$ (defined in Lemma 2.9) when

$$t = \frac{p^{f-1} - p^i}{q} \quad \text{for } 0 \leq i \leq f-1.$$

This includes all values of t occurring in the expression for θ for $f \leq 2$ but not for $f > 2$. In order to get a Honda eigenseries, we must exclude the unwanted values of t by setting the corresponding a_ν s equal to zero. Hence we pass from \overline{R} to \overline{R}' , where R' is the quotient of R defined in (1.5).

Theorem 3.8. Let R' be as in (1.5), and \overline{R}' the quotient obtained by setting u equal to 1. Let θ be the power series over $\overline{R}'/(a_\nu)^2 \otimes \mathbf{Q}_p$ of Lemma 3.7, and let θ' be its

image over $\overline{R}'/(a_\nu)^2 \otimes \mathbf{Q}_p$. Then θ' is a Honda eigenseries satisfying

$$\left(1 - \sum_{r=1}^h \frac{v_r T^r}{p}\right) * \theta' \equiv 0$$

where

$$v_r = \begin{cases} \tau(r) \left(\frac{m-p^r}{m}\right) (pa_{m+p^r-1} + a_{p^r-1}) & \text{if } 1 \leq r \leq \min(f, h-1) \\ \tau(r) \left(\frac{m-se-p^i}{m}\right) a_{se+p^i-1} & \text{if } f < r < h \text{ and } p > 2 \\ \tau(h) \left(\frac{m-2a_{2e}-a_e}{m}\right) & \text{if } r = h \text{ and } p = 2 \\ \tau(h) \left(\frac{m-a_m}{m}\right) & \text{if } r = h \text{ and } p > 2 \\ 0 & \text{if } r > h; \end{cases}$$

here $\tau(r)$ is the p -adic unit defined in Theorem 2.10, $r = sf + i$ with $1 \leq i \leq f$, and $h = (p-1)f$.

We will prove this below.

The resulting 1-dimensional formal group law over $\overline{R}'/(a_\nu)^2$ is induced by a homomorphism to that ring from BP_* sending v_r for $r \leq h$ to the values indicated above and v_r for $r > h$ to 0. We can lift this to \overline{R} by sending each v_r to the elements of the same name there.

We can derive Theorem 1.2 from Theorem 3.8 using the homomorphism $\overline{R}' \rightarrow L$ given by

$$a_i \mapsto \begin{cases} u_{j+sf} & \text{if } i = se + p^{j-1} \text{ with } 0 \leq s \leq p-1 \text{ and } 1 \leq j \leq f \\ 0 & \text{otherwise.} \end{cases}$$

We can lift Theorem 3.8 from the ungraded ring $\overline{R}'/(a_\nu)^2$ to its graded counterpart $R'/(a_\nu)^2$ as follows. Replace y by $u^{-p}y$ and a_ν by $u^{-\nu}a_\nu$, making θ' a homogeneous expression of degree 0. We want the lifting of v_r to have degree $2(p^r-1)$, so we replace the congruence of Theorem 3.8 by

$$\left(1 - \sum_{r=1}^h \frac{u^{1-p^r} v_r T^r}{p}\right) * \theta' \equiv 0.$$

This means that in $R'/(a_\nu^2)$ we need to define

$$v_r = \begin{cases} \tau(r) \left(\frac{m-p^r}{m} \right) (pu^{-m}a_{m+p^r-1} + a_{p^r-1}) & \text{if } 1 \leq r \leq \min(f, h-1) \\ \tau(r)u^{p^r-se-p^i} \left(\frac{m-se-p^i}{m} \right) a_{se+p^i-1} & \\ \tau(h)u^{2^h-1} \left(\frac{m-2a_{2e}-a_e}{m} \right) & \text{if } f < r < h \text{ and } p > 2 \\ \tau(h)u^{2^h-1} \left(\frac{m-a_m}{m} \right) & \text{if } r = h \text{ and } p = 2 \\ \tau(h)u^{p^h-1} \left(\frac{m-a_m}{m} \right) & \text{if } r = h \text{ and } p > 2 \\ 0 & \text{if } r > h. \end{cases} \quad (3.9)$$

We now define a lifting to the formal group law over $R'/(a_\nu)^2$ to one R' by a homomorphism to R' from

$$BP_* = \mathbf{Z}_{(p)}[v_1, v_2, \dots]$$

in which the image of v_r is given by (3.9). Since the image of v_h is a unit, the functor

$$X \mapsto BP_*(X) \otimes_{BP_*} R'$$

defined on finite complexes X is Landweber exact.

We are not claiming that this formal group law over R' is a formal summand of the Jacobian of the curve over R defined by (1.25). We have not dealt with holomorphic 1-forms and related series over R' itself, but only with their ‘linear approximations’ lifted from $R'/(a_\nu)^2$.

Proof. From the formula for θ given in Lemma 3.7 we have

$$\begin{aligned}
\theta' - \psi_\ell &= \sum_{i=0}^{f-1} \left(\frac{m - p^{i+1}}{m} \right) (pa_{m+p^{i+1}-1} + a_{p^{i+1}-1}) \psi_{m-p^i} \\
&\quad + \sum_{s=1}^{p-2} \sum_{i=0}^{f-1} \left(\frac{se - p^{i+1}}{m} \right) a_{m-se+p^{i+1}-1} \psi_{se-p^i} \\
&= \sum_{i=1}^f \left(\frac{m - p^i}{m} \right) (pa_{m+p^i-1} + a_{p^i-1}) \psi_{m-p^{i-1}} \\
&\quad + \sum_{s=1}^{p-2} \sum_{i=1}^f \left(\frac{m - se - p^i}{m} \right) a_{se+p^i-1} \psi_{m-se-p^{i-1}} \\
&= \sum_{i=1}^f \left(\frac{m - p^i}{m} \right) (pa_{m+p^i-1} + a_{p^i-1}) \psi_{\lambda(i)} \\
&\quad + \sum_{s=1}^{p-2} \sum_{i=1}^f \left(\frac{m - se - p^i}{m} \right) a_{se+p^i-1} \psi_{\lambda(i+sf)} \\
&= \sum_{r=1}^f \left(\frac{m - p^r}{m} \right) (pa_{m+p^r-1} + a_{p^r-1}) \psi_{\lambda(r)} \\
&\quad + \sum_{r=f+1}^h \left(\frac{m - se - p^i}{m} \right) a_{se+p^i-1} \psi_{\lambda(r)}
\end{aligned}$$

where $r = se + i$ with $1 \leq i \leq f$.

We now apply Theorem 2.10 and get

$$\begin{aligned}
\theta' &\equiv \psi_\ell + \sum_{r=1}^f \left(\frac{m - p^r}{m} \right) (pa_{m+p^r-1} + a_{p^r-1}) \psi_{\lambda(r)} \\
&\quad + \sum_{r=f+1}^h \left(\frac{m - se - p^i}{m} \right) a_{se+p^i-1} \psi_{\lambda(r)} \\
&\equiv \frac{\tau(h)T^h}{p} * \theta' + \sum_{r=1}^f \left(\frac{m - p^r}{m} \right) (pa_{m+p^r-1} + a_{p^r-1}) \frac{\tau(r)T^r}{p} * \theta' \\
&\quad + \sum_{r=f+1}^h \left(\frac{m - se - p^i}{m} \right) a_{se+p^i-1} \frac{\tau(r)T^r}{p} * \theta' \\
&\equiv \sum_{r=1}^h \frac{v_r T^r}{p} * \theta'
\end{aligned}$$

with v_r as indicated in the theorem. The result follows. \square

References

- [Hon70] Taira Honda. On the theory of commutative formal groups. *J. Math. Soc. Japan*, 22:213–246, 1970.
- [Hon73] Taira Honda. On the formal structure of the Jacobian variety of the Fermat curve over a p -adic integer ring. In *Symposia Mathematica, Vol. XI (Convegno di Geometria, INDAM, Rome, 1972)*, pages 271–284. Academic Press, London, 1973.
- [Mil86] J. S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.
- [Mor75] Yasuo Morita. A p -adic analogue of the Γ -function. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 22(2):255–266, 1975.
- [Rav07] D. C. Ravenel. Toward higher chromatic analogs of elliptic cohomology. In D. C. Ravenel H. R. Miller, editor, *Elliptic Cohomology Geometry, Applications, and Higher Chromatic Analogues*, pages 286–305, Cambridge, 2007. Cambridge University Press. Preprint available online at www.math.rochester.edu/u/doug/preprints.html.
- [Rob00] Alain M. Robert. *A course in p -adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
- [WW62] E. T. Whittaker and G. N. Watson. *A course of modern analysis. An introduction to the general theory of infinite processes and of analytic functions: with an account of the principal transcendental functions*. Fourth edition. Reprinted. Cambridge University Press, New York, 1962.

Douglas C. Ravenel douglas.ravenel@rochester.edu

University of Rochester, Rochester, NY 14627