TOWARD HIGHER CHROMATIC ANALOGS OF ELLIPTIC COHOMOLOGY

DOUGLAS C. RAVENEL

Abstract. We show that the Jacobian of a certain Artin-Schreier curve over the field $\mathbf{F}_p$ has a a 1-dimensional formal summand of height $(p-1)f$ for any positive integer f. We give two proofs, the classical one which was known to Manin in 1963 and which requires knowledge of the zeta function of the curve, and a new simpler one using methods of Honda. This is the first step toward contructing the cohomology theories indicated in the title.

1. Introduction

A starting point for elliptic cohomology is a homomorphism φ from a cobordism ring to some ring R, which is often called an R-valued genus. When the cobordism theory is MU_*, we know by Quillen's theorem [Qui69] that φ is equivalent to a 1-dimensional formal group law over R. It is also known that the functor

$$X \mapsto MU_*(X) \otimes_\varphi R$$

is a homology theory if φ satisfies certain conditions spelled out in Landweber's Exact Functor Theorem [Lan76].

Now suppose E is an elliptic curve defined over R. It is a 1-dimensional algebraic group, and choosing a local paramater at the identity leads to a formal group law $\widehat{E}$, the formal completion of E. Thus we can apply the machinery above and get an R-valued genus.

For example, the *Jacobi quartic*, defined by the equation

$$y^2 = 1 - 2\delta x^2 + \epsilon x^4,$$

is an elliptic curve over the ring

$$R = \mathbf{Z}[1/2, \delta, \epsilon].$$

The resulting formal group law is the power series expansion of

$$F(x,y) = \frac{x\sqrt{1-2\delta y^2+\epsilon y^4} + y\sqrt{1-2\delta x^2+\epsilon x^4}}{1-\epsilon x^2y^2};$$

this calculation is originally due to Euler. The resulting genus is known to satisfy Landweber's conditions [LRS95], and this leads to one definition of elliptic cohomology.

The rich structure of elliptic curves leads to interesting calculations with the cohomology theory and to the theory of topological modular forms due to Hopkins *et al*, [HM] and [AHS01]. In [HM] they consider the elliptic curve defined by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Under the affine coordinate change

$$x \mapsto x + r \qquad \text{and} \qquad y \mapsto y + sx + t$$

Date: March 22, 2007.

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

we get

$$\left\{\begin{array}{rcl} a_6 & \mapsto & a_6 + a_4\, r + a_3\, t + a_2\, r^2 \\ & & \quad + a_1\, r\, t + t^2 - r^3 \\ a_4 & \mapsto & a_4 + a_3\, s + 2\, a_2\, r \\ & & \quad + a_1(r\, s + t) + 2\, s\, t - 3\, r^2 \\ a_3 & \mapsto & a_3 + a_1\, r + 2\, t \\ a_2 & \mapsto & a_2 + a_1\, s - 3\, r + s^2 \\ a_1 & \mapsto & a_1 + 2\, s. \end{array}\right. \tag{1.1}$$

This can be used to define an action of the affine group on the ring

$$A = \mathbf{Z}[a_1, a_2, a_3, a_4, a_6].$$

Its cohomology is the E_2-term of a spectral sequence converging to the homotopy of tmf, the spectrum representing topological modular forms.

However it is known that the formal group law associated with an elliptic curve over a finite field can have height at most 2; see Corollary 2.4 below. Hence elliptic cohomology cannot give us any information about v_n-periodic phenomena for $n > 2$.

The purpose of this paper is to suggest a way to construct similar cohomology theories that go deeper into the chromatic tower. Suppose we have an algebraic curve C of genus g. Then its Jacobian $J(C)$ is an abelian variety of dimension g. $J(C)$ has a formal completion $\widehat{J}(C)$ which is a g-dimensional formal group. If $\widehat{J}(C)$ has a 1-dimensional summand, then Quillen's theorem gives us a genus associated with the curve C. A result in this direction is the following.

Theorem 1.2. *Let $C(p, f)$ be the Artin-Schreier curve over $\mathbf{F}_p$ defined by*

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

for a positive integer f. Then the Jacobian $J(p, f)$ of this curve (possibly after extension of scalars) has a 1-dimensional formal summand of height $(p-1)f$.

This result was stated by Manin in [Man63]. The case $f = 1$ was treated by Gorbunov and Mahowald in [GM00]. Most of what is needed for the proof can be found in Katz's 1979 Bombay Colloquium paper [Kat81]. Koblitz' Hanoi notes [Kob80] covers much of the same material in a less formal way. In §2 we will sketch the original proof since some of the ideas behind it will be needed later. In §3 we will give a new proof using some methods developed by Honda. It has the advantage of being both simpler and more flexible than the classicial proof. In a future paper we will use it to explore deformations of the Artin-Schreier curve and changes of coordinates leading to formulae analogous to (1.1).

It is a pleasure to thank the Isaac Newton Institute for their generous hospitality during the preparation of this paper, and to thank Neil Strickland, Spencer Bloch and Mike Hopkins for helpful conversations.

2. The classical proof of Theorem 1.2

An important tool in studying commutative formal groups in characteristic p is the theory of Dieudonné modules.

Theorem 2.1. [Die55] *The category of commutative formal groups over a finite field k is equivalent to the category of modules over the ring*

$$\mathbf{D}(k) = \mathbf{W}(k)\langle F, V\rangle/(FV = VF = p)$$

where $\mathbf{W}(k)$ is the ring of Witt vectors over k, $w \mapsto w^\sigma$ is its Frobenius automorphism, $Fw = w^\sigma F$ and $Vw^\sigma = wV$ for $w \in \mathbf{W}(k)$. F is the Frobenius or pth power map, and V is the Verschiebung, the dual of F.

A $\mathbf{W}(k)$-module equipped with an action of such an F is called an *F-crystal*, and a similar module over $\mathbf{Q}\otimes\mathbf{W}(k)$ is called an *F-isocrystal*. $\mathbf{D}(k)$ is the endomorphism ring of a certain projective object P in the category of commutative formal groups, and the Dieudonné module $D(G)$ of a formal group G is group of homomorphisms from P to G. There is also a contravariant Dieudonné module $D^*(G)$ defined as the set of morphisms from G to a certain injective object I also having $\mathbf{D}(k)$ as its endomorphism ring. See Hazewinkel [Haz78] for more information.

Here are some examples.

- The Dieudonné module for the formal group associated with the nth Morava K-theory is
$$\mathbf{D}(\mathbf{F}_p)/(V-F^{n-1}),$$
so in it we have $F^n = p$.
- More generally, for m and n relatively prime, let
$$G_{m,n} = \mathbf{D}(k)/(V^m - F^n).$$
It corresponds to an m-dimensional formal group of height $m+n$.

Theorem 2.2. *[Dieudonné* [Die57]*]*

(i) Structure theorem. *Any simple Dieudonné module M is isogenous over $\mathbf{W}(\overline{\mathbf{F}}_p)$ to some $G_{m,n}$. (This means there is a map $M \to G_{m,n}$ with finite kernel and cokernel.)*

(ii) *Let the characteristic polynomial for F in M be*
$$Q(T) = T^m + \sum_{i>0} c_i T^{m-i}$$
for $c_i \in \mathbf{W}(k)$. If its Newton polygon has a line segment of horizontal length n and slope j/n, then up to isogeny over $\mathbf{W}(\overline{k})$, M has a summand of the form $G_{j,n-j}$.

The Newton polygon is the lower convex hull of the set of points
$$\{(i, \operatorname{ord}_p(c_i)) \colon 0 \le i \le m\},$$
where $c_0 = 1$. The condition on $Q(T)$ above is equivalent to the existence of n roots having p-adic valuation j/n. For more information, see [Kob80, pp. 19–23].

There are severe restrictions on the formal group attached to an abelian variety, as the following result indicates.

Theorem 2.3.

(i) *[Manin* [Man63]*]* Riemann symmetry condition. *If A is an abelian variety with formal completion $\widehat{A}$, and its Dieudonné module $D(\widehat{A})$ has a summand $G_{m,n}$ up to isogeny over $\mathbf{W}(\overline{\mathbf{F}}_p)$, then it also has a summand $G_{n,m}$.*

(ii) *[Tate* [Tat66]*] More precisely, if A has dimension g and is defined over $\mathbf{F}_q$ with $q = p^a$, then the characteristic polynomial for F^a has the form*
$$Q_a(T) = T^{2g} + \sum_{0<i<2g} c_i T^{2g-i} + q^g$$
with $c_i \in \mathbf{Z}$, and
$$Q_a\left(\frac{q}{T}\right) = \frac{q^g Q_a(T)}{T^{2g}},$$
so $c_{g+i} = q^i c_{g-i}$ for $0 < i < g$. (The Newton polygon for $Q(T)$ is determined by that of $Q_a(T)$.)

(iii) *[Honda* [Hon68]*]* Classification of abelian varieties up to isogeny over $\mathbf{F}_q$. *There is a one-to-one correspondance between isogeny classes of abelian varieties over $\mathbf{F}_q$ and polynomials of the above form, all of whose roots have absolute value $\sqrt{q}$.*

Corollary 2.4.

(i) *For an elliptic curve C, either*

$$D(\widehat{C}) \cong G_{0,1} \oplus G_{1,0},$$

(the ordinary height 1 case) or

$$D(\widehat{C}) \cong G_{1,1},$$

(the supersingular height 2 case), up to isogeny over $\mathbf{W}(\overline{\mathbf{F}}_p)$.

(ii) *If an abelian variety A has a 1-dimensional formal summand of height n for $n > 2$, then the dimension of A is at least n.*

The key to finding the Dieudonné module of the formal completion of the Jacobian of a curve C is the following fortunate isomorphism.

Theorem 2.5. *[Grothendieck, Berthelot] Let C be a smooth curve of genus g over $\mathbf{F}_q$, where $q = p^a$. Then its crystalline (or de Rham) H^1 is a free $\mathbf{W}(\mathbf{F}_q)$-module of rank $2g$ isomorphic to the contravariant Dieudonné module of its Jacobian $D^*(\widehat{J}(C))$, with the induced action of the Frobenius $\tilde{F}$ relative to $\mathbf{F}_q$ coinciding with the action of F^a.*

This result is originally due to Grothendieck in 1966. A proof can be found in [MM74, Appendix 2] and in [Ill79]. The crystalline cohomology of C is the same as the de Rham cohomology of a lifting of C to characteristic 0, i.e., from $\mathbf{F}_q$ to $\mathbf{W}(\mathbf{F}_q)$. For the curve $C(p, f)$, this H^1 is the free $\mathbf{Z}_p$-module with basis

$$\left\{\omega_{i,j} = \frac{x^i y^j \mathrm{d}x}{y^{e-1}} \colon 0 \le i \le p-2,\ 0 \le j \le e-2\right\},$$

the genus of the curve being $g = (p-1)(e-1)/2$. This can be derived from the fact that the curve is a d-fold branched cover of the projective line with $p+1$ branch points. We will have occasion to extend scalars in the ground field, in which case H^1 gets tensored with the appropriate ring of Witt vectors. The space of holomorphic 1-forms on $C(p, f)$ is spanned by

$$\{\omega_{i,j} \colon ei + pj < (e-1)(p-1) - 1\}. \tag{2.6}$$

This space is isomorphic to the cotangent space of the Jacobian. We will need it later in an alternate proof of Theorem 1.2.

At this point is useful to state the Weil conjectures, although we will only need them in the case of algebraic curves. Given a smooth d-dimensional variety X over $\mathbf{F}_q$, its ZETA FUNCTION is defined by

$$Z(X, T) = \exp\left(\sum_{n>0} |X(\mathbf{F}_{q^n})| \frac{T^n}{n}\right).$$

where $|X(\mathbf{F}_{q^n})|$ denotes the number of points of X defined over $\mathbf{F}_{q^n}$. The following statements were conjectured by Weil in 1949 [Wei49] and proved by the indicated authors. Expository accounts have been given by Katz [Kat76] and Mazur [Maz75].

Theorem 2.7.

(i) *(Dwork* [Dwo60]*) $Z(X, T)$ is a rational function of T.*

(ii) *$Z(X, T)$ satisfies a functional equation*

$$Z\left(X, \frac{1}{q^d T}\right) = \pm q^{d\chi/2} T^{\chi} Z(X, T),$$

where χ denotes the Euler-Poincaré characteristic of X.

(iii) *(Artin, Grothendieck et al,* [SGA73], [Gro95], [Gro77] *and Lubkin* [Lub68]*) More precisely,*

$$Z(X,T) = \frac{P_1(T)P_3(T)\cdots P_{2d-1}(T)}{P_0(T)P_2(T)\cdots P_{2d}(T)}$$

where $P_0(T) = 1-T$, $P_{2d}(T) = 1-q^dT$, and for $0 < i < 2d$, $P_i(T)$ is a polynomial whose degree is the rank of $H^i(X)$ suitably defined.

(iiv) Riemann hypothesis in characteristic p. *(Deligne* [Del74] *and* [Del80]*) Each reciprocal root of $P_i(T)$ has absolute value $q^{i/2}$.*

(v) *If X is the reduction of a variety $\overline{X}$ defined over a number field K, then*

$$P_i(T) = \det(1 - T\tilde{F}|H^i(\overline{X}(\mathbf{C})))$$

where $\tilde{F}$ is the Frobenius relative to $\mathbf{F}_q$. In particular the degree of $P_i(T)$ is the rank of $H^i(\overline{X}(\mathbf{C}))$, the ith Betti number of $\overline{X}$. Hence (ii) follows from an analog of the Lefschetz fixed point formula.

The formula (iii) follows from an analog of the Lefschtez Fixed Point Theorem once one has defined a cohomology theory for varieties in charatcteristic p with suitable properties. These statements were proved for curves by Weil in [Wei48]. If X is a smooth curve of genus g, then

$$Z(X,T) = \frac{P_1(T)}{(1-T)(1-qT)},$$

where the factors $(1-T)^{-1}$ and $(1-qT)^{-1}$ correspond to H^0 and H^2. $P_1(T)$, which corresponds to H^1, has degree $2g$ with

$$P_1(T) = 1 + \sum_{0<i<2g} c_i T^i + q^g T^{2g},$$

and $Q_a(T) = T^{2g}P_1(1/T)$ is the characteristic polynomial of $\tilde{F} = F^a$ in $D(\widehat{J}(X))$. The coefficients c_i are the same as those in Theorem 2.3. The functional equation (ii) implies the relations among the c_i given there.

In other words, the zeta function of a curve determines the formal completion of its Jacobian in an explicit way.

Now suppose X is acted on by a finite group G and let ρ be a representation of G over a number field K with enough roots of unity. Define

$$L(X,\rho,T) = \exp\left(\frac{1}{|G|}\sum_{\gamma\in G}\mathrm{Tr}(\rho(\gamma))\sum_{n>0}C_n^\gamma\frac{T^n}{n}\right),$$

where C_n^γ is the number of points in x in $X(\overline{\mathbf{F}}_p)$ satisfying $\gamma(x) = \tilde{F}^n(x)$.

Observe that if the action of G on X is trivial, and ρ is irreducible, then

$$\begin{aligned} L(X,\rho,T) &= \exp\left(\frac{1}{|G|}\sum_{\gamma\in G}\mathrm{Tr}(\rho(\gamma))\sum_{n>0}|X(\mathbf{F}_{q^n})|\frac{T^n}{n}\right) \\ &= \exp\left(\sum_{n>0}|X(\mathbf{F}_{q^n})|\frac{T^n}{n}\sum_{\gamma\in G}\frac{\mathrm{Tr}(\rho(\gamma))}{|G|}\right) \\ &= \begin{cases} 1 & \text{if } \rho \text{ is nontrivial} \\ Z(X,T) & \text{if } \rho \text{ is trivial.} \end{cases} \end{aligned}$$

If ρ is the regular representation, then

$$\mathrm{Tr}(\rho(\gamma)) = \begin{cases} |G| & \text{if } \gamma = e \\ 0 & \text{otherwise,} \end{cases}$$

so $L(X,\rho,T)$ is just the zeta function.

We also have

$$L(X, \rho_1 \oplus \rho_2, T) = L(X, \rho_1, T)L(X, \rho_2, T).$$

Recall that the regular representation decomposes as a sum of irreducible representations

$$\sum_{\rho \text{ irreducible}} \text{degree}(\rho)\rho,$$

so

$$Z(X,T) = \prod_{\rho \text{ irreducible}} L(X, \rho, T)^{\text{degree}(\rho)}.$$

Deligne proved an alternating product formula for $L(X, \rho, T)$ similar to Weil's for $Z(X,T)$, in which $P_i^\rho(T)$ is the characteristic polynomial of $\tilde{F}$ restricted to

$$\text{Hom}_G(\rho, H^i(X) \otimes_{\mathbf{W}(\mathbf{F}_q)} K).$$

Now suppose X is a curve of genus g and A is a finite abelian group with action defined over $\mathbf{F}_q$ such that in $H^1(X) \otimes_{\mathbf{W}(\mathbf{F}_q)} K$, each character of A occurs with multiplicity at most 1. A always acts trivially on H^0 and H^2, so we have

$$\begin{aligned} Z(X,T) &= \frac{P_1(T)}{(1-T)(1-qT)} \\ &= \frac{1}{(1-T)(1-qT)} \prod_\rho P_1^\rho(T) \\ &= \frac{1}{(1-T)(1-qT)} \prod_\rho L(X, \rho, T) \\ &= \frac{1}{(1-T)(1-qT)} \prod_\rho \left(1 + \frac{1}{|A|} \sum_{a \in A} \text{Tr}(\rho(a)) C_1^a T\right), \end{aligned}$$

where the product is over the $2g$ 1-dimensional representations ρ of A that occur as summands of $H^1(X) \otimes_{\mathbf{W}(\mathbf{F}_q)} K$. Since $P_1(T)$ has degree $2g$, each of its factors $P_1^\rho(T)$ must be linear.

Our curve $C(p,f)$ has an action of a certain finite group G on defined over the field $\mathbf{F}_{p^n}$, where $n = (p-1)f$. The group is the semidirect product

$$G = \mathbf{F}_p \rtimes \mu_{(p-1)e}.$$

It fixes the point at infinity and acts on the rest of the curve via

$$(x, y) \mapsto (\zeta^e x + a, \zeta^p y),$$

where ζ and a are generators of $\mu_{(p-1)e}$ (the group of $(p-1)e$th roots of unity) and $\mathbf{F}_p$ (regarded as an additive group) respectively. (G is isomorphic to a maximal finite subgroup of the extended Morava stabilizer group $\mathbf{G}_n$. It will follow from the isomorphism above that G acts on the 1-dimensional formal summand as expected.) The smallest field containing these roots is $\mathbf{F}_{p^n}$, and its Frobenius F^n respects the eigenspace decomposition associated with the action of $\mu_{(p-1)e}$.

Under this action we have

$$\omega_{i,j} \mapsto \sum_{0 \le k \le i} \binom{i}{k} a^{i-k} \zeta^{1+ek+pj} \omega_{k,j}.$$

It is easily seen to have following properties.

(a) In the restriction to the subgroup $\mu_{(p-1)e}$, each character which is nontrivial on μ_e occurs with multiplicity 1. Hence the subspace spanned by each $\omega_{i,j}$ is also an eigenspace for F^n.

(b) The subspace spanned by the $\omega_{i,j}$ for a fixed j is an eigenspace (with nontrivial eigenvalue) for the subgroup μ_e. We will denote it by $H^{1,\chi}$ where χ is the corresponding nontrivial character of μ_e. The action of $\mu_{(p-1)e}$ is the induction (from μ_e to $\mu_{(p-1)e}$) of χ.
(c) In the restriction to the subgroup $\mathbf{Z}/(p)$, each subspace $H^{1,\chi}$ is an irreducible representation of degree $p-1$ isomorphic to the augmentation ideal in the group ring of $\mathbf{Z}/(p)$, i.e., to the sum of the $p-1$ nontrivial characters of $\mathbf{Z}/(p)$.
(d) In the restriction to the abelian subgroup $A = \mathbf{Z}/(p) \times \mu_e$, each character which is nontrivial on both factors occurs with multiplicity 1. We will denote by $H^{1,\psi,\chi} \subset H^{1,\chi}$ the subspace corresponding to the nontrivial characters ψ and χ on $\mathbf{Z}/(p)$ and μ_e. Note that these 1-dimensional eigenspaces are not the same as those for the subgroup $\mu_{(p-1)e}$.
(e) Each $H^{1,\chi}$ is an irreducible representation of the full group G.

Next we need to define some Gauss sums associated with the characters ψ and χ. Let $q = p^f = e+1$. Let L be a number field containing the epth roots of unity. We extend the characters ψ and χ to $\mathbf{F}_{q^m}^\times$ in the following way. We compose the additive character ψ on $\mathbf{F}_p$ with the trace map $\mathbf{F}_{q^m} \to \mathbf{F}_p$, and we compose the multiplicative χ with with the map $\mathbf{F}_{q^m}^\times \to \mathbf{F}_q^\times$ sending x to $x^{(q^m-1)/(q-1)}$. We denote these composite characters by ψ_{q^m} and χ_{q^m}. Then our Gauss sum is

$$g_{q^m}(\psi,\chi) = -\sum_{x \in \mathbf{F}_{q^m}^\times} \psi_{q^m}(x)\chi_{q^m}(x).$$

The action of F^f commutes with the action of the subgroup $\mathbf{Z}/(p) \times \mu_e$, so it respects the corresponding eigenspace decomposition of H^1. This means that the action of F^{fn} on $H^{1,\psi,\chi}$ is multiplication by a scalar, and that scalar is known to be $g_{q^m}(\psi,\chi)$. This is originally due to Hasse-Davenport [HD34] and is explained by Katz in [Kat81, Lemma 2.1]. The proof involves counting certain points in $C(p,f)$.

It follows that the characteristic polynomial for the action of F^{fn} on H^1 is

$$P_{q^m}(T) = \prod_{\psi,\chi}(T - g_{q^m}(\psi,\chi)), \tag{2.7}$$

where the product is over all nontrivial ψ and all nontrivial χ. Recall that in light of Grothendieck's isomorphism, this is also the characteristic polynomial F^{fn} acting on the Dieudonné module for the Jacobian of our curve. The numerator of the zeta function of $C(p,f)$, regarded as a curve over $\mathbf{F}_{q^m}$ is

$$T^{2g}P_{q^m}(T^{-1}) = \prod_{\psi,\chi}(1 - g_{q^m}(\psi,\chi)T).$$

It turns out that for our purposes all we need to know about the $g_q(\psi,\chi)$ is their p-adic valuations. These were originally determined by Stickelberger [Sti90], but we will derive them from the Gross-Koblitz formula.

To state it we need to pick a p-adic place $\mathfrak{p}$ in L. Its residue field is isomorphic to $\mathbf{F}_q$. This choice allows us to identify (via reduction mod $\mathfrak{p}$) the target of χ with $\mathbf{F}_q^\times$. This means that χ can be defined as the ath power map for some integer a with $0 < a < e$, so we will denote χ by χ_a.

The choice of ψ amounts to choosing a primitive pth root of unity λ, and for each such λ there is a unique solution π to the equation $\pi^{p-1} = -1$ such that

$$\lambda \equiv 1 + \pi \bmod \quad (\pi)^2,$$

so we will write such a ψ as ψ_π.

Finally, let $\alpha(k)$ denote the sum of the digits in the p-dic expansion of k. Then the Gross-Koblitz formula says

$$g_{q^m}(\psi_\pi, \chi_a) = u(a)^m \frac{q^m}{\pi^{\alpha((q^m-1)a/e)}}. \tag{2.8}$$

Here $u(a)$ is the p-adic unit

$$u(a) = (-1)^f \prod_{0\le j<f} \Gamma_p\left(1 - \left[\frac{ap^j}{e}\right]\right)$$

where $[x]$ denotes the fractional part of x and Γ_p is the p-adic Gamma function.

Lemma 2.9. *In the polynomial $P_{q^{p-1}}(T)$ of (2.7), there are n factors for which $\mathrm{ord}_p(g_{q^{p-1}}(\psi,\chi)) = 1$, and the other Gauss sums have higher p-adic valuation. More specifically, for each integer i with $0 < i < n$, there are $(p-1)b_i$ factors with $\mathrm{ord}_p(g_{q^{p-1}}(\psi,\chi)) = i$, where the numbers b_i are given below in (2.10).*

Proof. We will derive this from the Gross-Koblitz formula (2.8). The most interesting thing about it for us is the power of π in the denominator. Note that find that

$$\alpha((q^{p-1}-1)a/(q-1)) = \alpha(a)\alpha((q^{p-1}-1)/(q-1)) = \alpha(a)(p-1).$$

It follows that

$$\mathrm{ord}_p(g_{q^{p-1}}(\psi_\pi, \chi_a)) = (p-1)f - \alpha(a).$$

For $0 < a < p^f - 1$, we have $0 < \alpha(a)n$, so the number

$$\mathrm{ord}_p(g_{q^{p-1}}(\psi_\pi, \chi_a))$$

is an integer between 0 and n.

We need to know how many times each of these integers occurs, which amounts to computing how many integers a between 0 and $p^f - 1$ have a given value of α. If there are b_i such values of a with $\alpha(a) = i$, then the b_i are given by the generating function

$$\begin{aligned}
\sum_i b_i t^i &= \left(\frac{1-t^p}{1-t}\right)^f \\
&= (1-t^p)^f (1-t)^{-f} \\
&= \sum_{0\le j\le f} (-1)^j \binom{f}{j} t^{pj} \sum_{k\ge 0} (-1)^k \binom{-f}{k} t^k \\
&= \sum_{0\le j\le f} \sum_{k\ge 0} (-1)^j \binom{f}{j}\binom{f+k-1}{f-1} t^{pj+k},
\end{aligned}$$

so

$$b_i = b_{n-i} = \sum_{0\le j\le i/p} (-1)^j \binom{f}{j}\binom{f+i-pj-1}{f-1}. \tag{2.10}$$

In particular we have

$$b_1 = b_{p^f-2} = f.$$

There are $p-1$ characters for each value of a, so the result follows. □

Next we need to recall some facts about the Newton polygon for a polynomial. For a polynomial $P(T) = \sum_{c_k T^k}$, the Newton polygon is the convex hull of the set $\{(k, \mathrm{ord}_p(c_k))\}$. If this polygon has a line segment of slope m and horizontal length N, then $P(T)$ has precisely N roots (counting multiplicities) r_i with $\mathrm{ord}_p(r_i) = 1/m$. Thus the Newton polygon determines and is determined by the ordinals of the reciprocal roots.

Hence Lemma 2.9 enables us to construct the Newton polygon for $P_{q^{p-1}}(T)$. Recall that $P_{q^{p-1}}(T)$ is the characteristic polynomial for the action of F^n on H^1. It follows that the Newton polygon for F itself is similar but with all vertical coordinates divided by n.

Here is an example. Let $(p, f) = (3, 2)$. In this case the degree of the polynomial is 14, and we have

$$b_1 = b_3 = 2 \qquad \text{and} \qquad b_2 = 3$$

since

$$(1 + t + t^2)^2 = 1 + 2t + 3t^2 + 2t^3 + t^4.$$

It follows that the Newton polygon for F^4 has vertices at $(0, 0)$, $(4, 4)$, $(10, 16)$ and $(14, 28)$, the one for F has vertices at $(0, 0)$, $(4, 1)$, $(10, 4)$ and $(14, 7)$, and the slopes of the latter are $1/4$, $1/2$, and $3/4$.

The Riemann symmettry condition of Theorem 2.3(i) has the following implication. If the Newton polygon for F has a line segment of length N and slope m, then the Dieudonné module over the algebraic closure has a summand isogenous to $G_{mN,(1-m)N}$, so the formal group has an mN-dimensional summand of height N. Thus in our case the first slope leads to a 1-dimensional summand of height n as claimed.

3. A Honda theoretic proof of Theorem 1.2

In this section we will give a second proof of Theorem 1.2 using methods introduced by Honda in [Hon70] and [Hon73]. Unlike the classical proof, it makes no use of the group action on $C(p, f)$. In a future paper we will generalize to some deformations of $C(p, f)$ which do not have a group action.

We now recall the results of [Hon70]. Let F be a formal group of dimension n defined over the ring of integers A of a discrete valuation field K. Let $\mathfrak{m}$ be the maximal ideal of A, $A_{\mathfrak{m}}$ the completion of A at $\mathfrak{m}$, and k the residue field $A/\mathfrak{m}$. Assume that k has characteristic $p > 0$. Suppose that K has an endomorphism σ such that there is a power q of p with $a^\sigma \equiv a^q$ modulo $\mathfrak{m}$ for any $a \in A$. Let $A_\sigma\langle\langle T\rangle\rangle$ be the ring of noncommutative power series in T over A subject to the rule $Ta = a^\sigma T$. Let $M_n(A_{\mathfrak{m}})$ denote the ring of $n \times n$-matrices over $A_{\mathfrak{m}}$, and define the ring $M_n(A_{\mathfrak{m}})_\sigma\langle\langle T\rangle\rangle$ in a similar way.

F is characterized by its logarithm f, which is a vector of n power series $f_1, \dots, f_n$ over K in n variables $x_1, \dots, x_n$ with $f_i \equiv x_i$ modulo term of degree 2. (Honda calls f the transformer of F.) F is given by the formula $F(x, y) = f^{-1}(f(x) + f(y))$, where x and y are n-dimensional vectors.

Let f^{σ^i} be the power series obtained from f by applying σ^i to each coefficient. Given a matrix $H = \sum_i C_i T^i$ in $M_n(A_{\mathfrak{m}})_\sigma\langle\langle T\rangle\rangle$, define

$$(H * f)(x) = \sum_i C_i f^{\sigma^i}(x^{q^i}).$$

If f is the logarithm for F, we say that H is a *Honda matrix* for F (or for the vector f) and that F *is of type* H, if $H \equiv \pi I_n$ modulo T (where π is a uniformizing element for $\mathfrak{m}$ and I_n is the $n \times n$ identity matrix) and $(H * f)(x) \equiv 0$ modulo $\mathfrak{m}$. (Honda calls such a matrix special with respect to F.)

We say that two matrices $H_1, H_2 \in M_n(A_{\mathfrak{m}})_\sigma\langle\langle T\rangle\rangle$ are equivalent if $H_1 = UH_2$ for an invertible matrix $U \in M_n(A_{\mathfrak{m}})_\sigma\langle\langle T\rangle\rangle$.

Theorem 3.1.

(i) [Hon70, Theorem 4] *Suppose that the field K as above is unramified at p, i.e., that $A_{\mathfrak{m}}$ is the ring of Witt vectors $W(k)$ and $\mathfrak{m} = (p)$. Then the strict isomorphism classes of n-dimensional formal group laws over A correspond bijectively to the equivalence classes of matrices $H \in M_n(A_p)_\sigma\langle\langle T\rangle\rangle$*

congruent to pI_n modulo degree 1. H and f are related by the formula

$$f(x) = (H^{-1} * p)(x).$$

(ii) [Hon70, Corollary to Theorem 4] *Moreover, given a set $B \subset A$ of representatives of the residue field $A/(p)$, for each F there is a unique Honda matrix of the form*

$$H = pI_n + \sum_{i>0} C_i T^i$$

such that each C_i has coefficients in B.

(iii) [Hon70, 5.5] *Suppose that the coefficients of C_i are all invariant under the endomorphism σ, let ξ denote the Frobenius endomorphism of the mod p reduction $\overline{F}$ of the formal group F, and let*

$$\det H = p^n + \sum_{i>0} c_i T^i.$$

Then this is also the characteristic polynomial (or power series) of the Frobenius endomorphism of F.

Here are some examples of Honda matrices.

Example 3.2. *For $n = 1$ and $A = \mathbf{Z}$, let H be the 1×1 matrix with entry $u = p - T^h$ for a positive integer h. Then*

$$u^{-1} = p^{-1}\left(1 - p^{-1}T^h\right)^{-1} = p^{-1}\sum_{i\geq 0} p^{-i}T^{hi}$$

so

$$f(x) = \sum_{i\geq 0} \frac{x^{p^{hi}}}{p^i}$$

and F is the formal group law for the Morava K-theory $K(h)_*$. More generally the mod p reduction of a 1-dimensional formal group law over $\mathbf{Z}$, $\mathbf{Z}_{(p)}$ or $\mathbf{Z}_p$ has height h iff u is congruent to a unit multiple of T^h modulo (p, T^{h+1}).

Example 3.3. *Let $A = \mathbf{Z}_p[[u_1, u_2, \dots u_{h-1}]]$ for a positive integer h, and let $u_i^\sigma = u_i^p$. Let H be the 1×1 matrix with entry*

$$u = p - T^h - \sum_{0<i<h} u_i T^i.$$

Then $f(x)$ is the logarithm for the Lubin-Tate lifting of the formal group law of 3.2.

Example 3.4. *Let $A = BP_* = \mathbf{Z}_{(p)}[v_1, v_2, \dots]$ (where the v_i are defined by Hazewinkel's formula) with endomorphism σ defined by $v_i^\sigma = v_i^p$. Let H be the 1×1 matrix with entry*

$$u = p - \sum_{i>0} v_i T^i.$$

Then $f(x)$ is the logarithm for the universal p-typical formal group law, i.e., the usual formal group law over BP_*.

Example 3.5. *The Honda matrix for the Dieudonné formal group $G_{n,m}$ is*

$$H = pI_n - C_1 T - C_{m+1}T^{m+1}$$

where

$$C_1 = \begin{bmatrix} 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix} \qquad \text{and} \qquad C_{m+1} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{bmatrix}.$$

Details can be found in [Hon70, 5.2].

Next we recall some results from [Hon73] about the formal completion of the Jacobian J of an algebraic curve C of genus g over K. Let $\{\omega_1, \dots \omega_g\}$ be a basis of the holomorphic 1-forms on C. (For our curve $C(p,f)$, such a basis is given in (2.6).) Choose a local parameter z at some point $P \in K(C)$ and denote by $\omega_i(z)$ the expansion of ω_i at P. There are power series $\psi_i(z)$ over K with $\psi_i(0) = 0$ and $\mathrm{d}\psi_i(z) = \omega_i(z)$.

Let $y = (y_1, \dots, y_g)$ be a system of local parameters at the origin of the Jacobian $J(C)$, and let $\nu_1, \dots, \nu_g$ be the invariant differentials of J such that $\nu_i \circ \Lambda = \omega_i$, where $\Lambda : C \to J$ is the canonical map corresponding to the point P. Let $\nu_i(y)$ denote the local expansion of ν_i at the origin. There are power series $\phi_i(y)$ over K with $\phi_i(0) = 0$ and $\mathrm{d}\phi_i(y) = \nu_i(y)$. Then the vector $\phi(y) = (\phi_i(y))$ is the logarithm for the formal completion $\widehat{J}(C)$ of $J(C)$ with respect to the local parameters y, whichl we denote by $F(C)$.

Theorem 3.6 (Honda [Hon73])**.** *With notation as above there is a finite set S of prime ideals in K such that if $\mathfrak{m} \notin S$ and $H \in M_g(A_{\mathfrak{m}})_\sigma\langle\langle T\rangle\rangle$ is a Honda matrix for the vector $\psi(z)$, then it is also a Honda matrix for the logarithm $\phi(y)$, so $F(C)$ is of type H as a formal group law over $A_{\mathfrak{m}}$.*

This means there is a close connection between power series expansions of holomorphic 1-forms on the curve C and the formal group law for its Jacobian $J(C)$. For the curve $C(p,f)$ we will use y as a local parameter about the origin. A basis for the space of holomorphic 1-forms is given in (2.6). Since $y^e = x^p - x$, we can solve for x and get a power series expansion of the form

$$x = y^e g_0(y^m) \qquad \text{where } m = (p-1)e,$$

for some power series g_0. It follows that

$$\begin{aligned} \mathrm{d}x &= y^{e-1} g_1(y^m)\mathrm{d}y, \\ \omega_{i,j} &= \frac{x^i y^j \mathrm{d}x}{y^{e-1}} \\ &= y^{ei+j}\tilde{g}_{i,j}(y^m)\mathrm{d}y, \\ \text{and} \qquad \psi_{i,j} &= y^{ei+j+1} g_{i,j}(y^m) \end{aligned}$$

for some power series $g_1, \tilde{g}_{i,j} \in \mathbf{Z}_p[[y^m]]$ and $g_{i,j} \in \mathbf{Q}_p[[y^m]]$.

These conditions on the $\psi_{i,j}$ put some restrictions on the Honda matrix. Let

$$E = \{ei + j + 1 \colon i, j \geq 0,\ ei + pj < (p-1)(e-1) - 1\} \subset \mathbf{Z}/(m). \tag{3.7}$$

Note that these conditions on i and j are the same as those in (2.6). In particular this set has g elements, where the genus g is $(p-1)(e-1)/2$. The following description of it is useful.

Lemma 3.8. *The set E of (3.7) is the image of*

$$\left\{ei + j + 1 \colon 0 \leq i \leq p-2,\ 0 \leq j < e\left(\frac{p-1-i}{p}\right) - 1\right\}$$

Proof. By definition E is the image of

$$\bigcup_{0 \leq i \leq p-2} \{ei + j + 1 \colon ei \leq ei + pj < (p-1)(e-1) - 1\}$$

We have

$$\begin{aligned} ei+pj &< pe-p-e+1-1 = m-p \\ pj &< (p-1-i)e-p \\ j &< e\left(\frac{p-1-i}{p}\right)-1, \end{aligned}$$

and the result follows. □

Thus for $k \in E$, the values of i and j are uniquely determined. We will denote $\psi_{i,j}$ and $g_{i,j}$ by ψ_{ei+j+1} and g_{ei+j+1} respectively. Let $h_{s,t} \in \mathbf{Z}\langle\langle T\rangle\rangle$ denote the coefficient in the tth column of the sth row of $H(p,f)$, where it is understood that some rows and columns are empty. Thus we have

Lemma 3.9. *With notation as above, $h_{s,t}$ (for appropriate s and t) is nonzero only if*

$$s \equiv p^n t \bmod (m)$$

for some integer n, and in that case

$$h_{s,t} = \sum_{n\geq 0} h_{s,t,n}T^n,$$

where the sum is over all such nonnegative integers n.

This implies that $H(p,f)$ has a block decomposition as follows. The pth power map acts on the group $\mathbf{Z}/(m) \cong \mu_m$ of eigenvalues. The set $E \subset \mu_m$ is the union of its intersections with the orbits of the action on μ_m. The cardinality of each orbit is a divisor of $(p-1)f$. Each nonempty intersection of cardinality g' corresponds to a $g' \times g'$ factor of $H(p,f)$, and hence to a g'-dimensional formal summand of the Jacobian $J(p,f)$.

Example 3.10. *Consider the case $(p,f) = (3,2)$, for which $m = 16$. The values of $ei+j+1$ for the integrals of the seven holomorphic 1-forms $\omega_{i,j}$ listed in (2.6) are indicated in the following table.*

j	0	1	2	3	4
$i=0$	1	2	3	4	5
$i=1$	9	10			

Meanwhile, the orbits in $\mathbf{Z}/(m)$ under the multiplication by p include

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

Each value listed in the table is in one of these. The first orbit contains three such elements, and the other orbits contain one each.

It follows that the Honda matrix H (with empty rows and columns omitted) has the form

$$\begin{bmatrix} \widehat{h}_{1,1}(T^4) & 0 & T^3\widehat{h}_{1,3}(T^4) & 0 & 0 & T^2\widehat{h}_{1,9}(T^4) & 0 \\ 0 & \widehat{h}_{2,2}(T^2) & 0 & 0 & 0 & 0 & 0 \\ T\widehat{h}_{3,1}(T^4) & 0 & \widehat{h}_{3,3}(T^4) & 0 & 0 & T^3\widehat{h}_{3,9}(T^4) & 0 \\ 0 & 0 & 0 & \widehat{h}_{4,4}(T^2) & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \widehat{h}_{5,5}(T^4) & 0 & 0 \\ T^2\widehat{h}_{9,1}(T^4) & 0 & T\widehat{h}_{9,3}(T^4) & 0 & 0 & \widehat{h}_{9,9}(T^4) & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \widehat{h}_{10,10}(T^2) \end{bmatrix}$$

where each power series $\widehat{h}_{i,i}$ *has constant term* p*, so*

$$\begin{aligned}\det(H) &= \widehat{h}_{2,2}(T^2)\widehat{h}_{4,4}(T^2)\widehat{h}_{5,5}(T^4)\widehat{h}_{10,10}(T^2)D,\\ \text{where } D &= \widehat{h}_{1,1}(T^4)\widehat{h}_{3,3}(T^4)\widehat{h}_{9,9}(T^4) + T^8\widehat{h}_{1,3}(T^4)\widehat{h}_{3,9}(T^4)\widehat{h}_{9,1}(T^4)\\ &\quad +T^4\widehat{h}_{1,9}(T^4)\widehat{h}_{3,1}(T^4)\widehat{h}_{9,3}(T^4) - T^4\widehat{h}_{9,1}(T^4)\widehat{h}_{3,3}(T^4)\widehat{h}_{1,9}(T^4)\\ &\quad -T^4\widehat{h}_{9,3}(T^4)\widehat{h}_{3,9}(T^4)\widehat{h}_{1,1}(T^4) - T^4\widehat{h}_{9,9}(T^4)\widehat{h}_{3,1}(T^4)\widehat{h}_{1,3}(T^4).\end{aligned}$$

We will study this by computing the various factors modulo $(3, T^n)$ *for appropriate* n*. Recall that* H *is congruent to* $3I_7$ *modulo* T*, so*

$$\begin{aligned}\widehat{h}_{2,2}(T^2) &\equiv h_{2,2,2}T^2 && \bmod(3,\, T^4),\\ \widehat{h}_{4,4}(T^2) &\equiv h_{4,4,2}T^2 && \bmod(3,\, T^4),\\ \widehat{h}_{5,5}(T^2) &\equiv h_{5,5,4}T^4 && \bmod(3,\, T^8),\\ \widehat{h}_{10,10}(T^2) &\equiv h_{10,10,2}T^2 && \bmod(3,\, T^4),\\ \text{and}\quad D &\equiv h_{1,3,0}h_{3,9,0}h_{9,1,0}T^4 && \bmod(3,\, T^8)\\ \text{so}\quad \det(H) &\equiv h_{2,2,2}h_{4,4,2}h_{5,5,4}h_{10,10,2}h_{1,3,0}h_{3,9,0}h_{9,1,0}T^{14} && \bmod(3,\, T^{16}),\end{aligned}$$

where the 3-adic integer $h_{i,j,k}$ *is the coefficient of* T^k *in the matrix entry* $h_{i,j}$*.*

On the other hand by Theorem 3.1(iii), $\det(H)$ *is the characteristic polynomial of the Frobenius, so by Theorem 2.3(ii) it must have the form*

$$T^{14} + \cdots + 3^7.$$

It follows that $h_{5,5,4}$ *is a unit, which gives us the desired 1-dimensional formal summand of height 4.*

In order to generalize the calculation above we need the following three easy lemmas.

Lemma 3.11. *Each orbit of* $\mathbf{Z}/(m)$ *other than* $\{ei\}$ *for* $0 \le i \le p-2$ *has a nonempty intersection with* E*. If* a *is in such an orbit, then* $a \in E$ *iff* $m - a \notin E$*.*

Lemma 3.11 is needed for the following.

Lemma 3.12. *The determinant of a block of the Honda matrix* $H(p, f)$ *associated with an orbit of cardinality* n *is congruent to an integer multiple of* T^n *modulo* $(p,\, T^{n+1})$*, and the sum of all such cardinalities is* $2g$*.*

Lemma 3.13. *The orbit of* $(m-1)$ *has* $(p-1)f$ *elements, but its intersection with* E *has only one element, namely* $(m-1)/p$*.*

Lemma 3.12 impies that $\det(H(p,f))$ is congruent to an integer multiple of T^{2g} modulo $(p,\, T^{2g+1})$. By Theorems 3.1(iii) and 2.3(ii), the coefficient of T^{2g} is 1, so the coefficients in 3.12 are all units. In particular the one for the orbit of $(m-1)/p$ is a unit, which gives us the desired 1-dimensional formal summand of height $(p-1)f$. This completes our alternate proof of Theorem 1.2.

Proof of Lemma 3.11. The only singleton orbits are the ones cited since $pk \equiv x$ modulo (m) implies that k is a multiple of e. These orbits do not intersect E.

Given k not divisible by e with $0 < k < m$, we write $k = ei + j + 1$ and $e - k = ei' + j' + 1$. Then $i' = p - 2 - i$ and $j' = e - 1 - j$. Now $k \in E$ iff

$$\begin{aligned}0 \le \quad j \quad &< e\left(\frac{p-1-i}{p}\right)\\ e-1 \ge \quad j' \quad &> e\left(\frac{p-1-i}{p}\right) - 1 = e\left(\frac{p-1-i'}{p}\right) - 1\end{aligned}$$

which holds iff $m - e \notin E$. □

Proof of Lemma 3.12. Suppose $e_1 \in E$ is in such an orbit. Define elements e_i inductively by letting $e_{i+1} \in E$ be congruent modulo (m) to $p^k e_i$ for the smallest possible positive value of k. Hence the intersection of the orbit with E has the form

$$\{e_1, e_2, \dots e_s\}$$

with $e_{i+1} \equiv p^{k_i} e_i$ for $1 \le i < s$, and $e_1 \equiv p^{k_s} e_s$. The cardinality n of the orbit is $\sum k_i$. The entries in the corresponding block of $H(p,f)$ are

$$h_{e_i,e_j} = \begin{cases} T^{k_i+\cdots+k_{j-1}}\widehat{h}_{e_i,e_j}(T^n) & \text{if} \quad i \le j \\ T^{n-k_j-\cdots-k_{i-1}}\widehat{h}_{e_i,e_j}(T^n) & \text{if} \quad j < i \end{cases}$$

Since $h_{e_i,e_i,0} = 0$, it follows that the determinant of this block is congruent to

$$h_{e_1,e_2,k_1} h_{e_2,e_3,k_2} \cdots h_{e_{s-1},e_s,k_{s-1}} h_{e_s,e_1,k_s} T^n$$

modulo (p, T^{2n}) as desired.

To find the sum of the cardinalities, we need Lemma 3.11. If an orbit intersecting E is self-conjugate, that is it contains both a and $-a$, then 3.11 implies that exactly half the elements in the orbit are in E. Otherwise if s out of n elements of an orbit are in E, then E also contains $n-s$ elements in the conjugate orbit. In either case half of the elements in the union of an intersecting orbit and its conjugate are in E. Since E has g elements, the sum of the cardinalities is $2g$. □

Proof of Lemma 3.13. The orbit of 1 is

$$\left\{p^k \colon 0 \le k < (p-1)f\right\} = \left\{p^k + ei \colon 0 \le k < f,\, 0 \le i \le p-2\right\}$$

since modulo (m)

$$p^{f+k}(d+1)p^k \equiv e + p^k.$$

It follows that the orbit of $m-1$ is

$$\left\{e - p^k - ei \colon 0 \le k < f,\, 0 \le i \le p-2\right\} = \left\{ei + e - p^k \colon 0 \le k < f,\, 0 \le i \le p-2\right\},$$

which has $(p-1)f$ elements. $(m-1)/p$ is among them since

$$\frac{m-1}{p} = p^f - p^{f-1} - 1 = e - p^{f-1}.$$

We need to show that no other elements of this orbit are in E. Using 3.8 we see that $ei + e - p^k$ is in E only if

$$\begin{aligned} e - p^k &< e\left(\frac{p-1-i}{p}\right) \\ -p^k &< e\left(\frac{-1-i}{p}\right) \\ p^k &> e\left(\frac{i+1}{p}\right), \end{aligned}$$

which means $i = 0$ and $k = f-1$. □

References

[AHS01] M. Ando, M. J. Hopkins, and N. P. Strickland. Elliptic spectra, the Witten genus and the theorem of the cube. *Invent. Math.*, 146(3):595–687, 2001.

[Del74] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[Del80] Pierre Deligne. La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.*, (52):137–252, 1980.

[Die55] Jean Dieudonné. Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$. IV. *Amer. J. Math.*, 77:429–452, 1955.

[Die57] Jean Dieudonné. Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$. VII. *Math. Ann.*, 134:114–133, 1957.

[Dwo60] Bernard Dwork. On the rationality of the zeta function of an algebraic variety. *Amer. J. Math.*, 82:631–648, 1960.

[GM00] V. Gorbounov and M. Mahowald. Formal completion of the Jacobians of plane curves and higher real K-theories. *J. Pure Appl. Algebra*, 145(3):293–308, 2000.

[Gro77] *Cohomologie l-adique et fonctions L*. Springer-Verlag, Berlin, 1977. Séminaire de Géometrie Algébrique du Bois-Marie 1965–1966 (SGA 5), Edité par Luc Illusie, Lecture Notes in Mathematics, Vol. 589.

[Gro95] Alexander Grothendieck. Formule de Lefschetz et rationalité des fonctions L. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 279, 41–55. Soc. Math. France, Paris, 1995.

[Haz78] M. Hazewinkel. *Formal Groups and Applications*. Academic Press, New York, 1978.

[HD34] H. Hasse and H. Davenport. Die Nullstellensatz der Kongruenz zeta-funktionen in gewissn zyklischen Fällen. *J. Reine Angew. Math.*, 172:151–182, 1934.

[HM] M. J. Hopkins and M. A. Mahowald. From elliptic curves to homotopy theory. Preprint in Hopf archive at `http://hopf.math.purdue.edu/Hopkins-Mahowald/eo2homotopy`.

[Hon68] Taira Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20:83–95, 1968.

[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.

[Ill79] Luc Illusie. Complexe de de Rham-Witt et cohomologie cristalline. *Ann. Sci. École Norm. Sup. (4)*, 12(4):501–661, 1979.

[Kat76] Nicholas M. Katz. An overview of Deligne's work on Hilbert's twenty-first problem. In *Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974)*, pages 537–557. Amer. Math. Soc., Providence, R. I., 1976.

[Kat81] Nicholas M. Katz. Crystalline cohomology, Dieudonné modules, and Jacobi sums. In *Automorphic forms, representation theory and arithmetic (Bombay, 1979)*, volume 10 of *Tata Inst. Fund. Res. Studies in Math.*, pages 165–246. Tata Inst. Fundamental Res., Bombay, 1981.

[Kob80] Neal Koblitz. *p-adic analysis: a short course on recent work*, volume 46 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1980.

[Lan76] P. S. Landweber. Homological properties of comodules over $MU_*(MU)$ and $BP_*(BP)$. *American Journal of Mathematics*, 98:591–610, 1976.

[LRS95] P. S. Landweber, D. C. Ravenel, and R. E. Stong. Periodic cohomology theories defined by elliptic curves. In Mila Cenkl and Haynes Miller, editors, *The Čech Centennial*, volume 181 of *Contemporary Mathematics*, pages 317–338, Providence, Rhode Island, 1995. American Mathematical Society.

[Lub68] Saul Lubkin. A p-adic proof of Weil's conjectures. *Ann. of Math. (2) 87 (1968), 105-194; ibid. (2)*, 87:195–255, 1968.

[Man63] Ju. I. Manin. Theory of commutative formal groups over fields of finite characteristic. *Uspehi Mat. Nauk*, 18(6 (114)):3–90, 1963.

[Maz75] B. Mazur. Eigenvalues of Frobenius acting on algebraic varieties over finite fields. In *Algebraic geometry (Proc. Sympos. Pure Math., Vol. 29, Humboldt State Univ., Arcata, Calif., 1974)*, pages 231–261. Amer. Math. Soc., Providence, R.I., 1975.

[MM74] B. Mazur and William Messing. *Universal extensions and one dimensional crystalline cohomology*. Springer-Verlag, Berlin, 1974. Lecture Notes in Mathematics, Vol. 370.

[Qui69] D. G. Quillen. On the formal group laws of oriented and unoriented cobordism theory. *Bulletin of the American Mathematical Society*, 75:1293–1298, 1969.

[SGA73] *Théorie des topos et cohomologie étale des schémas. Tome 3*. Springer-Verlag, Berlin, 1973. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de P. Deligne et B. Saint-Donat, Lecture Notes in Mathematics, Vol. 305.

[Sti90] L. Stickelberger. Über eine Verallgemeinerung der Kreistheilung. *Mathematische Annalen*, 37:321–367, 1890.

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[Wei48] André Weil. *Variétés abéliennes et courbes algébriques*. Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.

[Wei49] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.

University of Rochester, Rochester, NY 14627