Inventiones math. 12, 321–336 (1971)

Formal Groups and Zeta-Functions of Elliptic Curves

WALTER L. HILL (Princeton)

Abstract. The author shows that the isomorphism class of a formal group over Z/pZ (resp. over Z_p) of finite height (resp. having reduction mod p of finite height) is determined by its characteristic polynomial. It is then proved that the formal groups associated to a large class of Dirichlet series with integer coefficients are defined over Z.

Finally, these results are used to extend a theorem of Honda (Osaka J. Math. **5**, 199–213 (1968), Theorem 5) to include the case of supersingular reduction at the primes 2 and 3. Let E be an elliptic curve defined over Q, and $F(x, y)$ be a formal minimal model for E. Let $G(x, y)$ be the formal group associated to the global L-series $L(E, s)$ of E over Q. Honda's theorem now becomes: *$G(x, y)$ is defined over Z and is isomorphic over Z to $F(x, y)$.*

Introduction

In a recent paper, Honda [5] has shown that there is a close connection between certain arithmetically interesting Dirichlet series and the formal completions of certain one-dimensional algebraic groups. In particular, he shows [5; Theorem 5] that if E is an elliptic curve defined over Q satisfying certain conditions at the primes 2 and 3, then the formal group associated (as described in Section 4 below) to its L-series is defined over Z and furthermore is isomorphic over Z to the formal completion of the group law of E.

The work presented in this paper began as an attempt to prove Honda's theorem without those troublesome conditions on the behavior of E at the primes 2 and 3. The effort was fruitful and the blemish removed (cf. Theorem H). The essential difficulty which had to be overcome is that in the case of supersingular reduction, it is impossible to lift the Frobenius endomorphism back to characteristic zero. Honda was able to cope with this nemesis for primes bigger than 3 by noticing that in that case, the Riemann hypothesis for curves (see Section 2) forces the square of the Frobenius to lift. I succeeded in avoiding this problem by introducing a "virtual" lifting of the Frobenius; this is simply the power series x^p which reduces mod p to the Frobenius all right, but of course isn't an endomorphism of the formal group law of E. Together with a further refinement of the all-important lemma of Lubin-Tate [9], the virtual lifting provides the key to proving the integrality statements in a much broader context.

In order to extend this method to more general Dirichlet series with Euler product, it also became necessary to construct integral group laws to play the role of the formal group law of the elliptic curve. To do this I had to prove certain basic results on formal groups which are themselves quite interesting; they seem to be new—indeed, one of them gives a complete description of the isomorphism classes of formal groups over the ring of p-adic integers, which in turn yields Honda's theorem without further ado.

Section 1 contains a review of several definitions and the technique from the theory of formal groups, due mainly to Lazard and Lubin, which is needed in the later sections. In Section 2 we define some of the important invariants of an elliptic curve over a numberfield and mention some results and conjectures concerning them. The purpose of this section is mainly to point up the importance of the L-series in investigating the arithmetic of elliptic curves. In particular we state the conjecture of Birch and Swinnerton-Dyer on the relation between the behavior at $s=1$ of the L-series of an elliptic curve over Q and the numerical arithmetic invariants of the curve. We proceed then in Section 3 to classify the isomorphism classes of formal groups over the p-adic integers and over the prime fields in non-zero characteristic. In particular, we show the existence of a formal group over the p-adic integers whose associated characteristic polynomial (i.e. the characteristic polynomial of the Frobenius endomorphism of its reduction $\bmod p$) is any preassigned Eisenstein polynomial. This is crucial for the proof of Theorem F of Section 4. In Section 4 we prove that the formal groups of a large class of Dirichlet series with Euler product are integral and show when two are isomorphic. We piece together the local results to get a fairly good picture of the set of isomorphism classes of formal groups over Z. This gives a significant extension of Honda's results.

1. Preliminaries on Formal Groups

I include in this section only a sketch of the results needed in Sections 3 and 4. For a more thorough treatment of the theory of formal groups, the papers of Lazard [7] and Lubin [8] are quite helpful. Their approach is a bit different from that of Honda [5], which I follow here, but their exposition of the basics is more detailed.

1. Let R be a commutative ring with identity element and denote by $R[[x_1, x_2, \dots, x_n]]$ the ring of powerseries in n variables over R. For f and g in $R[[x_1, x_2, \dots, x_n]]$, write $f \equiv g \bmod \deg k$ if $f-g$ contains no monomials of total degree less than k

A *formal group* (sometimes a *formal group law* or simply *group law*) over R will always mean a commutative one-parameter formal group over R, i.e. a powerseries in two variables $F(x,y)$ with coefficients in R satisfying the following axioms:

FG 1) $F(x,y) \equiv x+y \bmod \deg 2$.

FG 2) $F(F(x,y),z) = F(x, F(y,z))$.

FG 3) $F(x,y) = F(y,x)$.

The condition FG 3) is very mild, for as is well known, if R has no nilpotents, FG 3) always holds (cf. [6]).

The easiest examples of formal groups are the *additive group* $G_a(x,y) = x+y$, and the *multiplicative group* $G_m(x,y) = x+y+xy$ which are defined over any ring R. In most other cases it is singularly unenlightening to write down the powerseries explicitly. In the next paragraph we will see how to generate all the formal groups over any Q-algebra. The most important examples of formal groups are gotten as follows: let G be a one-dimensional group variety over a field k. The group operation $G \times G \xrightarrow{\mu} G$ induces a map on local rings $\mathfrak{O}_e \xrightarrow{\mu^*} \mathfrak{O}_e \otimes \mathfrak{O}_e$, and thus a map on the completions $\hat{\mathfrak{O}}_e \xrightarrow{\hat{\mu}^*} \mathfrak{O}_e \hat{\otimes} \mathfrak{O}_e$ which are powerseries ring: $\hat{\mathfrak{O}}_e \simeq k[[t]]$ since G is non-singular. Identifying $\mathfrak{O}_e \hat{\otimes} \mathfrak{O}_e \simeq k[[x,y]]$ and setting $F(x,y) = \hat{\mu}^*(t)$, one can check that the group axioms for G force F to satisfy conditions FG 1) through FG 3).

If $F(x,y)$ and $G(x,y)$ are formal groups over R, an *R-homomorphism* from F to G is a powerseries $f(x) \in R[[x]]$ without constant term such that $f(F(x,y)) = G(f(x), f(y))$. Say f is a *weak isomorphism* if it has a two-sided inverse; an *isomorphism* is a weak isomorphism f with $f \equiv x \bmod \deg 2$. (Honda calls such an f a "strong isomorphism" in [5]. However, as it is the only notion of equivalence between formal groups considered in this paper, I have taken the liberty of dropping the adjective.) Axiom FG 3) assures that the set $\mathrm{Hom}_R(F,G)$ of R-homomorphisms from F to G is naturally an abelian group with addition defined by $(f+g)(x) = G(f(x), g(x))$. In the usual way then, $\mathrm{End}_R(F)$ is a ring with identity element (but not necessarily commutative). If R has no zero divisors, then neither does $\mathrm{End}_R(F)$. The function from $\mathrm{Hom}_R(F,G)$ to R which sends $f(x) = ax + \cdots$ to a is a group homomorphism; a ring homomorphism if $F=G$. Call this map $c(f)$.

2. If R is a Q-algebra, one can show [5, 7] that all formal groups over R are isomorphic. In fact, any $s(x) = 1 + a_1 x + \cdots$ in $R[[x]]$ gives rise to a formal group F_s on which $s(x)\,dx$ may be interpreted as the "canonical invariant differential" as follows: let $f(x) = x + \frac{1}{2} a_1 x^2 + \cdots$ and define $F_s(x,y) = f^{-1}(f(x)+f(y))$. (Note that f is an isomorphism from F_s to G_a.) Honda shows [5; Prop. 2] that any group law F over R (N.B. It is imperative here that R be a Q-algebra) is of the form F_s

where

$$s(x)=\left[\frac{\partial}{\partial x}F(0,z)\right]^{-1}.$$

It is important to note that over an integral domain R of characteristic zero, the map c: $\mathrm{Hom}_R(F,G)\to R$ is always injective. If we let K denote the quotient field of R, the K-endomorphisms of the additive group G_a are just the powerseries of the form ax with $a\in K$. A pair of K-isomorphisms from G_a to F and from G to G_a induce an isomorphism

$$\mathrm{Hom}_K(F,G)\xrightarrow{\sim}\mathrm{End}_K(G_a)\xrightarrow{\underline{c}}K$$

commuting with c. Since the vertical arrows in the diagram

$$\begin{array}{ccc}\mathrm{Hom}_R(F,G) & \xrightarrow{c} & R\\ \downarrow & & \downarrow\\ \mathrm{Hom}_K(F,G) & \xrightarrow{\underline{c}} & K\end{array}$$

are injective, so is the top one. Thus $\mathrm{Hom}_R(F,G)$ is canonically identified by means of c with a subgroup of R, $\mathrm{End}_R(F)$ with a subring of R. In the latter case, if $f\in\mathrm{End}_R(F)$ and $c(f)=a$, we will use the notation $f=[a]_F$. Of course, the notation $[n]_F$, $n\in Z$ makes sense for any formal group over any ring R. If moreover, R is a discrete valuation ring, then $c(\mathrm{Hom}_R(F,G))$ is a closed subgroup ([8]).

3. The situation is quite different in non-zero characteristic. The fundamental fact here [7, 8] is that if k is a field of characteristic $p>0$, F and G formal groups over k, and $\varphi\in\mathrm{Hom}_k(F,C)$, $\varphi\neq 0$, then $\varphi(x)\equiv a x^q \bmod \deg q+1$ for some $a\neq 0$, $q=p^r$ and $\varphi(x)$ is a powerseries in x^q. In particular, either $[p]_F=a x^{p^h}+\cdots$, $a\neq 0$, in which case we call h the *height* of F, or else $[p]_F=0$ and we then say that the height of F is *infinite*. Viewed as a subspace of $k[[x]]$ with the usual valuation topology, $\mathrm{Hom}_k(F,G)$ is a complete topological group, $\mathrm{End}_k(F)$ a complete topological ring (cf. [8]). As we have already noted, $\mathrm{End}_k(F)$ has no zero divisors. Consider the map from Z to $\mathrm{End}_k(F)$ sending n to $[n]_F$. Since $[n]_F\equiv n x \bmod \deg 2$, we see that the characteristic of $\mathrm{End}_k(F)$ is either zero—when F has finite height or else the same as that of k—when the height of F is infinite. If F has finite height, $\mathrm{End}_k(F)$ contains Z, and being complete, $\mathrm{End}_k(F)$ contains the ring Z_p of p-adic integers ($[p]_F\equiv a x^{p^h} \bmod \deg p^h+1$, $h>0$ shows that the valuation topology on $\mathrm{End}_k(F)$ induces the p-adic topology on Z). It is a classical result of Dieudonne [3] that over an algebraically closed field k of characteristic $p>0$, if F is a formal group over k with finite height h, then $\mathrm{End}_k(R)$ is the maximal order in the central division algebra with invariant $1/h$ over the field Q_p of p-adic rationals. Thus if $f\in\mathrm{End}_k(F)$,

f satisfies a monic irreducible polynomial of degree $\leqq h$ over Z_p, its *characteristic polynomial*. If k is a finite field with $q=p^r$ elements and F is a formal group over k having finite height, then the powerseries x^q is an endomorphism of F, called the *Frobenius endomorphism* of F over k. To simplify terminology, we define the *characteristic polynomial of* F over k to be that of its Frobenius. If F is instead a formal group over a $\mathfrak{p}$-adic integer ring $\mathfrak{o}$ which when reduced mod $\mathfrak{p}$ has finite height, the characteristic polynomial of F over $\mathfrak{o}$ will just mean the characteristic polynomial of $F/\mathfrak{p}$ over $\mathfrak{o}/\mathfrak{p}$.

4. The category $\mathscr{F}_R$ of formal groups over a ring R is an additive category and if $\varphi\colon R\to S$ is a ring homomorphism, then the natural extension to the powerseries $\tilde{\varphi}\colon R[[x,y]]\to S[[x,y]]$ sending

$$f(x,y)=a_{00}+a_{10}\,x+a_{01}\,y+\cdots$$

to

$$f^{\varphi}(x,y)=\varphi(a_{00})+\varphi(a_{10})\,x+\varphi(a_{01})\,y+\cdots$$

induces an additive functor $\mathscr{F}_R \rightsquigarrow \mathscr{F}_S$. Lazard's theorem (Theorem 1 below) says that if φ is an epimorphism, then the function from objects of $\mathscr{F}_R$ to objects of $\mathscr{F}_S$ is surjective. It is definitely false that every morphism of $\mathscr{F}_S$ can be lifted to a morphism of $\mathscr{F}_R$. For example, if F is a formal group over Z/pZ, then $\mathrm{End}_{Z/pZ}(F)$ contains Z_p as long as F has finite height, whereas for any lifting $\tilde{F}$ of F to Z, $\mathrm{End}_Z(F)=Z$. In fact, if the height of F is at least 2 and $\tilde{F}$ is any lifting of F to Z, then the Frobenius endomorphism of F cannot lift to an endomorphism of $\tilde{F}$ over any ring in characteristic zero (this is caused by the inability of $\tilde{F}$ to distinguish between a given lifting and a conjugate lifting). An important example of this phenomenon occurs in studying the completions of elliptic curves over Q at primes where the reduction is supersingular. In certain cases one can however conclude that the map $\mathrm{End}_R(F)\to\mathrm{End}_S(F^{\varphi})$ is injective. This is true, for example, if R is a $\mathfrak{p}$-adic integer ring and S its residue field, as long as F^{φ} has finite height (Lubin [8]).

An immediate consequence of Lazard's fundamental paper [7] is the following general lifting theorem, which is indispensible in Section 4.

Theorem 1. *Let $\varphi\colon R\to S$ be a ring epimorphism, and let F be a formal group over S. Then there exists a formal group $\tilde{F}$ over R such that $\tilde{F}^{\varphi}=F$.*

5. The following seemingly innocent lemma of Lubin and Tate [9] gives a remarkably powerful method both for constructing powerseries satisfying certain conditions, and showing (by uniqueness) that a powerseries satisfying those conditions must have its coefficients in a certain ring, i.e. the desired powerseries not only *can* be constructed with coefficients in the ring, but in fact its coefficients *must* be in the ring.

Lemma 2 ([9]). *Let* $\mathfrak{o}$ *be a discrete valuation ring having a finite residue field with* q *elements,* π *a prime element of* $\mathfrak{o}$. *Moreover, let* $f(x)$ *and* $g(x)$ *be powerseries over* $\mathfrak{o}$ *such that*

$$f(x) \equiv g(x) \equiv x^q \bmod \pi \quad \textit{and} \quad f(x) \equiv g(x) \equiv \pi x \bmod \deg 2.$$

Finally, let $L(x_1, \ldots, x_n) = a_1 x_1 + \cdots + a_n x_n$ be a linear form with coefficients in $\mathfrak{o}$. Then there exists a unique powerseries $F(x_1, \ldots, x_n)$ in $\mathfrak{o}[[x_1, \ldots, x_n]]$ satisfying the following conditions:

1. $F(x_1, \ldots, x_n) \equiv L(x_1, \ldots, x_n) \bmod \deg 2$.
2. $f(F(x_1, \ldots, x_n)) = F(g(x_1), \ldots, g(x_n))$.

The method of proof is straightforward; a judicious extension of this method, where condition 2. is replaced by a more delicate one, is used in the proof of Theorem E in Section 3.

Theorem 3 ([9]). *Let* $\mathfrak{o}$ *be a discrete valuation ring having a finite residue field with* q *elements,* π *a prime element of* $\mathfrak{o}$, *and* $f(x) \in \mathfrak{o}[[x]]$ *such that* $f(x) \equiv x^q \bmod \pi$ *and* $f(x) \equiv \pi x \bmod \deg 2$. *Then there is a unique formal group* F_f *over* $\mathfrak{o}$ *such that* $f \in \mathrm{End}_{\mathfrak{o}}(F_f)$.

To prove this, apply Lemma 2 twice: first with $L(x, y) = x + y$ to get F_f, then with $L(x, y, z) = x + y + z$ to show that F_f is associative. Since $\mathfrak{o}$ is a domain, F_f is automatically commutative ([6]).

6. Finally, we state Honda's useful congruence formula:

Lemma 4. *Let* π *be a prime element in a* $\mathfrak{p}$-adic *integer ring* $\mathfrak{o}$, $\mathfrak{p} = \pi\mathfrak{o}$. *Then for all integers* $v \geqq 0$, $a \geqq 1$, $m \geqq 1$,

$$\pi^{-v}(X + \pi Y)^{mp^{av}} \equiv \pi^{-v} X^{mp^{av}} \qquad (\bmod \mathfrak{p}).$$

The proof (see [5]) amounts to showing that the binomial coefficients $\binom{p^v}{i}$ are sufficiently divisible by p.

This formula enabled Honda to use the recursion formulas for the coefficients of the L-series he considered to prove a congruence formula for a certain endomorphism of their associated formal group. In Section 4, this same method is applied to virtual liftings.

2. Global L-Series of Elliptic Curves over a Numberfield

1. Let k be a finite field with $q = p^r$ elements. Any non-singular projective curve C of genus g defined over k determines in a natural way a sequence of integers $c_1, c_2, \ldots$ where c_n is the number of points of C defined over the extension k_n of k of degree n. Weil [12] defines the *zeta*-function $Z(C, x)$ of C over k by the formula

$$d[\log Z(x)] = \sum_{n=1}^{\infty} c_n x^n \frac{dx}{x}, \qquad Z(x) = Z(C, x),$$

and shows that Z is a *rational function* of x satisfying the *functional equation*

$$Z\left(\frac{1}{q\,x}\right)=q^{1-g}\,x^{2-2g}\,Z(x).$$

In fact, $Z(x)=\dfrac{P(x)}{(1-x)(1-q\,x)}$ where $P(x)$ is a polynomial of degree $2g$ with integer coefficients and has the form

$$P(x)=q^g\,x^{2g}+\cdots+a_1\,x+1.$$

The polynomial $x^{2g}P(1/x)$ can be interpreted as the characteristic polynomial of the Frobenius correspondence on C. This fact is the key link between the L-series we are about to define and the formal group laws of elliptic curves.

The *Riemann hypothesis* for $Z(x)$ states that the roots of $x^{2g}P(1/x)$ all have absolute value $q^{\frac{1}{2}}$, or equivalently

$$|1+q^n-c_n|\leqq 2g\,q^{n/2} \qquad \text{(cf. Weil [12]).}$$

When $g=1$, which is the only case of interest to us hereafter, $P(x)$ has the form $(1-\pi_1\,x)(1-\pi_2\,x)$ where π_1 and π_2 are conjugate complex numbers and $\pi_1\,\pi_2=p$.

2. By an *elliptic curve* over a field k we mean a one-dimensional abelian variety defined over k, i.e. a genus 1 curve defined over k having a k-rational point. If the characteristic of k is not 2 or 3, an elliptic curve E over k is always isomorphic over k to a plane curve C of the form

$$y^2\,z=4x^3-a\,x\,z^2-b\,z^3 \qquad a,b\in k \tag{1}$$

where the cubic $4x^3-a\,x-b$ has distinct roots. In this case C is called a *Weierstrass model* for E.

When $k=Q$, our needs require, however, a finer model which can be reduced mod any prime p, with the reduction as non-singular as possible.

$$F(x,y)=y^2+l\,x\,y+m\,y+x^3+a\,x^2+b\,x+c \tag{2}$$

is called a *global minimal Weierstrass model* for E if $l,m,a,b,c\in Z$, and the discriminant Δ of F is as small as possible. Such an F exists and is essentially unique (cf. [10]). In this case the reduction of F mod any prime is irreducible.

Letting $t=x/y$ be a local parameter at $\mathbf{o}$ on the global minimal Weierstrass model F, and expanding the group law as a powerseries in t_1 and t_2, we get a powerseries in two variables $G(t_1,t_2)$ with integer coefficients. We call $G(t_1,t_2)$ a *formal minimal model* for E over Z.

Now to define the L-series: If the reduction of F at p is non-singular (i.e. $p \nmid \Delta$), define the *L-series of E at p* to be

$$\begin{aligned} L_p(E, s) &= (1-p^{-s})^{-1}(1-p^{1-s})^{-1}(Z(F/p, p^{-s}))^{-1} \\ &= (1-a_p p^{-s}+p^{1-2s})^{-1}. \end{aligned}$$

When the reduction is singular, there are three possibilities:

1. The singular point is a cusp. E is then said to have *additive reduction* at p, and we set $L_p(E, s)=1$.

2. The singular point is an ordinary double point with tangents rational over Z/pZ. Call such a reduction *strongly multiplicative*, and set $L_p(E, s)=(1-p^{-s})^{-1}$.

3. The singular point is an ordinary double point with tangents not defined over Z/pZ. In this case, say E has *weakly multiplicative reduction* at p and set $L_p(s)=(1+p^{-s})^{-1}$.

The *global L-series* of E over Q is then defined as

$$L(E, s)=\prod_p L_p(E, s). \tag{3}$$

The product converges in the halfplane $\operatorname{Re}(s)>\frac{3}{2}$. Weil has conjectured that $L(E, s)$ has an analytic continuation to the whole plane and satisfies a functional equation. This has been proved for certain classes of curves (see Deuring [2], Eichler [4], and Shimura [11]). Theorem H in Section 4 shows why these factors at the primes for which the reduction is singular are the "right" ones.

If E is an elliptic curve over any field k, the set E_k of points of E defined over k forms an abelian group. The Mordell-Weil theorem shows that if k is a numberfield, then the group E_k is finitely generated. From the point of view of diophantine equations, i.e. finding all the solutions in the field of a given equation of the form (1), computing the rank g of the group E_k presents the greatest difficulty. The conjectures of Birch, Swinnerton-Dyer, and Tate (cf. [1]) would allow one to identify g as the order of vanishing at $s=1$ of $L(E, s)$.

3. The Classification of Formal Groups over Z_p and Z/pZ up to Isomorphism

The main results of this section are that over Z/pZ the isomorphism class of a formal group of finite height is completely determined by its characteristic polynomial, and that over Z_p, if the reduction of a formal group has finite height, then its isomorphism class is completely determined by its characteristic polynomial. Moreover, a polynomial over Z_p is the characteristic polynomial of some formal group over Z/pZ (or over Z_p) if and only if it is Eisenstein. The case $h=\infty$ is easy: any formal group over Z/pZ of infinite height is isomorphic over

Z/pZ to the additive group $G_a(x,y)=x+y$, and any formal group over Z_p with reduction of infinite height is isomorphic over Z_p to $G_a(x,y)$.

The program for obtaining these results runs as follows: after checking that the set of characteristic polynomials of formal groups over Z/pZ coincides with the set of Eisenstein polynomials over Z_p, take two formal groups F and G over Z_p with the same characteristic polynomial. Since their characteristic polynomials are Eisenstein, an extension of the Lubin-Tate method [9] shows that the Q_p-isomorphism from F to G is actually defined over Z_p. Lazard's lifting theorem then provides the complete classification over both Z_p and Z/pZ. The point about infinite height is taken care of by Lemma A and its corollary.

Lemma A. *Let F be a formal group over Z_p such that $F \bmod p$ has infinite height. Then F is isomorphic over Z_p to $G_a(x,y)$.*

Proof. Write $F(x,y)=f^{-1}(f(x)+f(y))$ where f is the unique element of $\mathrm{Hom}_{Q_p}(F, G_a)$ with $f(x)\equiv x \bmod \deg 2$. Since f is uniquely determined, we know that $d/dz\, f(z)=\left[\frac{\partial}{\partial x}F(0,z)\right]^{-1}$ and this is integral. Thus $f(x)$ has the form $\sum_{n=1}^{\infty} a_n/n\, x^n$ with $a_n \in Z_p$.

Then $[p]_F(x)=f^{-1}(pf(x))\equiv 0 \bmod p$ by assumption. So $f^{-1}(pf(x))=p\,u(x)$ with $u(x)\in Z_p[[x]]$, and thus

$$p f(x)=f(p\,u(x))=p\,u(x)+\sum_{n=2}^{\infty} a_n/n\,(p\,u(x))^n.$$

and

$$f(x)=u(x)+\sum_{n=2}^{\infty} a_n/n\, p^{n-1}(u(x))^n.$$

Therefore $f(x)\in Z_p[[x]]$ and we are done.

Corollary B. *Let F have infinite height over Z/pZ. Then F is isomorphic over Z/pZ to G_a.*

Proof. Lift F to a formal group $\tilde{F}$ over Z_p, and let f be the isomorphism over Z_p from $\tilde{F}$ to G_a. Then f reduces mod p to an isomorphism F to G_a.

This result is quite old (see Lazard [7], Prop. 6) and holds in greater generality. But the method of proof here is typical of what is to come: first prove that a certain isomorphism has coefficients in Z_p to get the result over Z_p (this is much more delicate when the reduction has finite height) and then use the lifting theorem to get the result over Z/pZ.

Proposition C. *Let F be a formal group over Z/pZ with finite height h. Then the characteristic polynomial of F has degree h and is Eisenstein.*

Proof. Let ζ_F denote the Frobenius endomorphism of F over Z/pZ. Letting $K = Q_p(\zeta_F) \subset \mathrm{End}_k(F) \underset{Z_p}{\otimes} Q_p$ where k denotes the algebraic closure of Z/pZ, we see that ζ_F is a prime element in K since $\mathrm{End}_k(F)$ is the maximal order in the central division algebra $D_{1/h}$ with invariant $1/h$ over Q_p and in any factorization $x^p = u \circ v$ with $u = u(x) = a\,x^m + \cdots$ and $v = v(x) = b\,x^n + \cdots$ in $\mathrm{End}_k(F)$, either m or n is 1, i.e. u or v is invertible. Thus p is a unit times a power of ζ_F. Since $[p]_F$ is a powerseries in x^{p^h}, $[p]_F = u(x^{p^h})$, $u(x) = a\,x + \cdots$, we see that the power is h. So $K = Q_p(\zeta_F)$ is the totally ramified maximal subfield of $D_{1/h}$. Hence the assertion.

Proposition D. *Let $p(x) \in Z_p[x]$ be an Eisenstein polynomial. Then there is a formal group over Z/pZ which has $p(x)$ as its characteristic polynomial.*

Proof. Let π be a root of $p(x)$, $f(x) = \pi\,x + x^p \in Z_p[\pi][[x]]$. Then there is a formal group $F_f(x, y) \in Z_p[\pi][[x, y]]$ for which $f(x)$ is an endomorphism (see Theorem 3 of Section 1).

Since $Q_p(\pi)/Q_p$ is totally ramified, the reduction of $F_f \bmod \pi$ is defined over Z/pZ and has $p(x)$ as its characteristic polynomial, since the Frobenius of $F_f \bmod \pi$ lifts to f, and $c(f) = \pi$.

Theorem E. *Let F and G be formal groups over Z_p having reductions of finite height with the same characteristic polynomial. Then F and G are isomorphic over Z_p.*

Proof. Let $p(x) = x^h + a_{h-1}\,x^{h-1} + \cdots + a_1\,x + a_0$ denote the characteristic polynomial of both F and G. Since $\mathrm{End}_{Z_p}(F)$ and $\mathrm{End}_{Z_p}(G)$ are canonically isomorphic to Z_p via the map c described in paragraphs 1 and 2 of Section 1, $[-a_i]_F(x)$ and $[-a_i]_G(x)$ are defined for $i = 0, 1, \ldots, h-1$.

Form the powerseries

$$\Phi(x) = F\big(\ldots\big(F(F([-a_0]_F(x), [-a_1]_F(x^p)), [-a_2]_F(x^{p^2})), \ldots\big), [-a_{h-1}]_F(x^{p^{h-1}})\big)$$

$$\Psi(x) = G\big(\ldots\big(G(G([-a_0]_G(x), [-a_1]_G(x^p)), [-a_2]_G(x^{p^2})), \ldots\big), [-a_{h-1}]_G(x^{p^{h-1}})\big).$$

So $\Phi(x)$ and $\Psi(x)$ are powerseries over Z_p with $\Phi(x) \equiv \Psi(x) \equiv -a_0\,x \bmod \deg 2$ and $\Phi(x) \equiv \Psi(x) \equiv x^{p^h} \bmod p$. Since $p(x)$ is Eisenstein, $-a_0$ is prime in Z_p.

Now let $f(x) = x + r_2\,x^2 + r_3\,x^3 + \cdots$ be the unique isomorphism from F to G over Q_p. We must show that $f(x)$ is defined over Z_p. Thus $f(F(x, y)) = G(f(x), f(y))$ and f is Z_p-linear, i.e. for all $a \in Z_p$, $f([a]_F(x)) = [a]_G(f(x))$, and thus $f([-a_i]_F(x^{p^i})) = [-a_i]_G(f(x^{p^i}))$ $i = 0, 1, \ldots, h-1$.

Hence we have

$$f(\Phi(x)) = G(\dots G([-a_{0G}](f(x)), [-a_1]_G(f(x^p))), \dots, [-a_{h-1}]_G(f(x^{p^{h-1}}))). \tag{1}$$

We now show inductively that the coefficients of f are integral. Noting that the first coefficient of f is 1, suppose that r_i is integral for $i=1, \dots, k$. Form the polynomials $f_n(x) = x + r_2 x^2 + \dots + r_n x^n$, $n = 1, 2, \dots$. So $f_{k+1}(x) = f_k(x) + r_{k+1} x^{k+1}$. Then

$$f_{k+1}(\Phi(x)) \equiv f_k(\Phi(x)) + (-a_0)^{k+1} r_{k+1} x^{k+1} \bmod \deg k+2$$

and

$$\begin{aligned} G(\dots G([-a_0]_G(f_{k+1}(x)), [-a_1]_G(f_{k+1}(x^p))), \dots, [-a_{h-1}]_G(f_{k+1}(x^{p^{h-1}}))) \\ \equiv G(\dots G([-a_0]_G(f_k(x)), [-a_1]_G(f_k(x^p))), \dots, \\ [-a_{h-1}]_G(f_k(x^{p^{h-1}})))) - a_0 r_{k+1} x^{k+1} \bmod \deg k+2. \end{aligned}$$

Thus

$$\begin{aligned} G(\dots G([-a_0]_G(f_k(x)), [-a_1]_G(f_k(x^p))), \dots, \\ [-a_{h-1}](f_k(x^{p^{h-1}}))) - f_k(\Phi(x)) \\ \equiv -a_0(1-(-a_0)^k) r_{k+1} x^{k+1} \bmod \deg k+2. \end{aligned}$$

Finally, to show that r_{k+1} is integral, we must show that the left hand side of (2) is divisible by p.

But reducing mod p, we have

$$\begin{aligned} G(\dots G([-a_0]_G(f_k(x)), [-a_1]_G(f_k(x^p))), \dots, [-a_{h-1}]_G(f_k(x^{p^{h-1}}))) \\ \equiv G(\dots G([-a_0]_G(f_k(x)), [-a_1]_G(f_k(x)^p)), \dots, [-a_{h-1}]_G(f_k(x)^{p^{h-1}})) \\ \equiv f_k(x)^{p^h} \bmod p \end{aligned}$$

and

$$f_k(\Phi(x)) \equiv f_k(x^{p^h}) \equiv f_k(x)^{p^h} \bmod p \qquad \text{q.e.d.}$$

Remark. If a power of the Frobenius endomorphisms of the reductions of F and G lifted back to characteristic zero (this is the case Honda treats), then one could modify the definition of Φ and Ψ so as to obtain $f(\Phi(x)) = \Psi(f(x))$ instead of (1). Then Lemma 2 of Section 1 would immediately force f to be integral.

Note moreover that if F were *a priori* defined only over Q_p and one could find an associated $\Phi(x)$ which were integral, then not only would the proof above have shown that f is integral, but also that F was actually defined over Z_p. We make much of this in Section 4.

Theorem E′. *Let two formal groups F and G of finite height over Z/pZ have the same characteristic polynomial. Then F and G are isomorphic over Z/pZ.*

Proof. Lift F and G to formal groups $\tilde{F}$ and $\tilde{G}$ over Z_p; this is always possible by Theorem 1. By Theorem E, $\tilde{F}$ and $\tilde{G}$ are isomorphic over Z_p, i.e. there exists an $f(x)=x+\cdots\in Z_p[[x]]$ such that $f(\tilde{F}(x,y))=\tilde{G}(f(x),f(y))$. Then f reduces $\bmod p$ to an isomorphism from F to G.

4. The Formal Groups of Dirichlet Series

Let $D(s)=\sum_{n=1}^{\infty} a_n n^{-s}$, $a_1=1$, be a formal Dirichlet series over an integral domain R of characteristic 0 with quotient field K. The *formal group* $F_D(x,y)$ *associated to* $D(s)$ is the formal group over K whose canonical invariant differential (see Section 1, paragraph 2) has the same coefficients as $D(s)$. Specifically, letting $f(x)=\sum_{n=1}^{\infty} a_n n^{-1} x^n$, then $F_D(x,y)=f^{-1}(f(x)+f(y))$.

In this section the basic question is the following: Given a formal Dirichlet series $D(s)$ with coefficients in R, when is $F_D(x,y)$ defined over R? (Note that *a priori* $F_D(x,y)$ is defined only over K. In fact, in some sense most formal groups F_D associated to Dirichlet series over R *won't* be defined over R.)

Our main interest here is in the case when R is Z, and especially with certain Dirichlet series important in number theory. If $D(s)$ is in fact the global L-series of an elliptic curve E over Q, then not only is the associated formal group defined over Z, but moreover it is isomorphic over Z to any formal minimal model for E. To get our results over Z, we first construct a large class of Dirichlet series over Z_p with formal groups defined over Z_p. It is in the nature of things that it is then very easy to pass from local to global (for a powerseries over Q is defined over Z_p only when p doesn't divide the denominators of its coefficients).

It turns out that every isomorphism class of formal groups over Z_p contains formal groups of Dirichlet series over Z_p, but this doesn't seem to be the case over Z (using Theorem 1 of Section 1, one can construct formal groups over Z which definitely aren't isomorphic to any formal group associated to a Dirichlet series with an Euler product). It is true, however, that an isomorphism class containing a formal group $F(x,y)$ over Z contains the formal group of a Dirichlet series over Z if the Frobenius element of $F \bmod p$ is an algebraic integer for every p.

Theorem F. *Let*

$$D(s)=(1-b_1 p^{-s}-\cdots-b_n p^{-ns})^{-1}\sum_{m=1}^{\infty} u_m m^{-s}$$

be a formal Dirichlet series with $b_i, u_m \in Z_p$, $u_1 = 1$, *and* $u_m \in m Z_p$ *for all m. If* $\operatorname{ord}_p(b_n) = n-1$, *and* $\operatorname{ord}_p(b_i) \geqq i-1$ *for* $i = 1, 2, \ldots, n-1$, *then the formal group associated to* $D(s)$ *is defined over* Z_p, *and its characteristic polynomial divides the polynomial* $x^n + (b_{n-1}/b_n) p x^{n-1} + \cdots + (b_1/b_n) p^{n-1} x - (p^n/b_n)$.

Proof. So $D(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ where a_n are in Z_p and satisfy the following:

1. $a_{mp^r} \equiv a_m a_{p^r} \bmod p$ if $(m, p) = 1$.
2. $a_m \equiv b_1 a_{m/p} + b_2 a_{m/p^2} + \cdots \bmod m$ where $a_t = 0$ if $t \notin Z$.

Let $f(x) = \sum_{n=1}^{\infty} a_n/n\, x^n$. The formal group associated to $D(s)$ is $F(x, y) = f^{-1}(f(x) + f(y))$. Define $r_0 = -p^n/b_n$, $r_1 = b_1 r_0/p = (b_1/b_n) p^{n-1}$, $r_2 = (b_2/b_n) p^{n-2}, \ldots, r_{n-1} = (b_{n-1}/b_n) p$. Since $\operatorname{ord}_p(b_n) = n-1$, we have $\operatorname{ord}_p(r_0) = 1$, and since $\operatorname{ord}_p(b_i) \geqq i-1$, $\operatorname{ord}_p(r_i) \geqq 0$, i.e. $r_i \in Z_p$ for $i = 1, 2, \ldots, n-1$.

To show that $F(x, y)$ is defined over Z_p, it is necessary first of all to show that the powerseries

$$\begin{aligned}\Phi(x) &= F\big(\ldots F\big(F([-r_0]_F(x), [-r_1]_F(x^p)), [-r_2]_F(x^{p^2})\big), \ldots, [-r_{n-1}]_F(x^{p^{n-1}})\big)\\ &= f^{-1}\big(-r_0 f(x) - r_1 f(x^p) - r_2 f(x^{p^2}) - \cdots - r_{n-1} f(x^{p^{n-1}})\big)\end{aligned}$$

is integral and congruent $\bmod p$ to x^{p^n}.

Write $\Phi(x) = x^{p^n} + p\,u(x)$. We must show that

$$u(x) = \sum_{i=1}^{\infty} c_i x^i \quad \text{is in } Z_p[[x]].$$

We have $-r_0 f(x) - r_1 f(x^p) - \cdots - r_{n-1} f(x^{p^{n-1}}) = f\big(x^{p^n} + p\,u(x)\big)$. So

$$-p\big((r_0/p)\, x + u(x)\big) = x^{p^n} + \sum_{i=2}^{\infty} a_i/i\,\big[(x^{p^n} + p\,u(x))^i + r_0 x^i\big] + \sum_{j=1}^{n-1} r_j f(x^{p^j}). \quad (1)$$

Now $c_1 = -r_0/p$ is in Z_p by assumption. The idea now is to show inductively using Honda's congruence formula (Lemma 4 of Section 1) that the c_i are all integral. So assume $c_i \in Z_p$ for all $i \leqq k$. To show c_{k+1} is integral, we must verify that p divides the coefficient of x^{k+1} in the right-hand side of (1). Now letting

$$u_k(x) = \sum_{i=1}^{k} c_i x^i,$$

we see that

$$\begin{aligned}-p\big((r_0/p)\, x + u(x)\big) \equiv x^{p^n} &+ \sum_{i=2}^{\infty} a_i/i\,\big[(x^{p^n} + p\,u_k(x))^i + r_0 x^i\big]\\ &+ \sum_{j=1}^{n-1} r_j f(x^{p^j}) \bmod \deg k+2.\end{aligned}$$

Since $u_k(x)\in Z_p[x]$ by assumption, we can apply Honda's congruence formula to get $(a_i/i)(x^{p^n}+p\,u_k(x))^i\equiv(a_i/i)\,x^{ip^n} \bmod p$. So the problem reduces to showing that p divides the coefficient d_{k+1} of x^{k+1} in

$$\sum_{i=2}^{\infty} a_i/i(x^{ip^n}+r_0\,x^i)+\sum_{j=1}^{n-1} r_j\,f(x^{p^j}).$$

But writing $k+1=m$, we have (for $m\geqq n$)

$$\begin{aligned} d_m &= r_0\left\{\frac{a_m}{m}+\frac{r_1}{r_0}\,\frac{a_{m/p}}{m/p}+\cdots+\frac{r_{n-1}}{r_0}\,\frac{a_{m/p^{n-1}}}{m/p^{n-1}}+\frac{a_{m/p^n}}{r_0\,m/p^n}\right\} \\ &= \frac{r_0}{m}\{a_m-b_1\,a_{m/p}-\cdots-b_{n-1}\,a_{m/p^{n-1}}-b_n\,a_{m/p^n}\} \\ &\equiv 0 \bmod p. \end{aligned}$$

Hence p divides c_{k+1} and thus by induction, $\Phi(x)\in Z_p[[x]]$ and $\Phi(x)\equiv x^{p^n} \bmod p$.

The next step now is to find a formal group $G(x,y)$ over Z_p which we can show to be isomorphic over Z_p to $F(x,y)$, thus showing that $F(x,y)$ is defined over Z_p, and proving the theorem. To do this, consider the polynomial

$$p(x)=x^n+r_{n-1}\,x^{n-1}+\cdots+r_1\,x+r_0\in Z_p[x].$$

Since $\operatorname{ord}_p(r_0)=1$, $p(x)$ factors uniquely over Z_p into a product $e(x)\,s(x)$ with $e(x)$ Eisenstein. Let $G(x,y)$ be a formal group over Z_p having $e(x)$ as its characteristic polynomial. (The existence of such a G is assured by Proposition D of Section 3.) Let

$$g(x)=\sum_{i=1}^{\infty} s_i\,x^i$$

denote the isomorphism from F to G defined over Q_p, i.e. $F(x,y)=g^{-1}(G(g(x),g(y)))$. To prove that $g(x)$ is integral, we will proceed exactly as in the proof of Theorem E in Section 3. Form the powerseries

$$\begin{aligned} \Psi(x)=G\big(\ldots G\big(G([-r_0]_G(x)\cdot[-r_1]_G(x^p)),[-r_2]_G(x^{p^2})\big),\ldots,\\ [-r_{n-1}]_G(x^{p^{n-1}})\big) \end{aligned}$$

$\Psi(x)\in Z_p[[x]]$ and since $e(x)$ divides $p(x)$, we have $\Psi(x)\equiv x^{p^n} \bmod p$. Then

$$g(\Phi(x))=G\big(\ldots G([-r_0]_G(g(x)),[-r_1]_G(g(x^p))),\ldots,[-r_{n-1}]_G(g(x^{p^{n-1}}))\big)$$

and for the induction step, letting

$$g_k(x)=\sum_{i=1}^{k} s_i\,x^i,$$

we get

$$\begin{aligned} &G\big(\dots G([-r_0]_G(g_k(x)), [-r_1]_G(g_k(x^p))), \dots, [-r_{n-1}]_G(g_k(x^{p^{n-1}}))\big) \\ &\quad - g_k(\Phi(x)) \equiv -r_0\big(1-(-r_0)^k\big)\, s_{k+1}\, x^{k+1} \bmod \deg k+2. \end{aligned} \tag{5}$$

Since $\operatorname{ord}_p(r_0)=1$, it suffices to show that p divides the left-hand side of (5). But the left-hand side reduces mod p to $g_k(x)^{p^n}-g_k(x)^{p^n}=0$. q.e.d.

In any isomorphism class of formal groups over Z_p, one can find formal groups associated to Dirichlet series. For if $p(x)=x^n+\dots+r_1x+r_0$ is an Eisenstein polynomial over Z_p, then the formal group associated to any Dirichlet series over Z_p with Euler p-factor,

$$\big(1+(r_1/r_0)\,p^{1-s}+\dots+(r_{n-1}/r_0)\,p^{(n-1)(1-s)}-(1/r_0)\,p^{n(1-s)}\big)^{-1}$$

is defined over Z_p and has $p(x)$ as characteristic polynomial by Theorem F.

Over Z, however, in order for a formal group F to be isomorphic to a formal group coming from a Dirichlet series over Z with an Euler product, it is necessary that the Frobenius endomorphism of $F \bmod p$ be an algebraic integer for every prime p. From Proposition D of Section 3 and the lifting theorem, we see that this need not be the case at all. For if $\pi\in Z_p$ has order 1 and is not algebraic, Proposition D assures the existence of a formal group $\tilde{F}$ over Z/pZ with π as Frobenius. Lifting $\tilde{F}$ to F defined over Z then gives the counterexample. That the condition is sufficient, however, is a consequence of the following

Theorem G. *Let*

$$D(s)=\prod_p (1-b_{1p}\,p^{-s}-b_{2p}\,p^{-2s}-\dots-b_{n_p p}\,p^{-n_p s})^{-1}$$

be a formal Dirichlet series with Euler product, $b_{ij}\in Z$. If for every p, $\operatorname{ord}_p(b_{n_p p})=n_p-1$, and $\operatorname{ord}_p(b_{ip})\geqq i-1$ for $i=1,2,\dots,n_p-1$, then the formal group F_D associated to D is defined over Z. Moreover the characteristic polynomial of $F_D \bmod p$ divides

$$x^{n_p}+(b_{n_p-1,p}/b_{n_p p})\,p\,x^{n_p-1}+\dots+(b_{1p}/b_{n_p p})\,p^{n_p-1}\,x-p^{n_p}/b_{n_p}.$$

Proof. F_D has rational coefficients, and is defined over Z_p for all p by Theorem F. Hence F_D is defined over Z. The statement about the characteristic polynomial of $F_D \bmod p$ also follows immediately from Theorem F.

Finally we prove Honda's theorem for an arbitrary elliptic curve over Q.

Theorem H. *Let E be an elliptic curve over Q and let $G(x,y)$ be a formal minimal model for E over Z. Let $F(x,y)$ be the formal group associated to the global L-series of E over Q. Then $F(x,y)$ is defined over Z and is isomorphic over Z to $G(x,y)$.*

Proof.

$$L(E,s)=\prod L_p(E,s)=1\cdot\prod_{p\text{ mult.}}(1-\varepsilon_p p^{-s})^{-1}\cdot\prod_{p\text{ good}}(1-a_p p^{-s}+p^{1-2s})^{-1}.$$

So $L(E,s)$ satisfies the conditions of Theorem G, and hence $F(x,y)$ is defined over Z.

Let f be the Q-isomorphism from F to G. It remains to show that f is defined over Z_p for all p. For this, it suffices by Lemma A and Theorem E, to show that the reductions of F and $G \bmod p$ either both have infinite height, or both have the same finite height and the same characteristic polynomial.

For the primes at which E has bad reduction, this is worked out completely by Honda ([5], Theorem 3 and Proposition 3).

When E has good reduction at p, we know from Theorem F that the characteristic polynomial of $F(x,y) \bmod p$ divides $x^2-a_p x+p$. But $x^2-a_p x+p$ is the characteristic polynomial of the Frobenius endomorphism of $E \bmod p$ and the characteristic polynomial of $G(x,y) \bmod p$ is its Eisenstein factor. q.e.d.

References

1. Cassels, J.W.S.: Diophantine equations with special reference to elliptic curves. J. London Math. Soc. **41**, 193–291 (1966).
2. Deuring, M.: Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins *I*. Nachr. Akad. Wiss. Göttingen 85–94 (1953).
3. Dieudonné, J.: Groupes de Lie et hyperalgèbres de Lie sur un corps de characteristique $p>0$ (VIII). Math. Ann. **134**, 114–133 (1957).
4. Eichler, M.: Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. Arch. Math. **5**, 355–366 (1954).
5. Honda, T.: Formal groups and zeta-functions. Osaka J. Math. **5**, 199–213 (1968).
6. Lazard, M.: La non-existence des groupes de Lie formels non-abéliens à un paramètre. C. R. Acad. Sc. **239**, 942–945 (1954).
7. – Sur les groupes de Lie Formels à un paramètre. Bull. Soc. Math. France **83**, 251–274 (1955).
8. Lubin, J.: One parameter formal Lie groups over p-adic integer rings. Ann. of Math. **80**, 464–484 (1964).
9. – Tate, J.: Formal complex multiplication in local fields. Ann. of Math. **81**, 380–387 (1965).
10. Ogg, A.: Abelian curves of small conductor. Crelles Jour. **226**, 204–215 (1967).
11. Shimura, G.: Correspondances modulaires et les fonctions de courbes algebriques. J. Math. Soc. Japan **10**, 1–28 (1958).
12. Weil, A.: Sur les courbes algébriques et les variétés qui s'en déduisent. Paris: Hermann 1948.

Walter L. Hill
Princeton University
Department of Mathematics
Princeton, New Jersey 08540
USA

(Received August 11, 1970)