ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 23, Number 1, Winter 1993

p-ADIC INTERPOLATION OF THE COEFFICIENTS OF HURWITZ SERIES ATTACHED TO HEIGHT ONE FORMAL GROUPS

C. SNYDER

1. Introduction. In a series of articles [**16, 17, 18**] we studied Kummer congruences for the coefficients of Hurwitz series associated with a differential on an algebraic curve. Actually, the proper setting turns out to be Hurwitz series attached to formal groups over integral rings. (See the definitions below.)

The object of this paper is to partially answer a question posed to us by J-P. Serre [**15**] as to whether we could strengthen the Kummer congruences considered in our earlier papers by using the concept of the Iwasawa algebra. We accomplish this with the aid of p-adic measure theory in the case that the formal groups are of height one.

2. Preliminaries. Throughout the paper we let p denote a fixed prime which, for convenience, we assume to be odd. We let $\mathbf{C}_p$ denote the completion of an algebraic closure of $\mathbf{Q}_p$, and O_p the ring of integers of $\mathbf{C}_p$. Let K be a finite extension of $\mathbf{Q}_p$ with ring of integers O_K.

Recall that $\mathbb{Z}_p^x$ may be written as a direct product $\mathbb{Z}_p^x = V \times U$ where V is the group of p-1st roots of unit in $\mathbb{Z}_p$ and $U = 1+p\mathbb{Z}_p$, the group of principal units in $\mathbb{Z}_p^x$. If $x \in \mathbb{Z}_p^x$, then we denote by $\omega(x)$ and $\langle x \rangle$ the projections of x onto V and U, respectively. Furthermore, recall that if u is a topological generator of U, then the mapping $\mathbb{Z}_p \to U$ given by $x \to u^x$ is a topological group isomorphism of $\mathbb{Z}_p$ with U.

We now summarize some of the standard material on formal groups which we use in the paper.

Definition. Let A be a commutative ring with 1. Then a (one parameter) *formal group* (law) *over* A is a power series $F(X,Y) \in A[[X,Y]]$ satisfying:

a) $F(X,Y) = X + Y +$ "higher degree terms",

Received by the editors on May 16, 1986.

b) $F(F(X,Y),Z) = F(X,F(Y,Z))$, (associative law)

c) $F(X,Y) = F(Y,X)$, (commutative law)

We sometimes write $X \underset{F}{+} Y$ for $F(X,Y)$.

Examples. 1) Let $G_a(X,Y) = X+Y$, the so-called additive formal group.

2) Let $G_m(X,Y) = X+Y+XY = (1+X)(1+Y)-1$, the so-called multiplicative formal group.

3) Let $G_e(X,Y) = (1-\kappa^2X^2Y^2)^{-1}(X\sqrt{(1-Y^2)(1-\kappa^2Y^2)} + Y\sqrt{(1-X^2)(1-\kappa^2X^2)})$ where we assume κ^2 is a nonzero algebraic number. This is the formal group induced by the addition law of the Jacobi sinus function $\mathrm{sn}(u)$ satisfying the differential equation $Y^2 - (1-X^2)(1-\kappa^2X^2)$ where $X = \mathrm{sn}u$ and $Y = (d/du)\mathrm{sn}u$. Notice G_e is defined over $\mathbb{Z}[1/2,\kappa^2]$, cf. [**3**, pp. 216, 217].

Definition. Let A be a characteristic zero integral domain with quotient field K. Let F be a formal group over A. Then the *formal logarithm of* F is (the unique) power series $\lambda(z) \in K[[z]]$ satisfying

a) $\lambda(z) = z +$ "higher degree terms",

b) $\lambda(X \underset{F}{+} Y) = \lambda(X) + \lambda(Y)$.

(Actually, $\lambda(z) = \sum_{k=1}^{\infty} \varepsilon_k(z^k/k)$ where $\varepsilon_k \in A$ and $\varepsilon_1 = 1$, cf. [**2**].)

The *formal exponential function* of F is (the unique) power series $\varepsilon(t) \in K[[t]]$ such that $\varepsilon(t) = \lambda^{-1}(t)$, the inverse power series of $\lambda(t)$, i.e., $\lambda(\varepsilon(t)) = t = \varepsilon(\lambda(t))$. ($\varepsilon(t) = \sum_{k=1}^{\infty} a_k(t^k/k!)$ where $a_k \in A$ and $a_1 = 1$.)

Remark . Notice $\varepsilon(s+t) = F(\varepsilon(s),\varepsilon(t))$.

Examples. (1) For G_a, $\lambda(z) = z = \varepsilon(z)$.

(2) For G_m, $\lambda(z) = \log(1+z)$ and $\varepsilon(t) = e^t - 1$.

(3) For G_e, $\lambda(z) = \int_0^z (dz/\sqrt{(1-z^2)(1-\kappa^2z^2)})$ and $\varepsilon(t) = \mathrm{sn}(t)$.

Definition. Let F and G be formal groups over A, a commutative

ring with 1. Then a *homomorphism ϕ over B from F to G*, denoted $\phi : F \to G$, is a power series $\phi(z) \in B[[z]]$, B an extension ring of A, satisfying

(a) $\phi(0) = 0$

(b) $\phi(X \underset{F}{+} Y) = \phi(X) \underset{G}{+} \phi(Y)$.

If $\phi : F \to G$ and $\phi(z) = \alpha z +$ "higher degree terms" where $\alpha \in B^x$, the units of B, then ϕ is called an *isomorphism* over B.

If $F = G$, then ϕ is called an endomorphism over B. We denote the homomorphisms over B from F to G by $\mathrm{Hom}_B(F, G)$ and the endomorphisms over B by $\mathrm{End}_B(F)$.

Remark . If $\phi, \psi \in \mathrm{Hom}_B(F, G)$ and we define $(\phi + \psi)(z)$ by $\phi(z) \underset{G}{+} \psi(z)$, then $\phi + \psi \in \mathrm{Hom}_B(F, G)$ and $(\mathrm{Hom}_B(F, G), +)$ is an abelian group. $(\mathrm{End}_B(F), +, o)$ is a ring, cf. [**12**].

Examples of endomorphisms. Let $n \in \mathbb{Z}$, $n > 0$. Define $[n]_F(z)$ as $\underbrace{z \underset{F}{+} \ldots \underset{F}{+} z}_{n\text{-times}}$. Define $[0]_F(z) = 0$. Let $[-1]_F(z)$ denote (the unique) power series such that $[-1]_F(z) \underset{F}{+} z = 0$. Define for $n < 0$, $[n]_F(z)$ as $\underbrace{[-1]_F(z) \underset{F}{+} \ldots \underset{F}{+} [-1]_F(z)}_{|n|\text{-times}}$. Then $[n]_F(z) \in \mathrm{End}_A(F)$. Moreover, if A is a characteristic zero integral domain with quotient field K so that $\lambda(z)$ and $\varepsilon(t)$ exist, then $[a]_F(z)$ is defined to be $\varepsilon(a\lambda(z))$ where $a \in K$. (If $a \in \mathbf{Z}$, then the two definitions of $[a]_F$ coincide.) $[a]_F(z)$ may not have coefficients in A even if $a \in A$, cf. [**13**].

From now on (to the end of this section) we assume that K is a finite extension of $\mathbf{Q}_p$ with ring of integers O_K and that F is a formal group defined over O_K. Also, let O_p be the ring of integers in $\mathbf{C}_p$.

Remark . $\mathrm{End}_{O_p}(F) \to O_p$ given by $\phi \to$ (linear coefficient of ϕ) is an injective ring homomorphism, cf. [**12**]. If $a \in \mathbb{Z}_p$, then $[a]_F(z) \in \mathrm{End}_{O_p}(F)$, again cf. [**12**].

Definition. Let P be the maximal ideal of O_K and $k = O_K/P$ the residue class field.

If $[p]_F(z) \not\equiv 0 \bmod P$, then by [**12**], $[p]_F(z) \equiv az^{p^h} +$ "higher degree terms" $\bmod P$ where $a \in O_K^x$. We define h to be *height* of F.

If $[p]_F(z) \equiv 0 \bmod P$, then we say F has *infinite height.*

Example. (1) G_a has infinite height.

(2) G_m has height one.

(3) Consider G_e where κ^2 is p-integral so that we may consider G_e defined over O_K for some K a finite extension of $\mathbf{Q}_p$. Suppose p does not divide the discriminant of $y^2 = (1 - X^2)(1 - \kappa^2 X^2)$. Then G_e has height one or two according to whether $\varepsilon_p \not\equiv 0(P)$ or $\varepsilon_p \equiv 0(P)$, cf. [**9**].

Remark . Suppose F has finite height. Then the image of $\mathrm{End}_{O_p}(F)$ in O_p is "not too big," namely, $\mathrm{End}_{O_p}(F) \to O_E$ where E is the composition of all (finitely many) extensions of $\mathbf{Q}_p$ of degree h. In particular, if $h = 1$, then $\mathrm{End}_{O_p}(F) \simeq \mathbb{Z}_p$, cf. [**12**].

We shall also use the following well-known result, cf. [**12**].

Proposition. *Let F be a formal group of height one defined over O_K. Then there exists an isomorphism from F to G_m defined over O_T where T is the maximal unramified extension of K.*

3. Kummer congruences and p-adic interpolation of Hurwitz series. As above, let F be a formal group defined over O_K, K a finite extension of $\mathbf{Q}_p$. Let λ and ε denote the formal logarithm and exponential functions, respectively. Recall that $\lambda(z) = \sum_{k=1}^{\infty} \varepsilon_k(z^k/k)$ where $\varepsilon_k \in O_K$ and $\varepsilon_1 = 1$. Now let $f(z) \in O_p[[z]]$. Then we define $f(\varepsilon(t)) = \sum_{k=0}^{\infty} c_k(t^k/k!)$ to be a Hurwitz series attached to the formal group F. For the coefficients of this Hurwitz series, we have the Kummer congruences:

$$\sum_{j=0}^{r} (-1)^{r-j} \binom{r}{j} \varepsilon_p^{r-j} c_{m+j(p-1)} \equiv 0 \bmod p^r O_p$$

for all positive integers r, m with $m \geq r$. This was proved in [**18**] for

$f(z) = z$; but then it holds for all $f(z)$ once we know it for z, [**2**, p. 299].

As an aside, we should mention that there is another way of obtaining the coefficients c_k in the Hurwitz series $f(\varepsilon(t))$. Let D be the invariant derivation defined by $Df(z) = (\partial/\partial w) f(z \underset{F}{+} w)|_{w=0}$. Then we claim that $Df(\varepsilon(t)) = (d/dt) f(\varepsilon(t))$. For $Df(\varepsilon(t)) = (\partial/\partial w) f(\varepsilon(t) \underset{F}{+} w)|_{w=0}$,

$$\frac{\partial}{\partial w} f(\varepsilon(t) \underset{F}{+} \varepsilon(\lambda(w)))|_{w=0} = \frac{\partial}{\partial w} f(\varepsilon(t + \lambda(w)))|_{w=0}$$
$$= f'(\varepsilon(t + \lambda(w)))\varepsilon'(t + \lambda(w))\lambda'(w)|_{w=0} = f'(\varepsilon(t))\varepsilon'(t)$$

since $\lambda(0) = 0$ and $\lambda'(0) = 1$. Thus, $Df(\varepsilon(t)) = (d/dt) f(\varepsilon(t))$. But then we have $c_k = D^k f(0)$ without reference to the formal exponential map.

We now wish to strengthen the Kummer congruences for the sequence $\{c_k\}_k$. We accomplish this by "twisting" the c_k to obtain a new sequence $\{\tilde{c}_k^*\}_k$ and then by constructing a function $c(s)$ which is p-adically continuous for all $s \in \mathbb{Z}_p$ and such that $c(s)$ agrees with $\tilde{c}_k^*$ on a dense sequence in $\mathbb{Z}_p$. From all of this, we shall then recover our original Kummer congruences.

Let us now introduce p-adic measures. Let X be a compact totally disconnected topological space. Denote by $M(X, O_p)$ the O_p-valued measures on X [**5,11**, p. 95, or even **8**, p. 36]. (For a very nice account of why it is desirable to introduce measures, see Katz's Arcata paper [**5**].)

Let $X = \mathbb{Z}_p$ and consider the mapping from $M(\mathbb{Z}_p, O_p)$ to $O_p[[z]]$ given by $\mu \to f(z) = \int_{\mathbb{Z}_p} (1+z)^x \, d\mu(x)$. By Mahler's theorem, cf. [**11**, p. 99], this mapping is a bijection. Moreover, if $f(e^t - 1) = \sum_{k=0}^{\infty} c_k (t^k/k!)$ so that $f(e^t - 1)$ is a Hurwitz series attached to G_m, the formal multiplicative group, then $c_k = \int_{\mathbb{Z}_p} x^k \, d\mu(x)$, cf. [**11**, p. 104]. Thus, we see that the coefficients of our Hurwitz series are given as the moments of a measure corresponding to $f(z)$. Our "twisted" coefficients in this case are given by $c_k^* = \int_{\mathbb{Z}_p^x} x^k \, d\mu(x)$ and the function $c(s)$ by $\int_{\mathbb{Z}_p^x} \langle x \rangle^s \, d\mu(x)$ or more generally by $\int_{\mathbb{Z}_p^x} \langle x \rangle^s \omega^m(x) \, d\mu(x)$ for any fixed integer m. Notice then (in the latter case) that if $k \equiv m(p-1)$, $c_k^* = c(k)$ so that c_k^* and $c(k)$ agree on a dense subset of $\mathbb{Z}_p$.

In the example above, two questions arise. In the bijection between measures and power series, why is $X = \mathbb{Z}_p$ and how does the integrand, $(1+z)^x$, arise? We shall try to answer these questions in a more general situation.

Let F be a formal group over O_K. Let $f(z) \in O_p[[z]]$ and $f(\varepsilon(t)) = \sum_{k=0}^{\infty} c_k(t^k/k!)$ a Hurwitz series attached to F. Suppose that there is an O_p-valued measure μ defined in some space A such that $c_k = \int_A x^k \, d\mu(x)$. Then we must have $f(\varepsilon(t)) = \sum_{k=0}^{\infty} c_k(t^k/k!) = \sum_{k=0}^{\infty} \int_A x^k \, d\mu(x)(t^k/k!) = \int_A \sum_{k=0}^{\infty} x^k(t^k/k!) \, d\mu(x) = \int_A \exp(xt) \, d\mu(x)$.

If we set $t = \lambda(z)$, we obtain

$$f(z) = \int_A \exp(x\lambda(z)) \, d\mu(x).$$

It seems natural to take $A = \{x \in \mathbf{C}_p : \exp(x\lambda(z)) \in O_p[[z]]\}$ so that the coefficients of the powers of z in $\exp(x\lambda(z))$ are O_p-valued functions of x. Notice then that if $x, y \in A$ and $a \in \mathbb{Z}_p$, then $x + y, ax \in A$ so that A is a $\mathbb{Z}_p$-module. Let us denote $\exp(x\lambda(z))$ by $\psi_x(z)$. Then $\psi_x(z)$ satisfies the properties $\psi_x(0) = 1$ (since $\lambda(0) = 0$) and $\psi_x(z \underset{F}{+} w) = \psi_x(z)\psi_x(w)$ (since $\lambda(z \underset{F}{+} w) = \lambda(z) + \lambda(w)$). By [**5**], $\{\psi_x(z) : x \in A\}$ is the so-called p-divisible dual of F and is isomorphic to A as a $\mathbb{Z}_p$-module. Then it is known that A is a free $\mathbb{Z}_p$-module of rank h where h is the height of F which we assume to be finite, cf. [**19**]. As an example, let $F = G_m$. Then $\psi_x(z) = \exp(x \log(1+z)) = (1+z)^x$. Furthermore, $A = \{x \in \mathbf{C}_p : (1+z)^x \in O_p[[z]]\}$. We claim $A = \mathbb{Z}_p$. For let $\tilde{\psi}_x(z) = (1+z)^x - 1$. Then $\tilde{\psi}_x(z)$ is an endomorphism of G_m over O_p. But G_m has height one and thus since $\mathrm{End}_{O_p}(G_m) \simeq \mathbb{Z}_p$, $x \in \mathbb{Z}_p$. This answers the two questions previously posed.

As a less standard example assume $F = G_a$. Then $\psi_x(z) = \exp(xz)$ since $\lambda(z) = z$. Moreover, $A = \{x \in \mathbf{C}_p : \exp(xz) \in O_p[[z]]\} = M^{1/p-1}$ where M is the maximal ideal of O_p, cf. [**20**]. Notice then that A is "very large" as a $\mathbb{Z}_p$-module compared with the previous example.

We now consider the case where the Hurwitz series are attached to a formal group F of height one. Then there exists an isomorphism $g : F \to G_m$ over O_T, the ring of integers of the completion of the maximal unramified extension, T, of K, i.e., $g(z) \in O_T[[z]]$ such that

$$g(z \underset{F}{+} w) = g(z) \underset{G_m}{+} g(w)$$

and

$$g(z) = \gamma z + O(z^2)$$

for some unit γ in O_T, see section 2 above.

We now want to determine A. But first we claim that the formal logarithm $\lambda(z) = \gamma^{-1}\log(1+g(z))$. For notice that $\lambda \circ g^{-1}$ is a homomorphism from G_m to G_a. But the only such homomorphisms are of the form $\alpha\log(1+z)$ for some constant α, [**12**, p. 31]. A comparison of the linear coefficients in $\lambda \circ g^{-1}(z)$ and $\alpha\log(1+z)$ shows that $\alpha = \gamma^{-1}$ as desired. Now, for A, $A = \{x \in \mathbf{C}_p : \exp(x\cdot\lambda(z)) \in O_p[[z]]\} = \{x \in \mathbf{C}_p : \exp(x\gamma^{-1}\log(1+g(z)))\} = \{y\gamma \in \mathbf{C}_p : \exp(y\log(1+z)) \in O_p[[g^{-1}(z)]] = O_p[[z]]\} = \mathbb{Z}_p\gamma$. Thus, given a measure, μ, on A we can associate with μ the power series $f(z) = \int_{\mathbb{Z}_p\gamma}\exp(x\lambda(z))\,d\mu(x) = \int_{\mathbb{Z}_p}(1+g(z))^x\,d\mu(\gamma x)$. This association gives a bijection between $M(\mathbb{Z}_p\gamma, O_p)$ and $O_p[[z]]$.

We are now ready to develop p-adic interpolation associated with the coefficients of $f(\varepsilon(t)) = \sum_{k=0}^{\infty} c_k(t^k/k!)$. Then we have $f(z) = \int_{\mathbb{Z}_p}(1+g(z))^x\,d\tilde{\mu}(x)$ where $\tilde{\mu} = \mu\circ\gamma$, μ as above. Then $c_k = \int_{\mathbb{Z}_p\gamma} x^k\,d\mu(x) = \int_{\mathbb{Z}_p}(\gamma x)^k\,d\tilde{\mu}(x)$. Let $\tilde{c}_k = \gamma^{-k}c_k$. Then $\tilde{c}_k = \int_{\mathbb{Z}_p} x^k\,d\tilde{\mu}(x)$. Also let $\tilde{c}_k^* = \int_{\mathbb{Z}_p^*} x^k\,d\tilde{\mu}(x)$ and let $c(s) = \int_{\mathbb{Z}_p^*}\langle x\rangle^s\omega^m(x)\,d\tilde{\mu}(x)$ for some fixed integer m. Then $c(s)$ is meaningful for all s in $\mathbb{Z}_p$ and $c(k) = \tilde{c}_k^*$ for all $k \equiv m \bmod (p-1)$. We now wish to see how $c(k)$ and $\tilde{c}_k^*$ are related to the original c_k. To this end, we need to see what power series is associated with $\tilde{\mu}|_{\mathbb{Z}_p^*}$, the restriction of $\tilde{\mu}$ to $\mathbb{Z}_p^*$. If $\chi_{\mathbb{Z}_p^*}$ denotes the characteristic function of $\mathbb{Z}_p^*$, then we have $\chi_{\mathbb{Z}_p^*}(x) = 1 - (1/p)\sum_{\zeta^p=1}\zeta^x$ for all $x \in \mathbb{Z}_p$. Thus, $\int_{\mathbb{Z}_p^*}\psi_x(z)\,d\tilde{\mu}(x) = \int_{\mathbb{Z}_p}\psi_x(x)\chi_{\mathbb{Z}_p^*}(x)\,d\tilde{\mu}(x) = \int_{\mathbb{Z}_p}\psi_x(z)(1 - 1/p\sum_\zeta\zeta^x)\,d\tilde{\mu}(x) = \int_{\mathbb{Z}_p}\psi_x(z)\,d\tilde{\mu}(x) - 1/p\sum_\zeta\int_{\mathbb{Z}_p}\psi_x(z)\zeta^x\,d\tilde{\mu}(x)$. But we claim that $\int_{\mathbb{Z}_p}\psi_x(z)\zeta^x\,d\tilde{\mu}(x) = f(z+g^{-1}(\zeta-1))$, for $\int_{\mathbb{Z}_p}\psi_x(z)\zeta^x\cdot d\tilde{\mu}(x) = \int_{\mathbb{Z}_p}(\zeta(1+g(z)))^x\,d\tilde{\mu}(x) = \int_{\mathbb{Z}_p}(1+(g(z)\underset{G_m}{+}(\zeta-1)))^x\,d\tilde{\mu}(x) = \int_{\mathbb{Z}_p}(1+(g(z)+g(g^{-1}(\zeta-1)))^x\,d\tilde{\mu}(x) = \int_{\mathbb{Z}_p}(1+g(z\underset{F}{+}g^{-1}(\zeta-1)))^x\,d\tilde{\mu}(x) = f(z\underset{F}{+}g^{-1}(\zeta-1))$, as desired. Putting this all together, we see $\int_{\mathbb{Z}_p^*}\psi_x(z)\,d\tilde{\mu}(x) = f(z) - 1/p\sum_\zeta f(z+g^{-1}(\zeta-1))$.

For each p^{th} root of unity, ζ, define $c_k(\zeta)$ $(k \geq 0)$ by $\sum_{k=0}^{\infty}c_k(\zeta)(t^k/k!)$

$= f(\varepsilon(t) \underset{F}{+} g^{-1}(\zeta - 1))$ and c_k^* by $\sum_{k=0}^{\infty} c_k^*(t^k/k!) = f(\varepsilon(t)) - 1/p\sum_\zeta f(\varepsilon(t)) \underset{F}{+} g^{-1}(\zeta - 1))$; thus, $c_k^* = c_k - 1/p\sum_\zeta c_k(\zeta)$. Notice that if $\zeta = 1$, then $c_k(\zeta) = c_k$, since $g^{-1}(0) = 0$ and $x \underset{F}{+} 0 = x$ (which follows from the definition of a formal group).

We shall now relate $\int_{\mathbb{Z}_p^*} \langle x\rangle^k \omega^m(x)\, d\tilde{\mu}(x)$ to the $c_k(\zeta)$. To this end, since $\mathbb{Z}_p^x = \cup_{n\in V} \eta U$, we have $\int_{\mathbb{Z}_p^*} \langle x\rangle^k \omega^m(x)\, d\tilde{\mu}(x) = \sum_\eta \int_{\eta U} \langle x\rangle^k \omega^m(x)$.

$d\tilde{\mu}(x) = \int_U x^k\, d\beta(x)$ where $\beta = \sum_\eta \eta^m \tilde{\mu}|_{\mathbb{Z}_p^*} \circ \eta$. We claim that $\int_{\mathbb{Z}_p} \psi_x(z)\, d\beta(x) = 1/p\sum_{\zeta^p=1} \zeta^{-1} \sum_{\eta\in V} \eta^m f([\eta^{-1}]_F(z \underset{F}{+} g^{-1}(\zeta - 1)))$ where $[\eta]_F(z)$ denotes the unique endomorphism of F with linear coefficients η, cf. our preliminaries. To see this, first notice that if $\int_{\mathbb{Z}_p} \psi_x(z)\, d\mu(x) = f(z)$, then $\int_{\mathbb{Z}_p} \psi_x(z)\, d\mu(\eta x) = f([\eta^{-1}]_F(z))$; for $\psi_{\eta^{-1}x}(z) = (\psi_x(z))^{\eta^{-1}} = \psi_x([\eta^{-1}]_F(x))$ so that $\int_{\mathbb{Z}_p} \psi_x(z)\, d\mu(\eta x) = \int_{\mathbb{Z}_p} \psi_{\eta^{-1}x}(z)\, d\mu(x) = \int_{\mathbb{Z}_p} \psi_x([\eta^{-1}]_F(z))\, d\mu(x) = f([\eta^{-1}]_F(z))$. Also if $\int_{\mathbb{Z}_p} \psi_x(z)\, d\mu(x) = f(z)$, then $\int_U \psi_x(z)\, d\mu(x) = 1/p\sum_{\zeta^p=1} \zeta^{-1} f(z \underset{F}{+} g^{-1}(\zeta - 1))$, for $\chi_U(x) = 1/p\sum_\zeta \zeta^{-1}\zeta^x$ so the argument is similar to the one we used before for $\chi_{\mathbb{Z}_p^*}$. Thus, we get

$$\begin{aligned}\int_{\mathbb{Z}_p} \psi_x(z)\, d\beta|_U(x) &= \int_{\mathbb{Z}_p} \psi_x(z)\, d\Big(\sum_{n\in V} \eta^m \tilde{\mu}\circ\eta\Big|_U(x)\Big)\\ &= \frac{1}{p}\sum_\zeta \zeta^{-1}\sum_\eta \eta^m f([\eta^{-1}]_F(z \underset{F}{+} g^{-1}(\zeta - 1))\end{aligned}$$

as we wished.

Notice that $V = \{\omega^{-1}(a) : a = 1, \dots, p-1\}$. Using this representation for V and letting $z = \varepsilon(t)$, the right-hand side of the last equation becomes

$$\begin{aligned}&\frac{1}{p}\sum_{\zeta^p=1} \zeta^{-1}\sum_{a=1}^{p-1} \omega^{-m}(a) f(\varepsilon(\omega(a)t) \underset{F}{+} g^{-1}(\zeta^a - 1))\\ &\qquad = \sum_{k=0}^{\infty} \frac{1}{p}\sum_\zeta \zeta^{-1}\sum_{a=1}^{p-1} \omega^{k-m}(a) c_k(\zeta^a)\frac{t^k}{k!}.\end{aligned}$$

Therefore,

$$\int_{\mathbb{Z}_p^*} \langle x\rangle^k \omega^m(x)\, d\tilde{\mu}(x) = \frac{1}{p}\sum_{\zeta^p=1} \zeta^{-1} \sum_{a=1}^{p-1} \tilde{c}_k(\zeta^a).$$

Notice that when $k \equiv m \bmod (p-1)$, we get

$$\begin{aligned}\int_{\mathbb{Z}_p^*} x^k\, d\tilde{\mu}(x) &= \frac{1}{p}\sum_{\zeta} \zeta^{-1} \sum_{a=1}^{p-1} \tilde{c}_k(\zeta^a) \\ &= \frac{p-1}{p}\tilde{c}_k + \frac{1}{p}\sum_{\zeta\neq 1} \zeta^{-1} \sum_{a=1}^{p-1} \tilde{c}_k(\zeta^a) \\ &= \tilde{c}_k - \frac{1}{p}\tilde{c}_k + \frac{1}{p}\sum_{\zeta\neq 1} \tilde{c}_k(\zeta) \sum_{\zeta\neq 1} \zeta^{-1} \\ &= \tilde{c}_k - \frac{1}{p}\sum_{\alpha} \tilde{c}_k(\zeta) \\ &= \tilde{c}_k^*\end{aligned}$$

which is as it should be.

We now show that $\int_{\mathbb{Z}_p^*} \langle x\rangle^s \omega^m(x)\, d\tilde{\mu}(x)$ $(s \in \mathbb{Z}_p)$ is an element of the Iwasawa algebra, cf. [**14**, p. 235–244]. From this, we obtain rather strong congruences for subsequences of $\{\tilde{c}_k^*\}_k$. At this point, we have $\int_{\mathbb{Z}_p^x} \langle x\rangle^s \omega^m(x)\, d\tilde{\mu}(x) = \int_U x^s\, d\beta(x)$. Let u be a topological generator for U; then $\int_U x^s\, d\beta(x) = \int_{\mathbb{Z}_p} u^{ys}\, d\beta(u^y)$. Let $G(z) = \int_{\mathbb{Z}_p} \psi_y(z)\, d\beta(u^y)$. Then notice that if we let $1+g(z) = u^s$, we get $z = g^{-1}(u^s-1)$. Therefore, $\int_{\mathbb{Z}_p} u^{ys}\, d\beta(u^y) = G(g^{-1}(u^s-1)) = H(u^s-1)$ where $H(z) = G(g^{-1}(z)) \in O_p[[z]]$. Thus, $\int_{\mathbb{Z}^*} \langle x\rangle^s \omega^m(x)\, d\tilde{\mu}(x)$ is in the Iwasawa algebra. In particular, by Serre [**14**, p. 243], the sequence $\{\tilde{c}^*_{m+j(p-1)}\}_{j=0}^{\infty}$ satisfies

$$\sum_{k=0}^{r} (-1)^{r-j} \binom{r}{j} \tilde{c}^*_{m+j(p-1)} \equiv 0 \bmod p^r O_p \qquad (r, m \geq 0)$$

and

$$\sum_{j=1}^{r} c_{jr}\delta_{m+j(p-1)} p^{-j} \equiv 0 \bmod r! O_p \qquad (r \geq 1)$$

where

$$\sum_{j=1}^{r} c_{jr} Y^j = r! \binom{Y}{r}$$

and where

$$\delta_k = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} \tilde{c}^*_{k-j}.$$

(Actually these congruences follow easily from the fact that $\int_U x^k \, d\beta(x) = \tilde{c}^*_k$.)

We now want to recover our original Kummer congruences for $\{c_k\}_k$. So in our equation $f(\varepsilon(t)) - 1/p \sum_\zeta f(\varepsilon(t) \underset{F}{+} g^{-1}(\zeta - 1)) = \sum_{k=0}^{\infty} c^*_k (t^k/k!)$ make a change of variable $t \to \gamma^{-1} t$ to obtain $f(\varepsilon(\gamma^{-1}(t))$ $-1/p \sum_\zeta f(\varepsilon(\gamma^{-1} t) \underset{F}{+} g^{-1}(\zeta - 1)) = \sum_{k=0}^{\infty} \tilde{c}^*_k (t^k/k!)$. We consider the left-hand side. First notice that since $\lambda(z) = \gamma^{-1} \log(1 + g(z))$, we get by inverting $\varepsilon(t) = \lambda^{-1}(t) = g^{-1}(e^{\gamma t} - 1)$. Hence, $\varepsilon(\gamma^{-1} t) = g^{-1}(e^t - 1)$. Also, let $f \circ g^{-1} = h$ and notice that $h(z) \in O_p[[z]]$. Then the left-hand side becomes

$$\begin{aligned} f(g^{-1}(e^t - 1)) - \frac{1}{p} \sum_\zeta f(g^{-1}(e^t - 1) \underset{F}{+} g^{-1}(\zeta - 1)) \\ = f(g^{-1}(e^t - 1)) - \frac{1}{p} \sum_\zeta f(g^{-1}((e^t - 1) \underset{G_m}{+} (\zeta - 1))) \\ = h(e^t - 1) - \frac{1}{p} \sum_\zeta h(\zeta e^t - 1). \end{aligned}$$

We now claim that $1/p \sum_\zeta h(\zeta e^t - 1) = \sum_{k=0}^{\infty} e_k (t^k/k!)$ where $e_k \equiv 0 \bmod p^k O_p$. To see this, let $h(z) = \sum_{\nu=0}^{\infty} d_\nu z^\nu$ $(d_\nu \in O_p)$. Then

$$\begin{aligned} \frac{1}{p} \sum_\zeta h(\zeta e^t - 1) &= \frac{1}{p} \sum_{\zeta, \nu} d_\nu (\zeta e^t - 1)^\nu \\ &= \frac{1}{p} \sum_{\substack{\nu=0 \\ \mu=0}}^{\infty} d_\nu \binom{\nu}{\mu} (-1)^{\nu - \mu} \sum_\zeta \zeta^\mu e^{\mu t} \\ &= \sum_{\nu=0}^{\infty} d_\nu \sum_{\substack{\mu=0 \\ p \mid \mu}}^{\nu} \binom{\nu}{\mu} (-1)^{\nu-\mu} e^{\mu t} = \sum_{k=0}^{\infty} \tilde{e}_k p^k \frac{t^k}{k!} \end{aligned}$$

with $\tilde{e}_k \in O_p$.

By all our previous considerations, we have

$$\begin{aligned} 0 &\equiv \sum_{j=0}^{r} (-1)^{r-j} \binom{r}{j} \tilde{c}^*_{m+j(p-1)} \\ &= \sum_{j=0}^{r} (-1)^{r-j} \binom{r}{j} \frac{c_{m+j(p-1)}}{\gamma^{m+j(p-1)}} - \sum_{j=0}^{r} (-1)^{r-j} \binom{r}{j} e_{m+j(p-1)} \\ &\equiv \sum_{j=0}^{r} (-1)^{r-j} \binom{r}{j} \frac{c_{m+j(p-1)}}{\gamma^{m+j(p-1)}} \bmod p^r O_p \end{aligned}$$

for all $r \geq m$. Multiplying this congruence by the unit $\gamma^{m+r(p-1)}$ we obtain

$$\sum_{k=0}^{\infty} (-1)^{r-j} \binom{r}{j} (\gamma^{p-1})^{r-j} c_{m+j(p-1)} \equiv 0 \bmod p^r O_p$$

for all $r \geq m$.

Finally, we claim $\gamma^{p-1} \equiv \varepsilon_p \bmod pO_p$. One way to see this is to differentiate $\lambda(z) = \gamma^{-1} \log(1 + g(z))$ p times with respect to z and set $z = 0$. Then $\lambda^{(p)}(z) = \sum_{k=1}^{\infty} (k+1) \dots (k+p-1) \varepsilon_{k+p} z^k$. So $\lambda^{(p)}(0) = (p-1)! \varepsilon_p \equiv -\varepsilon_p \bmod p$. On the other hand, by [**17**, p. 6],

$$\begin{aligned} &\left(\frac{d}{dz}\right)^p (\gamma^{-1} \log(1 + g(z))) \\ &\qquad \equiv \frac{-\gamma^{-1}}{(1+g(z))^p} (g'(z))^p + \frac{\gamma^{-1}}{1+g(z)} g^{(p)}(z) \bmod pO_p[[z]]. \end{aligned}$$

Thus,

$$\left(\frac{d}{dz}\right)^p (\gamma^{-1} \log(1 + g(z)))|_{z=0} \equiv -\gamma^{p-1} \bmod pO_p.$$

Therefore, $\varepsilon_p \equiv \gamma^{p-1} \bmod p$.

This implies that in the Kummer congruences above, we may replace γ^{p-1} by ε_p and still retain valid congruences, cf., e.g., [**9**].

In the case that the formal group has height greater than 1, two difficulties arise: Determining the exact structure of A, or, equivalently, the p-divisible dual of the formal group and, secondly, determining the image of the map $M(A, O_p) \to O_p[z]$ which is no longer onto. For partial results, see [**6, 7**]. Also, see Andrew Baker's article [**1**], which contains some rather extensive extensions of [**6, 7**].

REFERENCES

1. A. Baker, *Lubin-Tate formal groups and p-adic integration on rings of integers*, preprint.

2. L. Carlitz, *Congruences for the coefficients of the Jacobi elliptic functions*, Duke Math. J. **16** (1949), 297–302.

3. T. Honda, *Formal groups and zeta functions*, Osaka J. Math. **5** (1968), 199–213.

4. A. Hurwitz and R. Courant, *Funktionentheorie*, J. Springer, Berlin, 1925.

5. N. Katz, *p-adic L-functions via module of elliptic curves*, Algebraic Geometry, Proc. Symposium Pure Math, Arcata, Amer. Math. Soc. **29**, Providence, (1975), 479–506.

6. ———, *Formal groups and p-adic interpolation*, Asterisque **41-42** (1977), 55–65.

7. ———, *Divisibilities, congruences, and Cartier duality*, J. Fac. Sci. Univ., Tokyo, **28** (1982), 667–678.

8. N. Koblitz, *p-adic numbers, p-adic analysis, and Zeta-functions*, Graduate Texts in Math. **58**, Springer-Verlag, New York, 1977.

9. H. Lang, *Kummersche Kongruenzen für die normierten Entwicklungskoeffizienten der Weierstrassschen-Funktion*, Abh. Math. Sem. Univ. **33**, Hamburg, (1969), 183–196.

10. S. Lang, *Elliptic functions*, Addison Wesley, Reading, MA, 1973.

11. ———, *Cyclotomic fields*, Graduate Texts in Math. **59**, Springer-Verlag, New York, 1978.

12. S. Lichlenbaum, *On p-adic L-functions associated to elliptic curves*, Invent. Math. **56** (1980), 19–55.

13. J. Lubin, *One parameter formal Lie groups over p-adic integer rings*, Ann. Math. **80** (1964), 464–484.

14. J-P. Serre, *Formes modulaires et fonctions zêta p-adique*, Modular functions of one variable III (Antwerp 1972), 191–268, Springer Lecture Notes in Math. **350** (1973).

15. ———, private communication, 1982.

16. C. Snyder, *Kummer congruences for the coefficients of Hurwitz series*, Acta Arith. **40** (1982), 175–191.

17. ———, *A concept of Bernoulli numbers in algebraic function fields* II, Manuscripta Math. **35** (1981), 69–89.

18. ———, *Kummer congruences in formal groups and algebraic groups of dimension one*, Rocky Mountain J. Mathematics **15**, 1985, 1—11.

19. J. Tate, *p-divisible groups*, in Proc. Conf. Local Fields (T.A. Springer, ed.), Springer-Verlag, Berlin (1967), 158–183.

20. L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer-Verlag, New York, 1980.

University of Maine, Department of Mathematics, Orono, ME 04469