NICHOLAS M. KATZ

Formal groups and p-adic interpolation

Astérisque, tome 41-42 (1977), p. 55-65
<http://www.numdam.org/item?id=AST_1977__41-42__55_0>

Société Mathématique de France
Astérisque 41-42 (1977) p.55-65

Formal Groups and p-adic Interpolation

Nicholas M. Katz

The ideas in this paper grew out of discussions with Lichtenbaum about the "meaning" of Leopoldt's Γ-transform, and out of reading a letter of Tate to Serre dated January 12, 1965 which was kindly made available to me by Serre. I would like to thank them.

I. Statement of the problem

Let K be a field of characteristic zero, complete under a real-valued non-archimedean valuation "ord", with integer ring $\mathcal{O}_K$, and residue field k. We assume that k has characteristic $p > 0$, and we normalize the valuation so that $\operatorname{ord}(p) = 1$. We denote by $\mathbb{C}$ the completion of the algebraic closure $\overline{K}$ of K, and by $\mathcal{O}_{\mathbb{C}}$ its ring of integers. We denote by Gal the galois group of $\overline{K}/K$, which we will also view as the group of all continuous automorphisms of $\mathbb{C}/K$.

Let G be a one-parameter formal group over $\mathcal{O}_K$, of finite height h, and denote by $A(G)$ its coordinate ring. In terms of a parameter X for G, $A(G)$ is just $\mathcal{O}_K[[X]]$. Let D be the unique translation-invariant derivation of $A(G)$ into itself satisfying $DX(0) = 1$. Given a function on G, i.e., an element $f \in A(G)$, consider the sequence $c(n)$ of elements of $\mathcal{O}_K$ defined by

$$c(n) = (D^n f)(0).$$

It is natural to ask:

1. What are the divisibility properties of the numbers $c(n)$?

Give an explicit integer-valued function $*(n)$ such that $\operatorname{ord}(c(n)) \geq *(n)$.

2. What are the interpolation properties of the numbers $c(n)/*(n)$? Give p-adic congruences among them.

II. Two examples

1. Begin with the algebraic group $\mathbb{G}_m$ over $\mathcal{O}_K$, $\mathbb{G}_m = \operatorname{Spec}(\mathcal{O}_K[T, T^{-1}])$, and take for G the associated formal group $\hat{\mathbb{G}}_m$, with parameter $X = T - 1$. Then D is $T\frac{d}{dt} = (1 + X)\frac{d}{dX}$. Given a K-rational function $f \in K(T)$ on $\mathbb{G}_m$, f lies in $A(G)$ if and only if its Laurent series expansion at the origin, a priori in $K((X))$, actually lies in $\mathcal{O}_K((X)) \cap K[[X]] = \mathcal{O}_K[[X]]$. Choose any integer $b \geq 1$ prime to p. Then the functions

$$f_b(T) = \frac{T}{1 - T} - b\frac{T^b}{1 - T^b}$$

$$\tilde{f}_b(T) = f_b(T) - f_b(T^p).$$

both lie in $A(G)$. As was first observed by Euler, the $c(n)$ for these functions are essentially the values at negative integers $-n$ of the Riemann zeta function:

$$D^n f_b(0) = (1 - b^{n+1})\zeta(-n).$$

$$D^n \tilde{f}_b(0) = (1 - b^{n+1})(1 - p^n)\zeta(-n).$$

2. Begin with an elliptic curve E over $\mathcal{O}_K$. To fix ideas, suppose that $p \neq 2,3$, and write a Weierstrass equation for $E : y^2 = 4x^3 - g_2x - g_3$, with $(g_2)^3 - 27(g_3)^2$ invertible in $\mathcal{O}_K$. Take for G the associated formal group $\hat{E}$, with parameter $X = -2x/y$. Then D is the derivation $y\frac{d}{dx}$. Given a K-rational function $f \in K(x,y)$ on E, it lies in $A(G)$ if and only if its Laurent series expansion at the origin, a priori in $K((X))$, actually lies in $\mathcal{O}_K((X)) \cap K[[X]] = \mathcal{O}_K[[X]]$. Choose any

element $[b] \in \mathrm{End}_{\mathcal{O}_K}(E)$ which has degree prime to p, and let $b \in \mathcal{O}_K$ be the effect of $[b]$ on the invariant differential dx/y : $[b]^*(dx/y) = b \cdot dx/y$. Then the function

$$f_b = x - b^2 \cdot [b]^*(x)$$

lies in $A(G)$. Suppose further that E admits an endomorphism $[\pi]$ whose kernel on all of E is precisely the kernel of $[p]$ on $\hat{E}$. Then we define

$$\tilde{f}_b = f_b - \frac{\pi^2}{\deg([\pi])} [\pi]^*(f_b).$$

[If E has <u>supersingular</u> reduction, such an endomorphism always exists, namely $[p]$ itself, and the factor $\pi^2/\deg([\pi])$ disappears. If E has ordinary reduction, such a $[\pi]$ exists if and only if E is definable over $\mathbb{Z}_p$, and if E is the <u>canonical</u> <u>lifting</u> of its reduction.]

The $c(n)$ for these functions were first studied by Hurwitz [2], and more recently by H. Lang [6] and G. Robert [9]; they are essentially the "Bernoulli-Hurwitz numbers" of [3]:

$$D^n f_b(0) = (1 - b^{n+2}) \frac{BH_{n+2}}{n+2}$$

$$D^n \tilde{f}_b(0) = (1 - b^{n+2})\left(1 - \frac{\pi^{n+2}}{\deg([\pi])}\right) \frac{BH_{n+2}}{n+2} .$$

Recall that the BH_n are defined in terms of the Weierstrass $\wp$-function with invariants g_2 and g_3 by the power series expansion

$$\wp(z) = \frac{1}{z^2} + \sum_{n \geq 2} \frac{BH_{n+2}}{n+2} \cdot \frac{z^n}{n!} .$$

III. <u>An apparent digression: galois measures on Tate modules</u>

We denote by $T_p G^\vee$ Tate module of the "p-divisible dual" $G^\vee$ of G, i.e. the $\mathbb{Z}_p$-module

$$T_p G^\vee = \mathrm{Hom}_{\text{formal gp's}/\mathcal{O}_{\mathbb{C}}}(G_{\mathcal{O}_{\mathbb{C}}}, (\hat{\mathbb{G}}_m)_{\mathcal{O}_{\mathbb{C}}})$$

of all formal group homomorphisms, defined over $\mathcal{O}_{\mathbb{C}}$, from G to $\hat{\mathbb{G}}_m$. Elements $t \in T_p G^\vee$ are precisely the series $t(X) \in A(G) \hat{\otimes} \mathcal{O}_{\mathbb{C}} = \mathcal{O}_{\mathbb{C}}[[X]]$ which satisfy

$$\begin{cases} t(0) = 1 \\ t(X \underset{G}{+} Y) = t(X) \cdot t(Y) \end{cases}$$

where

$$X \underset{G}{+} Y = X + Y + \ldots \in \mathcal{O}_K[[X,Y]]$$

is the formal group law. As a $\mathbb{Z}_p$-module, $T_p G^\vee$ is free of rank h, and Gal operates continuously (by conjugating the coefficients of the series $t(X)$). By Tate [11], the formal group G over $\mathcal{O}_K$ is uniquely determined by $T_p G^\vee$ as a $\mathbb{Z}_p[\mathrm{Gal}]$-module.

Let us denote by $\mathrm{Contin}(T_p G^\vee, \mathcal{O}_{\mathbb{C}})$ the $\mathcal{O}_{\mathbb{C}}$-module of all continuous $\mathcal{O}_{\mathbb{C}}$-valued functions on $T_p G^\vee$, and by $\mathrm{Gal\text{-}Contin}(T_p G^\vee, \mathcal{O}_{\mathbb{C}})$ the $\mathcal{O}_K$-submodule of those continuous functions $h(t)$ which are Gal-equivariant:

$$h(\sigma t) = \sigma(h(t)) \quad \text{for all } \sigma \in \mathrm{Gal},\ t \in T_p G^\vee$$

For any p-adically complete and separated $\mathcal{O}_K$-algebra S, we define an "S-valued galois measure" μ on $T_p G^\vee$ to be an $\mathcal{O}_K$-linear map from $\mathrm{Gal\text{-}Contin}(T_p G^\vee, \mathcal{O}_{\mathbb{C}})$ to S, which we write symbolically as

$$h \longmapsto \int h(t)\,d\mu \ .$$

We denote by $T_p^\times G^\vee \subset T_p G^\vee$ the <u>complement</u> of $p \cdot T_p G^\vee$; it is open, closed, and stable by Gal. A galois measure μ on $T_p G^\vee$ is said to be supported in $T_p^\times G^\vee$ if

$$\int h(t)\,d\mu = 0 \quad \text{whenever } h \text{ vanishes on all of } T_p^\times G^\vee.$$

<u>Obvious Lemma</u> If $g,h \in \text{Gal-Contin}(T_pG^\vee, \mathcal{O}_{\mathbb{C}})$ satisfy $g(t) \equiv h(t) \bmod p^N \cdot \mathcal{O}_{\mathbb{C}}$ for all $t \in T_p^\times G^\vee$, then for any S-valued galois measure μ on $T_pG^\vee$ which is supported in $T_p^\times G^\vee$, we have

$$\int g(t)d\mu \equiv \int h(t)d\mu \qquad \bmod p^N \cdot S .$$

Let us denote by $\text{Diff}(G)$ the commutative algebra of all translation-invariant differential operators on G, and by $\text{Diff}^\wedge(G)$ its p-adic completion, which is itself the algebra of all (p,X)-adically continuous, translation-invariant $\mathcal{O}_K$-linear endomorphisms of $A(G)$(the (X)-adically continuous ones are precisely the elements of $\text{Diff}(G)$). We denote by

$$\langle\ ,\ \rangle : \text{Diff}^\wedge(G) \times A(G) \longrightarrow \mathcal{O}_K$$

the $\mathcal{O}_K$-linear pairing

$$\langle \mathcal{D}, f\rangle \overset{\text{dfn}}{=\!=} (\mathcal{D}(f)(0).$$

This pairing makes $A(G)$ the algebraic $\mathcal{O}_K$-dual of $\text{Diff}^\wedge(G)$, and it makes $\text{Diff}^\wedge(G)$ the (p,X)-adically continuous $\mathcal{O}_K$-dual of $A(G)$.

Every element $t \in T_pG^\vee$, viewed as a function $t(X) \in A(G) \hat{\otimes} \mathcal{O}_{\mathbb{C}}$, is an eigenfunction of every $\mathcal{D} \in \text{Diff}^\wedge(G)$, with eigenvalue $\langle \mathcal{D}, t\rangle$:

$$\mathcal{D}(t) = \langle \mathcal{D}, t\rangle \cdot t(X).$$

For fixed $\mathcal{D} \in \text{Diff}^\wedge(G)$, the $\mathcal{O}_{\mathbb{C}}$-valued function $t \longrightarrow \langle \mathcal{D}, t\rangle$ on $T_pG^\vee$ is Gal-equivariant and continuous, and the map

$$(*) \qquad \text{Diff}^\wedge(G) \longrightarrow \text{Gal-Contin}(T_pG^\vee, \mathcal{O}_{\mathbb{C}})$$

$$\mathcal{D} \longmapsto \text{the function } t \longmapsto \langle \mathcal{D}, t\rangle$$

is an $\mathcal{O}_K$-algebra homomorphism.

Applying the functor $\text{Hom}_{\mathcal{O}_K\text{-lin}}(?\ , S)$, we obtain an S-linear map

$$(**) \qquad \{\text{S-valued galois measures on } T_pG^\vee\} \longrightarrow A(G) \hat{\otimes} S.$$

It is not hard to show that this map is injective, at least if S is flat over $\mathcal{O}_K$ and if the valuation on K is discrete, and that its image is contained in

$$\{f \in A(G) \hat{\otimes} S \;\Big|\; \text{for all } n \geq 1, \text{ the function } \sum_{\zeta \in \operatorname{Ker}[p^n](\mathcal{O}_{\mathbb{C}})} f(X \underset{G}{+} \zeta) \text{ lies in } p^{nh} \cdot A(G) \hat{\otimes} S\} .$$

We can be more precise about the image of (**) only in some special cases.

IV. The main theorem

Theorem Suppose that either $h = 1$, with K arbitrary, or that $h = 2$ and that K is absolutely unramified (in the sense that p is a uniformizing parameter for K). Then:

1. For each p-adically complete and separated flat $\mathcal{O}_K$-algebra S, the (inverse of the)(**) construction establishes a bijection $f \longmapsto \mu_f$ between

$$\left\{ f \in A(G) \hat{\otimes} S \;\middle|\; \text{for all } n \geq 1, \sum_{\zeta \in \operatorname{Ker}[p^n](\mathcal{O}_{\mathbb{C}})} f(X \underset{G}{+} \zeta) \text{ lies in } p^{nh} A(G) \hat{\otimes} S \right\}$$

and

$$\{S\text{-valued galois measures on } T_p G^{\vee}\} ,$$

in such a way that we have the integration formulas

$$\begin{cases} \int \langle \mathcal{D}, t\rangle \cdot h(t) d\mu_f = \int h(t) d\mu_{\mathcal{D}(f)} \\ \int \langle \mathcal{D}, t\rangle \, d\mu_f = \langle \mathcal{D}, f\rangle = (\mathcal{D}(f))(0) . \end{cases}$$

for any $\mathcal{D} \in \operatorname{Diff}^{\wedge}(G)$ and any $h \in \text{Gal-Contin}(T_p G^{\vee}, \mathcal{O}_{\mathbb{C}})$.

2. The galois measure μ_f is supported in $T_p^{\times}\check{G}$ if and only if f satisfies

$$\sum_{\zeta \in \mathrm{Ker}[p](\mathcal{O}_{\mathbb{C}})} f(X \underset{G}{+} \zeta) = 0.$$

Remarks For $h = 1$, the map (*) is itself an isomorphism. To see this, one first reduces to the case $G = \hat{\mathbb{G}}_m$ over $\mathcal{O}_{\mathbb{C}}$ itself. Then Mahler's theorem [8], representing continuous functions on $\mathbb{Z}_p$ in terms of the "binomial coefficient" functions, says exactly that (*) is an isomorphism. The resulting identification of measures on $\mathbb{Z}_p$ with elements of $A(\hat{\mathbb{G}}_m)$ occurs prominently in the work of Iwasawa, where $A(\hat{\mathbb{G}}_m)$ is viewed as the group ring of $\mathbb{Z}_p$.

For $h = 2$, the proof depends heavily upon the fact that $\check{G}$ is a one-parameter formal group over an unramified ground-ring (so that by Eisenstein any two elements of $T_p^{\times}\check{G}$ are conjugate by Gal) and upon the Tate-Ax-Sen theorem ([1], [10], [11]) on the invariants of closed subgroups of Gal acting on $\mathcal{O}_{\mathbb{C}}/p^n\mathcal{O}_{\mathbb{C}}$.

V. Some applications

The congruence properties which flow from having a measure on $\mathbb{Z}_p$, or more generally on $T_p^{\times}\check{G}$ with G of height one, have been voluminously documented. In the first ($G = \hat{\mathbb{G}}_m$) example given in II, the function $\tilde{f}_b$ satisfies

$$\sum_{\zeta^p = 1} \tilde{f}_b(\zeta T) = 0 .$$

and the corresponding measure on $\mathbb{Z}_p^{\times}$ gives the theory of the Kubota-Leopoldt L-function for $\mathbb{Q}$(c.f. [4], [5], [7]). In the height one case of the second ($G = \hat{E}$) example given in II, the function $\tilde{f}_b$ differs by an additive constant from a function $\tilde{\tilde{f}}_b$ which satisfies

$$\sum_{\zeta \in \mathrm{Ker}[p]_G} \tilde{\tilde{f}}_b\,(X \underset{G}{+} \zeta) = 0\ ,$$

and the corresponding measure on $T_p^{\times}(\hat{E})^{\vee}$ gives the theory of the "one-variable" p-adic L-function attached to an elliptic curve with ordinary reduction (c.f. [4], [5], [7]).

Only in the case of height two do we obtain new results. For the remainder of this section, we consider a one-parameter, height two formal group G over $\mathcal{O}_K$ where K is absolutely unramified, given with a parameter X, and a function $f \in A(G)$ satisfying

$$\sum_{\zeta \in \mathrm{Ker}[p]_G(\mathcal{O}_{\mathbb{C}})} f(X \underset{G}{+} \zeta) = 0\ ,$$

so that the corresponding galois measure $\mu = \mu_f$ is supported in $T_p^{\times}G^{\vee}$.

Let us denote by $a_1(t), a_2(t), \ldots$ the Gal-equivariant continuous functions on $T_pG^{\vee}$ obtained by writing an element $t \in T_pG^{\vee}$ as a series in X:

$$t(X) = 1 + a_1(t)X + a_2(t)X^2 + \ldots\ .$$

The function $a_1(t)$ is none other than the function $\langle D, t\rangle$ corresponding to the invariant derivation D. Thus for $n \geq 0$ we have

$$\int (a_1(t))^n d\mu_f = \int \langle D, t\rangle^n d\mu_f = \int \langle D^n, t\rangle d\mu_f = D^n f(0) = c(n)\ .$$

Therefore, divisibility and congruence properties of the <u>numbers</u> $c(n)$ follow from the corresponding properties of the <u>functions</u> $(a_1(t))^n$ on $T_p^{\times}G^{\vee}$, which we given in Lemmas 1 and 2 below.

<u>Lemma 1</u> If $t \in T_p^{\times}G^{\vee}$, then $\mathrm{ord}(a_1(t)) = p/(p^2 - 1)$.

<u>Corollary 1</u> The function $(a_1(t))^n$ is divisible by $p^{[np/(p^2-1)]}$ Gal-Contin$(T_p^{\times}G^{\vee}, \mathcal{O}_{\mathbb{C}})$.

Corollary 2 $\quad \mathrm{ord}(c(n)) \geq [np/(p^2 - 1)]$.

Lemma 2 Let $u \in (\mathcal{O}_K)^\times$ be the coefficient of X^{p^2} in the series $[p]_G(X)$. Then for $t \in T_p^\times G^\vee$, we have

$$\mathrm{ord}\left(\frac{(a_1(t))^{p^2-1}}{-u \cdot p^p} - 1\right) \geq 1 - \frac{1}{p} .$$

Corollary 3 Let v be a unit in an unramified extension of K, such that $v^{p^2-1} \equiv -u \bmod p$. Then the function on non-negative integers $n \longrightarrow L(n)$ defined by

$$L(n) = \int \frac{(a_1(t))^n}{v^n \cdot p^{[np/(p^2-1)]}} \, d\mu_f = \frac{c(n)}{v^n \, p^{[np/(p^2-1)]}}$$

satisfies the congruences

1. $L(n) \equiv L(m) \mod p^N \quad$ if $\quad n \equiv m \mod (p^2 - 1)p^N$

2. $L(n) \equiv L(n + p^2 - 1) \mod p \quad$ if $\quad n \not\equiv 0, p, 2p, \ldots, (p-1)p \mod p^2 - 1$.

Suppose now that G is the formal group of an elliptic curve E over $\mathcal{O}_K$ (K absolutely unramified) having supersingular reduction, given with a nowhere-vanishing invariant differential ω. Then the function $\tilde{f}_b$ does in fact satisfy

$$\sum_{\zeta \in \mathrm{Ker}[p]} \tilde{f}_b(X \underset{G}{+} \zeta) = 0 ,$$

and therefore corollaries 2 and 3 apply to its $c(n)$:

$$c(n) = D^n \tilde{f}_b(0) = (1 - b^{n+2})(1 - p^n) \cdot \frac{BH_{n+2}}{n+2} .$$

(A weaker version of corollary 2 for these $c(n)$, namely $\mathrm{ord}\, c(n) \geq [n/p]$, is due to H. Lang [6]). If in addition we suppose that $\mathcal{O}_K$ is $\mathbb{Z}_p$, with $p \geq 5$, then we may take $v = 1$ in Corollary 3.

VI <u>A question</u> In the case of height two, the Hodge-Tate decomposition of $T_pG^\vee$, namely

$$(T_pG^\vee) \otimes \mathbb{C} \simeq \mathbb{C} \oplus \mathbb{C}(1) ,$$

together with the natural inclusion $T_pG^\vee \subset (T_pG^\vee) \otimes \mathbb{C}$, gives us Gal-equivariant $\mathbb{Z}_p$-linear maps

$$T_pG^\vee \longrightarrow \mathbb{C} \quad ; \quad T_pG^\vee \longrightarrow \mathbb{C}(1) .$$

The first of these is none other than the function $a_1(t)$. We can view the second as a $\mathbb{Z}_p$-linear $\mathbb{C}$-valued function $b_1(t)$ on $T_pG^\vee$, which satisfies the transformation rule

$$b_1(\sigma t) = \chi(\sigma) \cdot \sigma(b_1(t))$$

where $\chi : \mathrm{Gal} \longrightarrow \mathbb{Z}_p^\times$ is the standard cyclotomic character.

Suppose now that G is $\hat{E}$, where E is a CM elliptic curve with CM field K_0 in which p stays prime. What, if any, is the relation between the divisibility and congruence properties of the monomials $(a_1(t))^n \cdot (b_1(t))^m$, as functions on $T_p^\times G^\vee$, and the corresponding properties of the values at $s = 0$ of L-series with grössencharacter of type A_0 of the field K_0?

References

1. J. Ax, Zeroes of Polynomials over Local Fields - The Galois Action, J. Algebra 15 (1970), 417-428.

2. A. Hurwitz, Über die Entwicklungskoeffitzienten der Lemniscatischen Funktionen, Math. Ann. 51 (1899), 196-226.

3. N. Katz, The Congruences of Clausen-von Staudt and Kummer for Bernoulli Hurwitz Numbers, Math. Ann. 216 (1975), 1-4.

4. ______, The Eisenstein Measure and p-adic Interpolation, to appear in Am. J. Math.

5. ______, P-adic L-Functions Via Moduli of Elliptic Curves, in Algebraic Geometry, Arcata 1974, Proc. Symp. Pure Math. 29, A.M.S. Providence (1975), 479-506.

6. H. Lang, Kummersche Kongruenzen für die normierten Entwicklungskoeffitzienten der Weierstrass'schen $\wp$-Funktion, Abh. Math. Sem. Hamburg 33 (1969), 183-196.

7. S. Lichtenbaum, On p-adic L-functions associated to elliptic curves.

8. K. Mahler, An Interpolation Series for a Continuous Function of a p-adic variable. J. Reine Ang. Math. 199 (1958), 23-34.

9. G. Robert, Nombres de Hurwitz et Unités Elliptiques, to appear.

10. S. Sen, On Automorphisms of Local Fields, Ann. Math. (2) 90 (1969), 33-46.

11. J. Tate, p-divisible groups, in Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin (1967).

12. J. Tate, Letter to J.-P. Serre dated January 12, 1965.

Nicholas M. KATZ
Fine Hall
PRINCETON, N.J. 08540
(U.S.A.)