SMF/AMS TEXTS *and* MONOGRAPHS • *Volume* 3

Astérisque • *Numéro* 229 • 1995

p-adic L-Functions and p-adic Representations

Bernadette Perrin-Riou

Translated by
Leila Schneps

American Mathematical Society
Société Mathématique de France

Contents

Preface

The arithmetic interpretation of the values at integers of complex L-functions associated to projective varieties over number fields is fundamental in number theory. By means of a great deal of work, Bloch-Kato style conjectures have made it possible to understand how to interpret these numbers in a very general framework. Starting with the very first examples of p-adic interpolation of these numbers, it is natural to dream of constructing p-adic L-functions having properties as similar as possible to complex L-functions. Iwasawa theory, for example, can be used to construct two types of p-adic L-functions: the first type takes as its starting point the values of the complex L-functions, and the second type works with the arithmetic interpretation of these values. Relations between the two types of L-functions constructed by Iwasawa theory are for the present entirely conjectural.

Let us briefly survey some well-known cases. The first example of an L-function is Riemann's ζ function, which is defined as the meromorphic continuation $\zeta(s)$ of

$$\sum_{n>0} n^{-s} = \prod_{\ell} (1 - \ell^{-s})^{-1}$$

to all of $\mathbb{C}$, where the product is over all prime numbers ℓ. A p-adic analog of ζ was first constructed by Kubota-Leopoldt, and then by Iwasawa, not as a product of Euler factors, which does not (yet!) make sense p-adically, but by a process of p-adic interpolation of the values $\zeta(k)$ for all strictly negative odd integers k. Thus, the study of the p-adic properties of the values $\zeta(k)$, or rather of the values

$$\zeta_{\{p\}}(k) = (1 - p^{-k})\zeta(k) \tag{1}$$

shows that it is possible to construct a continuous function $\zeta_p(s, \omega^j)$ for every class j modulo $p-1$, where $s \in \mathbb{Z}_p - \{1\}$ and ω is the Teichmüller character, such that $\zeta_p(k, \omega^j) = \zeta_{\{p\}}(k)$ for $k \equiv j \mod p-1$ whenever k is a negative odd integer. Using the functional equation, this formula can also be rewritten in terms of the positive even integers: the interpolated values are then

$$\Gamma(k)(1 - p^{-k})^{-1}(1 - p^{k-1}) \frac{\zeta_{\{p\}}(k)}{(2\pi i)^k} \tag{2}$$

for every positive even integer k belonging to a fixed congruence class modulo $p-1$. In fact, this p-adic ζ function can also be defined by interpolating the values for fixed k of the L-functions associated to Dirichlet characters η whose conductor is a power of p and which satisfy $\eta(-1) = (-1)^k$.

Another example which has become classical is that of elliptic curves E over $\mathbb{Q}$ having good ordinary reduction at p, which are modular or have complex multiplication. The first constructions of the p-adic L-functions associated to such elliptic curves were due to Mazur and Swinnerton-Dyer in the first case, and to Coates and

Wiles in the second one. In the case of elliptic modular curves with ordinary reduction at p, the p-adic L-function is obtained by p-adic interpolation of the values of the Hasse-Weil function of $E/\mathbb{Q}$ at 1 twisted by a Dirichlet character of conductor an arbitrarily large power of p; the value at $\mathbf{1}$ of this p-adic L-function (in a sense to be defined) then has the form

$$(1-\alpha_p^{-1})(1-p^{-1}\alpha_p)^{-1}L_{\{p\}}(E/\mathbb{Q},1) \tag{3}$$

where $L_{\{p\}}(E/\mathbb{Q},1)$ is the "incomplete" L-function at p of $E/\mathbb{Q}$, i.e.

$$L_{\{p\}}(E/\mathbb{Q},s)=(1-\alpha_p p^{-s})(1-\beta_p p^{-s})L(E/\mathbb{Q},s),$$

and where $(1-\alpha_p p^{-s})(1-\beta_p p^{-s})$ is the Euler factor at p with α_p a p-adic unit.

The idea of Iwasawa theory is to construct an ideal of the Iwasawa algebra starting from the p-adic representation associated to the situation: $\mathbb{Q}_p(1)$ in the first case, the tensor product of $\mathbb{Q}_p$ with the Tate module of the points of order a power of p on the elliptic curve in the second case (Iwasawa, Mazur, Greenberg, Schneider...). In these much-studied cases, we are dealing with so-called ordinary representations, and the desired ideal is constructed as the characteristic ideal of a certain module (the Pontryagin dual of a Selmer group). The main conjectures give the precise relations between this characteristic ideal and the interpolated p-adic L-function.

In this book, we propose a generalization of the above theory to p-adic representations having good reduction at p. The simplest non-ordinary case is the case of the p-adic representation associated to a modular elliptic curve E having good supersingular reduction at p. Several new phenomena appear. On the side of L-functions, two p-adic L-functions can be constructed; their values at $\mathbf{1}$ are given respectively by

$$(1-\alpha_p^{-1})(1-p^{-1}\alpha_p)^{-1}L_{\{p\}}(E/\mathbb{Q},1) \tag{4}$$

and

$$(1-\beta_p^{-1})(1-p^{-1}\beta_p)^{-1}L_{\{p\}}(E/\mathbb{Q},1). \tag{5}$$

These functions no longer belong to the Iwasawa algebra (an algebra isomorphic to the algebra of formal power series in one variable with coefficients in $\mathbb{Z}_p$); their power series expansions have denominators. On the side of Iwasawa modules, the natural candidates are not torsion modules over the Iwasawa algebra.

Let us roughly indicate how to overcome these difficulties.

Firstly, all the p-adic L-functions we construct will depend on a parameter belonging to a suitable exterior power of the Dieudonné-Fontaine module D associated to the p-adic representation. When we evaluate them at the trivial character $\mathbf{1}$, the same exterior power of an operator $(1-\varphi)(1-p^{-1}\varphi^{-1})^{-1}$ will appear, where φ is the Frobenius operator acting on D. The eigenvalues of this operator provide the explanation of the "bizarre" Euler factors appearing in the interpolation formulas.

On the side of arithmetic Iwasawa theory, we do not attempt to construct a torsion module over the Iwasawa algebra, which we do not believe has any good reason to exist. Instead, very roughly, we use modules constructed starting from Galois cohomology groups H^1 and H^2 which are "unramified" outside of a "sufficiently large" finite number of places, and "measuring" them by means of an "expanded logarithm" or regulator with values in the tensor product of D with an algebra of functions contained in the Iwasawa algebra.

To make this a little more precise, let us give some notation.

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and $\overline{\mathbb{Q}}_p$ an algebraic closure of $\mathbb{Q}_p$. If F is a number field contained in $\overline{\mathbb{Q}}$, we set $\overline{F} = \overline{\mathbb{Q}}$, $G_F = \mathrm{Gal}(\overline{F}/F)$. Let p be an odd prime number. Throughout this book, we fix an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_p$. We fix a number field F **unramified at** p. We set $F_\infty = F(\mu_{p^\infty})$, $F_n = F(\mu_{p^{n+1}})$, $G_n = \mathrm{Gal}(F_n/F)$, $G_\infty = \mathrm{Gal}(F_\infty/F)$ and $\Lambda = \mathbb{Z}_p[[G_\infty]]$. The group G_∞ is canonically isomorphic to $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. If S is a finite set of places containing the places at infinity and the places of F lying over p, we write $G_{S,F}$ for the Galois group of the maximal algebraic extension of F unramified outside S.

Let V be a pseudo-geometric p-adic representation of G_F, (pseudo-geometric means unramified outside of a finite set of places of F and de Rham at the places of F lying over p) which is crystalline at the places of F lying over p. Let S be a finite set of places containing the places over p, the places at infinity and the places where V is ramified. Then V can be consider as a p-adic representation of $G_{S,F}$. To every lattice $\mathbf{T}$ of V stable under G_F, we attach a Λ-module of rank ≤ 1, which we denote by $\mathbb{I}_{arith,\{p\}}(\mathbf{T})$ and call **the module of the arithmetic p-adic L-functions of $\mathbf{T}$**. The construction is functorial in $\mathbf{T}$, multiplicative for exact sequences, and compatible with twisting homomorphisms by Tate's representation $\mathbb{Q}_p(j)$ for every integer j; we have a functional equation relating V to $V^*(1) = \mathrm{Hom}_{\mathbb{Q}_p}(V, \mathbb{Q}_p(1))$ and $\mathbf{T}$ to $\mathbf{T}^*(1) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbf{T}, \mathbb{Z}_p(1))$. More precisely, if $\mathbf{D}_p(V)$ is the filtered φ-module associated to $\mathrm{Ind}_{F/\mathbb{Q}}(V)$ over $\mathbb{Q}_p$ by Fontaine's theory, the Λ-module $\mathbb{I}_{arith,\{p\}}(\mathbf{T})$ is naturally (up to a particle of dust...) contained in $\mathcal{K}(G_\infty) \otimes \wedge^* \mathbf{D}_p(V^*(1))$ where $\mathcal{K}(G_\infty)$ is the total ring of fractions of an algebra $\mathcal{H}(G_\infty)$ containing the Iwasawa algebra Λ and where $\wedge^* \mathbf{D}_p(V^*(1))$ is the exterior algebra of $\mathbf{D}_p(V^*(1))$ (in fact, we can replace $\mathcal{K}(G_\infty)$ by $\mathcal{H}(G_\infty) \otimes \mathrm{Frac}(\Lambda)$ where $\mathrm{Frac}(\Lambda)$ is the total ring of fractions of Λ). If we consider the component $\mathbb{I}_{arith,\{p\}}(\mathbf{T})_+$ fixed by $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}(\mu_p)^+)$, the suitable exterior power is the d_+-th power where d_+ is the dimension of the vector subspace of $\mathrm{Ind}_{F/\mathbb{Q}}(V)$ fixed by a complex conjugation.

How is this Λ-module constructed? The first ingredient is the expanded logarithm $\mathcal{L}_V$ which is a homomorphism of Λ-modules

$$Z^1_{\infty,p}(F, \mathbf{T}) \to \mathcal{K}(G_\infty) \otimes \mathbf{D}_p(V)$$

where $Z^1_{\infty,p}(F, \mathbf{T})$ is the projective limit of the $\oplus_{v|p} H^1(F_{n,v}, \mathbf{T})$. This homomorphism (or rather its inverse Ω_V) is constructed in [**P94**] (it depends on an integer h, but we ignore this technical difficulty in this introduction, at the price of being slightly incorrect). The existence of Ω_V and of $\mathcal{L}_V$ depends on analytic properties of the Bloch-Kato logarithms associated to the twists $V(j)$ of V for sufficiently large j. For example, a consequence of these continuity properties is that for v lying over p, if j and j' are sufficiently large integers modulo $(p-1)p^n$, and if $P \in H^1(F_v, T(j))$ and $P' \in H^1(F_v, T(j'))$ are congruent modulo p^{n+1} (i.e. their projections to $H^1(F_v, T(j)/p^{n+1}T(j)) \cong H^1(F_v, T(j')/p^{n+1}T(j'))$ are equal), then the (suitably modified) Bloch-Kato logarithms of P and of P' relative to $V(j)$ and to $V(j')$ respectively are congruent modulo p^n. For a precise statement, see §4.5 and in particular §4.5.5.

Let us return to the construction of $\mathbb{I}_{arith,\{p\}}(\mathbf{T})$, or rather, to be simpler, of $\mathbb{I}_{arith,\{p\}}(\mathbf{T})_+$. If M is a $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$-module, we set M_+ to be the submodule of M fixed by $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}(\mu_p)^+)$. We can consider $\mathbb{I}_{arith,\{p\}}(\mathbf{T})_+$ as a Λ-submodule of

$$\mathrm{Hom}_{\mathbb{Q}_p}(\wedge^{d_+}\mathbf{D}_p(V),\mathcal{K}(G_\infty)_+)$$

via the isomorphism $\mathcal{K}(G_\infty)_+\otimes\wedge^{d_+}\mathbf{D}_p(V^*(1))\cong\mathrm{Hom}_{\mathbb{Q}_p}(\wedge^{d_+}\mathbf{D}_p(V),\mathcal{K}(G_\infty)_+)$. Let us consider the Λ-modules

$$H^i_{\infty,S}(F,\mathbf{T})=\varprojlim_n H^i(G_{S,F_n},\mathbf{T}).$$

By localization, we obtain a Λ_+-module homomorphism

$$H^1_{\infty,S}(F,\mathbf{T})_+\to Z^1_{\infty,p}(F,\mathbf{T})_+.$$

If $n\in\wedge^{d_+}\mathbf{D}_p(V)$, then $\mathbb{I}_{arith,\{p\}}(\mathbf{T})_+(n)$ is essentially (up to some technical factors) given by

$$\Lambda_+f_+(H^2_{\infty,S}(F,\mathbf{T}))\cdot n\wedge\det\nolimits_{\Lambda_+}\mathcal{L}_V(H^1_{\infty,S}(F,\mathbf{T})_+)$$

where $f_+(H^2_{\infty,S}(F,\mathbf{T}))$ is a characteristic series of the Λ_+-module $H^2_{\infty,S}(F,\mathbf{T})_+$. Thus, $\mathbb{I}_{arith,\{p\}}(\mathbf{T})_+$ simultaneously measures the position of $H^1_{\infty,S}(F,\mathbf{T})_+$ inside $\mathcal{K}(G_\infty)_+\otimes\mathbf{D}_p(V^*(1))$ by the logarithm (regulator) map and the size of $H^2_{\infty,S}(F,\mathbf{T})$.

In order to be sure that this definition does not give a Λ-module equal to zero, we need the so-called weak Leopoldt conjectures for V and for $V^*(1)$. We denote the union of these two conjectures by $\mathrm{Leop}(V,V^*(1))$: they state that $H^2(G_{S,F_\infty},V/\mathbf{T})$ and $H^2(G_{S,F_\infty},V^*(1)/\mathbf{T}^*(1))$ vanish. We show that if we assume $\mathrm{Leop}(V,V^*(1))$, then $\mathbb{I}_{arith,\{p\}}(\mathbf{T})$ is free of rank 1.

Under some regularity hypotheses, it is possible to compute the value at $\mathbf{1}$ of the leading coefficient of a generator of $\mathbb{I}_{arith,\{p\}}(\mathbf{T})$, up to a unit. In particular, the operator

$$\wedge^{d_+}(1-\varphi)(1-p^{-1}\varphi^{-1})^{-1}$$

which already arose in the interpolation properties of logarithms appears again here, as do the numbers (or their p-adic analogs when dealing with complex periods) occurring in the Bloch-Kato conjectures. This makes it possible for us to establish comparisons between our conjectures and the Bloch-Kato conjectures in the framework of motives.

Similarly, if V is still a pseudo-geometric representation crystalline at the places lying over p, and if c is a complex conjugation, we attach to (V,c) a free Λ-module $\mathbb{I}_{arith,\{p\}}(V,c)$ of rank 1 contained in the total ring of fractions $\mathbb{K}$ of $\mathbb{H}=B_{cris}\otimes\mathcal{H}(G_\infty)$. The Λ-module $\mathbb{I}_{arith,\{p\}}(V,c)$ is obtained from $\mathbb{I}_{arith,\{p\}}(\mathbf{T})$ by a suitable projection. Unlike $\mathbb{I}_{arith,\{p\}}(\mathbf{T})$, it is independent of the choice of $\mathbf{T}$.

When V is the p-adic representation of $G_\mathbb{Q}$ associated to an elliptic curve on $\mathbb{Q}$ having good reduction at p, $\mathbb{I}_{arith,\{p\}}(\mathbf{T})$ is related to the Λ-submodule $\mathcal{I}_{arith}(\mathbf{T})$ of $\mathcal{K}(G_\infty)\otimes\mathbf{D}_p(V)$ defined in [**P93**]. For $V=\mathbb{Q}_p(j)$, we find the characteristic ideal of classical Iwasawa modules (2.5, see also [**P94b**]).

Now, let M be a motivic structure on $\mathbb{Q}$ in the sense of [**FP94**], with de Rham realization M_{dR}, Betti realization M_B and ℓ-adic realization M_ℓ. Its p-adic realization M_p is a pseudo-geometric p-adic representation of G_F. Suppose moreover that it is crystalline at the places of F lying over p. The Euler factor at p of the complex L-function can be interpreted as the characteristic polynomial of the "Frobenius operator" φ acting on the $\mathbb{Q}_p$-vector space $\mathbf{D}_p(M_p) \cong \mathbb{Q}_p \otimes_{\mathbb{Q}} M_{dR}$ (in the examples above, M_p is the Tate module of the p-power order roots of unity or of the p-power order points on the elliptic curve, tensored with $\mathbb{Q}_p$).

Let $\mathcal{M}$ be a $\mathbb{Z}$-structure on M. This is given by the following data: a free maximal $\mathbb{Z}$-submodule $\mathcal{M}$ of M_B, and for every prime number l, a free maximal $\mathbb{Z}_l$-module $\mathcal{M}_l$ of M_l stable under $G_{\mathbb{Q}}$ such that $\mathbb{Z}_l \otimes \mathcal{M} = \mathcal{M}_l$. Then the Λ-module $\mathbb{I}_{arith,\{p\}}(\mathcal{M}_p)$ can be defined. Moreover, M admits a complete L-function $\mathbf{L}^\infty(M)$, defined by

$$\mathbf{L}^\infty(M,s) = \prod_{\ell \in \overline{P}} L_\ell(M,s)$$

where $\overline{P}$ is the union of the set of prime numbers and ∞. Let $\mathbf{L}^\infty(M,\eta,s)$ denote the L-function twisted by a Dirichlet character η. Using the special values of $\mathbf{L}^\infty(M,\eta,j)$, where j is an integer and η is a character of finite order whose conductor is a power of p, we give a conjecture on the existence of a **distinguished generator** of $\mathbb{I}_{arith,\{p\}}(\mathcal{M}_p)$, which will be denoted by $\mathbf{L}^{p,2\pi i}_{\{p\}}(\mathcal{M})$ (it also depends on the choice of a p-adic and complex $2\pi i$). It is the **p-adic L-function of $\mathcal{M}$**. Once the objects are defined, a large part of the work consists in verifying the compatibilities between the conjectures made here and the Bloch-Kato conjectures, the functional equation, the examples already known and so on.

Let us give some details on the properties (conjecturally) defining the p-adic L-function $\mathbf{L}^{p,2\pi i}_{\{p\}}(\mathcal{M})$. This L-function is characterized by its values on χ^j for j large enough (here χ denotes the cyclotomic character). Recall that for j sufficiently large, the Beilinson conjectures predict that the quotient of $L(M(j),0)$ by a certain period $\underline{\mathrm{Per}}_{\mathcal{M}(j)}$ is a rational number. This period is the determinant (in rational bases) of $H^1_f(\mathbb{Q},M(j)) \to \mathbb{C}\otimes M_{dR}(j)/\mathbb{C}\otimes M_B(j)^+$ where $H^1_f(\mathbb{Q},M(j))$ is the $\mathbb{Q}$-vector space of the motivic points of $M(j)$. We define similarly a p-adic period $\mathrm{Per}_{M(j)_p}(n)$ for $n \in \wedge^{d_+} M_B$. Set also $\mathbf{L}^\infty_{\{p,\infty\}}(M) = \prod_{l\neq p} L_\ell(M,s)$. Then,

$$\wedge^{d_+}((1-p^j\varphi)^{-1}(1-p^{-j-1}\varphi^{-1}))\chi^{-j}\mathbf{L}^{p,2\pi i}_{\{p\}}(\mathcal{M})$$

is essentially equal (for j even) to

$$\frac{\mathbf{L}^\infty_{\{p,\infty\}}(M(j),0)}{\underline{\mathrm{Per}}_{\mathcal{M}(j)}}\mathrm{Per}_{M(j)_p}$$

(up to some factorials which we leave out here). We refer to the main body of the text for the precise formulas (cf. also [**Pa**]).

This text follows [**P94**], where what we referred to above as the expanded logarithm was constructed. The special case of elliptic curves was considered in detail in [**P93**] (see also [**BP93**]). All the p-adic representations considered here are assumed **pseudo-geometric and crystalline at the places lying over p, and defined over a number field F unramified at p.** We would also have liked to consider the case of semi-stable p-adic representations, but we were prevented from doing so by the lack of a local theory in the semi-stable framework. We also refer to [**FP91**] or [**FP94**] for the "basic" notions on geometric representations, the $\mathbb{Z}_p$-modules $H^1_f(F, \mathbf{T})$, motivic structures ...

We also decided not to discuss motives and the cohomology of projective varieties in this book, especially in the first three chapters, but to stick to p-adic representations. Of course, if one wants to verify the fundamental conjectures on p-adic L-functions, the examples to consider lie in these cohomologies.

Let us outline the contents of the chapters.

In chapter 1, we construct the module of p-adic L-functions without factors at infinity of a representation V which is geometric and crystalline at p, using both results from Galois cohomology and the local theory developed in [**P94**].

In chapter 2, we define the factors at infinity and the module of the p-adic L-functions of V; we study some of their properties, in particular its functional equation.

In chapter 3, we define the p-adic periods and study their relation with the value at $\mathbf{1}$ (up to a unit) of a basis of the module of p-adic L-functions.

In chapter 4, we begin to develop a theory of the p-adic L-functions of a motive, whose the associated p-adic representation is of the type studied above.

There are also three appendices. The first contains no proofs; it recalls some classical results of Galois cohomology. The second gives precise details on the conjecture Leop(V) made in the text and gives examples. The cases where this conjecture is known are all easy applications of difficult theorems (of Kolyvagin, Rubin, Flach and others).

The third appendix, which was written jointly with J.-M. Fontaine, gives a conjecture on the computation of certain local Tamagawa numbers. We also show how this local conjecture makes it possible to verify the compatibility of the Bloch-Kato conjectures with the functional equation. It is totally independent from the rest of the book.

This book reflects research done over the past few years, at the university of Pierre and Marie Curie. I particularly want to thank the "Laboratoire de mathématiques fondamentales" (URA CNRS 747). Thanks are also due to Pierre Colmez for his many fruitful remarks.