Proceedings of the International Congress of Mathematicians
Helsinki, 1978

p-adic L-Functions, Serre-Tate Local Moduli, and Ratios of Solutions of Differential Equations

Nicholas M. Katz

Introduction. In recent years, there has been considerable progress in the constructions of p-adic L-functions attached to various sorts of "classical" L-functions. Unfortunately, the use of these p-adic functions to solve preexisting problems in number theory has so far met with less success; despite the recent work of Coates–Wiles [1] and Ferrero–Washington [4], conjectures remain more numerous than theorems. It may be hoped that a better understanding of the genesis of various p-adic L-functions will lead to progress in their exploitation. In that hope, we give yet another construction of the "two-variable" p-adic L-function attached to an elliptic curve with complex multiplication by a quadratic imaginary field in which p splits. This construction is based on the remarkable fact, discovered by Serre–Tate some fifteen years ago, that the local p-adic moduli space of such an elliptic curve has a canonical structure of one parameter formal group of height one. A rewriting of this construction in terms of ratios of local solutions of the associated Picard–Fuchs equations leads to universal formulas for the "algebraic part" of the classical L-values, which may shed light on the still mysterious situation when p is no longer assumed to split.

I. Let $K\subset \boldsymbol{C}$ be a quadratic imaginary field, with ring of integers $\mathcal{O}(K)$. Viewing $\mathcal{O}(K)$ as a lattice in $\boldsymbol{C}$, we may form the elliptic curve $E=\boldsymbol{C}/\mathcal{O}(K)$. Because E has complex multiplication, it is definable over the ring $\mathcal{O}(\overline{\boldsymbol{Q}})$ of all algebraic integers in $\boldsymbol{C}$, with everywhere good reduction. Further, we may choose a nowhere-vanishing invariant differential ω on E over $\mathcal{O}(\overline{\boldsymbol{Q}})$, so that the *pair* (E, ω) has everywhere good reduction over $\mathcal{O}(\overline{\boldsymbol{Q}})$, i.e. for any place $\mathcal{P}$ of $\overline{\boldsymbol{Q}}$, "$\omega$ mod $\mathcal{P}$" is nonzero on "E mod $\mathcal{P}$". Such an ω is *unique* up to multiplication by a *unit* in $\mathcal{O}(\overline{\boldsymbol{Q}})$.

The *period* lattice of (E, ω) is necessarily of the form $\Omega\mathcal{O}(K)$ for some $\Omega \in \boldsymbol{C}^\times$. For variable ω of the sort discussed above, this period Ω is well defined in the group $\boldsymbol{C}^\times/\mathcal{O}(\overline{\boldsymbol{Q}})^\times$.

We will denote by a the *area* of (a fundamental parallelogram of) the lattice $\mathcal{O}(K)$. In terms of the discriminant d of K, we have

$$a = \tfrac{1}{2}\sqrt{|d|}.$$

For integers $k \geqslant 3$, $r \geqslant 0$, consider the absolutely convergent series

$$A(k, r) = \sum_{\substack{\gamma \in \mathcal{O}(K) \\ \gamma \neq 0}} \frac{\bar{\gamma}^r}{\gamma^{k+r}}.$$

According to a fundamental result of Damerell [2] the product

$$B(k, r) = \frac{(-1)^k (k+r-1)!\, \pi^r}{2a^r \cdot \Omega^{k+2r}} \cdot A(k, r)$$

lies in $\overline{\boldsymbol{Q}}$; in fact it lies in the field obtained by adjoining to K the Weierstrass invariants g_2, g_3 of (E, ω). Further, for any integer $b \geqslant 1$, the product

$$b^k(b^k-1)\left(\sqrt{-|d|}\right)^r B(k, r)$$

is an algebraic integer.

The arithmetic of these numbers, and of their more sophisticated analogues ("with conductor", and extended to include $k=1$ or 2) is of interest because of their occurrence

(1) in the Birch–Swinnerton-Dyer conjecture for certain elliptic curves with complex multiplication (cf. [1]).

(2) as *periods* of cusp forms on congruence subgroups of $\mathrm{SL}(2, \boldsymbol{Z})$ (cf. [8]).

(3) as *special values* of holomorphic and nonholomorphic Eisenstein series on congruence subgroups of $\mathrm{SL}(2, \boldsymbol{Z})$ (cf. [6], [11]).

(4) as *special values* of Hecke L-series attached to grossencharacters of type A_0 of quadratic imaginary fields (cf. [7], [8]).

It would be of great interest to understand the *link* between (2) and (3) "directly"; both have been used to get information about occurrences (1) and (4).

II. At present, we have a reasonable understanding of the p-adic properties of the $B(k, r)$ only for primes p which *split* K. More precisely, fix a finite extension K'/K over which (E, ω) is defined and has everywhere good reduction. Let $\mathfrak{p}$ be a prime of K', $K'_\mathfrak{p}$ the $\mathfrak{p}$-adic completion of K', and W the ring of integers in the completion of the maximal unramified extension of $K'_\mathfrak{p}$. Denote by p the rational prime lying under $\mathfrak{p}$.

THEOREM. *If p splits in K, there exists a unit $c \in W^\times$ and, for all rational integers b prime to p, a W-valued p-adic measure $\mu(c, b)$ on $\mathbf{Z}_p \times \mathbf{Z}_p$, whose moments are given by the formula, valid for integers $k \geq 3$, $r \geq 0$,*

$$\int_{\mathbf{Z}_p \times \mathbf{Z}_p} x^{k-3} y^r \, d\mu(c, b) = 2 \cdot c^{k+2r}(b^k - 1) B(k, r).$$

In [6] we used the global theory of "p-adic modular functions" to construct this measure. Here we will outline a new construction, based on the Serre–Tate theory of local moduli of elliptic curves in terms of their p-divisible groups. This construction also leads to a universal computation of the $B(k, r)$ which may yield valuable information when p does not split in K.

Step I (Interpretation of measures). Over *any* p-adically complete and separated ring W, Cartier duality gives a canonical isomorphism between the convolution algebra of W-valued p-adic measures on $(\mathbf{Z}_p)^n$ and the coordinate ring $W[[X_1, \ldots, X_N]]$ of the n-fold self-product $(\hat{\mathbf{G}}_m)^n$ of the formal multiplicative group over W. Let $x_1, \ldots, x_n$ denote the standard coordinates on $(\mathbf{Z}_p)^n$, and let $D_1, \ldots, D_n$ be the standard invariant derivations $D_i = (1+X_i)\partial/\partial X_i$ on $(\hat{\mathbf{G}}_m)^n$. Given a function $f(X_1, \ldots, X_n) \in W[[X_1, \ldots, X_n]]$, the moments of the corresponding measure μ_f are given by

$$\int_{(\mathbf{Z}_p)^n} x_1^{i_1} \ldots x_n^{i_n} \, d\mu_f = D_1^{i_1} \ldots D_n^{i_n}(f)|_0.$$

Given a measure μ, the corresponding function $f_\mu(X_1, \ldots, X_n)$ is given by

$$f_\mu(X_1, \ldots, X_n) = \int_{(\mathbf{Z}_p)^n} (1+X_1)^{x_1} \ldots (1+X_n)^{x_n} \, d\mu.$$

Thus to construct our measure $\mu(c, b)$, we need a function f on a group $\hat{\mathbf{G}}_m \times \hat{\mathbf{G}}_m$.

Step II (Construction of $\hat{\mathbf{G}}_m \times \hat{\mathbf{G}}_m$ out of E and its local moduli). Returning to (E, ω) over $\mathcal{O}(K')$, we extend scalars to W. Because p splits in K, E has *ordinary* reduction at $\mathfrak{p}$, and hence, the formal group $\hat{E}$ of E is non-canonically isomorphic to $\hat{\mathbf{G}}_m$ over W. Fix one such isomorphism

$$\varphi : \hat{E} \xrightarrow{\sim} \hat{\mathbf{G}}_m \quad (\text{over } W).$$

The inverse image of the "standard" invariant differential $dX/(1+X)$ on $\hat{\mathbf{G}}_m$ is necessarily of the form $c^{-1}\omega$ for some unit $c \in W^\times$; this is the "c" occurring in the statement of the theorem.

Now consider the universal formal W-deformation E^{univ} of E, over the formal moduli space $\hat{\mathcal{M}}$. The chosen isomorphism φ extends uniquely to an isomorphism

$$\hat{E}^{\mathrm{univ}} \overset{\varphi}{\xrightarrow{\sim}} \hat{\mathbf{G}}_m \quad \text{over } \hat{\mathcal{M}}, \quad \text{i.e.} \quad \hat{E}^{\mathrm{univ}} \cong \hat{\mathcal{M}} \times \hat{\mathbf{G}}_m.$$

The Serre–Tate theory [9] gives an explicit isomorphism of the space $\hat{\mathcal{M}}$ with the formal group $\hat{\mathbf{G}}_m$ over W; the origin of this $\hat{\mathbf{G}}_m$ is the W-valued point of

$\hat{\mathcal{M}}$ which "is" E. Thus we have

$$\hat{E}^{\text{univ}} \cong \hat{\mathcal{M}} \times \hat{G}_m \cong \hat{G}_m \times \hat{G}_m.$$

Here are three equivalent descriptions of this isomorphism $\hat{\mathcal{M}} \xrightarrow{\sim} \hat{G}_m$.

(a) Because E has complex multiplication by $\mathcal{O}(K)$, and has ordinary reduction at $\mathfrak{p}$, its p-divisible is necessarily a *product*

$$E(p^\infty) \xrightarrow{\sim} \hat{E} \times E(p^\infty)^{\text{etale}} \xrightarrow[\sim]{\varphi \times (\check{\varphi})^{-1}} \hat{G}_m \times \mathbf{Q}_p/\mathbf{Z}_p.$$

Let $\mathbf{W}$ be a p-adically complete and separated augmented W-algebra, with nilpotent augmentation ideal, and let $\mathbf{E}/\mathbf{W}$ be a deformation of E/W. Then the p-divisible group of $\mathbf{E}$ sits in an *extension*

$$0 \to \hat{G}_m \to \mathbf{E}(p^\infty) \to \mathbf{Q}_p/\mathbf{Z}_p \to 0,$$

and so determines an element of $\operatorname{Ext}^1_{\mathbf{W}}(\mathbf{Q}_p/\mathbf{Z}_p, \hat{G}_m) \xrightarrow{\sim} \hat{G}_m(\mathbf{W})$. (Explicitly, let P_i be the point of order p^i in $E(W)$ corresponding to "$1/p^i$" in the $\mathbf{Q}_p/\mathbf{Z}_p$-factor of $E(p^\infty)$. Let $\mathbf{P}_i$ be *any* point in $\mathbf{E}(\mathbf{W})$ lifting P_i; then $p^i\mathbf{P}_i$ lies in $\hat{\mathbf{E}}(\mathbf{W}) \xrightarrow{\sim}{}^{\varphi} \hat{G}_m(\mathbf{W})$, and as $i \to \infty$ these points tend to a *limit* in $\hat{G}_m(\mathbf{W})$). The resulting morphism $\hat{\mathcal{M}} \to \hat{G}_m$ is an isomorphism.

(b) Consider once again the universal formal deformation E^{univ} over $\hat{\mathcal{M}}$. Via the Kodaira–Spencer isomorphism

$$(\omega_{E^{\text{univ}}/\hat{\mathcal{M}}})^{\otimes 2} \cong \Omega^1_{\hat{\mathcal{M}}/W}$$

the square of $\varphi^*(dX/(1+X))$ corresponds to a basis ξ of $\Omega^1_{\hat{\mathcal{M}}/W}$. The isomorphism $\hat{\mathcal{M}} \xrightarrow{\sim} \hat{G}_m$ is the unique morphism of pointed functors under which $dX/(1+X)$ pulls back to ξ.

(c) There is a unique basis u, v of $H^1_{DR}(E/W)$ such that

(1) $u = c^{-1}\omega$,

(2) $\langle u, v\rangle = 1$ (de Rham cup product),

(3) for $\gamma \in \mathcal{O}(K)$ acting, as $[\gamma]^*$, on $H^1_{DR}(E/W)$, we have

$$[\gamma]^*(u) = \gamma u, \quad [\gamma]^*(v) = \bar{\gamma} v.$$

Now consider $H^1_{DR}(E^{\text{univ}}/\hat{\mathcal{M}})$, with its Gauss–Manin connection. Let $\operatorname{Div}(\hat{\mathcal{M}})$ denote the ring of all "divided" power series centered at the marked W-point "E/W" of $\hat{\mathcal{M}}$. In terms of a parameter T for $\hat{\mathcal{M}}$ centered at "E/W"; this is the ring

$$W\langle\langle T\rangle\rangle = \left\{ \sum_{n \geq 0} a_n \frac{T^n}{n!} \,\middle|\, a_n \in W \right\};$$

intrinsically, it is the topological "divided power envelope" of the marked point "E/W" in $\hat{\mathcal{M}}$. On $H^1_{DR}(E^{\text{univ}}/\hat{\mathcal{M}}) \otimes \operatorname{Div}(\hat{\mathcal{M}})$, the connection necessarily becomes trivial, so we can find a *horizontal* basis U, V which extends the given basis u, v

of $H^1_{DR}(E/W)$. In terms of this basis, the invariant differential $\varphi^*(dX/(1+X))$ on E^{univ}, viewed as a de Rham cohomology class is expressed as

$$\varphi(dX/(1+X)) = U + LV \quad \text{with} \quad L \in \mathrm{Div}(\hat{\mathscr{M}}).$$

The isomorphism $\hat{\mathscr{M}} \xrightarrow{\sim} \hat{G}_m$ is the unique morphism of pointed functors under which L becomes the *logarithm* on $\hat{G}_m$:

$$L(X) = \log(1+X) \quad \text{i.e.} \quad dL = dX/(1+X) = \xi.$$

That these descriptions are in fact equivalent may be seen as follows. By "general principles", the function L must be a (divided-power) isomorphism from $\hat{G}_m$ to $\hat{G}_a$, i.e. we must have $L(X) = w\log(1+X)$ for some $w \in W^\times$. To see that $w=1$, it suffices to compute $L \bmod (X^2)$, and this amounts to explicitly computing the description (a) for deformations of E over the dual numbers $W[\varepsilon]/(\varepsilon^2)$. This last computation becomes routine if we exploit the autoduality of elliptic curves by systematically interpreting *points* on elliptic curves as (isomorphism classes of) *line bundles*.

A more sophisticated proof of this and more general equivalences has been announced by Messing [10].

Step III (Construction of a function f on $\hat{E}^{\mathrm{univ}} \simeq \hat{G}_m \times \hat{G}_m$). Given an integer $b \geqslant 1$ prime to p, the function f on $\hat{E}^{\mathrm{univ}}$ to be taken is, in "transcendental" notation,

$$f(z) = b^3\wp'(bz) - \wp'(z) = \sum_{\substack{\zeta \in \mathrm{Ker}[b] \\ \zeta \neq 0}} \wp'(z+\zeta).$$

This has purely algebraic meaning, as follows. Given *any* (E, ω) over any ring R, pick *any* parameter Z for $\hat{E}$ so that $\omega = (1+\ldots)dZ$. The functions on E with at worst double poles along the 0-section (i.e. $H^0(E, I(0)^{-2})$) which begin $Z^{-2}+\ldots$ all differ from each other by additive constants. If we apply to any of them the invariant derivation dual to ω, we get a well-defined $\wp'$. If b is invertible in R, then all nontrivial points of order b are disjoint from $\hat{E}$, so the Σ-expression for f shows that it's well-defined on $\hat{E}$. We apply this universal construction to $(E^{\mathrm{univ}}, \varphi^*(dX/(1+X)))$ over the coordinate ring of $\mathscr{M}$.

Step IV (Universal computation of the moments). We now return to the original (E, ω) over $\mathcal{O}(K')$, with complex multiplication by $\mathcal{O}(K)$. Let W be *any* overring of $\mathcal{O}(K')$ in which the discriminant d of K is invertible, and let $c \in W^\times$ be *any* unit of W. It still makes sense to take a basis u, v for $H^1_{DR}(E/W)$ as in Step II (c) and then to find the horizontal basis U, V of $H^1_{DR}(E^{\mathrm{univ}}/\hat{\mathscr{M}}) \otimes \mathrm{Div}(\hat{\mathscr{M}})$ which extends u, v. There is no longer a *preferred* invariant differential on E^{univ}, but we may simply choose one which extends ω/c. Its expression in terms of U, V will be

$$\alpha U + \beta V, \; \alpha, \beta \in \mathrm{Div}(\hat{\mathscr{M}}), \quad \alpha(0) = 1, \quad \beta(0) = 0.$$

Because $\alpha(0)=1$, it is invertible in $\mathrm{Div}(\hat{\mathcal{M}})$. Therefore there is a *unique* invariant differential ω on $E^{\mathrm{univ}} \otimes \mathrm{Div}(\hat{\mathcal{M}})$ whose expression in U, V is

$$\omega = U + LV \quad \begin{cases} L = \beta/\alpha \in \mathrm{Div}(\hat{\mathcal{M}}); \\ L(0) = 0. \end{cases}$$

This function $L \in \mathrm{Div}(\hat{\mathcal{M}})$ is simply the *direction* (i.e. the Plücker coordinate) of the subspace $H^{1,0} \subset H^1_{DR}$, measured with respect to the horizontal basis U, V. It is a "divided-power uniformizing parameter", in the sense that the natural map

$$W\langle\langle L \rangle\rangle \xrightarrow{\sim} \mathrm{Div}(\hat{\mathcal{M}})$$

is an isomorphism.

Let b be any integer invertible in W, and apply the construction of Step III to $(E^{\mathrm{univ}} \otimes \mathrm{Div}(\hat{\mathcal{M}}), \omega)$, to produce a function f on $\hat{E}^{\mathrm{univ}} \otimes \mathrm{Div}(\hat{\mathcal{M}})$. It follows easily from the cohomological analysis of ([7], 2.4.8) that we may compute the $B(k, r)$'s as follows.

ALGORITHM. Let D_1 be the invariant derivation of $\hat{E}^{\mathrm{univ}} \otimes \mathrm{Div}(\hat{\mathcal{M}})$ over $\mathrm{Div}(\hat{\mathcal{M}})$ which is dual to ω. For all integers $k \geqslant 3$, $r \geqslant 0$, we have

$$2c^{k+2r}(b^k - 1)B(k, r) = (d/dL)^r (D_1^{k-3}(f)_{|0})_{|0}.$$

III. When p splits in K, and W and c are as in Step II, the theorem follows immediately from this algorithm and Steps I, II, III. When p stays prime in K, this algorithm gives the known integrality results, and focuses attention on the very special role played by the divided power parameter L on the moduli space $\hat{\mathcal{M}}$. Arithmetic information about L should yield arithmetic information about the numbers $B(k, r)$. Is it conceivable that L is always the logarithm of a formal group structure on the pointed (by E/W) functor $\hat{\mathcal{M}}$?

IV. In this final section, we give an "elementary" description of L, valid over any ring containing 1/2, as the ratio of two particular local solutions of the Gauss hypergeometric equation with parameters (1/2, 1/2, 1). From this point of view, the function L has been studied extensively by Dwork, at least in the case when p splits in K, under the name "τ" ([3], [5]).

Consider the Legendre family of elliptic curves $y^2 = x(x-1)(x-\lambda)$ over $\mathcal{M} = \mathrm{Spec}(\mathbf{Z}[\lambda][1/(2\lambda(\lambda-1))])$. Let λ_0 be any value of λ at which this curve acquires complex multiplication by the ring of integers $\mathcal{O}(K)$ in a quadratic imaginary field. The formal moduli space $\hat{\mathcal{M}}$ is simply the formal completion of $\mathcal{M}$ at $\lambda = \lambda_0$.

Let D denote the derivation $2\lambda(\lambda-1)d/d\lambda$ of $\mathcal{M}$. The H^1_{DR} for the Legendre family is free over $\mathcal{M}$ with basis

$$\omega = dx/2y, \; D(\omega) = (x-\lambda)\, dx/2y$$

with

$$\langle \omega, D(\omega) \rangle = 1 \qquad \text{(de Rham cup-product)},$$

$$D^2(\omega) = -\lambda(\lambda-1)\omega \quad \text{(Gauss—Manin connection)}.$$

At λ_0, a basis u, v of H^1_{DR} which is adapted to the action of $\mathcal{O}(K)$ is given by

$$u = \omega_{|\lambda=\lambda_0}, \quad v = \bigl(D(\omega) - e\omega\bigr)_{|\lambda=\lambda_0}$$

for some unique constant e in $\bigl(1/\sqrt{-|d|}\bigr) \cdot \mathcal{O}(K')[1/2]$. Let $\alpha(\lambda), \beta(\lambda)$ be the local solutions near $\lambda=\lambda_0$ of the hypergeometric equation

$$D^2 f = -\lambda(\lambda-1)f,$$

normalized by the initial conditions

$$\alpha(\lambda_0) = 1, \ (D\alpha)(\lambda_0) = e,$$

$$\beta(\lambda_0) = 0, \ (D\beta)(\lambda_0) = 1.$$

The horizontal basis U, V passing through u, v at $\lambda=\lambda_0$ is given by

$$U = D(\beta)\,\omega - \beta D(\omega), \quad V = -D(\alpha) \cdot \omega + \alpha D(\omega).$$

Thus we find

$$\omega = \alpha U + \beta V,$$

whence

$$L = \beta/\alpha, \quad \omega = \omega/\alpha, \quad d/dL = \alpha^2 \cdot 2\lambda(\lambda-1)\, d/d\lambda,$$

$$D_1 = \alpha \cdot 2y\, d/dx, \quad f = 2\alpha^3\bigl(b^3[b]^*(y) - y\bigr).$$

References

1. J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent Math. **39** (1977), 223—251.

2. R. M. Damerell, *L-functions of elliptic curves with complex multiplication* I, Acta Arith. **17** (1970), 287—301.

3. B. Dwork, *P-adic cycles*, Inst. Hautes Études Sci. Publ. Math. **37** (1969), 327—415.

4. B. Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377—395

5. N. Katz, *Travaux de Dwork*, Séminaire Bourbaki 1971/72, Lecture Notes in Math., vol. 317 Springer-Verlag, Berlin and New York, 1973, pp. 167—200.

6. *P-adic interpolation of real analytic Eisenstein series*, Ann. of Math. **104** (1976), 459—571.

7. *P-adic L-functions for CM-fields*, Invent. Math. **49** (1978), 199—297.

8. J. Manin and S. Vishik, *p-adic Hecke series for quadratic imaginary fields*, Mat. Sb. **95 (137)**, (1974).

9. W. Messing, *The crystal associated to Barsotti-Tate groups, with applications to abelian schemes*, Appendix, Lecture Notes in Math., vol. 264, Springer-Verlag, Berlin and New York, 1972.

10. $q_{\text{Serre-Tate}} = q_{\text{Dwork}}$, Notices Amer. Math. Soc. (1976).

11. G. Shimura, *On some arithmetic properties of modular forms of one and several variables*, Ann of Math. **102** (1975), 491—515.

PRINCETON UNIVERSITY
PRINCETON, N. J. 08540, U.S.A.