MASSIMO BERTOLINI

Regulators, L-Functions and Rational Points

Bollettino dell'Unione Matematica Italiana, Serie 9, Vol. **6** (2013), n.1, p. 191–204.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2013_9_6_1_191_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2013.

Bollettino U. M. I.
(9) **VI** (2013), 191-204

Regulators, *L*-Functions and Rational Points (*)

Massimo Bertolini

Abstract. – *This article is a revised version of the text of the plenary conference I gave at the XIX Congress of "Unione Matematica Italiana", held in Bologna in September 2011. It discusses the arithmetic significance of the values at integers of the complex and p-adic L-functions associated to Dirichlet characters and to elliptic curves.*

Introduction

Values at integer points of L-functions attached to algebraic varieties, and their relations to arithmetic invariants, have received much attention over the last decades. Several authors, including Beilinson, Bloch, Deligne, and Kato, have formulated a comprehensive conjectural theory; see for example [Ki] for an up-to-date description and bibliography. Moreover, results have been obtained for the L-functions associated to certain automorphic representations, some of which are described here.

Recently, fragments of a p-adic analogue of this theory, in which complex L-functions are replaced by p-adic L-functions, have emerged; e.g., [Co], [MTT], [So], [Co-dS], [PR2], [Ka], [Br]. Furthermore, the theory of Euler systems [Ko], [Ru], [Ka], [Colz] has introduced powerful new tools for establishing connections between values of L-functions and arithmetic invariants.

Our exposition focuses mostly on the case elliptic curves, and provides an introduction to the ongoing research projects [BD1], [BD2], [BD3]. Modularity of elliptic curves gives rise to a mature theory of their complex and p-adic L-functions. Moreover, the Euler system of Heegner points and Kato's Euler system of étale regulators of modular units become available in this case, leading to the best known results on the Birch and Swinnerton-Dyer conjecture.

Along the way, we point out the remarkable parallelism between the setting of elliptic curves and the setting of Dirichlet L-functions, in which are rooted many classical questions of number theory.

(*) Conferenza Generale tenuta a Bologna il 15 settembre 2011 in occasione del XIX Congresso dell'Unione Matematica Italiana.

1. – Dirichlet L-functions

Let $N \geq 3$ be an integer, and let $\chi : (\boldsymbol{Z}/N\boldsymbol{Z})^{\times} \longrightarrow \boldsymbol{C}^{\times}$ be a primitive Dirichlet character of conductor N. The Dirichlet L-function $L(\chi, s)$ associated to χ (viewed as a function on $\boldsymbol{Z}$ in the usual way) is defined by the infinite series

$$L(\chi, s) = \sum_{n=1}^{\infty} \chi(n) n^{-s}. \tag{1}$$

Assuming that χ is different from the trivial character, the series (1) converges to an analytic function on the complex half plane $\Re(s) > 0$. Furthermore, $L(\chi, s)$ is represented by the infinite Euler product (taken over the rational primes)

$$L(\chi, s) = \prod_{p} (1 - \chi(p) p^{-s})^{-1}, \qquad \Re(s) > 1, \tag{2}$$

reflecting the unique factorization principle. It is known that $L(\chi, s)$ admits an analytic continuation to the whole complex plane, and satisfies a functional equation relating $L(\chi, s)$ to $L(\bar{\chi}, 1-s)$, where $\bar{\chi} = \chi^{-1}$ is the complex conjugate of χ.

In the following discussion, assume that the non-trivial character χ is *even*, i.e., $\chi(-1) = 1$. In this case, the functional equation becomes

$$\Gamma(s) \cos\left(\frac{\pi s}{2}\right) L(\chi, s) = \frac{\tau(\chi)}{2} \left(\frac{2\pi}{N}\right)^{s} L(\bar{\chi}, 1-s), \tag{3}$$

where $\Gamma(s)$ is the Γ-function, and $\tau(\chi)$ denotes the Gauss sum $\sum_{k=1}^{N} \chi(k) \zeta_N^k$, with $\zeta_N := e^{2\pi i/N}$. (See for example Chapter 4 of [Wa1].)

Let $n \geq 1$ be an integer. If n is even, equations (2) and (3) imply that $L(\chi, 1-n)$ is non-zero. On the other hand, $L(\chi, s)$ has a simple zero at $1-n$ if n is odd (the case $n = 1$, in which the non-vanishing of $L(\chi, 1)$ does not follow directly from (2), is discussed below). For n even, the points $s = n, 1-n$ are *critical* for $L(\chi, s)$ in the sense of Deligne [De]. This phenomenon is reflected in the following explicit formulae, expressing $L(\chi, 1-n)$ in terms of certain algebraic numbers $B_{n,\chi}$ called *generalized Bernoulli numbers*. They are defined by the equation

$$\sum_{k=1}^{N} \frac{\chi(k) x e^{kx}}{e^{Nx} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{x^n}{n!} .$$

Then, for all $n \geq 1$, a direct calculation shows

$$L(\chi, 1-n) = -\frac{B_{n,\chi}}{n} . \tag{4}$$

REMARK 1.1. – Formula (4) also holds when χ is odd, i.e., $\chi(-1) = -1$. In this case, the critical points are obtained when n is odd.

We now turn to the description of the *non-critical* value $L(\chi,1)$. First, we observe that $L(\chi,1)$ is non-zero. (This fact follows from the presence of a simple pole at $s=1$ in the Dedekind zeta function of a number field, and can be used to prove Dirichlet's theorem on primes in arithmetic progressions.) A manipulation of infinite series establishes the formula

$$L(\chi,1) = -\frac{\tau(\chi)}{N}\sum_{k=1}^{N}\bar{\chi}(k)\log|1-\zeta_N^k|. \tag{5}$$

The expression $\sum\bar{\chi}(k)\log|1-\zeta_N^k|$ appearing in the right hand side of (5) is an example of a (complex) *regulator*. Regulators make their appearance in the description of values of L-functions at integers, as will be discussed more thoroughly in later examples.

The algebraic integers $1-\zeta_N^k$ are (closely related to) so-called *cyclotomic units* in $\boldsymbol{Q}(\zeta_N)$ ([Wa1], Chapters 4 and 8). Cyclotomic units provide an avenue to establish relations between the values $L(\chi,1)$ and arithmetic invariants of cyclotomic fields, such as their class groups (see for example § 4 of [Ru]).

More generally, we remark that it is possible to describe the non-critical values $L(\chi,1+2k)$ for $k\geq 1$ in terms of cyclotomic elements, constructed by Beilinson, Bloch and Soulé, arising in the odd K-groups of the ring of integers of $\boldsymbol{Q}(\zeta_N)$. See the discussion in [So].

2. – *p*-adic Dirichlet *L*-functions

As in Section 1, assume that χ is a non-trivial even character of conductor N. We now focus on p-adic analogues of the L-functions $L(\chi,s)$. Let $p\geq 3$ be a rational prime, and let $\boldsymbol{Q}_p$ be the field of p-adic numbers. The p-adic absolute value $|\ |_p$ on $\boldsymbol{Q}_p$, normalised by the condition $|p|_p=p^{-1}$, extends in a unique way to the algebraic closure $\bar{\boldsymbol{Q}}_p$. The completion $\boldsymbol{C}_p$ of $\bar{\boldsymbol{Q}}_p$ should be viewed as the p-adic analogue of the field $\boldsymbol{C}$ of complex numbers.

Fix from now on embeddings of $\bar{\boldsymbol{Q}}$ into $\boldsymbol{C}$ and $\boldsymbol{C}_p$. They allow to identify an algebraic number both with a complex number and with an element of $\boldsymbol{C}_p$. Denote by $\boldsymbol{Z}_p$ the ring of p-adic integers. Every $\alpha\in\boldsymbol{Z}_p^\times$ can be written uniquely as

$$\alpha=\omega(\alpha)\langle\alpha\rangle, \tag{6}$$

where $\langle\alpha\rangle$ belongs to $1+p\boldsymbol{Z}_p$ and $\omega(\alpha)$ is a $(p-1)-st$ root of 1 in $\boldsymbol{Q}_p$. Occasionally ω – called the Teichmüller character – will be viewed as a complex Dirichlet character $(\boldsymbol{Z}/p\boldsymbol{Z})^\times\longrightarrow\boldsymbol{C}^\times$ via our fixed embeddings.

The *p-adic L-function* $L_p(\chi,s)$ (see [Wa1], [La]) is the (non-zero) $\boldsymbol{C}_p$-valued p-adic analytic function on $\boldsymbol{Z}_p$ satisfying the *interpolation* property

$$L_p(\chi,1-n) = -(1-\chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n} \tag{7}$$

for all integers $n \geq 1$. The reader should note the close analogy between equations (4) and (7), one difference being the presence of the Euler factor $(1-\chi\omega^{-n}(p)p^{n-1})$ – the reciprocal of the Euler factor at p in $L(\chi\omega^{-n}, 1-n)$ – in the p-adic formula. In particular, when $n \equiv 0 \pmod{p-1}$ (hence n is even), (4) and (7) imply that

$$L_p(\chi, 1-n) = -(1-\chi(p)p^{n-1})\,\frac{B_{n,\chi}}{n} = (1-\chi(p)p^{n-1})L(\chi, 1-n). \tag{8}$$

Equation (8) determines $L_p(\chi, s)$ uniquely, since the set of integers $1-n$ with $n \equiv 0 \pmod{p-1}$ is dense in $\boldsymbol{Z}_p$.

REMARK 2.1. – It is not known whether $L_p(\chi, s)$ satisfies a functional equation similar to (3); see the comments in [Wa2].

The value of $L_p(\chi, s)$ at the point $s = 1$, which lies outside the range of classical interpolation (7), can be described in terms of a *p-adic regulator* on cyclotomic units. Thus the situation is analogous to the complex setting described in equation (5). Let $\log_p : \boldsymbol{C}_p^\times \longrightarrow \boldsymbol{C}_p$ be the branch of the p-adic logarithm satisfying $\log_p(p) = 0$. Then

$$L_p(\chi, 1) = -\left(1 - \frac{\chi(p)}{p}\right)\frac{\tau(\chi)}{N}\sum_{k=1}^{N} \bar{\chi}(k)\log_p(1-\zeta_N^k). \tag{9}$$

It is a deep fact that $L_p(\chi, 1)$ is non-zero. It follows from the non-vanishing of the p-adic regulator for cyclotomic fields. (An open problem – Leopoldt's conjecture – states that the p-adic regulator attached to *any* number field is non-zero.) For generalizations of equation (9) to other values of $L_p(\chi, s)$ at integers outside the range of classical interpolation, we refer the reader to [So] and [Co].

We conclude our brief discussion of the properties of $L_p(\chi, s)$ by recalling its interpretation in terms of p-adic measures. This language is helpful in relating p-adic L-functions to objects of arithmetical interest. It is also convenient for stressing the analogy between the p-adic L-functions attached to Dirichlet characters and to elliptic curves.

Assume for simplicity that $p \nmid N$, and write $\boldsymbol{Z}_{N,p}^\times$ for the inverse limit of the groups $(\boldsymbol{Z}/Np^n\boldsymbol{Z})^\times$ of units modulo Np^n with respect to the natural projections. Thus

$$\boldsymbol{Z}_{N,p}^\times = (\boldsymbol{Z}/Np\boldsymbol{Z})^\times \times (1 + p\boldsymbol{Z}_p).$$

A *p-adic measure* on $\boldsymbol{Z}_{N,p}^\times$ is a $\boldsymbol{C}_p$-valued bounded functional on the space $\mathrm{Cont}(\boldsymbol{Z}_{N,p}^\times, \boldsymbol{C}_p)$ of continuous functions from $\boldsymbol{Z}_{N,p}^\times$ to $\boldsymbol{C}_p$. The Bernoulli numbers can be used to define a measure $\mu_{B,c}$, depending on the choice of an integer c coprime to Np. One has the following description of $L_p(\chi, s)$ as the *p-adic Mellin* *transform* of $\mu_{B,c}$:

$$L_p(\chi, s) = -(1 - \chi(c)\langle c\rangle^{1-s})^{-1} \int_{\mathbf{Z}_{N,p}^\times} \chi\omega^{-1}(t)\langle t\rangle^{-s} d\mu_{B,c}. \tag{10}$$

Generalizing the notation appearing in equation (6) somewhat, here $\langle t\rangle$ denotes the projection from $\mathbf{Z}_{N,p}^\times$ to $1 + p\mathbf{Z}_p$, and $\chi\omega^{-1}$ is viewed as a function on $\mathbf{Z}_{N,p}^\times$ in the natural way. Moreover, c is chosen so that $\chi(c)\langle c\rangle^{1-s} \not\equiv 1$. (See [Wa1], Chapter 12 and [La], Chapter 4.)

REMARK 2.2. – It follows from (10) that the values $L_p(\chi, 1-n)$, defining $L_p(\chi, s)$ in equation (7), can be obtained by integrating the continuous characters $t \mapsto \langle t\rangle^{n-1}$ against the measure $\chi\omega^{-1}(t)d\mu_{B,c}$ associated to χ. Another way of characterizing $L_p(\chi, s)$ amounts to setting $s = 0$ in equation (10), and integrating characters ψ of p-power conductor against the same measure. The latter point of view, based on "twisting" by the finite order characters ψ, will be adopted in the definition of the p-adic L-function $L_p(E, s)$ associated to an elliptic curve E. In this case, there is only one critical point for the complex L-function $L(E, s)$, that is, the central critical point $s = 1$. In order to define $L_p(E, s)$ by p-adic interpolation of special values of complex L-functions, one resorts to interpolating the values at 1 of the twisted L-functions $L(E, \psi, s)$.

REMARK 2.3. – An alternate description of $L_p(\chi, s)$ is obtained by integrating the characters of infinite order $\psi\langle t\rangle^{-1}$ (with ψ as in the previous remark) against the measure $\chi\omega^{-1}(t)d\mu_{B,c}$. In view of (9) (suitably generalized), the above description amounts to the p-adic interpolation of p-adic regulators associated to cyclotomic units. This point of view ties in with Iwasawa's theorem, in which logarithmic derivatives are used to relate the measure $\mu_{B,c}$ to the quotient module of local units by cyclotomic units. Iwasawa's theorem is a crucial ingredient in the proof of the cyclotomic Main Conjecture of Iwasawa theory explained in [Ru].

3. – L-functions of elliptic curves

Let E be an elliptic curve over $\mathbf{Q}$ of conductor N, defined by a minimal Weierstrass equation (cf. Chapter VIII of [Sil])

$$y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6, \qquad \alpha_i \in \mathbf{Z}. \tag{11}$$

The complex L-function of E is defined by the Euler product

$$L(E, s) = \prod_p (1 - a_p p^{-s} + \delta_p p^{1-2s})^{-1}. \tag{12}$$

Here $a_p = p - n_p$, where n_p denotes the number of solutions of (11) modulo p, and $\delta_p = 0$, resp. 1 if $p \mid N$, resp. $p \nmid N$. The infinite product (12) converges for $\Re(s) > 3/2$, by the Hasse bound $|a_p| \leq 2\sqrt{p}$. Write $L(E,s)$ as a Dirichlet series

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s},$$

where the coefficients $a_n \in \boldsymbol{Z}$ are given inductively in terms of the a_p defined above. Let $\mathcal{H}$ denote the complex upper half plane $\{z \in \boldsymbol{C} : \Im(z) > 0\}$. The *modularity theorem* [Wi1], [TW], [BCDT] shows that

$$f(z) := \sum_{n=1}^{\infty} a_n e^{2\pi i n z}, \qquad z \in \mathcal{H} \tag{13}$$

is the Fourier expansion of a newform on $\Gamma_0(N)$ (the Hecke congruence group of matrices in $\mathbf{SL}_2(\boldsymbol{Z})$ which are upper triangular modulo N). Conversely, writing $z = x + iy$ with $x, y \in \boldsymbol{R}$, $L(E,s)$ can be described as the Mellin transform of $f(z)$ as

$$L(E,s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^{\infty} f(iy) y^{s-1} dy. \tag{14}$$

Equation (14) implies that $L(E,s)$ can be analytically continued to the whole complex plane, and satisfies a functional equation relating $L(E,s)$ to $L(E,2-s)$. More precisely, setting $\Lambda(E,s) := L(E,s)N^{s/2}(2\pi)^{-s}\Gamma(s)$, one has

$$\Lambda(E,s) = w_E \Lambda(E, 2-s), \qquad w_E = \pm 1. \tag{15}$$

Note that the sign w_E of the functional equation is equal to $+1$, resp. -1 if $L(E,s)$ vanishes to even, resp. odd order at $s = 1$. It turns out that $s = 1$ – the center of symmetry for the functional equation – is the only critical point for $L(E,s)$. Let $\omega_E = dx/(2y + \alpha_1 x + \alpha_3)$ be the invariant differential associated to (11), and denote by Λ_E the lattice of periods attached to ω_E. Define the real period $\Omega_E^+ \in \boldsymbol{R}_{>0}$ by setting $\Lambda_E \cap \boldsymbol{R} = \boldsymbol{Z}\Omega_E^+$. Likewise, define the imaginary period $\Omega_E^- \in i\boldsymbol{R}_{>0}$ by $\Lambda_E \cap i\boldsymbol{R} = \boldsymbol{Z}\Omega_E^-$. From equation (14), one obtains [Man] the existence of a rational number C_E satisfying

$$\frac{L(E,1)}{\Omega_E^+} = C_E. \tag{16}$$

Equation (16) should be regarded as the analogue, in the setting of elliptic curves, of equation (4). More generally, let χ be a Dirichlet character, and denote by

$$L(E,\chi,s) = \sum_{n=1}^{\infty} a_n \chi(n) n^{-s}$$

the L-series of E twisted by χ. Then

$$\frac{L(E,\chi,1)}{\Omega_E^{\chi(-1)}} = C_{E,\chi}, \tag{17}$$

for an algebraic constant $C_{E,\chi}$.

Equation (16) shows that C_E is non-zero precisely when $L(E,1)$ is non-zero. In this case, the celebrated *Birch and Swinnerton-Dyer conjecture* (cf. for example [Wi2] and [Ber] for details and references) relates C_E to the arithmetic invariants of E, such as the order of its Shafarevich-Tate group. A large part of this prediction has now been settled, thanks to the work of Gross-Zagier [GZ], Kolyvagin [Ko] and Skinner-Urban [SU].

In general, $L(E,s)$ can vanish at $s=1$. In this case, the Birch and Swinnerton-Dyer conjecture states that that the order of vanishing of $L(E,s)$ at $s=1$ – the so-called *analytic rank* of E – is equal to the rank of the group $E(\boldsymbol{Q})$ of rational points of E. Furthermore, it gives an exact formula for the leading coefficient in the Taylor expansion of $L(E,s)$ at $s=1$, in terms of arithmetic invariants of E.

Assume now that the functional equation (15) has sign $w_E=-1$, so that $L(E,s)$ vanishes to odd order at $s=1$. The Gross-Zagier formula [GZ] yields

$$\frac{L'(E,1)}{\Omega_E^+} = C'_E \cdot h_{\boldsymbol{C}}(P), \tag{18}$$

where C'_E is a non-zero rational constant, P is a so-called *Heegner point* in $E(\boldsymbol{Q})$, and $h_{\boldsymbol{C}}(P)$ denotes the Néron-Tate height of P. Since the Néron-Tate height vanishes precisely on torsion points, it follows that $L(E,s)$ has a simple zero at $s=1$ if and only if P has infinite order.

Combining (18) with the results of Kolyvagin [Ko] yields a large part of the Birch and Swinnerton-Dyer conjecture for elliptic curves of analytic rank one.

The point P belongs to a system of algebraic points (Heegner points) on E, whose properties are analogous to those of the system of cyclotomic units (appearing in equations (5) and (9)). Both systems of elements are related to values of L-functions, and give rise to Euler systems in the sense of Kolyvagin (loc. cit.). The theory of Euler systems can be used to prove relations between these elements and the arithmetic invariants of cyclotomic fields and of elliptic curves.

REMARK 3.1. – The definition of P stems from the theory of complex multiplication and the modularity of E. It depends on the choice of an auxiliary imaginary quadratic field $K=\boldsymbol{Q}(\sqrt{-D})$. It is more natural to state the Gross-Zagier formula as the equality

$$\frac{L'(E,1)}{\Omega_E^+}\cdot\frac{L(E,\chi_D,1)}{\Omega_E^-} = C'_{E,D} \cdot h_{\boldsymbol{C}}(P), \tag{19}$$

where $C'_{E,D}$ is an explicit non-zero rational constant, and χ_D denotes the quadratic Dirichlet character associated to K. Formula (18) follows from (19) in view of (17).

We now turn to the description of the non-critical value $L(E,2)$. Note that $L(E,2)$ is always non-zero, since $s=2$ lies within the range of convergence of the infinite product (12).

Let $Y=Y_1(N)$ be the open modular curve over $\boldsymbol{Q}$, whose complex points are identified with the Riemann surface $\Gamma_1(N)\backslash\mathcal{H}$. Let $X=X_1(N)$ be the complete curve obtained by compactifying $Y_1(N)$ with a finite set of cusps. (See for example [GZ] for details on modular curves.)

Let $u,v\in\boldsymbol{C}(X)$ be modular units, i.e, rational functions on $X/\boldsymbol{C}$ whose divisor is concentrated on the set of cusps, and let η denote an anti-holomorphic 1-form on X. The value of the *complex regulator* of u,v on η is given by

$$\mathrm{reg}_{\boldsymbol{C}}\{u,v\}(\eta)=\int_{X(\boldsymbol{C})}\log|u|^2\mathrm{dlog}\,v\wedge\eta. \tag{20}$$

It can be checked that the expression (20) depends only on the class of η in the de Rham cohomology of X, and defines a map on the second K-group $K_2(\boldsymbol{C}(X))$ generated by Steinberg symbols of rational functions (see the discussion in [CodS] and [Bes2]).

One has the following formula of Beilinson [Bei] for $L(E,2)$; see also prior work of Bloch [Bl] in the case of elliptic curves with complex multiplication. In this note we follow the treatment given in [BD1], where an entirely explicit expression is obtained.

Let η_f^{ah} denote the anti-holomorphic 1-form

$$\eta_f^{\mathrm{ah}}=\frac{2\pi i\bar{f}(z)d\bar{z}}{\int_{X(\boldsymbol{C})}|f(z)|^2dxdy}, \tag{21}$$

where $f(z)$ is the modular form attached to E. Then

$$\frac{L(E,2)}{\Omega_E^-}\cdot\frac{L(E,\chi,1)}{\Omega_E^+}=C_{E,\chi}\cdot\mathrm{reg}_{\boldsymbol{C}}\{u_\chi,v_\chi\}(\eta_f^{\mathrm{ah}}). \tag{22}$$

Here χ is a suitable even Dirichlet character of modulus divisible by N, and u_χ, v_χ are modular units depending on χ, whose precise definition is provided in [BD1]. Furthermore, $C_{E,\chi}$ is a non-zero explicit algebraic constant. Equation (22) follows from an application of Rankin's method.

The article [Bei] also proved in a similar vein more general results describing the values of $L(E,s)$ at non critical integers ≥ 2 in terms of the motivic cohomology of modular curves.

REMARK 3.2. – Note the similarity between equations (19) and (22). It depends on the fact that both equations describe a special value of a Rankin L-function. The former equation involves the L-function of the convolution of f with a weight one theta-series attached to K. The latter, the L-function of the convolution of f with the weight 2 Eisenstein series $\mathrm{dlog}(v_\chi)$.

4. – p-adic L-functions of elliptic curves

We begin by reviewing the definition of the *Mazur-Swinnerton-Dyer p-adic L-function* attached to E (see [MSD], [MTT]).

Fix a prime $p \geq 3$ of good ordinary reduction for E, i.e., $p \nmid N a_p$. Let $\alpha \in \boldsymbol{Z}_p^\times$ be the unit root of $x^2 - a_p x + p$. The periods of the holomorphic 1-form

$$\omega_f := 2\pi i f(z) dz$$

give rise to a p-adic measure μ_E on $\boldsymbol{Z}_p^\times$, characterized by the following interpolation formulae:

$$(23) \qquad \int_{\boldsymbol{Z}_p^\times} \mu_E = (1-\alpha^{-1})^2 \frac{L(E,1)}{\Omega_E^+},$$

$$(24) \qquad \int_{\boldsymbol{Z}_p^\times} \psi(t)\mu_E = \frac{\tau(\psi)}{\alpha^n} \frac{L(E,\bar{\psi},1)}{\Omega_E^{\psi(-1)}}, \qquad \text{for } \psi : (\boldsymbol{Z}/p^n\boldsymbol{Z})^\times \longrightarrow \boldsymbol{C}^\times \text{ primitive.}$$

Define $L_p(E,s)$ to be the *p-adic Mellin transform* of the measure μ_E:

$$(25) \qquad L_p(E,s) = \int_{\boldsymbol{Z}_p^\times} \langle t \rangle^{s-1} d\mu_E.$$

This definition should be compared with equation (10). By combining (23) and (25), one obtains directly

$$(26) \qquad L_p(E,1) = (1-\alpha^{-1})^2 \frac{L(E,1)}{\Omega_E^+},$$

which should be viewed as the analogue of equation (8) in the context of elliptic curves. The p-adic L-function $L_p(E,s)$ satisfies the functional equation

$$(27) \qquad L_p(E,s) = w_E \langle N \rangle^{1-s} L_p(E, 2-s),$$

where the sign $w_E = \pm 1$ is the same as in (15).

Given a Dirichlet character χ, definition (25) can be generalized slightly in order to define a p-adic L-function $L_p(E,\chi,s)$ associated to E and χ interpolating the special values $L(E,\chi\psi,1)$, with ψ as above.

REMARK 4.1. – An alternate approach to the definition of the Mazur-Swinnerton-Dyer p-adic L-function $L_p(E,s)$ [Kit] consists in the p-adic interpolation of the critical values $L(f_k,j)$, $1 \le j \le k-1$ associated to the Hida family of modular forms $\boldsymbol{f} = (f_k)$ passing through f in weight 2. This yields a two-variable p-adic L-function $L_p(\boldsymbol{f},k,s)$ – called the *Mazur-Kitagawa p-adic L-function* – whose restriction to the line $k=2$ coincides with $L_p(E,s)$. (Cf. also Remark 2.2.)

Assume that the sign w_E of the functional equation (27) is -1, so that $L_p(E,s)$ and $L(E,s)$ vanish to odd order at $s=1$. The following p-adic analogue of the Gross-Zagier formula (18) was established by Perrin-Riou [PR1]. Let $h_p(P)$ denote the cyclotomic p-adic height of the Heegner point $P \in E(\boldsymbol{Q})$. Then

$$L'_p(E,1) = C'_{E,p} \cdot h_p(P), \tag{28}$$

where $C'_{E,p}$ is a non-zero rational constant, equal to the product of the constant C'_E appearing in equation (18) and of an Euler factor at p.

REMARK 4.2. – 1) It is expected that the cyclotomic p-adic height is always non-degenerate, and hence that $h_p(P)$ is non-zero precisely when P has infinite order. Assuming this, one deduces by comparing equations (18) and (28) that $L(E,s)$ has a simple zero at $s=1$ if and only if $L_p(E,s)$ has a simple zero at $s=1$.

2) Similarly to the complex case, equation (28) is deduced from a p-adic analogue of equation (19), involving a product of two Mazur-Swinnerton-Dyer p-adic L-functions. This product is identified with a Rankin p-adic L-function, attached to the convolution of f with a weight one theta-series.

We now turn to the description of the value of $L_p(E,s)$ at the point $s=2$, lying outside the range of classical interpolation for $L_p(E,s)$.

Following [Co-dS] and [Bes2], Coleman's theory of p-adic integration allows to define a p-adic counterpart $\mathrm{reg}_p\{u,v\}(\eta) \in \boldsymbol{C}_p$ of the complex regulator, where $u,v \in \boldsymbol{C}_p(X)$ are modular units, and η is a class in the de Rham cohomology group $H^1_{\mathrm{dR}}(X/\boldsymbol{C}_p)$.

The p-adic analogue of the anti-homomorphic class η_f^{ah} of equation (21) is defined to be the unique class η_f^{ur} in the "unit root subspace" of $H^1_{\mathrm{dR}}(X/\boldsymbol{C}_p)$ satisfying:

1. η_f^{ur} belongs to the f-isotypic part of $H^1_{\mathrm{dR}}(X/\boldsymbol{C}_p)$,
2. $\varphi(\eta_f^{\mathrm{ur}}) = \alpha\eta_f^{\mathrm{ur}}$, where φ denotes the Frobenius operator acting on $H^1_{\mathrm{dR}}(X/\boldsymbol{C}_p)$, and $\alpha \in \boldsymbol{Z}_p^\times$ is the p-adic unit appearing in equation (23),
3. η_f^{ur} lifts the image of η_f^{ah} in $H^1(X,\mathcal{O}_X)$ (cf. [BD1] for details).

The following *p-adic Beilinson formula*, proved in [BD1], is the analogue of equation (22) in the current context:

$$L_p(E,2) \cdot L_p(E,\chi,1) = C_{E,\chi,p} \cdot \mathrm{reg}_p\{u_\chi, v_\chi\}(\eta_f^{\mathrm{ur}}). \tag{29}$$

Here $C_{E,\chi,p}$ is a non-zero algebraic constant, which differs from $C_{E,\chi}$ by an Euler factor at p. The modular units u_χ and v_χ, depending on the choice of an even Dirichlet character χ, are the same as those appearing in (22). By a slight generalization of (26), $L_p(E,\chi,1)$ is equal to $L(E,\chi,1)/\Omega_E^+$, up to an non-zero algebraic constant. The functional equation (27) implies that (29) can also be written with $L_p(E,0)$ replacing $L_p(E,2)$. A judicious choice of χ ensures the non-vanishing of $L_p(E,\chi,1)$. In this case, equation (29) yields that the non-vanishing of $L_p(E,2)$ is equivalent to the non-vanishing of the p-adic regulator.

A special case of (29) is obtained by Brunault [Br], as a consequence of *Kato's reciprocity law* (see Remark 4.3). Moreover, prior work of Coleman-de Shalit [Co-dS] focused on the special case of elliptic curves with complex multiplication. The article [BD1] presents an alternate approach to (29) which by-passes Kato's reciprocity law. It is based on the direct evaluation of a Rankin p-adic L-function associated to the convolution of the Hida family $\boldsymbol{f} = (f_k)$ interpolating f with the Eisenstein series $\mathrm{dlog}(v_\chi)$, and on the factorization of this p-adic L-function as a product of two Mazur-Kitagawa p-adic L-functions. The work [BD2] uses [BD1] in order to obtain a new proof of Kato's reciprocity law. It is worth stressing the similarity of this approach with the description of $L_p(\chi,s)$ in terms of values at points outside the range of classical interpolation given in Remark 2.3.

Furthermore, [BD1] describes in a similar vein the values $L_p(E,n)$ at integer points ≥ 2 in terms of the motivic cohomology of the modular curve X. These values were studied previously by Gealy [Ge], by invoking Kato's reciprocity law.

REMARK 4.3. – The work of Kato [Ka], [Colz] relates $L_p(E,s)$ to the structure of the p-primary Selmer group of E over $\boldsymbol{Q}_\infty := \boldsymbol{Q}(\mu_{p^\infty})$, viewed as a module over the Galois group $\mathrm{Gal}(\boldsymbol{Q}_\infty/\boldsymbol{Q}) = \boldsymbol{Z}_p^\times$. Combined with recent work of Skinner-Urban [SU], it establishes the cyclotomic Main Conjecture of Iwasawa theory for the elliptic curve E. Let $V_p(E)$ denote the p-adic Galois representation of E. Kato's approach is based on the study of cohomology classes

$$\kappa_\chi(1) \in H^1(\boldsymbol{Q}_\infty, V_p(E)(1)) \tag{30}$$

arising from étale regulators of modular units attached to characters χ of p-power conductor. The comparison functor between étale and de Rham cohomology relates the restriction at p of the étale regulator to the p-adic regulator [Bes1]. By Tate twisting the classes (30), one obtains a system of classes

$$\kappa_\chi \in H^1(\boldsymbol{Q}_\infty, V_p(E)). \tag{31}$$

Kato's reciprocity law describes $L(E, \chi, 1)$ in terms of the singular part of κ_χ at p. In view of the interpolation formulae (24) and (25), this yields a cohomological description of $L_p(E, s)$ – a key step towards the proof of the cyclotomic Main Conjecture for E.

REMARK 4.4. – When χ is the trivial character, the class κ_χ of equation (31) arises from the restriction of a class κ in $H^1(\boldsymbol{Q}, V_p(E))$. Assume that $L(E, 1) = 0$. Kato's reciprocity law implies that the image κ_p of κ in $H^1(\boldsymbol{Q}_p, V_p(E))$ is crystalline, and hence belongs to the "finite subspace" $H^1_f(\boldsymbol{Q}_p, V_p(E))$. Perrin-Riou [PR2] conjectures that κ_p is non-zero if and only if $L'(E, 1)$ is non-zero, and predicts a precise relation between the logarithm of κ_p and the formal group logarithm of a global point in $E(\boldsymbol{Q})$. The goal of [BD3] is to obtain a proof of Perrin-Riou's conjecture, by combining the approach to Kato's Euler system developed in [BD1] and [BD2] with the results of [BDP1] and [DR]. This proof establishes a p-adic relation between Kato's Euler system and the Euler system of Heegner points.

REFERENCES

[Bei] A. A. BEILINSON *Higher regulators of modular curves*, Applications of algebraic K-theory to algebraic geometry and number theory, Part I, II (Boulder, Colo., 1983), 1-34, Contemp. Math., **55**, Amer. Math. Soc., Providence, RI, 1986.

[BCDT] C. BREUIL - B. CONRAD - F. DIAMOND - R. TAYLOR, *On the modularity of elliptic curves over* $\boldsymbol{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc., **14**, no. 4 (2001), 843-939.

[BD1] M. BERTOLINI - H. DARMON, *Kato's Euler system and rational points on elliptic curves I: A p-adic Beilinson formula*, Israel Journal of Math., to appear.

[BD2] M. BERTOLINI - H. DARMON, *Kato's Euler system and rational points on elliptic curves II: The explicit reciprocity law*, in preparation.

[BD3] M. BERTOLINI - H. DARMON, *Kato's Euler system and rational points on elliptic curves III: The conjecture of Perrin-Riou*, in preparation.

[BDP1] M. BERTOLINI - H. DARMON - K. PRASANNA, *Generalised Heegner cycles and p-adic Rankin L-series*, Duke Math. J., to appear.

[Ber] M. BERTOLINI, *Report on the Birch and Swinnerton-Dyer conjecture*, Milan J. Math., **78**, no. 1 (2010), 153-178.

[Bes1] A. BESSER, *Syntomic regulators and p-adic integration. I. Rigid syntomic regulators*, Proceedings of the Conference on p-adic Aspects of the Theory of Automorphic Representations (Jerusalem, 1998) Israel J. Math., **120**, part B (2000), 291-334.

[Bes2] A. BESSER, *Syntomic regulators and p-adic integration. II.* K_2 *of curves*, Proceedings of the Conference on p-adic Aspects of the Theory of Automorphic Representations (Jerusalem, 1998). Israel J. Math., **120**, part B (2000), 335-359.

[Bl] S. J. BLOCH, *Higher regulators, algebraic K-theory, and zeta functions of elliptic curves*, CRM Monograph Series, 11. American Mathematical Society, Providence, RI, 2000. x+97 pp.

[Br] F. BRUNAULT, *Régulateurs p-adiques explicites pour le K_2 des courbes elliptiques*, Actes de la Conférence "Fonctions L et Arithmétique", 29-57, Publ. Math. Besançon Algèbre Théorie Nr., Lab. Math. Besançon, Besançon, 2010.

[Co] R. F. COLEMAN, *Dilogarithms, regulators and p-adic L-functions*, Invent. Math., **69**, no. 2 (1982), 171-208.

[Co-dS] R. F. COLEMAN - E. DE SHALIT, *p-adic regulators on curves and special values of p-adic L-functions*, Inventiones Math., **93** (1988), 239-266.

[Colz] P. COLMEZ, *La conjecture de Birch et Swinnerton-Dyer p-adique*, (French) Astérisque No. 294 (2004), ix, 251-319.

[De] P. DELIGNE, *Valeurs de fonctions L et périodes d'intégrales*, With an appendix by N. Koblitz and A. Ogus. Proc. Sympos. Pure Math., XXXIII, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, pp. 313-346, Amer. Math. Soc., Providence, R.I., 1979.

[DR] H. DARMON - V. ROTGER, *Diagonal cycles and Euler systems I: A p-adic Gross-Zagier formula*, submitted.

[Ge] M. GEALY, *On the Tamagawa number conjecture for motives attached to modular forms*, PhD Thesis, California Institute of Technology, 2006.

[GZ] B. H. GROSS - D. B. ZAGIER, *Heegner points and derivatives of L-series*, Invent. Math., **84**, no. 2 (1986), 225-320.

[Ka] K. KATO, *p-adic Hodge theory and values of zeta functions of modular forms. Cohomologies p-adiques et applications arithmétiques. III*, Astérisque No. 295 (2004), ix, 117-290.

[Ki] M. KIM, *Classical motives and motivic L-functions*, Autour des motifs-École d'été Franco-Asiatique de Géométrie Algébrique et de Théorie des Nombres/ Asian-French Summer School on Algebraic Geometry and Number Theory. Volume I, 1-25, Panor. Synthèses, 29, Soc. Math. France, Paris, 2009.

[Kit] K. KITAGAWA, *On standard p-adic L-functions of families of elliptic cusp forms*, in p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), 81-110, Contemp. Math., **165**, Amer. Math. Soc., Providence, RI, 1994.

[Ko] V. A. KOLYVAGIN, *Euler systems*, The Grothendieck Festschrift, Vol. II, 435-483, Progr. Math., **87**, Birkhäuser Boston, Boston, MA, 1990.

[La] S. LANG, *Cyclotomic fields I and II*. Combined second edition. With an appendix by Karl Rubin. Graduate Texts in Mathematics, **121**. Springer-Verlag, New York, 1990, xviii+433.

[Man] JU. I. MANIN, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat., **36** (1972), 19-66.

[MSD] B. MAZUR - P. SWINNERTON-DYER, *Arithmetic of Weil curves*, Invent. Math., **25** (1974), 1-61.

[MTT] B. MAZUR - J. TATE - J. TEITELBAUM, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math., **84**, no. 1 (1986), 1-48.

[PR1] B. PERRIN-RIOU, *Points de Heegner et dérivées de fonctions L p-adiques*, Invent. Math., **89**, no. 3 (1987), 455-510.

[PR2] B. PERRIN-RIOU, *Fonctions L p-adiques d'une courbe elliptique et points rationnels*, Ann. Inst. Fourier (Grenoble), **43**, no. 4 (1993), 945-995.

[Ru] K. C. RUBIN, *The main conjecture*, Appendix to [La].

[Sil] J. H. SILVERMAN, *The arithmetic of elliptic curves*. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009. xx+513 pp.

[So] C. SOULÉ, *Éléments cyclotomiques en K-théorie*, Journées arithmétiques de Besançon, Astérisque No. 147-148 (1987), 225-257.

[SU] C. Skinner - E. Urban, *The Iwasawa Main Conjecture for* GL_2, preprint.

[TW] R. Taylor - A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2), **141**, no. 3 (1995), 553-572.

[Wa1] L. C. Washington, *Introduction to cyclotomic fields*. Second edition. Graduate Texts in Mathematics, **83**. Springer-Verlag, New York, 1997. xiv+487 pp.

[Wa2] L. C. Washington, *Euler factors for p-adic L-functions*, Mathematika, **25**, no. 1 (1978), 68-75.

[Wi1] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2), **141**, no. 3 (1995), 443-551.

[Wi2] A. Wiles, *The Birch and Swinnerton-Dyer conjecture*, on the Clay Mathematics Institute web site: http://www.claymath.org/millennium/

Università degli Studi di Milano, Dip.to di Matematica,
Via Saldini 50, 20133 Milano
E-mail: massimo.bertolini@unimi.it

Received December 24, 2011 and in revised form March 26, 2012