Astérisque

JOHN COATES

On p-adic L-functions

Astérisque, tome 177-178 (1989), Séminaire Bourbaki,
exp. n° 701, p. 33-59

<http://www.numdam.org/item?id=SB_1988-1989__31__33_0>

Séminaire Bourbaki
40ème année, 1987-88, no 701.

Novembre 1988

On p-adic L-functions.

by

John Coates.

1. **Introduction.** Our goal in this seminar will be the modest one of outlining the general definition of the p-adic L-function of a motive over the rational field $\mathbf{Q}$, and discussing several concrete examples where this p-adic L-function can be shown to exist. As definitions are inevitably tedious, we shall begin by briefly explaining why p-adic L-functions are of interest to number-theorists. The ultimate reason is that their zeroes always seem to occur as the eigenvalues of elements of Galois groups acting on certain arithmetically defined p-adic spaces. The precise formulation of this statement amounts to a series of deep arithmetic conjectures, which are usually called the main conjectures of Iwasawa theory, and which, in common with most other general conjectures about L-functions, are still largely unproven (although there has been dramatic recent progress on several important examples of these main conjectures by Kolyvagin and Rubin). While we do not have time to discuss these general conjectures here, their arithmetic flavour can be captured by stating several down to earth consequences of them,which have been proven. Recall that the Riemann zeta function $\zeta(s)$, where s is a variable in the complex plane, is defined by the Euler product

$$\zeta(s) = \prod (1 - q^{-s})^{-1} \qquad (R(s) > 1) \qquad (1),$$

where q runs over all prime numbers. Apart from a simple pole at $s = 1$, it has a holomorphic continuation over the whole complex plane. Euler proved that the value of $\zeta(s)$ at each odd odd negative integer s is a rational number. We owe to Kummer the remarkable discovery that these rational numbers are deeply related to the arithmetic of the field $F = \mathbf{Q}(\mu_p)$, where p is a prime

S.M.F.
Astérisque 177-178 (1989)

number, and μ_p is the group of p-th roots of unity. Let Δ denote the Galois group of F over $\mathbf{Q}$, and C the ideal class group of F. Let $\mathbf{F}$ denote the field with p elements,and let ω be the $\mathbf{F}$ - valued character giving the action of Δ on μ_p. Now we can view $C_p = C/C^p$ as a vector space over $\mathbf{F}$, which is endowed with a natural action of Δ.

Theorem 1. Let n be an odd negative integer, which is not congruent to 1 modulo (p-1). Then the character $\chi = \omega^n$ occurs in the representation of Δ on C_p if and only if p divides the numerator of the rational number $\zeta(n)$. Moreover, $\chi = \omega$ does not occur in this representation.

Today, we view this as a corollary of the main conjecture on cyclotomic fields (proven first by Mazur-Wiles [25], and again recently by a different method by Kolyvagin and Rubin), although it was established earlier by Kummer, Herbrand, and Ribet. As a numerical example, take p = 12613 (see [34]). If n is an odd negative integer, which is not congruent to 1 modulo 12612, then $\zeta(n)$ is divisible by p if and only if

$$n \equiv -307, -501, -9399, -10535 \bmod 12612 \qquad (2),$$

and so it follows that, if n is any odd integer,then $\chi = \omega^n$ occurs in C_p if and only if n satisfies one of the congruences (2).

After the cyclotomic theory, it is natural to turn to elliptic curves for further examples. Let E be an elliptic curve over $\mathbf{Q}$, which we can suppose given by an equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad (a_i \text{ in } \mathbf{Z}) \qquad (3),$$

which is minimal in the sense that the absolute value of its discriminant is minimal. The arithmetic of E is concerned with the study of the group $E(\mathbf{Q})$ of rational points on E, together with its inseparable arithmetic companion the Tate-Safarevic group $Ш(E)$ of E. Recall that $Ш(E)$ is defined as follows. Let $\mathbf{Q}^a$ denote an algebraic closure of $\mathbf{Q}$, and let G be the Galois group of $\mathbf{Q}^a$. For each place v of $\mathbf{Q}$, let $\mathbf{Q}_v$ be the completion at v, K_v an algebraic closure of this completion,and G_v its Galois group. Then $Ш(E)$ is the subgroup of $H^1(G,$

$E(\mathbf{Q}^a)$) consisting of all cohomology classes which restrict to 0 in $H^1(G_v, E(K_v))$ for all places v. The conjecture of Birch and Swinnerton-Dyer links the determination of these two groups with the behaviour of the L-function L(E,s) attached to E (see §3) at s = 1. It is still unknown, in general, whether L(E,s) satisfies Conjecture A of §3, but it is true when E is a modular elliptic curve (Eichler - Shimura) or E admits complex multiplication (Deuring-Weil). Let $H_1(E(\mathbf{C}), \mathbf{Z})$ be the first homology group, with integral coefficients, of the torus $E(\mathbf{C})$ of complex points of E. If ε denotes + or - ,write γ^ε for a generator of the free rank 1 $\mathbf{Z}$ - submodule of this homology group, on which the involution induced by the action of complex conjugation on $E(\mathbf{C})$ acts via the sign ε. We then define the periods

$$u^\varepsilon(E) = \int_{\gamma^\varepsilon} dx/(2y + a_1x + a_3) \qquad (4).$$

When E is modular or admits complex multiplication,it is known that $L(E,1)/u^+(E)$ is a rational number. The proof of the following recent result of Rubin,which is in accord with the conjecture of Birch and Swinnerton-Dyer, depends heavily on the ideas of Kolyvagin.

Theorem 2. Assume that E admits complex multiplication,and let K be the imaginary quadratic field $\mathrm{End}_{\mathbf{C}}(E) \otimes \mathbf{Q}$. Assume that $L(E,1) \neq 0$. Then $E(\mathbf{Q})$ and $Ш(E)$ are finite, and, for each prime p which does not divide the order of the group of roots of unity of K, we have

$$p\text{ - part of } L(E,1)/u^+(E) = p\text{-part of } \#(Ш(E))/\#(E(\mathbf{Q}))^2 \qquad (5).$$

For example,take $E : y^2 = x^3 - x$, which admits complex multiplication by $\mathbf{Z}[i]$. Then

$$L(E,1) = u^+(E)/4 \quad .$$

Now Fermat's celebrated argument shows that $E(\mathbf{Q})$ has order 4,and that the 2 - primary part of $Ш(E)$ is trivial. Hence the above theorem shows that $Ш(E)$ is trivial for this elliptic curve. We note that Kolyvagin has proven the first

assertion of Theorem 2 for modular elliptic curves, but that (5) has still not been fully established for such curves.

As a final example, consider the L-function $L(Sym^2(E),s)$ attached to the motive which is the symmetric square of E (see §3). When E is either modular, or admits complex multiplication, Conjecture A of §3 is valid for $Sym^2(E)$, and if we put

$$u(Sym^2(E)) = u^+(E)u^-(E)/(2\pi i) \qquad (6)$$

then it is known that $L(Sym^2(E),1)$ is a non-zero rational multiple of $u(Sym^2(E))$. The following result, proven in [3], gives some indication of the interest of this rational number. Assume that E admits complex multiplication. Let p be a prime number, E_p the group of p-division points on E, $F = \mathbf{Q}(E_p)$ the field obtained by to $\mathbf{Q}$ adjoining the coordinates of the p-division points, and C the ideal class group of F. Let Δ denote the Galois group of F over $\mathbf{Q}$. If p is an odd prime where E has good reduction, the order of Δ is known to be prime to p, and so all representations of Δ over the field $\mathbf{F}$ with p elements are semi-simple. Recall that a prime p of good reduction is said to be ordinary for E if the reduction of (3) mod p has non-trivial p-torsion over the algebraic closure of $\mathbf{F}$.

Theorem 3. Assume that E has complex multiplication. Let $p \neq 2,3$ be a prime number, where E has good ordinary reduction. Then, if p does not divide the numerator of the rational number $L(Sym^2(E),1)/u(Sym^2(E))$, no irreducible component of either $Sym^2(E_p)$ or $Hom(Sym^2(E_p),\mu_p)$ can occur in the representation of Δ on $C_p = C/C^p$.

For example,if E is the curve $y^2 = x^3 - x$,we have

$$L(Sym^2(E),1)/u(Sym^2(E)) = 1/4.$$

Since E has good ordinary reduction for all primes $p \equiv 1 \bmod 4$,it follows that the conclusion of Theorem 3 is valid for all such p.

Notation. If K/F is a Galois extension of fields, we write G(K/F) for the Galois group of K over F. Let $\mathbf{Q}^a$ denote the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$, and write $G = G(\mathbf{Q}^a/\mathbf{Q})$. For each integer $m > 1$, μ_m will denote the group of m-th roots of unity in $\mathbf{Q}^a$. Throughout, p will denote an arbitrary prime number (we do not exclude p = 2), and $\mathbf{Q}_p$, Z_p the field of p-adic numbers,and the ring of p-adic integers. Let $\mathbf{C}_p$ be the completion of an algebraic closure of $\mathbf{Q}_p$. We fix an embedding of $\mathbf{Q}^a$ in $\mathbf{C}_p$,which we do not make explicit in our notation. Write

$$H = G(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}) \quad , \quad D = G(\mathbf{Q}(\mu_{p^\infty})^+/\mathbf{Q}) \qquad (7)$$

for the Galois groups over $\mathbf{Q}$ of the field generated by all p-power roots of unity, and of its maximal real subfield. The action of H on the group of all p-power roots of unity defines a canonical isomorphism

$$\psi : H \to Z_p^{\times} \qquad (8),$$

which is called the cyclotomic character. If χ is a Dirichlet character,we write $c(\chi)$ for the conductor of χ. Recall that χ can also be viewed as a character (which we again denote by χ) of the Galois group G, which is unramified outside $c(\chi)$ and ∞, and which satisfies $\chi(\mathrm{Frob}_q) = \chi(q)$ for all primes q with $(q,c(\chi)) = 1$. Here Frob_q denotes the arithmetic Frobenius, i. e. it operates on the algebraic closure of the field with q elements by sending x to x^q.

2. The p-adic analogue of the Riemann zeta function. The construction of the p-adic analogue of $\zeta(s)$ is due to Kubota - Leopoldt [19] and Iwasawa [17], although most of the ingredients used in it were already known to Kummer. The definition (1) of $\zeta(s)$ as an Euler product is simply not applicable in the p-adic case, and all known approaches today involve p-adic interpolation, where the obvious question to ask is whether there exists a continuos function of a p-adic variable s in Z_p , whose values at the odd negative integers s = n are essentially the rational numbers $\zeta(n)$. However, both the analogy with the adelic description of $\zeta(s)$ given in Tate's thesis, and the connexion with Iwasawa modules mentioned in the Introduction, make it desirable, following Iwasawa and Mazur, to express the result in terms of p-adic measures on Galois groups, and we begin by briefly recalling the

definition of these (see [31]).

The Iwasawa algebra I of D is defined to be the projective limit of the group rings $\mathbf{Z}_p[D/U]$, where U runs over the open subgroups of D. It is a compact algebra, which contains $\mathbf{Z}_p[D]$ as a dense sub-algebra. The elements of I are called integral p-adic measures on D. This terminology is justified because, if μ is in I and f is any continuous function from D to $\mathbf{C}_p$, we can define the integral $\int_D f\, d\mu$ by passage to the limit from the case when f is locally constant. In this latter case, if U is an open subgroup of D such that f is constant modulo U, and if the image of μ in $\mathbf{Z}_p[D/U]$ is equal to $\sum \mu(s)s$, then the value of the above integral is $\sum \mu(s)f(s)$, where, in both sums, s runs over D/U. We need two slight generalizations of the notion of an integral measure. Let I^* be the ring of quotients of I, i.e. the set of all quotients α/β, where α, β are in I and β is not a divisor of 0. We say an element μ of I^* is a measure if there exists a non-zero β in $\mathbf{Z}_p$ such that $\beta\mu$ is in I. Now let ϕ be any continuous homomorphism from D to $\mathbf{C}_p^{\times}$. We say an element μ of I^* is a ϕ - pseudo - measure, if there exists an integer $k \geq 0$ such that $(\phi(\sigma) - \sigma)^k\mu$ is a measure for all σ in D. We then say that such a ϕ - pseudo -measure μ has a pole of order $\leq k$ at ϕ. Given such a μ, and any continuous homorphism $\lambda \neq \phi$ from D to the multiplicative group of $\mathbf{C}_p$, we can define the integral of λ against μ to be $(\phi(\sigma) - \lambda(\sigma))^{-k}$ times the integral of λ against $(\phi(\sigma) - \sigma)^k\mu$, where σ is any element of D such that $\phi(\sigma) \neq \lambda(\sigma)$.

The following is the basic existence theorem for the p-adic analogue of Riemann zeta function. As usual, if χ is a Dirichlet character, $L(\chi,s) = \Pi(1 - \chi(q)q^{-s})^{-1}$, where the product is taken over all primes q with $(q,c(\chi)) = 1$. Formula (11) below shows that $L(\chi,r)$ belongs to $\mathbf{Q}$ for all integers $r \geq 0$. Recall that ψ denotes the cyclotomic character (9). Let χ be a Dirichlet character of p-power conductor,and let n be any integer. Then $\chi\psi^n$ is a character of the Galois group H,and it will be a character of the quotient D of H if and only if

$$\chi(-1) = (-1)^n \qquad (9).$$

Theorem 4. Let m be an odd integer < 0. There exists a unique ψ^{1-m} - pseudo-measure ρ_m, with a pole of order 1 at ψ^{1-m}, on D as follows. For all Dirichlet

characters χ of p-power conductor, and all integers n such that $n+m \leq 0$ and (9) holds,we have

$$\int_D \chi \psi^n \, d\rho_m = L(\chi^{-1}, n+m)(1 - \chi^{-1}(p)p^{n+m}) \qquad (10).$$

We sketch what is essentially Iwasawa's proof of this theorem. Put $r = 4$ or p, according as p is even or odd, and put $r_k = rp^k$ for all $k \geq 0$. For each p-adic unit u, write $[u]_k$ for its class in the group of relatively prime residue classes modulo r_k . Consider the partial zeta function

$$\zeta(u, r_k ; s) = \sum m^{-s} \qquad (R(s) > 1) ,$$

where the sum is over all positive integers m in the class $[u]_k$. It has an analytic continuation over the whole complex plane, apart from a simple pole at s = 1. For each non-negative integer t, we have

$$\zeta(u, r_k ; -t) = -r_k^t B_{t+1}(\{u\}_k/r_k)/(t+1) \qquad (11),$$

where $\{u\}_k$ denotes the unique representative in Z of $[u]_k$ such that $0 < \{u\}_k < r_k$; here $B_{t+1}(x)$ denotes the (t+1)-th Bernoulli polynomial, defined by

$$we^{wx}/(e^w - 1) = \sum B_h(x) w^h/h! \quad ,$$

the sum being over all integers $h \geq 0$. In particular,we have

$$B_1(x) = x - 1/2 \quad , \quad B_{t+1}(x) = x^{t+1} - (t+1)/2\, x^t + ... \qquad (12).$$

For t fixed, let p^e denote the largest power of p occurring in the denominators of the coefficients of $B_{t+1}(x)/(t+1)$. One deduces immediately from (11) and (12) that, for all integers $k \geq 0$ and all p-adic units u, we have

$$\zeta(u , r_{k+e} ; -t) \equiv t\, u^{t+1}/((t+1)r_{k+e}) + u^t \zeta(u , r_{k+e} ; 0) \bmod r_k \qquad (13).$$

If v is also a p-adic unit,we define

$$\delta_t(u, v; r_k) = v^{t+1}\,\zeta(u, r_k; -t) - \zeta(uv, r_k; -t).$$

Then we claim that, for all integers $k \geq 0$, we have

$$\delta_t(u, v; r_k) \equiv (uv)^t\,\delta_0(u, v; r_k) \mod r_k \qquad (14).$$

Note that (13) only implies the weaker congruence in which the first two r_k 's appearing in (14) are replaced by r_{k+e}. But it is easy to see that this weaker congruence implies (14), when combined with the additional identity

$$\sum \zeta(z, r_h; s) = \zeta(u, r_k; s) \qquad (15),$$

where h is any integer $\geq k$, and z runs over any set of representatives in the p-adic units of those classes modulo r_h which map to the class of u modulo r_k. Note that one obvious consequence of (14) is that $\delta_t(u, v; r_k)$ is integral at p for all $t \geq 0$, because this is plainly true for $t = 0$ from the explicit formula for $B_1(x)$. We can now construct our desired pseudo - measure on D. Let F_k be the maximal real subfield of the field obtained by adjoining the r_k - th roots of unity to $\mathbf{Q}$. For each p-adic unit u, let $\sigma_k(u)$ denote the restriction to F_k of the automorphism of $\mathbf{Q}(\mu_{p^\infty})$ which acts on μ_{p^∞} by raising to the u - th power. Now let W_k be any subset of the p-adic units, which is a set of representatives of the relatively prime residue classes modulo r_k. For each p-adic unit v, define

$$\lambda_k(v,m) = (v^{1-m} - \sigma_k(v)) \sum \zeta(u, r_k; m)\,\sigma_k(u)^{-1} = \sum \delta_{-m}(u, v; r_k)\,\sigma_k(u)^{-1},$$

where both sums are over the u in W_k. This belongs to the $\mathbf{Z}_p$ - group ring of the Galois group of F_k over $\mathbf{Q}$. It should be thought of as a twisted version of the classical element arising from the factorization of Gauss sums. The identity (15) shows that $(\lambda_k(v,m) : k=0,1,...)$ defines an element $\lambda(v,m)$ of the Iwasawa algebra I of D. Let $\sigma(v)$ be the element of D defined by the $\sigma_k(v)$ $(k=0,1,...)$. If v is not of finite order, it is clear that $(v^{1-m} - \sigma(v))$ is not a zero divisor in I. Hence $\rho_m = \lambda(v,m)/(v^{1-m} - \sigma(v))$ is a ψ^{1-m} - pseudo-measure, which is independent of the choice of the p-adic unit v of infinite order. Using the congruence (14), one verifies easily that (10) holds.

3. Complex L-functions. The complex L-functions of primary interest in number theory are those attached to the cohomology of an algebraic variety over $\mathbf{Q}$, or, more generally, to a motive over $\mathbf{Q}$. We briefly recall Serre's definition [30] of these L - functions.

We simply view motives in the naive sense, as being defined by a collection of realisations, satsfying certain axioms. Thus, by a homogeneous motive M over $\mathbf{Q}$ of weight w(M) and dimension d(M), we mean a collection of Betti $H_B(M)$, de Rham $H_{DR}(M)$, and l-adic $H_l(M)$ (one for each prime l) realisations, which are, respectively, vector spaces over $\mathbf{Q}$, $\mathbf{Q}$, and $\mathbf{Q}_l$,all of the same dimension d(M). Moreover, these realisations are endowed with the following additional structure :- (i). $H_B(M)$ admits an involution F_∞ ; (ii). The Galois group G of $\mathbf{Q}^a$ over $\mathbf{Q}$ has a continuos action on $H_l(M)$ for each prime l, and there is an isomorphism g_l from $H_B(M) \otimes \mathbf{Q}_l$ to $H_l(M)$, which transforms F_∞ into the complex conjugation; (iii). There is a decreasing exhaustive filtration $\{F^kH_{DR}(M) : k \in \mathbf{Z}\}$ on $H_{DR}(M)$; (iv). There is a Hodge decomposition into $\mathbf{C}$ - vector spaces

$$H_B(M) \otimes \mathbf{C} = \oplus H^{i,j}(M) \qquad (16),$$

where i,j run over a finite set of indices satisfying i+j = w(M), and where F_∞ maps $H^{i,j}(M)$ to $H^{j,i}(M)$; (v). There is a $G_\infty = G(\mathbf{C}/\mathbf{R})$ - isomorphism of $\mathbf{C}$ - vector spaces

$$g_\infty : H_B(M) \otimes \mathbf{C} \rightarrow H_{DR}(M) \otimes \mathbf{C} \qquad (17),$$

where complex conjugation acts on the space on the left via its action on $\mathbf{C}$, and on the space on the right via F_∞ on $H_B(M)$ and its natural action on $\mathbf{C}$. (vi). Finally, for all $k \in \mathbf{Z}$, we have

$$g_\infty^{-1} (F^kH_{DR}(M) \otimes \mathbf{C}) = \oplus_{(i \geq k)} H^{i,j}(M) \qquad (18).$$

Example 1. Let E be an elliptic curve over $\mathbf{Q}$. Then E defines a motive (which we again denote by E) over $\mathbf{Q}$ of weight 1 and dimension 2, with the following realisations :- $H_B(E)$ is the Betti cohomology with coefficients in $\mathbf{Q}$ of the torus $E(\mathbf{C})$ of complex points of E, $H_{DR}(E)$ is the de Rham cohomolgy of E as

an algebraic variety over $\mathbf{Q}$, and, for each prime l, $H_l(E)$ is given by $\mathrm{Hom}(V_l(E) , \mathbf{Q}_l)$; here $V_l(E)$ is the tensor product with $\mathbf{Q}_l$ of the projective limit of the groups E_{l^n} (n=1,2,...) of l^n - division points on E, endowed with their natural action of G. The above axioms reduce to classical facts about elliptic curves. Similarly, for each integer $k \geq 1$, we can define a motive $\mathrm{Sym}^k(E)$ by taking its realisations to be the k-th symmetric powers of the realisations of E.

Example 2. For each integer m, we now define the Tate motive $\mathbf{Q}(m)$ of weight - 2m and dimension 1. Let $V_l(\mu)$ be the tensor product with $\mathbf{Q}_l$ of the projective limit of the groups μ_{l^n} (n=1,2,...) of l^n - th roots of unity, and let $V_l(\mu)^{\otimes m}$ be the m-th tensor power of $V_l(\mu)$. The realisations of $\mathbf{Q}(m)$ are given by

$$H_B(\mathbf{Q}(m)) = \mathbf{Q} \ , \ H_{DR}(\mathbf{Q}(m)) = \mathbf{Q} \ , \ H_l(\mathbf{Q}(m)) = V_l(\mu)^{\otimes m} .$$

The involution F_∞ is $(-1)^m$, and the action of G is the natural one. The Hodge decomposition is specified by taking $H^{-m,-m} = \mathbf{C}$, and the k-th term in the filtration of the De Rham cohomology is either $\mathbf{Q}$ or 0, according as $k \leq -m$ or $k > -m$. The isomorphism (17) is given by $g_\infty(1) = (2\pi i)^m$.

If M is any motive over $\mathbf{Q}$, we can construct the following motives from M :- (i). The twists M(n), for any n in $\mathbf{Z}$; by definition M(n) is the motive of weight $w(M(n)) = w(M) - 2n$, whose realisations are simply the tensor products of the corresponding realisations of M and $\mathbf{Q}(n)$; (ii) The dual motive M^ ; by definition, the realisations of M^ are the dual vector spaces of the realisations of M.

For simplicity, we shall assume for the rest of this seminar that our motive M satisfies the following :-

Hypothesis. If w(M) is even, then F_∞ acts on $H^{k,k}(M)$ ($k = w(M)/2$) via a scalar.

The assumption made later that M is critical at s = 0 will automatically imply this. We also put

$$\Gamma_{\mathbf{R}}(s) = \pi^{-s/2}\,\Gamma(s/2)\ ,\ \Gamma_{\mathbf{C}}(s) = 2(2\pi)^{-s}\,\Gamma(s)\ ,\ H^{i,j} = H^{i,j}(M)\ ,\ h(i,j) = \dim_{\mathbf{C}} H^{i,j}.$$

The underlying idea of the definition of the complex L-series of M is to specify it as an Euler product, all of whose terms are determined by purely local data. The Euler factor at ∞ is given by

$$L_\infty(M\ ,\ s) = \prod L_\infty(U,\ s) \qquad (19),$$

where U runs over the direct summands of $H_B(M) \otimes \mathbf{C}$ of the form either $U = H^{j,k} \oplus H^{k,j}$ with $j<k$, or $U = H^{k,k}$, and $L_\infty(U,s)$ is given explicitly by :- (a). If $U = H^{j,k} \oplus H^{k,j}$ with $j<k$, then $L_\infty(U,s) = \Pi_{(j<k)}\,\Gamma_{\mathbf{C}}(s-j)^{h(j,k)}$; (b). If $U = H^{k,k}$ and F_∞ acts on U by $(-1)^k$, then $L_\infty(U,s) = \Gamma_{\mathbf{R}}(s-k)^{h(k,k)}$; (c). If $U = H^{k,k}$ and F_∞ acts on U by $(-1)^{k+1}$,then $L_\infty(U,s) = \Gamma_{\mathbf{R}}(s+1-k)^{h(k,k)}$. If q is a finite prime, let I_q denote the inertia group of some fixed prime of $\mathbf{Q}^a$ lying above q. The Euler factor at q is given by

$$L_q(M,s) = \det(1 - \mathrm{Frob}_q^{-1}.q^{-s}\ |H_l(M)^{I_q})^{-1},$$

where l is any prime different from q, and Frob_q denotes the arithmetic Frobenius. We impose the standard hypothesis that this Euler factor is a rational function in q^{-s} ,with coefficients in $\mathbf{Q}$, which are independent of $l \neq q$. The complex L - function of M is then defined by

$$\Lambda(M\ ,\ s) = \Pi\, L_v(M\ ,\ s) \qquad (20),$$

where v runs over all primes of $\mathbf{Q}$, including $v = \infty$. We also put

$$L(M\ ,\ s) = \Lambda(M\ ,\ s)/L_\infty(M\ ,\ s).$$

Note that we have $\Lambda(M(n)\ ,\ s) = \Lambda(M\ ,\ s+n)$ for all n in $\mathbf{Z}$. We assume, as usual, that there exists a finite set of primes S such that (i) for each prime l, and each $q \neq l$ which is not in S, the inertia group I_q operates trivially on

$H_l(M)$, and (ii) for q not in S, the reciprocal complex roots of $L_q(M,s)^{-1}$ (viewed as a polynomial in q^{-s}) have absolute value equal to $q^{w(M)/2}$. Under an additional hypothesis, one can define (see [9]) Deligne's global ε-factor $\varepsilon(M,s)$. Here is the standard conjecture about the analytic continuation and functional equation of these L-functions.

Conjecture A (Complex Version). $\Lambda(M , s)$ has a meromorphic continuation over the whole complex plane to a function of order ≤ 1, and satisfies the functional equation

$$\Lambda(M , s) = \varepsilon(M , s)\Lambda(M\hat{}(1) , - s) \qquad (21).$$

Moreover, $\Lambda(M , s)$ is entire, unless w(M) is even and $\mathbf{Q}(-w(M)/2)$ is a direct summand of M.

It follows that $\Lambda(M,s)$ should be holomorphic everywhere, except for a possible pole at the point $s = 1+w(M)/2$. We write e(M) for the order of the pole of L(M,s) at this point (take e(M) = 0 if L(M,s) is holomorphic at this point). We note that e(M) is conjectured to be the maximal number of copies of $\mathbf{Q}(-w(M)/2)$, which are direct summands of M. Also, for each prime l, e(M) is conjectured to be equal to the $\mathbf{Q}_l$ - dimension of the subspace of $H_l(M(w(M)/2))$, which is fixed by the global Galois group G.

One of the delicate points of the complex theory (which also turns out to be basic for the non-archimedean theory) is that the global factor $\varepsilon(M) = \varepsilon(M,0)$ can be written as a product of local ε-factors (see [9]). Let $\mathbf{A}$ denote the adele group of $\mathbf{Q}$. Fix, once and for all, the Haar measure $dx = \prod dx_v$ on $\mathbf{A}$,where dx_∞ is the usual Haar measure on $\mathbf{R}$, and, for each prime q, dx_q is the Haar measure on $\mathbf{Q}_q$ which gives $\mathbf{Z}_q$ volume 1. We also must choose a complex character of $\mathbf{A}/\mathbf{Q}$,and there are two natural choices. Let $\eta^{(i)}$ denote the character of $\mathbf{A}/\mathbf{Q}$ with components $\eta_\infty{}^{(i)}(x) = \exp(2\pi ix)$, and, for each finite prime q, $\eta_q{}^{(i)}(x) = \exp(-2\pi ix)$, where we have identified $\mathbf{Q}_q/\mathbf{Z}_q$ with the q- primary subgroup of $\mathbf{Q}/\mathbf{Z}$. The second natural choice is $\eta^{(-i)}(x) = \eta^{(i)}(-x)$. For the rest of this seminar, ι will denote one of i or -i. We then have

$$\varepsilon(M) = \varepsilon(M , 0) = \prod_v \varepsilon_v(M , \eta^{(\iota)}) \qquad (22),$$

where $\varepsilon_v(M, \eta^{(\iota)})$ denotes Deligne's local ε_v-factor (with the fixed measure dx_v suppressed in the notation), and the product is taken over all primes v of $\mathbf{Q}$, including $v = \infty$. Note that we have

$$\varepsilon_v(M, \eta^{(\iota)})\, \varepsilon_v(M\hat{}(1), \eta^{(-\iota)}) = 1 \qquad (23).$$

Finally, we recall the notion of a twisting a motive M by a Dirichlet character. If χ is a Dirichlet character, and K is any finite extension of $\mathbf{Q}$ containing the values of χ, we can attach to χ a motive $[\chi]$ over $\mathbf{Q}$, with coefficients in K, in the following manner (see [10], §6). As remarked earlier, we can view χ as a character of the global Galois group G, and, for each finite prime λ of K, we define $H_\lambda(\chi)$ to be the completion K_λ, with G acting via χ. Similarly, we take $H_B(\chi)$ to be K with G acting via χ (and so the action of F_∞ is given by $\chi(-1)$). The de Rham realisation is then $H_{DR}(\chi) = (H_B(\chi) \otimes \mathbf{Q}^a)^G$, with the trivial filtration $F^0 H_{DR}(\chi) = H_{DR}(\chi)$. By the twist $M(\chi)$, we mean the motive over $\mathbf{Q}$, with coefficients in K, whose realisations are the tensor products of the realisations of M (with coefficients extended to K) with the realisations of $[\chi]$.

4. Critical Points. No approach to the construction of the p-adic analogue of L(M,s) via local data is known, and so we are forced to define this p-adic analogue using interpolation of special values of the complex L-function. For this to make sense, the relevant special values must be essentially algebraic numbers, and this leads us to the notion of critical points and the period conjecture (see Deligne [10]). It also places an important restriction on our motive M, namely we can only consider those M which admit at least one critical point. Our aim in this section is to briefly recall a modified form of Deligne's period conjecture, which is the same as that given in [4] up to a power of $i = \sqrt{-1}$, and which seems essential for the p-adic theory.

Recall that an integer $s = n$ is said to be critical for M if both the Euler factors at infinity $L_\infty(M,s)$ and $L_\infty(M\hat{}(1),2-s)$ are holomorphic at $s = n$. There are various equivalent forms of this definition (due to Bloch, Deligne, Scholl, ...). Let $H_B(M)^+$ denote the subspace of $H_B(M)$ which is fixed by F_∞. Recall that we assume that F_∞ acts on $H^{k,k}$ via a scalar.

Lemma 5. The following three assertions are equivalent for M :- (i). M is critical at s = 0; (ii). If j < k and h(j,k) ≠ 0, then j < 0 and k ≥ 0, and, in addition, F_∞ acts on $H^{k,k}$ by +1 if k < 0 and by -1 if k ≥ 0. (iii). The map

$$h_\infty : H_B(M)^+ \otimes \mathbf{R} \rightarrow (H_{DR}(M)/F^0 H_{DR}(M)) \otimes \mathbf{R} \qquad (24),$$

induced by (17), is an isomorphism.

Henceforth, we shall assume the following (which, in turn, implies the hypothesis imposed in §3) :-

Hypothesis. The point s = 0 is critical for M.

Note also that our normalization here is different from that in [4], where s = 1 was taken to be the fixed critical point. Following [10], we view the motive M as varying, and write

$$\Lambda(M) = \Lambda(M,0)\ ,\ L(M) = L(M,0)\ ,\ L_\infty(M) = L_\infty(M,0)\ ,\ \varepsilon(M) = \varepsilon(M,0) \text{ etc.}$$

We now define the modified Euler factor at infinity, which we denote by $P_{\infty,\iota}(M)$, and which will depend on the choice of $\iota = +i$ or $-i$. In parallel with (19), we put

$$P_{\infty,\iota}(M) = \prod P_{\infty,\iota}(U) \qquad (25),$$

where U runs over the direct summands of $H_B(M) \otimes \mathbf{C}$ as specified after (19), and where $P_{\infty,\iota}(U)$ is given by :-

(a). If $U = H^{j,k} \oplus H^{k,j}$ with j<k, then $P_{\infty,\iota}(U) = \iota^{jh(j,k)}\, L_\infty(U)$;
(b). If $U = H^{k,k}$ with k≥0, then $P_{\infty,\iota}(U) = 1$;
(c). If $U = H^{k,k}$ with k<0, then $P_{\infty,\iota}(U) = L_\infty(U)/(\varepsilon_\infty(U,\eta^{(\iota)})\, L_\infty(U\text{^}(1)))$.

In case (a), we have $\varepsilon_\infty(U,\eta^{(\iota)}) = \iota^{(k-j+1)h(j,k)}$. Note also that case (b) holds for U if and only if case (c) holds for U^(1). It is therefore clear that, if we define the modified L-function

$$\Lambda_{(\infty),\iota}(M) = P_{\infty,\iota}(M)\ L(M) \qquad (26),$$

then it satisfies the functional equation

$$\Lambda_{(\infty),\iota}(M) = (\prod_{(v\neq\infty)} \varepsilon_v(M,\eta^{(\iota)})).\ \Lambda_{(\infty),-\iota}(M^\wedge(1)) \qquad (27).$$

If x ,y are complex numbers, we write $x \sim y$ if there exists a non-zero rational number u such that $x = uy$. The following lemma (see [5]) is a strengthening of Lemma 2.4 of [4]. Let $d^+(M)$ denote the $\mathbf{Q}$ - dimension of $H_B(M)^+$. Recall that we assume M is critical at $s = 0$.

Lemma 6. Let χ be a Dirichlet character, and let n be an integer such that (9) holds and $M(n)(\chi)$ is also critical at $s = 0$. Then

$$P_{\infty,\iota}(M(n)(\chi)) \sim (2\pi i)^{-nd^+(M)} P_{\infty,\iota}(M).$$

We can now give an equivalent form of Deligne's period conjecture in [10], which seems better suited for questions of p-adic interpolation. Let $c^+(M)$ be the period defined in [10]. Equivalently, $c^+(M)$ is the determinant of the isomorphism (24), computed with respect to $\mathbf{Q}$ - bases of $H_B(M)^+$ and $H_{DR}(M)/F^0H_{DR}(M)$. Thus $c^+(M)$ is only determined up to multiplication by a non-zero rational number. Now the arguments used to prove Lemma 6 show that

$$P_{\infty,\iota}(M) \sim (2\pi\,\iota)^{r(M)}\ ,\ \text{where } r(M) = \Sigma_{(j<0)}\, jh(j,k) \qquad (28).$$

Having made a choice of $c^+(M)$, we define the modified period

$$\Omega_\iota(M) = c^+(M)(2\pi\,\iota)^{r(M)} \qquad (29).$$

For the Dirichlet character χ, we define the Gauss sum

$$G_\iota(\chi) = \Sigma\, \chi(x) \exp(-2\pi\,\iota\, x/c(\chi)) \qquad (30),$$

where x runs over a complete set of representatives of the relatively prime residue classes modulo the conductor $c(\chi)$ of χ. It is not difficult to prove that the quantity

$$\Lambda_{(\infty),\iota}\,(M(n)(\chi))/(\Omega_\iota(M)G_\iota(\chi^{-1})^{d^+(M)}) \qquad (31)$$

is independent of the choice of $\iota = i$ or $-i$.

Period Conjecture. Let χ be a Dirichlet character, whose conductor is prime to the conductor of M, and let n be an integer such that (9) holds, and $M(n)(\chi)$ is critical at $s = 0$. Then the expression (31) belongs to $\mathbf{Q}^a$. Moreover, the effect of an automorphism σ in G on (31) is to replace χ by χ^σ.

Using Lemma 6 and (28), one sees that this conjecture is equivalent to the basic periond conjecture of [10]. The interest of the new version is that it gives a natural variation of the period as n and χ vary.

Example 3. Conjecture A and the Period Conjecture are known for motives attached to primitive cusp forms of congruence subgroups of $SL_2(\mathbf{Z})$ (Mordell, Hecke, Manin, Shimura, Deligne, ...). For simplicity, we only discuss the case of the unique normalized cusp form

$$\Delta(z) = q\prod_{(n\geq 1)}(1-q^n)^{24} = \Sigma_{(n\geq 1)}\,\tau(n)\,q^n \qquad (q = \exp(2\pi i z)),$$

of weight 12 for $SL_2(\mathbf{Z})$. This cusp form determines a motive over $\mathbf{Q}$, which we again denote by Δ, of weight 11 and dimension 2. For this motive, we have $h(0,11) = h(11,0) = 1$, and, for each prime l, $H_l(\Delta)$ is the l-adic representation attached to Δ by Deligne. Now, for all Dirichlet characters χ,

$$L(\Delta(\chi),s) = \Sigma_{(n\geq 1)}\,\chi^{-1}(n)\tau(n)/n^s\,,\quad \Lambda(\Delta(\chi),s) = \Gamma_{\mathbf{C}}(s)L(\Delta(\chi),s).$$

Since $\Delta(\chi)^\wedge = \Delta(11)(\chi^{-1})$, it follows that s=1,...,11 are the critical points for $\Delta(\chi)$. Put $M = \Delta(1)$, so that M is critical at $s = 0$. Hence $M(n)(\chi)$ will be critical at $s = 0$ and (9) will hold when either (i) n = 0,2,...,10 and $\chi(-1) = 1$, or (ii) n = 1,3,...,9 and $\chi(-1) = -1$. We assume that either (i) or (ii) is valid. It is known (see §7 of [10]) that we can take $c^+(M) = L(\Delta,1)$. Since $r(M) = -1$, it follows that $\Omega_\iota(M) = L(\Delta,1)(2\pi\,\iota)^{-1}$. Applying case (a) of the rule for modifying the Euler factor at

infinity, we obtain $P_{\infty,\iota}(M(n)(\chi)) = (2\pi\,\iota)^{-1-n}$. Since $d^+(M) = 1$, it follows that the expression (31) is, in this case, equal to

$$\Lambda(\Delta(\chi)\,,\,n+1)/(\Lambda(\Delta\,,\,1)G_\iota(\chi^{-1})\,\iota^n) \qquad (32).$$

It is known (see [20]) that (32) satisfies the assertion of the Period Conjecture. If χ is the trivial character, and n = 2 or 4, the following numerical values for (32) are calculated in [20] :-

$$-691/(2^2.3^4.5) \quad (n=2)\;; \quad 691/(2^3.3^2.5.7) \quad (n=4)\;.$$

Example 4. Let E be an elliptic curve over $\mathbf{Q}$, and consider the motive $N = \mathrm{Sym}^2(E)$, which is of dimension 3 and weight 2. By the Weil pairing, we have $N^\wedge = N(2)$. Also, $L_\infty(N,s) = \Gamma_{\mathbf{R}}(s)\Gamma_{\mathbf{C}}(s)$, since $h(0,2) = h(1,1) = h(2,0) = 1$, and F_∞ acts on $H^{1,1}$ by +1. Hence s = 1 and s = 2 are the critical points for N. Put $M = N(1)$, so that M is critical at s = 0. A simple calculation in linear algebra (see §7 of [10]) shows that $c^+(M) = u(\mathrm{Sym}^2(E))$, where this latter quantity is given by (6). Assume now that E is modular. Conjecture A is known to be true for M twisted by any Dirichlet character χ (Rankin, Shimura, Jacquet, Gelbart, ...). Now $M(n)(\chi)$ will be critical at s = 0 and (9) will hold only when n = 0 and $\chi(-1) = 1$. Assuming we are in this case, a simple calculation shows that the expression (31) is equal to

$$L(\mathrm{Sym}^2(E)(\chi)\,,\,1)/(u(\mathrm{Sym}^2(E))\,G_\iota(\chi^{-1}))\;.$$

The Period Conjecture then holds for this expression, and is due essentially to Sturm [32], [33].

5. Modification of the Euler factor at p. It is essential for the p-adic theory that we carry out a modification of the Euler factor at p similar to that carried out on the Euler factor at ∞. Unlike the situation at the ∞ factor, there is no need to assume that M is critical at s = 0 to define this modification. Let G_p be the local Galois group of $\mathbf{Q}_p{}^a$ over $\mathbf{Q}_p$, and write I_p for its inertial subgroup. Let W_p (resp. W_p') be the Weil group (resp. the Weil - Deligne group) of $\mathbf{Q}_p$. For each prime l, let $\tau_l : G_p \to \mathrm{Aut}\,(H_l(M))$ be the homomorphism giving the action of the local Galois group on the l-adic

realisation of M. We impose the following condition on p for the rest of this section.

Hypothesis on p. M has potential good reduction at p, in the sense that, for each prime $l \neq p$, $\tau_l(I_p)$ is a finite group.

If $l \neq p$, this implies that the nilpotent matrix N attached to τ_l by Grothendieck is, in fact, the zero matrix $N = 0$, and the associated representation of the Weil - Deligne group is given by the pair $(\tau_l , 0)$ (see [9], §8). Let Φ denote any element of G_p , which maps to $Frob_p^{-1}$ in G_p/I_p . We fix a prime $l \neq p$.

One further technical remark is needed to deal with problems of non-semi-simplicity. It is necessary to replace our representation of W_p' on $H_l(M)$ by its Φ - semi-simplification (see [9], §8.5). We assume from now on that this has been done, and abuse notation by again writing $(\tau_l , 0)$ for the Φ - semi-simplified representation (this is harmless, we can equally well use the Φ - semi-simplification to compute the local Euler factor and ε -factor at p). Now fix an embedding of $\mathbf{Q}_l$ in the complex field $\mathbf{C}$. Then $H_l(M) \otimes \mathbf{C}$ is a semi-simple complex representation of W_p , and so breaks up as a direct sum $H_l(M) \otimes \mathbf{C} = \oplus\ U$, where U ranges over a finite set of irreducible representations of W_p . Hence, putting $L_p(U,s) = \det(1 - \tau_l(\Phi).\, p^{-s} \mid U^{I_p})^{-1}$, we have

$$L_p(M,s) = \prod L_p(U,s) , \quad \varepsilon_p(M,\eta^{(\iota)}) = \prod \varepsilon_p(U,\eta^{(\iota)}) ,$$

where both products are taken over all U. Let us also assume that the coefficients of the polynomial

$$Z_p(M,X) = \det(1 - \tau_l(\Phi).X \mid H_l(M)) \tag{33}$$

are algebraic numbers. Let ord_p denote the order valuation of $\mathbf{C}_p$, normalized so that $ord_p(p) = 1$. Fixing U, we claim that $ord_p(\alpha)$ is constant as α ranges over the inverse roots of the polynomial $\det(1 - \tau_l(\Phi).X \mid U)$. This is because U, being a simple complex representation of W_p , can be twisted by a quasi-character, trivial on I_p , so as to become a representation whose image is a finite group. We define $ord_p(U)$ to be $ord_p(\alpha)$ for any such inverse root α.

This is also independent of the choice of Φ because of the above hypothesis on p. Finally, for simplicity, we assume for the rest of this section that $ord_p(\alpha)$ is in **Z** for all roots α of (33).

As always, let ι = i or -i. In parallel with (25), we put

$$P_{p,\iota}(M) = \prod P_{p,\iota}(U) \qquad (34),$$

where U runs over the simple factors of $H_l(U)\otimes\mathbf{C}$ as above, and where :-

(a). If $ord_p(U) \geq 0$, then $P_{p,\iota}(U) = 1$;
(b). If $ord_p(U) < 0$, then $P_{p,\iota}(U) = L_p(U)/(\varepsilon_p(U,\eta^{(\iota)})\, L_p(U\hat{}(1)))$.

Note that $P_{p,\iota}(U)$ is always well defined, i. e. in case (b), $L_p(U,s)$ cannot have a pole at s = 0 because $ord_p(U) < 0$. In addition, it is plain that case (a) holds for U if and only if case (b) holds for U^(1), because of our assumption that $ord_p(U)$ is in **Z**. Thus, if we define the modified L-function

$$\Lambda_{(\infty,p),\iota}(M) = P_{\infty,\iota}(M)\, P_{p,\iota}(M).\ \Lambda(M)/(L_\infty(M)\, L_p(M)) \qquad (35),$$

it is clear from our construction of the modified Euler factors that it satisfies the functional equation

$$\Lambda_{(\infty,p),\iota}(M) = (\prod_{(v\neq\infty,p)} \varepsilon_v(M,\eta^{(\iota)}))\ .\ \Lambda_{(\infty,p),-\iota}(M\hat{}(1)) \qquad (36).$$

We say that M has good reduction at p if $\tau_l(I_p) = 1$ for all primes $l \neq p$. Let $d_p(M)$ denote the number of inverse roots α of the polynomial (33), counted with multiplicity, such that $ord_p(\alpha) < 0$. The following lemma gives an explicit calculation of the modified Euler factors at p, in the case of most interest to us.

Lemma 7. Suppose that M has good reduction at p. Let β (resp. α) run over all inverse roots, counted with multiplicity, of $Z_p(M,X)$ such that $ord_p(\beta) \geq 0$ (resp. $ord_p(\alpha) < 0$). Then, we have

$$R_{p,\iota}(M)/L_p(M) = \prod_{(\beta)}(1 - \beta)\ .\ \prod_{(\alpha)}(1 - 1/(p\alpha))\ .$$

Moreover, if χ is a non-trivial character of p-power conductor, say $c(\chi) = p^g$, we have

$$R_{p,\iota}(M(\chi))/L_p(M(\chi)) = G_\iota(\chi^{-1})^{-d_p^{(M)}} \cdot (\prod_{(\alpha)} \alpha)^{-g} ,$$

where $G_\iota(\chi^{-1})$ is given by (30).

6. p-adic L-functions. Let M be a motive, which is critical at $s = 0$, and which satisfies the Period Conjecture. Let p be a prime where M has potential good reduction. Write $\Theta(p)$ for the group of all Dirichlet characters of p-power conductor. As χ ranges over $\Theta(p)$ and n ranges over integers satisfying (9), the values

$$\Lambda_{(\infty,p),\iota}(M(n)(\chi))/\Omega_\iota(M) \qquad (37)$$

are algebraic numbers, and hence can be viewed as lying in $\mathbf{C}_p$ via our fixed embedding. Our aim is to seek a continuous p-adic interpolation of these numbers as n and χ vary. While it is very likely that such an interpolation exists for all such p, our knowledge of the general case is still very fragmentary, and we shall henceforth restrict our attention to those primes p, which are ordinary for M (see [1]). Put $V = H_p(M)$. We say that p is ordinary for M if (i) M has good reduction at p, and (ii) there exists a decreasing filtration F^mV of V (with $F^m V = V$ (resp. 0) for m sufficiently small (resp. large)), which is stable under the action of the local Galois group G_p, and which is such that the inertia group I_p operates on $F^mV/F^{m+1}V$ via ψ^m, for all m in $\mathbf{Z}$; here ψ is the cyclotomic character (8). We shall require two further properties of an ordinary prime, which we shall impose as axioms, but which we understand have been proven in many cases. These are that, for each m in $\mathbf{Z}$, we have (iii) the m-th p-adic Hodge-Tate number of V (or equivalently the $\mathbf{Q}_p$ - dimension of $F^mV/F^{m+1}V$) is equal to the complex Hodge number h(-m, w(M)+m), and (iv) the number, counted with multiplicity, of inverse roots α of the polynomial $Z_p(M,X)$, given by (33), with $\mathrm{ord}_p(\alpha) = -m$ is equal to the complex Hodge number h(-m, w(M)+m). When M is of the form $H^k(X)(n)$, for a smooth projective variety X over $\mathbf{Q}$, (iii) has been proven by

Faltings [12], and (iv) has been established in many cases by Fontaine - Messing [14].

Lemma 8. Let α run over the inverse roots of $Z_p(M,X)$. Then (a). The number $d_p(M)$ of α with $ord_p(\alpha) < 0$ is equal to $d^+(M)$; (b). For each α, we have $ord_p(\alpha) < 0$ if and only if $ord_p(\alpha) < n$, where n is any integer such that there exists a Dirichlet character χ, satisfying (9), with $M(n)(\chi)$ critical at $s = 0$.

By Lemma 5, $d^+(M) = \Sigma_{(j<0)}\, h(j,k)$, and so (a) is plain from property (iv) above. Part (b) follows on applying Lemma 5 to the motives M and $M(n)(\chi)$. An important cosequence of Lemmas 7 and 8, and the fact that (31) is independent of the choice of ι, is that the expression (37) is also independent of the choice of ι.

We can at last state the p-adic analogue of Conjecture A. As before, let e(M) denote the order of the pole of the complex L- function L(M,s) at $s = 1+w(M)/2$. As remarked earlier, it is conjectured in the complex theory that (i) if w(M) is odd, then $e(M) = 0$, and (ii) if w(M) is even, then e(M) is the maximal number of copies of $\mathbf{Q}(-w(M)/2)$ which are direct summands of M. When combined with the hypothesis that M is critical at $s = 0$, we conclude from these conjectures that, if $e(M) > 0$, we must have (a) w(M) even and non-zero, and (b) $w(M)/2$ even (resp. odd) when $w(M) < 0$ (resp. $w(M) > 0$). When $e(M) > 0$, we assume (a) and (b) in what follows. As in (7), let D denote the Galois group of $\mathbf{Q}(\mu_{p^\infty})^+$ over $\mathbf{Q}$. Let ψ denote the cyclotomic character of H, as in (8). Recall that our two basic assumptions are that M is critical for $s = 0$, and that p is ordinary for M.

Conjecture A (p - adic Version). For each choice of the period $c^+(M)$, there exists a unique pseudo - measure $\mu(c^+(M))$ on D as follows. For all n in Z and all Dirichlet characters χ of p-power conductor such that (9) holds and $M(n)(\chi)$ is critical at $s = 0$, we have

$$\int_D \chi\psi^n \, d\mu(c^+(M)) \;=\; \Lambda_{(\infty,p),\iota}(M(n)(\chi))/\,\Omega_\iota(M) \qquad (38).$$

If $e(M) = 0$, $\mu(c^+(M))$ is a measure. If $e(M) > 0$, we put $k = w(M)/2$, and have

(i). $(\psi^k(\sigma) - \sigma)^{e(M)}\ \mu(c^+(M))$ is a measure, for all $\sigma \in D$, when $w(M) < 0$;
(ii). $(\psi^{1+k}(\sigma) - \sigma)^{e(M)}\ \mu(c^+(M))$ is a measure, for all $\sigma \in D$, when $w(M) > 0$.

The pseudo-measure $\mu(c^+(M))$ satisfies a simple p-adic analogue of the functional equation (21) of the complex L- function. The involution $\sigma \to \sigma^{-1}$ induces an involution of the ring of quotients of the Iwasawa algebra I of D, which we denote by $\mu \to \mu^*$. Also, if μ is a pseudo-measure and ρ is in I, the product $\mu.\rho$ in the ring of quotients of I is clearly again a pseudo measure. Now the conductor of M is an integral ideal of Z, which is prime to M, and we write $\sigma(M)$ for its Artin symbol in D. Put

$$\gamma(M) = \Omega_\iota(M)\ \varepsilon(M)/(\Omega_{-\iota}(M\text{^}(1))\ \varepsilon_\infty(M, \eta^{(\iota)})).$$

The arguments of [10], §5 show that $\gamma(M)$ is a rational number, which is independent of the choice of $\iota = i$ or $-i$. The following is now an immediate consequence of (36), and the fact that, for $v \neq p, \infty$ and χ of p-power conductor, we have $\varepsilon_v(M(n)(\chi), \eta^{(\iota)}) = \varepsilon_v(M, \eta^{(\iota)})\ v^{\,na(v)}\ \chi^{-1}(v^{a(v)})$, where a(v) denotes the power of v occurring in the conductor of M.

p-adic functional equation. We have

$$\mu(c^+(M)) = \gamma(M)\ (\mu(c^+(M\text{^}(1)))^*.\ \sigma(M)^*) \qquad (39),$$

where $\sigma(M)$ is the Artin symbol in D of the conductor of M.

Example 5. Take $M = \mathbf{Q}(m)$, so that $w(M) = -2m$. Then M will be critical at s=0 if and only if either (a) m is odd and < 0, or (b) m is even and > 0. Suppose first we are in case (a). We can take $c^+(M) = 1$, whence $\Omega_\iota(M) = 1$. Also $w(M) > 0$, and if (9) holds and $M(n)(\chi)$ is critical at $s = 0$, then $w(M(n)(\chi)) \geq 0$. One verifies easily that the right hand sides of (10) and (38) are then equal, so that $\mu(c^+(M)) = \rho_m$ in this case. Suppose next that we are in case (b). We can take $c^+(M) = (2\pi i)^m$, whence $\Omega_\iota(M) = 1$. Also $w(M) < 0$, and if (9) holds and $M(n)(\chi)$ is critical at s=0, then $w(M(n)(\chi)) < 0$. Applying (36) to $M(n)(\chi)$, we deduce

easily that $\mu(c^+(M)) = \rho_{1-m}^*$. Note also that the functional equation (39) is simply $\mu(c^+(M)) = \mu(c^+(M^\wedge(1))^*$, in both cases.

Example 6. Conjecture A (p-adic version) holds for motives attached to primitive cusp forms of congruence subgroups of $SL_2(\mathbf{Z})$ (see [20], [21], [23], [24]). As in Example 3, we only discuss here the special case of $M = \Delta(1)$. Let α_1 , α_2 denote the roots of the polynomial $1 - \tau(p)X + p^{11}X^2$. It is known that p is ordinary for M if and only if $\tau(p)$ is prime to p, or equivalently one of these roots is a p-adic unit. Suppose p is ordinary for M, and let α_1 be the unit root. Take $c^+(M) = L(\Delta,1)$. Applying Lemma 7, we see that, in this case, the right hand side of (38) is given explicitly by

$$\Lambda(\Delta(\chi) , n+1)/(\Lambda(\Delta , 1)\, G_\iota(\chi^{-1})\, \iota^n)\, (\alpha_1\, p^{-n-1})^{-g}\, (1 - \alpha_1\chi^{-1}(p)p^{-n-1})(1 - \alpha_2\chi(p)p^{n-11}),$$

where $c(\chi) = p^g$. The p-adic functional equation for M is particularly interesting (as was pointed out to me by Greenberg). We have $M^\wedge = M(9)$. It is therefore naturel (see [10], §5) to take $c^+(M^\wedge(1)) = c^+(M)(2\pi i)^{10}$, whence $\Omega_\iota(M^\wedge(1)) = c^+(M)(2\pi\,\iota)^{-1} = \Omega_\iota(M)$. As $\varepsilon_\infty(M,\eta^{(\iota)}) = 1$, we conclude that $\gamma(M) = -1$, and so the p-adic functional equation becomes

$$\mu(c^+(M)) = -\,\mu(c^+(M^\wedge(1))^* \qquad (40).$$

In particular, it follows from (38), by integrating ψ^k (k=0,2,...,10) against both sides of (40), that

$$\int_D \psi^k\, d\mu(c^+(M)) = -\int_D \psi^{10-k}\, d\mu(c^+(M)) \ .$$

Example 7. Let E be a modular elliptic curve over $\mathbf{Q}$, and, as in Example 4, take $M = Sym^2(E)(1)$. Let p be a prime where E has good ordinary reduction. Then p is an ordinary prime for M, and the p-adic version of Conjecture A has been proven by Schmidt [29] (see also Hida [37]), except for the delicate case of formula (38) when χ is the character of a real quadratic field. Take $c^+(M) = u(Sym^2(E))$,given by (6), so that $\Omega_\iota(M) = c^+(M)(2\pi\,\iota)^{-1}$. Recall that (9) holds and $M(n)(\chi)$ is critical at s=0 only when n=0 and $\chi(-1)=1$. Suppose the p-Euler factor of E is $L_p(E,s) = (1 - up^{-s})(1 - vp^{-s})^{-1}$, where say u is a p-adic unit, because

E has good ordinary reduction at p. Then the inverse roots of the polynomial (33) are given by $\alpha_1 = u^2/p$, $\alpha_2 = 1$, $\alpha_3 = v^2/p$. Thus, when χ is the trivial character, Lemma 7 shows that the right hand side of (38) is 0. This is a simple example of a so called trivial zero of the p-adic L-function, which is of great importance in Iwasawa theory. Suppose now that χ is not the trivial character. A simple calculation, using Lemma 7, shows that the right hand side of (38) is given explicitly by

$$L(\mathrm{Sym}^2(E)(\chi), 1)\, u(\mathrm{Sym}^2(E))^{-1}\, G_\iota(\chi^{-1})^{-1}\, (v^2/p)^{-g},$$

where $c(\chi) = p^g$. Finally, we note that the p-adic functional equation has a very simple form in this case. By the Weil pairing, we have $M^\wedge = M$, and simple arguments of linear algebra show that we can take $c^+(M^\wedge(1)) = u(\mathrm{Sym}^2(E))(2\pi i)^2$. Since $r(M^\wedge(1)) = -3$, it follows that $\Omega_\iota(M^\wedge(1)) = \Omega_\iota(M)$. Also, we have $\varepsilon(M) = \varepsilon_\infty(M, \eta^{(\iota)}) = 1$. Thus we obtain $\gamma(M) = -1$, and so the functional equation is

$$\mu(c^+(M)) = -\,\mu(c^+(M^\wedge(1)))^*.\ \sigma(M)^* \qquad (41).$$

7. Concluding Remarks. (a). It is of considerable interest to generalize the p-adic version of Conjecture A to motives defined over an arbitrary finite extension F of $\mathbf{Q}$. The Galois group D will then have to be replaced by the Galois group D(F) of the maximal abelian extension of F, which is unramified outside the primes of F above p. By class field theory, the structure of D(F) as an abelian group is given by $B \times \mathbf{Z}_p^k$, where B is a finite group and $k \geq 1+r_2$, with r_2 equal to the number of pairs of complex conjugate embeddings of F ($k = 1+r_2$ if and only if the global units of F are p-adically independent). Some special cases are already known (see [2], [11], [31], [18], [22], [35]). (b). While we have stressed the p-adic analogues of the complex L-functions of motives, much interesting work has also been done on the p-adic analogues of the complex L-functions attached to automorphic forms (see [16], [26], [36], [37]). (c). For further interesting results on the analogy between complex and p-adic L-functions, see [6], [7], [8], [27].

Acknowledgements. I am greatly indebted to B. Perrin-Riou and P. Deligne for their help in the formulation of the p-adic conjectures in this seminar.

These conjectures are basically taken from my joint paper [4] with B. Perrin-Riou. However, in a letter to me Deligne pointed out that there is a much more elegant and succinct way of expressing our conjectures using the local ε-factors of the motive. His remark also made it clear that, in some cases, the conjectures of [4] should be modified by a suitable power of $i = \sqrt{-1}$, which depends on the ε-factor at ∞. I have now revised an earlier version of this seminar so as to take Deligne's remarks into account.

References.

1. Bloch,S., Kato,K., p-adic étale cohomology, Publ. Math. I.H.E.S. No. 63 (1986),107-152.
2. Cassou-Nogues,P.,Valeurs aux entiers negatifs des fonctions zêta et fonctions zêta p-adiques, Invent. Math. 51 (1979),29-59.
3. Coates,J., Flach,M.,The symmetric square of an elliptic curve, to appear.
4. Coates,J., Perrin-Riou,B., On p-adic L-functions attached to motives over **Q**, Advanced Studies in Pure Math. 17 (1989), 23-54.
5. Coates,J., On the main conjectures of Iwasawa theory, to appear in Proceedings of 1989 Durham Symposium on L-functions in Arithmetic.
6. Coleman,R., Dilogarithms, regulators, and p-adic L-functions, Invent. Math. 69 (1982), 171-208.
7. Coleman,R., de Shalit,E., p-adic regulators on curves and special values of p-adic L-functions, Invent. Math. 93 (1988), 239-266.
8. Colmez,P., Résidu en s=1 des fonctions zêta p-adiques, Invent. Math. 91 (1988), 371-389.
9. Deligne,P., Les constantes des équations fonctionelles des fonctions L, Antwerp II,Springer L.N. 349 (1973), 501-595.
10. Deligne,P.,Valeurs de fonctions L et périodes d'intégrales, Proc. Symp. Pure Math. A.M.S. 33 (1979), Vol. 2, 313-346.
11. Deligne,P., Ribet, K., Values of abelian L-functions at negative integers over totally real fields, Invent. Math. 59 (1980), 227-286.
12. Faltings,G., p-adic Hodge theory, Journal A.M.S. 1 (1988), 255-299.
13. Ferrero,B., Greenberg,R., On the behaviour of p-adic L-functions at s=0, Invent. Math. 50 (1978), 91-102.

14. Fontaine,J-M., Messing,W., p-adic periods and p-adic etale cohomology, Contemp. Math. A.M.S. 67 (1987), 179-207.
15. Gelbart,S., Jacquet,H., A relation between automorphic representations of GL(2) and GL(3), Ann. Sc. E.N.S. 11 (1978), 471-542.
16. Haran,S., p-adic L-functions for modular forms, Compositio Math. 62 (1987), 31-46.
17. Iwasawa,K., On p-adic L-functions, Ann. of Math. 89 (1969), 198-205.
18. Katz,N., p-adic interpolation of real analytic Eisenstein series, Ann. of Math. 104 (1976), 459-571.
19. Kubota,T., Leopoldt,H., Eine p-adische theorie der zetawerte, Crelle 214/215 (1964), 328-339.
20. Manin,J., Periods of parabolic forms and p-adic Hecke series, Math. Sbornik A.M.S. 21 (1973), 371-393.
21. Manin,J.,Values of p-adic Hecke series at integer points of the critical strip, Math. Sbornik A.M.S. 22 (1974), 631-637.
22. Manin,J.,Vishik,M., p-adic Hecke series of imaginary quadratic fields, Math. Sbornik A.M.S. 24 (1974), 345-371.
23. Mazur,B., Swinnerton-Dyer,P., Arithmetic of Weil curves, Invent. Math. 18 (1972), 183-266.
24. Mazur,B.,Tate,J., Teitelbaum,J., On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Invent. Math. 84 (1986), 1-48.
25. Mazur,B., Wiles,A., Class fields of abelian extensions of $\mathbf{Q}$, Invent. Math. 76 (1984), 179-330.
26. Panciskin,A., Non-archimedean automorphic L-functions (in Russian), Moscow University (1988).
27. Perrin-Riou,B., Points de Heegner et dérivées de fonctions L p-adiques, Invent. Math. 89 (1987), 455-510.
28. Rubin,K., Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication, Invent. Math. 89 (1987), 527-560.
29. Schmidt,C-G., p-adic measures attached to automorphic representations of GL(3), Invent. Math. 92 (1988), 597-631.
30. Serre,J-P., Facteurs locaux des fonctions zêta des variétés algébriques, Oeuvres, Vol.2, 581-592.
31. Serre,J-P., Sur le résidu de la fonction zêta p-adique d'un corps de nombres, C.R.A.S. Paris 287 (1978), 183-188.

32. Sturm, J., Special; values of zeta functions and Eisenstein series of half integral weight, Amer. J. Math. 102 (1980), 219-240.
33. Sturm, J., Evaluation of the symmetric square at the near center point, to appear.
34. Wagstaff,S., The irregular primes to 125000, Math. Computation 32 (1978), 583-591.
35. Yager,R., p-adic measures on Galois groups, Invent. Math. 76 (1984), 331-343.
36. Hida,H,. A p-adic measure attached to the zeta functions associated with two elliptic modular forms I, Invent. Math. 79 (1985), 159-195.
37. Hida,H., p-adic L-functions for base change lifts of GL(2) to GL(3), to appear.

John COATES

D.P.M.M.S.
University of Cambridge
16 Mill Lane
GB-CAMBRIDGE CB2 1SB
(England)