Invent. math. 84, 1–48 (1986)

Inventiones mathematicae

On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer

B. Mazur, J. Tate, and J. Teitelbaum

Harvard University, Dept. of Mathematics, 1 Oxford Street, Cambridge, MA 02138, USA

The conjectures of Birch and Swinnerton-Dyer connect arithmetic invariants of an elliptic curve E over $\mathbf{Q}$ (or more generally of an abelian variety over a global field) with the order of zero and the leading coefficient of the Taylor expansion of its Hasse-Weil zeta function at the "central point". One of the arithmetic invariants entering into this conjecture is the "regulator of E", i.e., the discriminant of the quadratic form on $E(\mathbf{Q})$ defined by the "canonical height pairing".

If E is an elliptic curve over $\mathbf{Q}$ parametrized by modular functions (a *Weil curve*, cf. Chap. II, §7 below) then the p-adic analogue of its Hasse-Weil L-function has been defined, and recently p-adic theories analogous to the theory of canonical height have been developed. It seemed to us, then, to be an appropriate time to embark on the project of formulating a p-adic analogue of the conjecture of Birch and Swinnerton-Dyer, and gathering numerical data in its support. It also seemed, at the outset, that this would be a relatively routine project.

The project has proved to be anything but routine, and this article is an attempt to report on our findings so far.

The first curiosity one encounters is that a certain factor, which we call the "p-adic multiplier", enters into the formulation of the conjecture, this factor being the discrepancy between the p-adic and classical special values. The p-adic multiplier is a simple local term, having the appearance of an Euler factor. It is, however, not equal to any recognizable Euler factor nor does it appear to interpolate to a p-adic meromorphic function. Panciskin [P] (cf. also: [A]) has given the general form of the corresponding factor which occurs in a very broad class of p-adic interpolation problems. What conceptual significance, if any, this factor may have is a mystery. More puzzling, however, is the fact that the p-adic multiplier can vanish at the central point (it does so if and only if E has split multiplicative reduction at p) and thereby "throw off" the order of vanishing of the p-adic L-function at that point. When this happens, we say that we are in the "exceptional case". In this case other strange things happen as well: The sign of the p-adic functional equation is the *opposite* of the sign of the classical functional equation. We expect that in the exceptional case, the order of vanishing of the p-adic L-function is one greater than the order of vanishing of the classical L-function. Somewhat in harmony with this phenomenon is the fact that when E has split multiplicative reduction at p, one can define quite naturally a finitely generated group which we call the "extended Mordell-Weil group", the rank of which is one more than the rank of the Mordell-Weil group, and one can define a p-adic height pairing on this extended Mordell-Weil group.

We formulate a p-adic analogue of the conjecture of Birch and Swinnerton-Dyer which, in the exceptional case, involves the "regulator" of the extended Mordell-Weil group, computed via the "extended" height pairing. We collect a substantial amount of numerical evidence in support of this analogue in both cases, exceptional and non-exceptional. A novelty of the "exceptional" conjecture is that it is an assertion which goes beyond the "classical" conjecture of Birch and Swinnerton-Dyer even when the Mordell-Weil group is finite. Indeed, in that case, using the classical Birch and Swinnerton-Dyer conjecture together with the "exceptional" conjecture, one can produce an again conjectural relationship between the special value of the first derivative of the p-adic L-function of E and the "algebraic part" of the special value of the classical L-function of E. We conjecture that the former quantity is the product of the latter quantity and the factor

$$\mathscr{L}_p(E) = \log_p(q_p(E))/\mathrm{ord}_p(q_p(E)),$$

where $q_p(E) \in \mathbf{Q}_p$ is the p-adic multiplicative period of E, i.e., is the number $q \in \mathbf{Q}_p^*$ with $\mathrm{ord}_p q > 0$ such that E is the rigid analytic quotient of the multiplicative group by the infinite cyclic subgroup generated by q.

This is a surprising relationship, because both "main quantities" involved in the conjectured formula (i.e., the special value of the derivative of the p-adic L-function of E, and the "algebraic part" of the special value of the classical L-function of E) are computed by integrating along specific paths on the Riemann surface of E, the paths determined by the "modular parametrization" of E, while their conjectured ratio $\mathscr{L}_p(E)$ is a p-adic "period" determined by the p-adic analytic uniformization of $E_{/\mathbf{Q}}$. It is quite remarkable to see the p-adic digits of this p-adic period be "reproduced" in the print-out of a computing machine programmed to compute the ratio of the two "main quantities" described above, which are given as certain expressions involving modular symbols.

The type of conjectured relationship we have just described we call an "exceptional zero conjecture" and we formulate a quite general "exceptional zero conjecture" to cover all instances of exceptional zeroes of p-adic L-functions attached to newforms of weight 2. We also formulate an analogous conjecture for forms of even weight $k \geq 4$, but this analogous conjecture is weaker, for a reason to be explained presently. We collect numerical evidence supporting these conjectures for various newforms f (in weight 2, where f runs through a collection of quadratic twists of the cusp form parametrizing the elliptic curve $X_0(11)$, and for selected newforms f of weights 4 and 6). If f is a newform of weight k, level N and nebentypus character ε, then

$$L_p(f, \psi, s)$$

has an exceptional zero at the central point if and only if k is even, $p \| N$ (i.e., p divides N but p^2 does not), p does not divide the conductor of the primitive version of ε, and the Dirichlet character ψ has the "correct" value at p (i.e., $\psi(p)p^{k-2} = a_p$, the p-th Fourier coefficient of f).

In this case, when the weight k is equal to 2, the "exceptional zero conjecture" involves a factor $\mathscr{L}_p(f)$ which is a direct generalization of $\mathscr{L}_p(E)$ and can be defined via the rigid analytic p-adic uniformization of the abelian variety A_f attached to the newform f.

An examination of the quantity $\mathscr{L}_p(f)$ (which lies in $K_f \otimes \mathbf{Q}_p$, where K_f is the field generated by the Hecke eigenvalues of f) shows that it can be defined using even less: it is an invariant of the representation of $G_p = \mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ on the p-adic vector space

$$V_p(f) = T_p(A_f) \otimes \mathbf{Q}_p$$

which is a free $K_f \otimes \mathbf{Q}_p$ module of rank 2. This definition of $\mathscr{L}_p(f)$ rests partially on the fact that in the "exceptional case" the inertia subgroup of G_p acts on $V_p(f)$ through a Borel subgroup, when f is of weight 2.

What happens in the "exceptional case" when the weight of f is greater than two? At first we had expected that in this situation the action of the inertia subgroup I_p of G_p on $V_p(f)$ (the p-adic Deligne-(Kuga-Sato) representation attached to f) would factor through a Borel subgroup as it does in weight 2, and that we could define $\mathscr{L}_p(f)$ in terms of this representation. But this expectation was too optimistic, as we show by examples, and we are at a loss to give a local definition of a higher weight analogue of $\mathscr{L}_p(f)$.

Thus our "weaker" exceptional zero conjecture in higher weight is simply as follows. For f with an exceptional zero at the midpoint, *define* $\mathscr{L}_p(f)$ to be the value at that point of the ratio

$$\frac{\text{first derivative of } L_p(f)}{\text{algebraic part of classical value of } f},$$

assuming that the denominator does not vanish. Then we conjecture that $\mathscr{L}_p(f)$ is unchanged when f is twisted by a Dirichlet character ψ for which $\psi(p) = 1$. We have verified that this is so modulo reasonably high powers of p for several twists of two newforms, of weights 4 and 6.

Table of contents

Chapter I. Modular symbols, measures, and L-functions attached to modular forms of weight $k \geqq 2$

The object of the first part of this chapter is to review the work of Amice-Vélu and Vishik, [A–V] and [V], in which they obtain a p-adic Mellin transform of a modular form of weight $k \geqq 2$. Although their treatment does not include primes p dividing the level, it is easy to do so (provided an "allowable p-root" α exists; see below). We also obtain a functional equation in the more general case. Our special interest in the last part of this chapter is in the phenomenon of "exceptional zeroes", i.e., zeroes at integral points which seem to emerge from the p-adic interpolation process and have no counterpart in the classical L-function. We are particularly interested in such an exceptional zero when it occurs at the central point for the functional equation. This can happen only for primes p dividing the level.

When such an exceptional zero occurs (and the hypotheses of §18 hold so that, in particular, the "sign" of the functional equation makes sense) the sign of the p-adic functional equation is opposite to the sign of the classical functional equation. Consequently the parity of the order of vanishing at the central point is thrown off. In such a case, any p-adic analogue of the classical Birch-Swinnerton-Dyer conjecture will have a form departing somewhat from its classical prototype. Towards the end of this chapter we make some preliminary conjectures of "Birch-Swinnerton-Dyer type" concerning order of vanishing and the "nature" of the extra zeroes (see § 16, § 19).

Notation. Let $GL_2(\mathbf{R})^+$ be the subgroup of $GL_2(\mathbf{R})$ consisting of matrices with positive determinant. If $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is in $GL_2(\mathbf{R})^+$, set

$$\rho(A)=\frac{\det(A)^{1/2}}{cz+d}.$$

Recall that $GL_2(\mathbf{R})$ operates on the Riemann z-sphere via $A(z)=\dfrac{az+b}{cz+d}$, $A(\infty)=a/c$.

Fix an integer $k\geqq 2$. Let $\mathscr{C}(N,\varepsilon,k)$ denote the space of holomorphic cusp forms of weight k with character ε on $\Gamma_0(N)$. Here $N\geqq 1$ is an integer and ε is a (not necessarily primitive) Dirichlet character on $(\mathbf{Z}/N\mathbf{Z})^*$.

Let

$$\mathscr{C}_k=\sum_{N,\varepsilon}\mathscr{C}(N,\varepsilon,k)$$

denote the space of all cusp forms of weight k which are on $\Gamma_1(N)$ for some N.

Let

$$\mathscr{P}_k(\mathbf{C})=\mathbf{C}\oplus\mathbf{C}\cdot z\oplus\ldots\oplus\mathbf{C}\cdot z^{k-2}$$

denote the space of polynomials (in the variable z) of degree $\leqq k-2$, with coefficients in $\mathbf{C}$. More generally, $\mathscr{P}_k(R)$ will denote polynomials of degree $\leqq k-2$ with coefficients in a ring R.

Define actions of $GL_2(\mathbf{Q})^+$ on $\mathscr{C}_k$ and on $\mathscr{P}_k(\mathbf{C})$ by the formulae:

$$(f|A)(z):=\rho(A)^k\cdot f(A(z)) \qquad \text{for } f\in\mathscr{C}_k,$$
$$(P|A)(z):=\rho(A)^{2-k}\cdot P(A(z)) \qquad \text{for } P\in\mathscr{P}_k(\mathbf{C}).$$

§ 1. Modular integrals

Since $dz=\rho(A)^{-2}\cdot d(A(z))$ we have:

$$(f|A)(z)(P|A)(z)\,dz=f(A(z))\,P(A(z))\,d(A(z)). \tag{1.1}$$

Let $\mathbf{P}^1(\mathbf{Q})=\mathbf{Q}\cup\{\infty\}$ and define a map

$$\phi\colon\ \mathscr{C}_k\times\mathscr{P}_k(\mathbf{C})\times\mathbf{P}^1(\mathbf{Q})\to\mathbf{C}$$

by the formula

$$\phi(f,P,r)=2\pi i\int_\infty^r f(z)\,P(z)\,dz=\begin{cases}2\pi\int_0^\infty f(r+it)\,P(r+it)\,dt, & \text{if } r\in\mathbf{Q},\\ 0, & \text{if } r=\infty.\end{cases} \tag{1.2}$$

We adopt the convention that if one argument is to be kept constant in a discussion, it may be relegated to the position of subscript in our notation. Thus, $\phi(f, P, r) = \phi_f(P, r) = \phi_{f,P}(r)$.

Clearly,

(a) $\phi(f, P, r)$ is $\mathbf{C}$-bilinear in f, P for any $r \in \mathbf{P}^1(\mathbf{Q})$.

Also, integrating (1.1) from ∞ to r and using Cauchy's theorem in the triangle with vertices ∞, $A(\infty)$, $A(r)$ we get:

(b) $\phi(f \mid A, P \mid A, r) = \phi(f, P, A(r)) - \phi(f, P, A(\infty))$.

By a *modular integral* (of weight k with values in V) we shall mean a mapping

$$\Phi: \mathscr{C}_k \times \mathscr{P}_k(\mathbf{C}) \times \mathbf{P}^1(\mathbf{Q}) \to V,$$

where V is a complex vector space, and such that Φ satisfies axioms (a) and (b) above. Fix such a modular integral Φ. Axiom (b) applied to $A = \textit{identity}$ yields:

$$\Phi(f, P, \infty) = 0.$$

§ 2. The module of values

If ε is a complex Dirichlet character, let $\mathbf{Z}[\varepsilon] \subset \mathbf{C}$ denote the subring of $\mathbf{C}$ generated by the values of ε.

Let $A_j \in SL_2(\mathbf{Z})$ be coset representatives of $\Gamma_0(N)$ so that

$$SL_2(\mathbf{Z}) = \coprod_{j \in \mathscr{R}} \Gamma_0(N) \cdot A_j,$$

where $\mathscr{R}$ is a finite index set.

Fix $f \in \mathscr{C}_k$ and let $L_f \subset V$ denote the $\mathbf{Z}$-module generated by the image of $\mathscr{P}_k(\mathbf{Z}) \times \mathbf{P}^1(\mathbf{Q})$ under the mapping Φ_f.

Proposition. *The* $\mathbf{Z}$*-module* L_f *is the* $\mathbf{Z}[\varepsilon]$*-submodule of* V *generated by the elements:*

$$\Phi(f, z^i, A_j(\infty)) - \Phi(f, z^i, A_j(0)); \quad 0 \leqq i \leqq k-2; \quad j \in \mathscr{R}. \tag{1.3}$$

Proof. For $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$, put $\varepsilon(A) = \varepsilon(d)$. Then:

$$f \mid A = \varepsilon(A) \cdot f.$$

By axiom (a),

$$\varepsilon(A) \cdot \Phi(f, P, r) = \Phi(f, P \mid A^{-1}, A(r)) - \Phi(f, P \mid A^{-1}, A(\infty)),$$

so L_f is a $\mathbf{Z}[\varepsilon]$-module. Here we use that if $A \in SL_2(\mathbf{Z})$, then $P \mapsto P \mid A$ preserves the lattice $\mathscr{P}_k(\mathbf{Z}) \subseteq \mathscr{P}_k(\mathbf{C})$.

Now let $L_f^0 \subseteq L_f$ denote the $\mathbf{Z}[\varepsilon]$-submodule generated by the quantities (1.3). Let $a, m \in \mathbf{Z}$ with $m \geqq 0$ and a relatively prime to m. We shall show that

$$\Phi(f, P, a/m) \in L_f^0$$

by induction on m. If $m=0$, then $\Phi(f, P, a/m)=0$. Suppose $m>0$. Let m' be the integer such that $am'\equiv 1 \bmod m$ and $0 \leqq m' < m$. Put $a'=(am'-1)/m$ and $A=\begin{bmatrix} a & a' \\ m & m' \end{bmatrix} \in SL_2(\mathbf{Z})$. We have $A=B\cdot A_j$ for some $j\in\mathcal{R}$ and $B\in\Gamma_0(N)$. Then:

$$\begin{aligned}\Phi(f, P, a/m)-\Phi(f, P, a'/m') &= \Phi(f, P, A(\infty))-\Phi(f, P, A(0))\\ &= \Phi(f, P, BA_j(\infty))-\Phi(f, P, BA_j(0))\\ &= \varepsilon(B)\cdot[\Phi(f, P\,|\,B, A_j(\infty))-\Phi(f, P\,|\,B, A_j(0))].\end{aligned}$$

But this shows that $\Phi(f, P, a/m)$ is in L_f^0 since we may suppose that $\Phi(f, P, a'/m')$ is in L_f^0 by induction.

§ 3. Modular symbols

We now use our modular integral Φ to define a *modular symbol* λ. For $a, m\in\mathbf{Q}$, $m>0$, $f\in\mathscr{C}_{k'}$ and $P\in\mathscr{P}_k(\mathbf{C})$ we put

$$\lambda(f, P; a, m) := \Phi\left(f, P(mz+a), -\frac{a}{m}\right) \tag{i}$$

$$:= m^{\left(\frac{k}{2}\right)-1}\,\Phi\left(f, P\left|\begin{bmatrix} m & a \\ 0 & 1 \end{bmatrix}, -\frac{a}{m}\right.\right) \tag{ii}$$

$$:= m^{\left(\frac{k}{2}\right)-1}\,\Phi\left(f\left|\begin{bmatrix} 1 & -a \\ 0 & m \end{bmatrix}, P, 0\right.\right). \tag{iii}$$

The proof that (i)=(ii) comes from $\rho\left(\begin{bmatrix} m & a \\ 0 & 1 \end{bmatrix}\right)=m^{1/2}$ and the definition of the action $|A$ on $\mathscr{P}_k$. The proof that (ii)=(iii) comes from axiom (b) with $r=0$, $A=\begin{bmatrix} 1 & -a \\ 0 & m \end{bmatrix}$, and P replaced by $P\,|\,A^{-1}=P\left|\begin{bmatrix} m & a \\ 0 & 1 \end{bmatrix}\right.$.

Proposition. *The modular symbol $\lambda(f, P;\ a, m)$ is $\mathbf{C}$-bilinear in (f, P). For fixed $f, P\in\mathscr{P}_k(\mathbf{Z})$, and $a, m\in\mathbf{Z}$ the modular symbol $\lambda_f(P;\ a, m)=\lambda(f, P;\ a, m)$ takes values in L_f. For fixed f and P, $\lambda_{f,P}(a, m)=\lambda(f, P; a, m)$ depends only upon a modulo m.*

Proof. The $\mathbf{C}$-bilinearity of λ follows from $\mathbf{C}$-bilinearity of Φ. To see that $\lambda_f(P;\ a, m)$ takes values in L_f for $P\in\mathscr{P}_k(\mathbf{Z})$ and $a, m\in\mathbf{Z}$ use formula (i). The last assertion follows from

$$f\left|\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right.=f, \quad\text{and}\quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\cdot\begin{bmatrix} 1 & -a \\ 0 & m \end{bmatrix}=\begin{bmatrix} 1 & -a+m \\ 0 & m \end{bmatrix}.$$

Concerning "homogeneity" in a and m, we have:

$$\lambda_f(P(z);\ a, m)=\lambda_f(P(z/t);\ ta, tm) \tag{3.1}$$

as is clear from (i).

We also have the following "divisibility":
For $0 \leqq i \leqq k-2$, $a, m \in \mathbf{Z}$, $m>0$

$$\lambda(f, (z-a)^i;\, a, m) \in m^i \cdot L_f \tag{3.2}$$

as is clear from (i).

§ 4. Action of the Hecke operators

Let $f \in \mathscr{C}(N, \varepsilon, k)$. For *every* prime number l consider the operator

$$f \mapsto f \mid T_l := l^{(k/2)-1} \left(\sum_{u=0}^{l-1} f \,\middle|\, \begin{bmatrix} 1 & u \\ 0 & l \end{bmatrix} + \varepsilon(l) \cdot f \,\middle|\, \begin{bmatrix} l & 0 \\ 0 & 1 \end{bmatrix} \right). \tag{4.1}$$

When $l \nmid N$, then T_l is the usual Hecke operator; when $l \mid N$, $\varepsilon(l)=0$, and we have the formula for the operator U_l. Nevertheless we adopt this uniform notation. The operation T_l preserves $\mathscr{C}(N, \varepsilon, k)$ for every l.

Proposition. *For $f \in \mathscr{C}(N, \varepsilon, k)$ and for each prime number l we have the formula:*

$$\lambda(f \mid T_l, P;\, a, m) = \sum_{u=0}^{l-1} \lambda(f, P;\, a-um, lm) + \varepsilon(l) \cdot l^{k-2} \cdot \lambda(f, P;\, a, m/l). \tag{4.2}$$

Verification of this formula is straightforward using (iii) of § 3 and is left to the reader. It is also easy to check that

$$L_{f \mid T_l} \subseteq L_f, \tag{4.3}$$

where L_f is the module of values defined in § 2.

§ 5. Action of the w_Q's

Let $N = Q \cdot Q'$ be a factorization of N into relatively prime factors Q and Q'. Let $\varepsilon = \varepsilon_Q \cdot \varepsilon_{Q'}$ where ε_Q (resp. $\varepsilon_{Q'}$) is a character mod Q (resp. mod Q').

For $f \in \mathscr{C}(N, \varepsilon, k)$, we can produce a well-defined modular form $w_Q(f)$ in $\mathscr{C}(N, \varepsilon_Q^{-1} \cdot \varepsilon_{Q'}, k)$ by the following formula (cf. [A-L]):

If $x, y, z, t \in Z$ with $Qxt - Q'yz = 1$, then

$$w_Q(f) = \varepsilon_Q(y) \cdot \varepsilon_{Q'}(x) \cdot f \mid W_Q \quad \text{where } W_Q = \begin{bmatrix} Qx & y \\ Nz & Qt \end{bmatrix}. \tag{5.1}$$

Moreover,

$$w_Q^2(f) = \varepsilon_Q(-1) \cdot \varepsilon_{Q'}^{-1}(Q) f = \varepsilon(-1)\, \varepsilon_{Q'}^{-1}(-Q) f = (-1)^k \varepsilon_{Q'}^{-1}(-Q) f \tag{5.2}$$

and if l is a prime not dividing Q, then

$$w_Q(f \mid T_l) = \varepsilon_Q(l) \cdot w_Q(f) \mid T_l. \tag{5.3}$$

A simple computation together with the proposition of § 2 shows that

$$L_{w_Q(f)} = L_f. \tag{5.4}$$

§ 6. The functional equation for modular symbols

We keep the notation of § 5.

Proposition. *Let a, m be relatively prime integers such that $m>0$, $(m, Q)=1$ and $Q'|m$. Let a' be an integer such that $a'aQ\equiv -1 \bmod m$. Then:*

$$\lambda(f, P; a, m) = -\varepsilon_Q(-m)\,\varepsilon_{Q'}^{-1}(-a)\cdot\lambda\left(w_Q(f), P\left|\begin{bmatrix}0 & -1\\ Q & 0\end{bmatrix}\right.; a', m\right) \qquad (6.1)$$

for all P in $\mathscr{P}_k(\mathbf{C})$.

Proof. Let $b=-(Qa'a+1)/m$ so that $-Qa'a-mb=1$. Then $\varepsilon_Q^{-1}(b)=\varepsilon_Q(-m)$. Put

$$W_Q=\begin{bmatrix}-Qa & b\\ Qm & Qa'\end{bmatrix}$$

and compute the right-hand side of (6.1) to be:

$$-\lambda\left(f|W_Q, P\left|\begin{bmatrix}0 & -1\\ Q & 0\end{bmatrix}\right.; a', m\right) = -m^{(k/2)-1}\,\Phi\left(f|W_Q\cdot\begin{bmatrix}1 & -a'\\ 0 & m\end{bmatrix}, P\left|\begin{bmatrix}0 & -1\\ Q & 0\end{bmatrix}\right., 0\right).$$

Now use axiom (b) with $r=0$, $A=\begin{bmatrix}0 & -1\\ Q & 0\end{bmatrix}$ with f replaced by $f|W_Q\begin{bmatrix}1 & -a'\\ 0 & m\end{bmatrix}$ and P by $P|A$. Thus:

$$\Phi\left(f|W_Q\cdot\begin{bmatrix}1 & -a'\\ 0 & m\end{bmatrix}A; P|A^2, 0\right) = -\Phi\left(f|W_Q\begin{bmatrix}1 & -a'\\ 0 & m\end{bmatrix}, P\left|\begin{bmatrix}0 & -1\\ Q & 0\end{bmatrix}\right., 0\right).$$

But $W_Q\begin{bmatrix}1 & -a'\\ 0 & m\end{bmatrix}A = -Q\begin{bmatrix}1 & -a\\ 0 & m\end{bmatrix}$ and $A^2=-Q\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ yielding (6.1).

§ 7. Relation of the modular symbols to the values of the complex L-function $L(f, s)$

From now on we suppose our modular symbol λ is that made with $\Phi=\phi$, the explicit modular integral defined in § 1.

If $f\in\mathscr{C}(\varepsilon, k)$ has Fourier expansion $f(z)=\sum_{n\geqq 1} a_n e^{2\pi i n z}$ then the corresponding L-function $L(f, s)$ is defined by

$$L(f, s) := \sum_{n\geqq 1} a_n n^{-s} = \frac{(2\pi)^s}{\Gamma(s)}\int_0^\infty f(it)\,t^s(dt/t).$$

We therefore have

$$\lambda(f, z^n; 0, 1) = \phi(f, z^n, 0) = -2\pi i\int_0^{i\infty} f(z)\,z^n\,dz$$

$$= i^n\frac{n!}{(2\pi)^n}L(f, n+1) \qquad \text{for } 0\leqq n\leqq k-2.$$

§ 8. Twists

Let χ be a Dirichlet character mod m. The Gauss sums are defined by the formulae:

$$\tau(n,\chi):=\sum_{a \bmod m}\chi(a)\cdot e^{2\pi i n a/m}$$

$$\tau(\chi):=\tau(1,\chi).$$

We have

$$\tau(n,\chi)=\bar{\chi}(n)\cdot\tau(\chi) \quad \begin{array}{l}\text{for all } n\in\mathbf{Z}, \text{ if } \chi \text{ is primitive mod } m, \text{ and}\\ \text{for } (n,m)=1, \text{ if } \chi \text{ is any character mod } m.\end{array} \tag{8.1}$$

Conversely, if (8.1) holds for all $n\in\mathbf{Z}$ then χ is primitive mod m, and in that case

$$|\tau(\chi)|^2=\chi(-1)\,\tau(\chi)\,\tau(\bar{\chi})=m. \tag{8.2}$$

For $f(z)=\sum_{n\geqq 1} a_n e^{2\pi i n z}$ we put

$$f_\chi(z):=\sum_n \chi(n)\,a_n\,e^{2\pi i n z}.$$

Then, using (8.1) to replace $\bar{\chi}(n)$ by $\tau(n,\chi)/\tau(\chi)$ and rearranging sums we find (Birch's lemma) that if χ is primitive mod m,

$$f_{\bar{\chi}}(z)=\frac{1}{\tau(\chi)}\sum_{a \bmod m}\chi(a)\,f\left(z+\frac{a}{m}\right). \tag{8.3}$$

For the modular integral, this gives the twisting rule

$$\begin{aligned}\phi(f_{\bar{\chi}},P,r)&=\frac{1}{\tau(\chi)}\sum_{a \bmod m}\chi(a)\,\phi\left(f\,\middle|\begin{bmatrix}1 & a/m\\ 0 & 1\end{bmatrix},P,r\right)\\ &=\frac{1}{\tau(\chi)}\sum_{a \bmod m}\chi(a)\,\phi\left(f,P\,\middle|\begin{bmatrix}1 & -a/m\\ 0 & 1\end{bmatrix},r+\frac{a}{m}\right)\end{aligned} \tag{8.4}$$

if χ is primitive mod m. For the modular symbol λ we find by a straightforward computation:

$$\lambda(f_{\bar{\chi}}(z),P(mz);b,n)=\frac{1}{\tau(\chi)}\sum_{a \bmod m}\chi(a)\,\lambda(f,P;mb-na,mn), \tag{8.5}$$

for χ primitive mod m.

Putting $b=0$, $n=1$ in (8.5) and combining it with § 7 we have, for $0\leqq n\leqq k-2$,

$$L(f_{\bar{\chi}},n+1)=\frac{1}{n!}\,\frac{(-2\pi i)^n}{m^{n+1}}\,\tau(\bar{\chi})\sum_{a \bmod m}\chi(a)\,\lambda(f,z^n;a,m), \tag{8.6}$$

which expresses the special values of the L-functions of all twists of f in terms of the modular symbols for f.

§ 9. A numerical example

Let $\eta(z)=q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$ be the Dedekind η-function and let $\eta_b(z):=\eta(bz)$.

Set

$$f=\eta^6\cdot\eta_3^6.$$

Then f is the unique normalized cusp form of weight 6 on $\Gamma_0(3)$ with $\varepsilon=1$. The ring of Hecke operators is $\mathbf{Z}$ and there are two complex numbers Ω^+ and Ω^- ("periods") such that

$$\Lambda^{\pm}(f,z^n;a,m):=[\lambda(f,z^n;a,m)\pm\lambda(f,z^n;-a,m)]/\Omega^{\pm}$$

are integers with greatest common divisor 1. This pins down the "periods" up to sign. For χ a primitive character of conductor m, define

$$\Lambda(f,\chi,n+1):=\sum_{a \bmod m}\chi(a)\cdot\Lambda^{\mathrm{sign}(\chi)}f(z^n;a,m)\in\mathbf{Z}[\chi].$$

Here $\mathbf{Z}[\chi]$ is the ring of cyclotomic integers generated by the values of the character χ.

These are the "algebraic parts" of the special values of L-functions of twists of the modular form f in the sense that

$$L(f_{\bar{\chi}},n+1)=\frac{\Omega^{\mathrm{sign}(\chi)}}{n!}\,\frac{(-2\pi i)^n}{m^{n+1}}\,\tau(\bar{\chi})\cdot\Lambda(f,\chi,n+1). \tag{9.1}$$

In the table below we consider primitive quadratic characters χ of conductor m, and record the factorized integers $\Lambda(f,\chi,n+1)$ for $n=0,1,2$. Note that the functional equation then enables one to predict the value for $n=3$ and 4. Explicitly,

$$-\varepsilon\cdot\Lambda(f,\chi,4)=\sigma/3\cdot\Lambda(f,\chi,2)$$
$$\varepsilon\cdot\Lambda(f,\chi,5)=(\sigma/3)^2\cdot\Lambda(f,\chi,1),$$

m	$n=0$	$n=1$	$n=2$
5	$2^5\cdot3^5\cdot13$	$2^4\cdot3^4$	0
12	$-2^5\cdot3^5\cdot5\cdot13$	$2^5\cdot3^5$	0
28	$2^8\cdot3^5\cdot5\cdot13\cdot53$	$-2^6\cdot3^4\cdot103$	$-2^8\cdot3^4\cdot13$
40	$2^9\cdot3^5\cdot5\cdot7\cdot13\cdot19$	$-2^8\cdot3^4\cdot97$	$-2^{10}\cdot3^4\cdot13$
44	$-2^6\cdot3^5\cdot5\cdot13\cdot19\cdot79$	$2^7\cdot3^4\cdot191$	0
13	$2^9\cdot3^5\cdot5\cdot13$	$-2^7\cdot3^4\cdot5$	$-2^6\cdot3^4\cdot13$
17	$-2^7\cdot3^5\cdot13\cdot43$	$2^7\cdot3^4\cdot5$	0
21	$-2^6\cdot3^5\cdot13\cdot37$	$2^6\cdot3^5\cdot5$	0
29	$-2^5\cdot3^7\cdot5\cdot13\cdot61$	$2^4\cdot3^7\cdot19$	0
37	$2^9\cdot3^5\cdot5\cdot13\cdot109$	$-2^7\cdot3^4\cdot7\cdot23$	$-2^6\cdot3^4\cdot13$
41	$-2^9\cdot3^5\cdot5\cdot13\cdot113$	$2^7\cdot3^4\cdot107$	0
53	$-2^5\cdot3^5\cdot13\cdot41017$	$2^4\cdot3^4\cdot17\cdot233$	0
60	$-2^9\cdot3^6\cdot5\cdot13\cdot29$	$2^7\cdot3^6\cdot23$	0

where ε is the "sign of the functional equation" and $\sigma = \text{g.c.d.}(3, m)$. The zeroes in our table at the central point $n=2$ are all forced by the sign ε.

§ 10. *p*-adic distributions

Let p be a prime number, fixed from now on. Suppose that $f \in \mathscr{C}(N, \varepsilon, k)$ is an eigenform for T_p with eigenvalue a_p (necessarily an algebraic integer in $\mathbf{C}$).

Suppose that the polynomial

$$X^2 - a_p X + \varepsilon(p)\, p^{k-1} \tag{10.1}$$

has a non-zero root. *Choose such a root* $\alpha \neq 0$.

Let $v(m) = \operatorname{ord}_p(m)$ be the integer such that $mp^{-v(m)}$ is a p-adic unit. Define:

$$\mu_{f,\alpha}(P; a, m) = \frac{1}{\alpha^{v(m)}}\, \lambda_{f,P}(a, m) - \frac{\varepsilon(p)\, p^{k-2}}{\alpha^{v(m)+1}}\, \lambda_{f,P}(a, m/p) \tag{10.2}$$

for $a, m \in \mathbf{Z}$, $m > 0$.

An elementary computation using the Proposition of § 4, the fact that a_p is the eigenvalue of the action of T_p on f and that α is a root of (10.1) gives the *distribution property:*

Proposition. *For* $a, m \in \mathbf{Z}$, $m > 0$ *we have* $\sum_{\substack{b \equiv a \bmod m \\ b \bmod pm}} \mu_{f,\alpha}(P; b, pm) = \mu_{f,\alpha}(P; a, m)$.

Suppose ψ is a Dirichlet character with conductor M relatively prime to p. Then, using (8.5) we find, for n prime to M:

$$\mu_{f_{\bar\psi}, \alpha\bar\psi(p)}(P(Mz); b, n) = \frac{\psi(p)^{v(n)}}{\tau(\psi)} \sum_{a \bmod M} \psi(a)\, \mu_{f,\alpha}(P, Mb - na, Mn). \tag{10.3}$$

§ 11. *p*-adic integrals

Let M be a fixed integer > 0 and prime to p. Set

$$\begin{aligned} \mathbf{Z}_{p,M} &= \varprojlim_{v} (\mathbf{Z}/p^v M\mathbf{Z}) = \mathbf{Z}_p \times (\mathbf{Z}/M\mathbf{Z}) \\ \mathbf{Z}^*_{p,M} &= \varprojlim_{v} (\mathbf{Z}/p^v M\mathbf{Z})^* = \mathbf{Z}^*_p \times (\mathbf{Z}/M\mathbf{Z})^*. \end{aligned} \tag{11.1}$$

We view $\mathbf{Z}^*_{p,M}$ as a p-adic analytic Lie group with a fundamental system of open disks $D(a, v)$ indexed by integers a prime to pM and natural numbers $v \geq 1$, where

$$D(a, v) := a + p^v M\mathbf{Z}_{p,M} \subset \mathbf{Z}^*_{p,M}.$$

Thus, $D(a, v)$ depends only on $a \bmod p^v M$.

Let $\bar{\mathbf{Q}}$ be the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$. *Fix an imbedding*

$$\bar{\mathbf{Q}} \xrightarrow{\iota} \mathbf{C}_p := \text{the completion of an algebraic closure of } \mathbf{Q}_p.$$

Let $\mathcal{O}_p \subset \mathbf{C}_p$ denote the ring of integers, and $\mathcal{O}_p^*$ its topological group of units.

Now fix a modular form $f \in \mathscr{C}(N, \varepsilon, k)$ as in § 10, and consider the finite dimensional $\mathbf{C}^p$-vector space

$$V_f := \mathbf{C}_p \otimes_{\bar{Q}} L_f \bar{\mathbf{Q}}$$

and the $\mathcal{O}_p$-lattice $\Omega_f \subset V_f$ generated by L_f.

Extend the definitions of $\phi(f, P, r)$, $\lambda(f, P; a, m)$ and $\mu_{f,\alpha}(P; a, m)$ to the case where P has coefficients in $\mathbf{C}_p$ yielding values in V_f.

Our aim is now to follow Vishik [V] and Amice-Vélu [A-V] to define a *V_f-valued integral*

$$(U, F) \mapsto \int_U F, \tag{11.2}$$

where U ranges through compact open subsets of $\mathbf{Z}_{p,M}^*$ and F ranges through locally analytic functions on U (see below), such that, denoting by $x \mapsto x_p$ the projection of $\mathbf{Z}_{p,M}$ onto $\mathbf{Z}_p$, we have

$$\int_{D(a,\nu)} P(x_p) = \mu_{f,\alpha}(P; a, p^\nu M), \tag{11.3}$$

for $\nu, a \in \mathbf{Z}$, $\nu \geqq 1$, $(a, pM) = 1$, $P \in \mathscr{P}_k(\mathbf{C}_p)$. Here the condition $\nu \geqq 1$ is essential; for the value of the integral in case $\nu = 0$ (with the natural definition of $D(a, 0)$) see the end of § 14.

Definition. If $U \subseteq \mathbf{Z}_{p,M}$ is an open subset, a function

$$F: U \to \mathbf{C}_p$$

is called *locally analytic* if there is a covering of U by disks $D(a, \nu)$ such that on each $D(a, \nu)$, F is given by the convergent power series

$$F(x) = \sum_{n \geqq 0} c_n (x - a)_p^n.$$

Note that convergence of the above power series on $D(a, \nu)$ is equivalent to the condition that $p^{n\nu} c_n$ tend to zero as n goes to ∞.

Theorem (Vishik, Amice-Vélu). *Fix an integer h such that $1 \leqq h \leqq k-1$. Suppose the polynomial $X^2 - a_p X + \varepsilon(p) p^{k-1}$ has a root $\alpha \in \mathbf{C}_p$ such that $\mathrm{ord}_p \alpha < h$. Fix such an α. Then there exists a unique V_f-valued integral* (11.2) *satisfying these axioms, in which $\nu \geqq 1$, $a \in \mathbf{Z}$ throughout:*

I. *It is $\mathbf{C}_p$-linear in F and finitely additive in U.*

II. (*Evaluation on polynomials of small degree*):

$$\int_{D(a,\nu)} x_p^j = \mu_{f,\alpha}(z^j; a, p^\nu M) \quad \textit{for} \quad 0 \leqq j < h.$$

III. (*Divisibility*): *For any $n \geqq 0$,*

$$\int_{D(a,\nu)} (x - a)_p^n \in \left(\frac{p^n}{\alpha}\right)^\nu \alpha^{-1} \Omega_f.$$

IV. (*Continuity*): *If* $F(x)=\sum_{n\geq 0} c_n(x-a)_p^n$ *is convergent on the disk* $D(a,v)$, *then* $\int_{D(a,v)} F=\sum_{n\geq 0} c_n \int_{D(a,v)} (x-a)_p^n$.

Remark. The V_f-valued integral whose existence and uniqueness is given by the above theorem is independent of choice of h in the sense that, given α, for any choice of integer h with

$$\operatorname{ord}_p \alpha < h \leqq k-1$$

one gets the same integral, as follows directly from the uniqueness assertion of the theorem. The integral *does*, however, depend upon the choice of α. If α is a root of $X^2-a_p X+\varepsilon(p)p^{k-1}$ such that $\operatorname{ord}_p\alpha<k-1$, we shall call α an *allowable p-root for f* and we sometimes write $\int_U F d\mu_{f,\alpha}$ for the corresponding integral.

Proof. First, given any $F(x)=\sum c_n(x-a)_p^n$ convergent on $D(a,v)$, define a fractional ideal in $\mathbf{C}_p$ by

$$I(F,a,v)=p^{-hv}\sum_{n\geq h} c_n p^{nv}\mathcal{O}_p$$

noting that this *is* a fractional ideal (i.e., finitely generated over $\mathcal{O}_p$) because $c_n p^n \to 0$, as $n\to\infty$.

Lemma. *If* $D(a',v')\subset D(a,v)$ *then* $I(F,a',v')\subset I(F,a,v)$.

Proof. Obviously, if $v'\geqq v$, then $I(F,a',v')\subset I(F,a',v)$ so we may assume that $v'=v$. Suppose

$$F(x)=\sum_{n\geq 0} c'_n(x-a')_p^n=\sum_{n\geq 0} c_n(x-a)_p^n$$

for x in $D(a,v)=D(a',v)$. Then

$$c'_j=\sum_{n\geq j} c_n\binom{n}{j}(a'-a)_p^{n-j}$$

and therefore, since $a'\equiv a(\operatorname{mod} p^v)$,

$$p^{jv}c'_j\in\sum_{n\geq j} c_n p^{nv}\mathcal{O}_p\subseteq p^{hv}I(F,a,v).$$

Uniqueness. For this we may suppose that we are given a V_f-valued integral (11.2) satisfying I, III, IV, and the following replacement of II:

$$\mathrm{II}_0 \qquad \int_{D(a,v)} P(x_p)=0 \quad \text{for degree}(P)<h.$$

We must show that such an integral vanishes identically. By I and the lemma it suffices to show that for $F(x)=\sum c_n(x-a)_p^n$ convergent on $D(a,v)$

$$\int_{D(a,v)} F\in(p^h/\alpha)^v\cdot I(F,a,v)\,\alpha^{-1}\cdot\Omega_f \tag{11.4}$$

for then, taking coverings of an open set U by disks $D(a_i,v)$ for v increasing, (11.4) shows that $\int_U F=0$. But (11.4) follows from II_0, III, and IV.

Existence. For this we may take $h=k-1$. Note, first, the following "internal consistencies" among the axioms:

(i) I and II imply

$$\mathrm{III}_n: \quad \int_{D(a,\nu)} (x-a)_p^n \in \left(\frac{p^n}{\alpha}\right)^\nu \alpha^{-1} \cdot \Omega_f$$

for $n \leq k-2$.

This follows directly from (3.2), and the relevant definitions.

(ii) If F is convergent on $D(a, \nu)$ and III_n holds for all n, then the right-hand side of the equation in IV is convergent.

Now we need an approximation lemma.

Let $a' \equiv a \bmod p^\nu M$ so that $D(a', \nu) = D(a, \nu)$. Let F be convergent on $D(a, \nu)$ and write

$$F(x) = \sum_{n \geqq 0} c_n (x-a)_p^n = \sum_{n \geqq 0} c'_n (x-a')_p^n.$$

Consider the "truncations"

$$F_a(x) = \sum_{n<h} c_n (x-a)_p^n, \qquad F_{a'}(x) = \sum_{n<h} c'_n (c-a')_p^n$$

and put

$$F_a(x) - F_{a'}(x) = \sum_{n<h} b_n (x-a)_p^n.$$

Then

Lemma. $p^{n\nu} b_n \in p^{h\nu} \cdot I(F, a, \nu)$.

Proof. We have

$$b_n = \sum_{j \geqq h} c'_j \binom{j}{n} (a-a')^{j-n}$$

and since $a - a' \in p^\nu Z$,

$$p^{n\nu} b_n \in \sum_{j \geqq h} c'_j p^{j\nu} \cdot \mathcal{O}_p \subseteq p^{h\nu} I(F, a, \nu).$$

A consequence of the above lemma and (i) is the following estimate:

$$\int_{D(a,\nu)} (F_a - F_{a'}) \in \left(\frac{p^h}{\alpha}\right)^\nu I(F, a, \nu)\, \alpha^{-1} \Omega_f. \tag{11.5}$$

Therefore if F is locally analytic on U and U is the disjoint union of $D(a_i, \nu)$ for $\nu \gg 0$, then a "ν-th Riemann sum"

$$\sum_i \int_{D(a_i,\nu)} F_{a_i} \quad \text{for} \int_U F$$

(in which each summand is defined via II), is determined modulo $\left(\frac{p^h}{\alpha}\right)^\nu \alpha^{-1} \cdot I_\nu \Omega_f$, where

$$I_\nu = \sum_i I(F, a_i, \nu).$$

Since $I_\nu \supset I_{\nu+1}$, one can check that the "ν-th Riemann sums" converge, yielding our integral. For the details, see [V] and [A-V].

§ 12. On the choice of α

Let $\alpha, \bar{\alpha}$ be the two roots of $X^2 - a_p X + \varepsilon(p) p^{k-1}$ and let

$$\sigma = \operatorname{ord}_p \alpha, \qquad \bar{\sigma} = \operatorname{ord}_p \bar{\alpha}.$$

Order the roots so that $\sigma \leqq \bar{\sigma}$.

Definition. The form f is *ordinary at* p if and only if $\sigma = 0$, i.e., if and only if $a_p \in \mathcal{O}_p^*$. Note that this notion depends on our choice of embedding $\bar{\mathbf{Q}} \to \mathbf{C}_p$ (§ 11). Here are some general remarks about the roots α and $\bar{\alpha}$.

I) *Suppose that* $p \nmid N$:

In this case both roots are nonzero and $\sigma + \bar{\sigma} = k - 1$. Consider the two "extreme" cases:

1) The ordinary case: $\sigma = 0$, $\bar{\sigma} = k - 1$.

2) The "most supersingular case": $\sigma = \bar{\sigma} = (k-1)/2$.

In the ordinary case there is a unique allowable p-root (α is allowable; $\bar{\alpha}$ is not). Note that if $a_p = 0$, we are in the "most supersingular case". If f is a modular form of CM-type, then a_p is zero for all $p \nmid N$ which are inert in the field of complex multiplications of f.

II) *Suppose that* $p \mid N$:

In this case $\bar{\alpha} = 0$ and $\alpha = a_p$. Let $\tilde{\varepsilon}$ be the primitive character associated to ε. According to [L], a_p is nonzero (for $p \mid N$) if and only if:

either

(i) $p^2 \nmid N$, $\tilde{\varepsilon}(p) \neq 0$, in which case $a_p^2 = \tilde{\varepsilon}(p) p^{k-2}$, or

(ii) $\operatorname{ord}_p(\operatorname{cond} \tilde{\varepsilon}) = \operatorname{ord}_p N > 0$, in which case

$$|a_p| = p^{(k-1)/2}.$$

In case (i) $\operatorname{ord}_p \alpha = (k-2)/2$ and so α is an allowable p-root (and f is ordinary at p if and only if $k = 2$). In case (ii) [L] says nothing about $\operatorname{ord}_p \alpha$ in general, but in the special case where a_p is real, we have $a_p = \pm p^{(k-1)/2}$ and hence α is allowable, and f is not ordinary at p.

Remarks. For a fixed modular form f without CM, a_p vanishes infrequently. For the best results along these lines, to date, see [S] 7, Theorem 15. If f has CM, then $a_p = 0$ (and hence we are in the "most supersingular case") with Dirichlet density 1/2. It would be of interest to have detailed statistics for the relative frequency of a given "slope" σ.

Numerical examples

Consider the following triples (N, ε, k):

N	11	7	5	3	2	1
ε	1	ε_7	1	1	1	1
k	2	3	4	6	8	12

where ε_7 is the quadratic character attached to the field $\mathbf{Q}(\sqrt{-7})$.

For each k, let ω_k denote the modular form in $\mathscr{C}(N, \varepsilon, k)$ defined by $\omega_k = \eta^k \eta_N^k$ where η is the Dedekind η-function and $\eta_N(z) = \eta(Nz)$. In each case, ω_k is a generator of the one-dimensional vector space $\mathscr{C}(N, \varepsilon, k)$. The modular form ω_2 is the well-studied form parametrizing the elliptic curve $X_0(11)$. Its supersingular primes $p = 2, 19, 29, \ldots$ have been tabulated by Lang-Trotter [L-T] up to $p = 2{,}590{,}717$. We have $a_p = 0$ for all the supersingular primes $p > 2$. The modular form ω_3 has complex multiplication by $\mathbf{Q}(\sqrt{-7})$ and consequently $a_p = 0$ if and only if p is inert in $\mathbf{Q}(\sqrt{-7})$, i.e., $p \equiv 3, 5, 6 \bmod 7$. The modular form ω_{12} is Δ, and for Δ it has been conjectured by Lehmer that a_p is never zero (this is proved for $p < 10^{15}$, cf. [S 3]).

We are grateful to Robert Kuhn who computed the first 128 Fourier coefficients of each of the six forms ω_k for us.

For $p \leqq 127$, and with the exceptions given above, $a_p \neq 0$. Excluding the cases where $a_p = 0$, all primes p in the range $11 < p \leqq 127$ are ordinary for ω_k ($k = 2, 3, 4, 6, 8, 12$). The following table gives the values of σ for the range $2 \leqq p \leqq 11$. The starred entries are the cases where $p \mid N$ (in fact $p = N$), for which the values in the table are predicted by the results cited from [L].

	2	3	5	7	11
ω_2	1/2	0	0	0	0*
ω_3	0	0	0	1*	0
ω_4	3/2	0	1*	0	0
ω_6	1	2*	0	0	0
ω_8	3*	1	1	0	0
ω_{12}	3	2	1	1	0

In the cases where $p = N$ here are the actual values of $a_p(\omega_k)$:

k	2	3	4	6	8
$a_N(\omega_k)$	1	-7	-5	9	-8

For $k = 12$, 16, 18, 20, 22, and 26, let Δ_k denote the unique normalized cusp form of weight k on the full modular group $SL_2(\mathbf{Z})$. Bob Kuhn has kindly computed for us the first 300 Fourier coefficients of each of these six forms, checking for non-ordinary primes. There are no non-ordinary primes p in the range $23<p<300$ for any of the six. For primes $p \leqq 23$ there are plenty of non-ordinary cases, as the following table of values of σ shows:

	2	3	5	7	11	13	17	19	23
Δ_{12}	3	2	1	1	0	0	0	0	0
Δ_{16}	3	3	1	1	1	1	0	0	0
Δ_{18}	4	2	2	1	1	1	0	0	0
Δ_{20}	3	3	1	2	1	1	1	0	0
Δ_{22}	5	3	2	1	0	1	1	1	0
Δ_{26}	4	3	2	2	1	1	1	1	1

§ 13. The p-adic L-function

By a *p-adic character* we mean a continuous homomorphism

$$\chi: \mathbf{Z}_{p,M}^* \to \mathbf{C}_p^*,$$

for some p and M as in § 11. If M_1 divides M, then $\mathbf{Z}_{p,M_1}^*$ is a quotient of $\mathbf{Z}_{p,M}^*$, and we can identify characters of $\mathbf{Z}_{p,M_1}^*$ with certain characters of $\mathbf{Z}_{p,M}^*$ in the obvious way. We say that a character χ as above is *primitive on* $\mathbf{Z}_{p,M}^*$ if it does not factor through $\mathbf{Z}_{p,M_1}^*$ for any proper divisor M_1 of M. For each p-adic character χ there is a unique M such that χ is primitive on $\mathbf{Z}_{p,M}^*$. We call this M the *p′-conductor* of χ; it is an integer $\geqq 1$, prime to p.

Using our chosen embedding $\imath: \bar{\mathbf{Q}} \to \mathbf{C}_p$, and viewing $(\mathbf{Z}/p^\nu M\mathbf{Z})^*$ as quotient of $(\mathbf{Z}_{p,M})^*$, we can identify a primitive Dirichlet character of conductor $p^\nu M$ with a p-adic character of p'-conductor M, and every p-adic character of finite order arises in this way, for some M.

For $x \in \mathbf{Z}_p^*$ we can write, uniquely,

$$x = \omega(x)\langle x\rangle,$$

with $\omega(x)$ a root of unity and with

$$\langle x\rangle \in \begin{cases} 1+p\mathbf{Z}_p, & \text{if } p \text{ odd} \\ 1+4\mathbf{Z}_2, & \text{if } p=2. \end{cases}$$

Then $x \mapsto \omega(x)$ and $x \mapsto \langle x\rangle$ are p-adic characters of p'-conductor 1.

Here are two types of p-adic characters important in the following:

1. Special characters

These are characters χ of the form

$$\chi(x) = x_p^j \cdot \psi(x)$$

where j is an integer, $0 \leqq j \leqq k-2$, and ψ is a character of finite order.

2. *The characters χ_s*

For $s \in \mathbf{Z}_p$, define

$$\chi_s(x) := \langle x \rangle^s = \exp(s \log x) = \sum_{r=0}^{\infty} \frac{s^r}{r!} (\log \langle x \rangle)^r.$$

Remark. If s is an integer in the range $0 \leqq s \leqq k-2$, then χ_s is a special character:

$$\chi_s(x) = x_p^s \, \omega^{-s}(x).$$

Let f be as in § 10, and suppose α is an allowable p-root for f. For each p-adic character χ we put

$$L_p(f, \alpha, \chi) = \int_{\mathbf{Z}^*_{p,M}} \chi \, d\mu_{f,\alpha}$$

where M is the p'-*conductor of* χ, and where the integral is that defined in § 11. This makes sense, because p-adic characters χ are locally analytic.

Warning. If M_1 divides M, the measure $\mu_{f,\alpha}$ on $\mathbf{Z}^*_{p,M}$ is not in general the direct image of that on $\mathbf{Z}^*_{p,M}$. Thus the Eq. $(*)$ is in general valid only for χ primitive on $\mathbf{Z}^*_{p,M}$.

Notation.

$$L_p(f, \alpha, \chi, s) := L_p(f, \alpha, \chi\chi_s).$$

Proposition. *This p-adic L-function is a locally analytic function in s, defined for $s \in \mathbf{Z}_p$. For ψ a primitive Dirichlet character of conductor $p^\nu M$ we have*

$$L_p(f, \alpha, \psi, s) = \sum_{r=0}^{\infty} \frac{s^r}{r!} \sum_{a \bmod p^\nu M} \psi(a) \int_{D(a,\nu)} (\log_p(x_p))^r.$$

Proof. This follows from the fact that the n-th coefficient of the locally analytic function $\log^r(\langle x \rangle)$ lies in $(1/n!)\mathbf{Z}_p$ for any $r \geqq 0$, together with estimates stemming from III. For a closer analysis, see [V].

Proposition. *Suppose ψ is a primitive Dirichlet character with conductor M prime to p. Then for all p-adic characters χ with p'-conductor M_χ prime to M we have*

$$L_p(f, \alpha, \chi\psi) = \chi(M)\, \psi(-M_\chi)\, \tau(\psi)\, L_p(f_{\bar\psi}, \alpha\bar\psi(p), \chi).$$

In particular, for $j \in \mathbf{Z}$ and $s \in \mathbf{Z}_p$ we have

$$L_p(f, \alpha, \psi x_p^j, s) = M^j \langle M \rangle^s \psi(-1)\, \tau(\psi)\, L_p(f_{\bar\psi}, \alpha\bar\psi(p), x_p^j, s).$$

Proof. Indeed, using (10.3) with $n = p^\nu M_\chi$ and $\nu \to \infty$, we find that for locally analytic F on $\mathbf{Z}^*_{p,M_\chi}$ we have

$$\psi(-M_\chi)\,\tau(\psi)\int_{\mathbf{Z}^*_{p,M_\chi}} F(Mx)\,d\mu_{f_{\bar\psi},\alpha\bar\psi(p)}(x)=\int_{\mathbf{Z}^*_{p,MM_\chi}} \psi(x)\,F(x)\,d\mu_{f,\alpha}(x).$$

For $F=\chi$, this gives the desired result.

§ 14. The p-adic "multiplier" and interpolation of special values

If $\chi(x)=x_p^j\cdot\psi(x)$ is a special character, as in § 13, (1), and ψ is of conductor $m=p^\nu M$ define the p-adic "multiplier"

$$e_p(\alpha,\chi)=e_p(\alpha,j,\psi):=\frac{1}{\alpha^\nu}\left(1-\frac{\bar\psi(p)\,\varepsilon(p)\,p^{k-2-j}}{\alpha}\right)\left(1-\frac{\psi(p)\,p^j}{\alpha}\right).$$

Here, $\bar\psi$ is the conjugate, or inverse, character to ψ. Note that $e_p(\alpha,\chi)=\frac{1}{\alpha^\nu}$ if p divides the conductor of ψ, i.e., if $\nu>0$.

Proposition. *If χ is the special character above, then*

$$\begin{aligned}L_p(f,\alpha,\chi)&=e_p(\alpha,\chi)\cdot\frac{m^{j+1}}{\tau(\bar\psi)}\cdot\lambda(f_{\bar\psi},z^j;0,1)\\&=e_p(\alpha,\chi)\cdot\frac{m^{j+1}}{(-2\pi i)^j}\cdot\frac{j!}{\tau(\bar\psi)}\cdot L(f_{\bar\psi},j+1).\end{aligned}$$

Proof. When $\nu>0$, this is a straightforward computation. It uses the discussion of § 7, § 8, (10.2) and (11.3). In the important case of $\nu=0$, i.e., $m=M$, there is the following further calculation to make. If a is an integer prime to M, let $D(a,0)=\mathbf{Z}^*_{p,M}\cap(a+M\mathbf{Z}_{p,M})$. Then:

$$D(a,0)=\coprod_{\substack{b\equiv a \bmod M,\ b\not\equiv 0 \bmod p\\ b \bmod pM}} D(b,1).$$

The $b \bmod pM$ which we must omit from the above disjoint union, i.e., the solution of $b\equiv a \bmod M$, $b\equiv 0 \bmod p$ is $b\equiv pap' \bmod pM$ where $pp'\equiv 1 \bmod M$. By the distribution property of § 10,

$$\begin{aligned}\int_{D(a,0)} P(x_p)&=\mu_{f,\alpha}(P;a,M)-\mu_{f,\alpha}(P,pap',pM)\\&=\lambda_{f,P}(a,M)-\frac{\varepsilon(p)\,p^{k-2}}{\alpha}\,\lambda_{f,P}(a,M/p)\\&\quad-\frac{1}{\alpha}\,\lambda_{f,P}(pap',pM)+\frac{\varepsilon(p)\,p^{k-2}}{\alpha^2}\,\lambda_{f,P}(pap',M)\\&=\lambda_f(P;a,M)-\frac{\varepsilon(p)\,p^{k-2}}{\alpha}\,\lambda_f(P(z/p);pa,M)\\&\quad-\frac{1}{\alpha}\,\lambda_f(P(pz);ap',M)+\frac{\varepsilon(p)\,p^{k-2}}{\alpha^2}\,\lambda_f(P;a,M).\end{aligned}$$

In particular, we have:

$$\int_{D(a,0)} x_p^j = \left(1+\frac{\varepsilon(p)\,p^{k-2}}{\alpha^2}\right)\lambda_{f,z^j}(a,M)$$
$$-\frac{\varepsilon(p)\,p^{k-2-j}}{\alpha}\lambda_{f,z^j}(pa,M)-\frac{p^j}{\alpha}\lambda_{f,z^j}(ap',M).$$

Using this formula, one readily computes $\int_{\mathbf{Z}_{p,M}^*} \psi(x)\,x_p^j$.

§ 15. The phenomenon of extra zeroes

Retaining the notation of § 14, if $\chi(x)=x_p^j\psi(x)$ is a special character, the proposition of § 14 has the following immediate consequence:

Proposition. *The value of the p-adic L-function at the special character χ, i.e.,*

$$L_p(f,\alpha,\chi)=L_p(f,\alpha,\omega^j\psi,j),$$

is nonzero if and only if both the special value $L(f_{\bar\psi},j+1)$ of the classical L-function, and the p-adic multiplier $e_p(\alpha,\chi)=e_p(\alpha,j,\psi)$ are non-zero.

It may happen, however, that the classical special value is not zero, yet the p-adic multiplier, and consequently also the special value of the p-adic L-function, is zero.

Definition. The pair (α,j) is *exceptional* if there exists a finite character ψ such that $e_p(\alpha,\chi)=0$ for $\chi=x_p^j\psi$.

Note that the finite character ψ enters into the formula for $e_p(\alpha,\chi)$ only via its value at p. Consequently if there is some ψ such that $e_p(\alpha,j,\psi)=0$ then $e_p(\alpha,j,\psi')=0$ for every ψ' such that $\psi'(p)=\psi(p)$.

Proposition. *The pair (α,j) is exceptional in these cases and only in these cases:*

I. *k is even, $p\,\|\,N$, $\tilde\varepsilon(p)\neq 0$ and $j=(k-2)/2$ (the "central point").*

II. *k is odd, $p\nmid N$, $\alpha=\zeta p^{(k-1)/2}$ where ζ is a root of unity and $j=(k-1)/2$ or $(k-3)/2$ (the "near-central points").*

III. *k is odd,* $\operatorname{ord}_p(N)=\operatorname{ord}_p(\operatorname{cond}\tilde\varepsilon)>0$ *(the case of "primitive nebentypus"), $a_p=\zeta_{p^{(k-1)/2}}$, where ζ is a root of unity, and $j=(k-1)/2$.*

Remarks. 1. Case II is symmetrical in the sense that if (α,j) is exceptional, then $(\alpha,k-2-j)$ and $(\bar\alpha,j)$ are also. Examples of this case are easy to obtain: Take any newform of odd weight and $p\,|\,N$ such that $a_p=0$ (e.g., if f is of CM type, roughly half the primes are of this sort).

2. Case III is also easily obtainable. By [O], if k is odd and $\operatorname{ord}_p(N)=\operatorname{ord}_p(\operatorname{cond}\tilde\varepsilon)>0$, then $|a_p|=p^{(k-1)/2}$. Thus, if a_p is real, $a_p=\pm p^{(k-1)/2}$.

3. For specific examples of each case one can take the ω_k $(k=2,4,6,8)$ all of which have trivial ε and prime level $p=N$ (Case I); ω_3 with p inert in $\mathbf{Q}(\sqrt{-7})$ (Case II); ω_3 with $p=7$ (Case III).

4. It is enlightening (and puzzling: cf. § 19 and Chap. II, § 14 below) to compare the "phenomenon of extra zeroes" with the so-called "trivial zeroes"

of the Kubota-Leopoldt L-functions. Recall that if ψ is a finite character, the Kubota-Leopoldt p-adic L-function $L_p(\psi, s)$ is related to the classical Dirichlet L-function $L(\psi, s)$ by the following formula:

$$L_p(\psi, 1-k) = (1 - \tilde{\psi}\omega^{-k}(p)\, p^{k-1}) \cdot L(\tilde{\psi}\omega^{-k}, 1-k),$$

where ω is the Teichmüller character, $\tilde{}$ denotes associated primitive character, and $k = 1, 2, \ldots$.

Here, the classical L-function never vanishes at $1-k$, and so the p-adic L-function is zero if and only if

$$(1 - \psi\omega^{-k}(p)\, p^{k-1}) = 0 \tag{15.1}$$

which can happen only for $k=1$ (the analogue of a "near central point") and when $\tilde{\psi}\omega^{-1}(p) = 1$.

Proof of the proposition

Lemma. *Given any root of unity, ζ, there exists a Dirichlet character ψ such that $\psi(p) = \zeta$.*

Indeed, let ζ have order n. Since p has exact order $n \bmod (p^n - 1)$ there exists a character $\psi \bmod (p^n - 1)$ such that $\psi(p) = \zeta$.

From this lemma and the definition of $e_p(\alpha, \chi)$ it is immediate that (α, j) is exceptional if and only if

either $p \nmid N$, and $\alpha \sim p^j$, or $\alpha \sim p^{k-2-j}$
or $p \mid N$, and $a_p \sim p^j$,

where $a \sim b$ means ab^{-1} is a root of unity.

If $p \nmid N$, then Deligne's proof of the generalized Ramanujan conjecture shows that each archimedean absolute value of α is $p^{\frac{k-1}{2}}$, and from this it follows that for an exceptional pair (α, j) we have $j = \frac{k-1}{2}$ or $j = \frac{k-3}{2}$, so k is odd and we are in Case II.

If $p \mid N$, then in order that a_p be non-zero we must have ([L], Theorem 3) *either* $p \| N$ and $\tilde{\varepsilon}(p) \neq 0$, in which case $a_p^2 = \tilde{\varepsilon}(p)\, p^{k-2}$ so we are in Case I if (α, j) is exceptional, *or* $\mathrm{ord}_p(\mathrm{cond}\, \tilde{\varepsilon}) = \mathrm{ord}_p N$, in which case the archimedean absolute values of a_p are $p^{\frac{k-1}{2}}$, so we are in Case III if (α, j) is exceptional.

§ 16. Conjectures about orders of vanishing

Define:

$$\rho_\infty(f, \psi, j) := \text{order of zero}_{s=j+1}\, L(f_{\bar{\psi}}, s)$$

$$\begin{aligned} \rho_p(f, \alpha, \psi, j) &:= \text{order of zero}_{s=j}\, L_p(f, \alpha, \psi\omega^j, s) \\ &= \text{order of zero}_{s=0}\, L_p(f, \alpha, \chi, s), \text{ for } \chi = x_p^j \cdot \psi \\ &\quad \text{and } \alpha \text{ an allowable } p\text{-root for } f. \end{aligned}$$

As mentioned above, both numbers ρ_∞ and ρ_p are conjectured to be zero unless k even and j is central, or k is odd and j is near-central.

Conjecture. If α is an allowable p-root for f and $0 \leq j \leq k-2$, then

$$\begin{aligned}\rho_p(f, \alpha, \psi, j) &= \rho_\infty(f, \psi, j), &&\text{if } e_p(\alpha, j, \psi) \neq 0\\ &= \rho_\infty(f, \psi, j)+1, &&\text{if } e_p(\alpha, j, \psi) = 0.\end{aligned}$$

Remarks. When $k=2$ and j is the central point, one may view these conjectures as a piece of the p-adic analogue of the classical Birch Swinnerton-Dyer conjectures. The full "p-adic Birch Swinnerton-Dyer conjectures" will include a formula for the leading coefficient of the p-adic L-function at $s=j$, in that case. See Chap. II, § 10 below.

2. One implication of the above conjecture is that when there are two allowable choices of p-roots $\alpha, \bar{\alpha}$, the order of vanishing of the p-adic L-function $L_p(f, \alpha, \psi, s)$ at integers j in the critical range is independent of the choice of α. There is a special case where this latter assertion is fairly evident. However it is not at all evident in general, and the question of what the relationship is betweeen the two p-adic L-functions $L_p(f, \alpha, \psi, s)$ and $L_p(f, \bar{\alpha}, \psi, s)$ seems very interesting, and, perhaps, more accessible than the above conjectures.

The special case we have alluded to is the following: Let f be a newform and let K denote the subfield of $\mathbf{C}_p$ generated over $\mathbf{Q}_p$ by the values of the character ε and the eigenvalues of all the Hecke operators T_p acting on the newform f. Let $K(\psi)$ denote the field extension of K generated by the values of the character ψ. Then, up to a scalar multiple, the p-adic L function $L_p(f, \alpha, \psi\omega^j, s)$ may be expressed as a power series in s with coefficients in $K(\psi, \alpha)$. Suppose, now, that both α and $\bar{\alpha}$ are allowable. Then $K(\psi, \alpha) = K(\psi, \bar{\alpha})$. Suppose, further, that $K(\psi) \neq K(\psi, \alpha)$ or equivalently that $K(\psi, \alpha)$ is of degree 2 over $K(\psi)$. It then follows that the conjugation automorphism of $K(\psi, \alpha)$ over $K(\psi)$ brings the "normalized" power series $L_p(f, \alpha, \psi\omega^j, s)$ to $L_p(f, \bar{\alpha}, \psi\omega^j, s)$ and consequently these power series have the same order of vanishing at $s=0$. This case can happen, of course (e.g., $k=2$, $a_p=0$).

§ 17. The functional equation

Returning to the terminology of § 5, § 6, fix an integer M prime to p and define Q to be the largest positive divisor of N which is relatively prime to pM; write

$$N = Q \cdot Q' \qquad \varepsilon = \varepsilon_Q \cdot \varepsilon_{Q'}$$

as in § 5.

We make the hypothesis that *Q' divides $p^\nu M$* for large ν.

Since Q is prime to pM we can, and do, view Q as an element of $\mathbf{Z}_{p,M}^*$.

Since $Q' \mid p^\nu M$ for large ν, we can, and do, view $\varepsilon_{Q'}$ as a character on $\mathbf{Z}_{p,M}^*$.

Let $\varepsilon^* = \varepsilon\varepsilon_Q^{-2} = \varepsilon_{Q'}\varepsilon_Q^{-1}$. Recall the w_Q operator

$$w_Q: \mathscr{C}(N, \varepsilon, k) \to \mathscr{C}(N, \varepsilon^*, k)$$

which, now that Q is fixed, we will denote by

$$f \mapsto f^* := w_Q(f).$$

If f is an eigenvector for T_l $(l \nmid Q)$ with eigenvalue a_l, then f^* is an eigenvector for T_l with eigenvalue $a_l \varepsilon_Q^{-1}(l)$.

If α is an allowable root of $X^2 - a_p X + \varepsilon(p) p^{k-1}$, then $\alpha^* := \varepsilon_Q^{-1}(p)\alpha$ is an allowable root of the equation

$$X^2 - a_p \varepsilon_Q^{-1}(p) X + \varepsilon(p) \varepsilon_Q^{-2}(p) p^{k-1},$$

i.e., α^* is an allowable p-root for f^*.

If U is an open compact subset of $\mathbf{Z}_{p,M}^*$, let U^* denote the image of U under the mapping $x \mapsto -1/Qx$. Thus

$$D(a, v)^* = D(a', v),$$

where a' is any integer such that

$$a \cdot a' \cdot Q \equiv -1 \bmod p^v M. \tag{17.1}$$

If $F(x)$ is a locally analytic function on the open set U, let F^* denote the locally analytic function on U^* given by the formula:

$$F^*(x) = Q^{(k-2)/2} x_p^{k-2} F(-1/Qx).$$

Note that if $P \in \mathscr{P}_k(\mathbf{C}_p)$, then $P^* = P \left| \begin{bmatrix} 0 & -1 \\ Q & 0 \end{bmatrix} \right.$, it being understood that here, and in the following, we interpret a polynomial P in $\mathscr{P}_k(\mathbf{C}_p)$ as the function $x \mapsto P(x_p)$ on $\mathbf{Z}_{p,M}^*$.

Formula (6.1) rewritten in terms of the distribution μ and the terminology we have just introduced reads as follows:

Proposition. *Suppose that v is $\geqq 1$ and is large enough so that Q' divides $p^{v-1}M$. Then*

$$\mu(f, \alpha, P; a, p^v M) = -\varepsilon_Q(-M)\, \varepsilon_{Q'}^{-1}(-a)\, \mu(f^*, \alpha^*, P^*; a', p^v M),$$

where a' is as in (17.1).

Corollary 1. *For F locally analytic on a compact open subset $U \subset \mathbf{Z}_{p,M}^*$, we have*

$$\int_U F \cdot d\mu_{f,\alpha} = -\varepsilon_Q(-M)\, \varepsilon_{Q'}(Q) \int_{U^*} \varepsilon_{Q'} \cdot F^* \cdot d\mu_{f^*,\alpha^*}.$$

Proof. Recall the proof of the theorem of Vishik and Amice-Vélu (§ 10). Take the cut-off value h to be $k-1$. It suffices to prove the corollary for $U = D(a, v)$ with v sufficiently large. Take v such that Q' divides $p^{v-1}M$. In this case $\varepsilon_{Q'}$ takes the constant value $\varepsilon_{Q'}(a')$ on $D(a', v)$ and we must prove:

$$\int_{D(a,v)} F \cdot d\mu_{f,\alpha} = -\varepsilon_Q(-M)\, \varepsilon_{Q'}^{-1}(-a) \int_{D(a',v)} F^* \cdot d\mu_{f^*,\alpha^*} \tag{17.2}$$

(using (17.1)).

If F_a denotes the "h-cut-off" of the Taylor expansion of F at $x_p = a$ as in the proof of the theorem of § 10, we have

$$(F_a)^* = (F^*)_{a^*}, \qquad \text{where } a^* = -\frac{1}{Qa},$$

and consequently (17.2) would follow in general, if it were true for polynomials $P \in \mathscr{P}_k(\mathbf{C}_p)$, for then the ν'-th Riemann sum approximation to the right hand side would be equal to the same for the left hand side for any $\nu' \geqq \nu$. But for $F = P$, (17.2) is just a paraphrase of the formula in the previous proposition. Taking F to be a continuous character χ, we get:

Corollary 2 (Functional equation). *If χ and $\varepsilon_{Q'}^{-1}\chi$ are primitive on $Z_{p,M}^*$ then*

$$L_p(f, \alpha, \chi, s)$$
$$= -\varepsilon_Q(-M)\,\varepsilon_{Q'}(Q)\,Q^{(k-2)/2}\chi^{-1}(-Q)\langle Q\rangle^{-s} L_p(f^*, \alpha^*, \varepsilon_{Q'}\,x_p^{k-2}\chi^{-1}, -s).$$

To analyze the sign of the functional equation conveniently, we shall "abbreviate" the constant in the above functional equation as follows. We assume that N, ε, and k are fixed. Let ψ be a (finite) Dirichlet character, and let M denote the p'-conductor of ψ. Let Q and Q' be the factors of N determined by p and M as in the beginning of this section. Define

$$\eta_p(\psi, j) := (-1)^{j+1}\,\varepsilon_Q(-M)\,\varepsilon_{Q'}(Q)\,Q^{((k-2)/2)-j}\,\bar{\psi}(-Q).$$

Then for χ the special character ψx_p^j the formula of Corollary 2 reads

$$L_p(f, \alpha, \psi x_p^j, s) = \eta_p(\psi, j)\langle Q\rangle^{-s} L_p(f^*, \alpha^*, \varepsilon_{Q'}\,x_p^{k-2-j}\psi^{-1}, -s), \tag{17.3}$$

if $\varepsilon_{Q'}\psi^{-1}$ has the same p'-conductor, M, as ψ.

§ 18. The sign in the functional equation

We retain the notation of § 17 and make the following further hypothesis:

$$\text{The character } \varepsilon \text{ is trivial, and the modular form } f \text{ is a newform of even weight } k. \tag{18.1}$$

Under this hypothesis, f is also an eigenform for the operator w_Q. We have in fact

$$f^* = c_Q \cdot f, \qquad \text{with } c_Q = \pm 1.$$

Since ε_Q is trivial, it also follows that $\alpha^* = \alpha$. Suppose further:

$$j = (k-2)/2 \quad \text{and} \quad \psi \text{ is of order two.} \tag{18.2}$$

Then (17.3) becomes:

$$L_p(f, \alpha, \psi x_p^{(k-2)/2}, s) = \langle Q\rangle^{-s}(-1)^{k/2}\,\psi(-Q)\,c_Q\,L_p(f, \alpha, \psi x_p^{(k-2)/2}, -s). \tag{18.3}$$

Define $\operatorname{sign}_p(f, \psi)$, the *$p$-adic sign of f and ψ*, to be $(-1)^{k/2}\psi(-Q)\,c_Q$.

Remark. Using [A-L] one can prove that if ψ is any Dirichlet character such that there is a factorization $N=qq'$ with $(q,m)=1$ and $q'\mid m$, where $m=$ conductor of ψ, and f is any newform of type (N,ε,k) such that $\varepsilon_{q'}\psi$ has conductor m, then f_ψ is a newform of type $(qm^2, \varepsilon\psi^2, k)$, and its Mellin transform satisfies the functional equation

$$\frac{1}{\tau(\psi)}\,\xi(f_\psi,s)=i^k(qm^2)^{\frac{k}{2}-s}\,\varepsilon_q(m)\,\bar{\phi}(-q)\,\frac{1}{\tau(\phi)}\,\xi(g_\phi,k-s),$$

where

$$\phi=\bar{\varepsilon}_{q'}\bar{\psi},\qquad g=f\mid w_q,\quad\text{and}\quad \xi(f,s)=\frac{\Gamma(s)}{(2\pi)^s}\,L(f,s).$$

If f and ψ satisfy (18.1) and (18.2) we obtain

$$\xi\left(f_\psi,\frac{k}{2}+s\right)=(-1)^{k/2}(qm^2)^{-s}\,\psi(-q)\,c_q\,\xi\left(f_\psi,\frac{k}{2}-s\right).$$

We refer to the sign in this functional equation, i.e., to $(-1)^{\frac{k}{2}}\psi(-q)\,c_q$, (where q is the largest divisor of N relatively prime to the conductor of ψ), as the "generic sign" of f and ψ.

When can it occur that the p-adic sign differs from the generic sign?

Proposition. *Suppose that f and ψ satisfy* (18.1) *and* (18.2). *Suppose further that an allowable p-root exists for f. Then the p-adic sign of f and ψ differs from the generic sign if and only if $e_p(\alpha,j,\psi)=0$ (where $j=(k-2)/2$).*

Suppose the signs differ. Then $q\neq Q$, which is the case if and only if $p\mid N$ and $p\nmid\operatorname{cond}\psi$. Since k is even, an allowable p-root then exists if and only if $p\,\|\,N$, in which case the p-root is $a_p=-c_p p^{\frac{k-2}{2}}$ (cf. [A-L]). Under these circumstances, we have $q=pQ$, so the ratio of the two signs is $\psi(p)\,c_p$. This ratio is -1 if and only if $a_p=\psi(p)\,p^{\frac{k-2}{2}}$, which is precisely the condition that $e_p\left(a_p,\frac{k-2}{2},\psi\right)=0$.

Remark. This proposition is compatible with (and indeed would be implied by) our conjecture that the p-adic order of vanishing (at the central point) is one greater than the classical order of vanishing when the p-adic multiplier is zero, and is equal to the classical order when it is non-zero.

§ 19. Extra zeros of "local type"

One reason for studying p-adic L-functions is that they provide p-adic interpolation information about the classical special values of L-functions. When, however, the p-adic multiplier vanishes one can no longer retrieve the classical special value from the p-adic special value. Is there a way of recapturing the classical special value, nevertheless, by taking values of the *first derivative* of the p-adic L-function?

Definition. Let $f \in \mathscr{C}(N, \varepsilon, k)$, let α be an allowable p-root for f, and j an integer such that (α, j) is exceptional. Say that (α, j) is *exceptional of local type* for f if there is a constant $\mathscr{L}_p(f, \alpha, j)$ such that

$$\frac{d}{ds} L_p(f, \alpha, \psi x_p^j, s)|_{s=0} = \mathscr{L}_p(f, \alpha, j) \cdot \sum \psi(a)\, \lambda(f, z^j; a, m),$$

where ψ is any character of finite order such that $e_p(\alpha, j, \psi) = 0$, and m = conductor (ψ).

Remark. From the discussion of § 15, Remark 4, (and in view of Leopoldt's p-adic analytic formula [1]) the trivial zeroes of the Kubota-Leopoldt p-adic L-function are very unlikely to be of "local type" (with an analogous definition of "local type" tailored to cover the case of Kubota-Leopoldt p-adic L-functions).

On the other hand, it seems likely that if (α, j) is exceptional at the central point $j=0$ for a newform f *of weight* 2, then it is exceptional of local type. We also have numerical evidence which strongly suggests that this remains the case for newforms of arbitrary even weight k.

Chapter II. Arithmetic conjectures

§ 1. The $\mathscr{L}$-invariant of an elliptic curve over a local field

Recall the classical expression for the elliptic modular function j in terms of $q = e^{2\pi i z}$:

$$j = q^{-1} + 744 + 196884\, q + 21493760\, q^2 + \ldots = q^{-1} + \sum_{n=0}^{\infty} A_n q^n. \tag{1}$$

The "reverted" power series expression for q in terms of j^{-1} has coefficients in $\mathbf{Z}$ and begins

$$q = j^{-1} + 744\, j^{-2} + 750420\, j^{-3} + 872769632\, j^{-4} + \ldots = \sum_{n=1}^{\infty} B_n j^{-n}. \tag{2}$$

We are grateful to Bill McCallum for proving us with the following table of the first few coefficients of the power series (1) and (2).

$A_0 = 744$	
$A_1 = 196884$	$B_1 = 1$
$A_2 = 21493760$	$B_2 = 744$
$A_3 = 864299970$	$B_3 = 750420$
$A_4 = 20245856256$	$B_4 = 872769632$
$A_5 = 333202640600$	$B_5 = 1102652742882$
$A_6 = 4252023300096$	$B_6 = 1470561136292880$
$A_7 = 44656994071935$	$B_7 = 2037518752496883080$
$A_8 = 401490886656000$	$B_8 = 2904264865530359889600$
$A_9 = 3176440229784420$	$B_9 = 4231393254051181981976079$
$A_{10} = 22567393309593600$	$B_{10} = 6273346050902229242859370584$
$A_{11} = 146211911499519294$	$B_{11} = 9433668720359866477436486024652$
$A_{12} = 874313719685775360$	$B_{12} = 14354283113962706185538044113452448$

Now let K be a finite extension of $\mathbf{Q}_p$ and let $E_{/K}$ be an elliptic curve with *nonintegral* j-invariant. Substituting $j(E)^{-1}$ for j^{-1} in the power series (2) yields a convergent series in K whose limit we denote by $q(E)\in K^*$. We have:

$$\operatorname{ord}(q(E)) = -\operatorname{ord}(j(E)) > 0.$$

We refer to $q(E)$ as the *multiplicative period* of E. It forms the basis of the theory of analytic parametrization of the group of L-valued points of E for suitable field extensions L/K [R, La, Mo].

Definition. Let λ: $K^* \to Q_p$ be a continuous homomorphism. We put

$$\mathscr{L}_\lambda(E) := \lambda(q(E))/\operatorname{ord}(q(E)) \in \mathbf{Q}_p.$$

The "*$\mathscr{L}$-invariant*" $\mathscr{L}_\lambda(E)$ is an isogeny-invariant of E, and is linear in λ. If λ is the homomorphism obtained by composition of Norm_{K/Q_p}: $K^* \to \mathbf{Q}_p^*$ with Iwasawa's logarithm $\log_p$: $\mathbf{Q}_p^* \to \mathbf{Q}_p$ we refer to λ simply as $\log_p$: $K^* \to Q_p$ and put $\mathscr{L}_p(E) := \mathscr{L}_\lambda(E)$.

Conjecture. If E comes from an algebraic number field (or equivalently, if $j(E)$ is an algebraic number) then $\mathscr{L}_p(E)$ does not vanish.

§ 2. Sigma functions

The basic references are [P-R] and [M-T 1, 2]. See also [N]. Let K be a finite extension of $\mathbf{Q}_p$. Let $E_{/K}$ be an elliptic curve, with $E_{/\mathcal{O}}$ its Néron model over the ring of integers of K. Recall that $E_{/K}$ is said to be *ordinary* if, equivalently:

(1) The formal completion $E^f_{/\mathcal{O}}$ (of $E_{/\mathcal{O}}$ along the zero-section) is a formal group (on one parameter) of height 1.

(2) The Néron model of E either has multiplicative reduction, or has good reduction the special fiber of which possesses a point of order p over the algebraic closure of the residue field.

We assume that $E_{/K}$ is ordinary, and we choose a regular differential ω on $E_{/K}$ which extends to a regular (and not identically zero) differential on the connected component of the special fiber of the Néron model of E. We also choose some uniformizing parameter t on the formal group $E^f_{/\mathcal{O}}$, so that $E^f_{/\mathcal{O}}$ is the formal spectrum of $\mathcal{O}[[t]]$. We suppose that t is *normalized with respect to* ω in the sense that

$$\left.\frac{dt}{\omega}\right|_0 = 1.$$

In the above context one can define a "sigma function" (cf. [M-T]) if the residual characteristic of K is $\neq 2$, and the "square of a sigma function" in general. In [M-T1], eleven different characterizations of the "square of the sigma function" are given. We recall one characterization particularly relevant to the calculations below. Let D_ω denote the *second logarithmic derivative with respect to* ω. That is, if f is a nonvanishing (formal) function on $E^f_{/\mathcal{O}}$, such that

$f \in \mathcal{O}[[t]]$ is of the form $f \equiv t^m \bmod t^{m+1}$ for some m, put:

$$D_\omega(f) = \frac{d}{\omega}\left(f^{-1}\frac{df}{\omega}\right) = -\frac{m}{t^2} + \ldots \in t^{-2}\mathcal{O}[[t]]$$

Our $E_{/\mathcal{O}}$ can be given by a minimal Weierstrass equation

$$y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{3}$$

with $a_j \in \mathcal{O}$, and $\omega = dx/(2y + a_1 x + a_3)$.

A model for $E_{/\mathcal{O}}$ of the form (3) is not uniquely determined by $E_{/K}$ and ω, but the x-coordinate is determined up to an additive constant; in fact, the function $\wp_\omega = x + \frac{b_2}{12}$, where $b_2 = a_1^2 + 4a_2$, *is* uniquely determined by $E_{/K}$ and ω.

Proposition. (cf. [M-T]): *There is a unique formal function $\sigma_\omega^2 = \sigma_{E,\omega}^2$ on $E^f_{/\mathcal{O}}$ whose power series expression is in $t^2 \cdot (1 + t \cdot \mathcal{O}[[t]]) \subseteq \mathcal{O}[[t]]$, and which satisfies the conditions:*

(i) *$\sigma_\omega^2(P)$ is an even function of $P \in E^f(\mathcal{O})$.*
(ii) *$D_\omega \sigma_\omega^2(P) - D_\omega \sigma_\omega^2(Q) = 2x(Q) - 2x(P)$, for $P, Q \in E^f(\mathcal{O})$.*

If $\omega' = u\,\omega$ is another choice of differential, then $\sigma_{u\omega}^2 = u^2 \sigma_\omega^2$. Thus we can define $\sigma_{\omega'}$ for every regular differential ω' on $E_{/K}$ uniquely in such a way that that relation holds for every $u \in K$, not only for $u \in \mathcal{O}^*$.

Put $X_\omega = -1/2 \cdot D_\omega \sigma_\omega^2$.

Then, by (ii), X_ω extends to a rational function on $E_{/K}$ equal to the rational function x plus a constant. Define a constant $e = e(E, \omega)$ by the relation

$$X_\omega = x + \frac{b_2 - e}{12} = \wp_\omega - \frac{e}{12}, \tag{4}$$

where $b_2 = a_1^2 + 4a_2$. One easily checks from (4) and the definition of X_ω that e depends only upon the isomorphism class of the pair (E, ω) and not on the model (1). Moreover, it is of weight two:

$$e(E, c\,\omega) = c^{-2}\, e(E, \omega).$$

The constant $e = e(E, \omega)$ is equal to the p-adic modular form of weight two denoted by the letter P in Katz's [K] (the "Eisenstein series of weight two").

The difficulty in computing the function σ_ω^2 is traceable to the difficulty in determining the constant e. Given $e \in \mathcal{O}$ one has the function X_ω by (4) and σ_ω^2 may then be computed, via the method of undetermined coefficients, to be the unique even function $\equiv t^2 \bmod t^3$ whose second logarithmic derivative with respect to ω is $-2X_\omega$. In fact, e is that unique element of $\mathcal{O}$ such that the corresponding σ_ω^2, so computed, again has coefficients in $\mathcal{O}$. (See forthcoming publications of Bernardi and Goldstein concerning the computation of p-adic sigma functions.)

§ 3. Sigma functions when j is nonintegral

Retaining the hypotheses of § 1 and § 2, let $E_{/K}$ be an ordinary elliptic curve with *nonintegral* j-invariant and let $q = q(j(E)^{-1})$ be its multiplicative period. For such an elliptic curve, there is a field extension K' of K of degree at most two and a rigid analytic parametrization of $E_{/K'}$ as a quotient of $\mathbf{G}_{m/K'}$ (in the rigid analytic category) by a discrete subgroup of rank one. Such a rigid analytic parametrization is unique up to sign. *Choose one such parametrization.* This gives us, for each finite extension field L of K' an exact sequence:

$$0 \to \mathbf{Z} \to L^* \xrightarrow{i} E(L) \to 0$$
$$1 \mapsto q$$

The analytic parametrization i induces an isomorphism between the group of units $\mathcal{O}(L)^*$ and $E^0(L)$, the subgroup of points which specialize to the connected component of 0 on the special fiber of the Néron model. If $P \in E^0(L)$ is such a point, let $w = w(P) \in \mathcal{O}(L)^*$ be the unit such that $i(w) = P$, let ω be a regular differential on $E_{/K}$ as in § 2 and let $C \in K^*$ be that constant such that

$$i^*(\omega) = C \cdot dw/w.$$

We have the following formulas ("q-expansions") for σ_ω^2 and for the constant $e(E, \omega)$:

$$\sigma_\omega^2(P) = C^2(w + w^{-1} - 2) \prod_{n=1}^{\infty} (1 - wq^n)^2 (1 - w^{-1} q^n)^2 (1 - q^n)^{-4} \qquad (1)$$

$$e(E, \omega) = C^{-2} \left(1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n\right), \qquad (2)$$

where $\sigma_k(n)$ is the sum of k-th powers of positive divisors of n, and $w = w(P)$.

Note that formula (1) converges for *all* $w \in \mathcal{O}(L)^*$ and hence all P in $E^0(L)$.

For a numerical example, let $K = \mathbf{Q}_{11}$ and $E = X_0(11)$ whose model over $\mathbf{Z}_{11}$ is given by the equation:

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

One has $\Delta = -11^5$, $j = -2^{12} 31^3/11^5$ so that

$$j^{-1} \equiv 11^5 \cdot 8744 \bmod 11^9$$

and hence

$$q \equiv 11^5 \cdot 8744 \bmod 11^9$$

as well. From (1) we have

$$\sigma_\omega^2(P) \equiv C^2 \cdot (w + w^{-1} - 2) \bmod 11^5. \qquad (3)$$

Now consider the rational function X on E given in terms of the analytic parametrization by the formula:

$$X := \sum_{n \in \mathbf{Z}} \frac{q^n w}{(1 - q^n w)^2} = \frac{1}{(w + w^{-1} - 2)} + \sum_{\substack{n \in \mathbf{Z} \\ n \neq 0}} \frac{q^n w}{(1 - q^n w)^2}$$

so that on E_0

$$X \equiv \frac{1}{(w+w^{-1}-2)} \bmod 11^5.$$

One has that $X = ax + b$ for suitable constants a and b which can be computed to be:

$$a \equiv 4291 \bmod 11^4; \qquad b \equiv 4670 \bmod 11^4.$$

Consequently, if $\omega = dx/(2y+1)$ is the Néron differential, we have:

$$\sigma_\omega^2(P) \equiv \frac{1}{x(P) - 6350} \bmod 11^4, \tag{4}$$

for all $P \in E^0(L)$.

§ 4. The canonical height via sigma functions

The basic references are [P-R, MT1, MT2].

Let K be a global number field, and $E_{/K}$ an elliptic curve defined over K. Let $\mathcal{O} \subset K$ denote the ring of integers, and $E_{/\mathcal{O}}$ the Néron model of E, over the base $\mathcal{O}$.

Let S be a finite set of nonarchimedean primes satisfying the hypothesis that for each $v \in S$, the reduction of E at v is *ordinary* in the sense of § 2, i.e., that either E has good ordinary reduction at v or E has multiplicative reduction at v.

Define $E_S(K) \subseteq E(K)$ to be the subgroup of finite index in the Mordell-Weil group defined by the rule: $P \in E_S(K)$ if and only if $P(\in E(K))$ specializes to the connected component of zero on the special fiber of the Néron model of E for all nonarchimedean places v, and P specializes to 0 for primes v in S.

Fix ω a nontrivial K-rational differential of K. For each nonarchimedean place v of K choose a uniformizing parameter t_v of the formal completion $E^f_{/\mathcal{O}_v}$ and let $c_v \in K_v^*$ be defined by the equation:

$$\left.\frac{dt_v}{\omega}\right|_0 = c_v \in K_v^*.$$

Let ω_v be the $\mathcal{O}_v$-rational differential $\omega_v = c_v \cdot \omega$.

Dependent upon all these choices, for a nonzero point $P \in E_S(K)$ define an idele $i(P)$ whose component $i_v(P)$ at the place v is given by the following rules:

(1) If v is archimedean, then $i_v(P) = 1$.

(2) If v is nonarchimedean, $v \notin S$, and P does not specialize to zero at v, then $i_v(P) = c_v^{-2}$.

(3) If v is nonarchimedean, $v \notin S$, and P does specialize to zero at v, then

$$i_v(P) = c_v^{-2}\, t_v^2(P).$$

(4) If $v \in S$, then

$$i_v(P) = c_v^{-2} \cdot \sigma_{\omega_v}^2(P) = \sigma^2_{(E/K_v,\, \omega)}(P).$$

Here $\sigma^2_{\omega_v}$ is the square of the sigma function attached to $(E_{/K_v}, \omega_v)$ as in §2.

Note that almost all v fall under category (2) above, and therefore $i(P)$ is an idele.

Define $U_v \subset K_v^*$ to be $\mathcal{O}_v^*$ if v is nonarchimedean, and K_v^* if v is archimedean.

The idele $i(P)$ is independent of the choice of parameters t_v modulo $\prod_{v \notin S} U_v \subseteq \mathbf{A}_K^*$ and is independent of choice of K-rational differential ω modulo K^*. Hence it determines a well-defined element in the quotient group:

$$i(P) \in K^* \backslash \mathbf{A}_K^* / \prod_{v \notin S} U_v.$$

Proposition. *There is a bilinear symmetric pairing*

$$E_S(K) \times E_S(K) \to K^* \backslash \mathbf{A}_K^* / \prod_{v \notin S} U_v$$
$$(P, Q) \mapsto \langle P, Q \rangle$$

(the analytic height pairing), such that $\langle P, P \rangle = i(P)$ *for all nonzero points* P *in* $E_S(K)$.

For a proof of the above proposition cf. [MT1]. One should note that the above pairing is the *inverse* of the canonical height pairing obtained via biextensions in [M-T2]. If

$$\lambda\colon K^* \backslash \mathbf{A}_K^* / \prod_{v \notin S} U_v \to \mathbf{Q}_p$$

is any continuous homomorphism, composition of the analytic height pairing with λ yields a bilinear symmetric $\mathbf{Q}_p$-valued pairing which extends $\mathbf{Q}_p$-linearly to $E(K) \otimes \mathbf{Q}_p$:

$$(E(K) \otimes Q_p) \times (E(K) \otimes Q_p) \to \mathbf{Q}_p$$
$$(P, Q) \mapsto \langle P, Q \rangle_\lambda,$$

and which is uniquely characterized by the fact that $\langle P, P \rangle_\lambda = \lambda(i(P))$ for nonzero P in $E_S(K)$. We refer to $\langle\ ,\ \rangle_\lambda$ as the *analytic λ-height pairing.*

§5. The p-adic analytic height in a special case

Here we retain the hypotheses of §4, but suppose $K = \mathbf{Q}$, $S = \{p\}$, and let $\lambda\colon \mathbf{Q}^* \backslash A_{\mathbf{Q}}^* / \prod_{v \notin S} U_v \to \mathbf{Q}_p$ be the unique continuous homomorphism whose p-component is given by Iwasawa's p-adic logarithm

$$\log_p\colon \mathbf{Q}_p^* \to \mathbf{Q}_p \qquad (\log_p(p) = 0).$$

Now let $E_{/\mathbf{Q}}$ be an elliptic curve with ordinary reduction at p, in the sense of §2. Let $E_{/\mathbf{Z}}$ denote the Néron model over the base $\mathbf{Z}$, with minimal cubic equation $y^2 + a_1 xy + a_3 = x^3 + a_2 x^2 + a_4 x + a_6$. Let $\omega = dx/(2y + a_1 x + a_3)$ be a Néron differential.

For the t_v's chosen as in §4 we have that $x^{-1} \equiv t_v^2 \bmod t_v^3$ in $\mathcal{O}_v\,[[t_v]]$, for all nonarchimedean v of $\mathbf{Q}$.

It follows that, in this case, we have the following formula for the analytic λ-height:

Proposition. *If $P \in E_S(Q)$, then $\langle P, P\rangle_\lambda = \log_p(\sigma_{p,\omega}^2(P)/d)$ where d is the denominator of the rational number $x(P)$ written as a fraction in lowest terms.*

§6. The extended Mordell-Weil group

In this section let K be a global number field, and fix p a prime number. Let $E_{/K}$ be an elliptic curve defined over K. The places v dividing p fall into two classes:

I. Places v such that the Néron model of E is split multiplicative at v. For such places, let $q_v = q(j^{-1}(E)) \in K_v^*$ be the multiplicative period. For each such place, fix an analytic parametrization

$$i_v\colon K_v^* \to E(K_v).$$

II. The other places dividing p.

Let $K_p = K \otimes \mathbf{Q}_p = \prod_{v|p} K_v$ so that $E(K_p) = \prod_{v|p} E(K_v)$. Put:

$$E^\dagger(K_p) := \prod_{v \text{ of type I}} K_v^* \times \prod_{v \text{ of type II}} E(K_v),$$

giving us an exact sequence:

$$0 \to \mathbf{Z}^N \xrightarrow[\phi]{} E^\dagger(K_p) \xrightarrow[\psi]{} E(K_p) \to 0, \tag{1}$$

where N is the number of v's of type I and, if $a_v \in \mathbf{Z}^N$ is the vector with entry 1 in the v-th place and 0 in all other places, $\phi(a_v)$ is the vector in $E^\dagger(K_p)$ with entry q_v in the v-th place and entry 1 in all other places. The mapping ψ is defined by the requirement that it respect the direct product decompositions, and for v of type I it is i_v on the v-th coordinate, while for v of type II it is the identity mapping on the v-th coordinate.

Consider the natural inclusion of the Mordell-Weil group $E(K) \subset E(K_p)$ and let $E^\dagger(K) \subset E^\dagger(K_p)$ denote its full inverse image under ψ.

We have an exact sequence

$$0 \to \mathbf{Z}^N \to E^\dagger(K) \to E(K) \to 0 \tag{2}$$

induced from (1) and consequently, if $E(K)$ is of rank r, $E^\dagger(K)$ is a finitely generated abelian group of rank $r+N$.

Now let S denote a set of places v of K dividing p. Suppose that E has ordinary reduction at all $v \in S$ and suppose, further, that S contains all v of type I. Let $E_S(K) \subset E(K)$ denote the subgroup defined in §4. Although the exact sequence (2) doesn't necessarily split, we do have a canonical splitting over $E_S(K)$. That is, there is a mapping $E_S(K) \to E^\dagger(K)$ $(P \mapsto \tilde{P})$ such that $\psi(\tilde{P}) = P$, defined as follows. If v is of type I, let $w_v(P)\in\mathcal{O}_v^*$ be the unique unit such that $i_v(w_v(P))$ is the image of P in $E(K_v)$, for $P\in E_S(K)$. Then let $\tilde{P}$ be the unique vector in $E^\dagger(K_p)$ whose entry at v is $w_v(P)$ for all v of type I and is the image of P in $E(K_v)$ for all v of type II.

Now fix $\lambda\colon K^*\backslash\mathbf{A}_K^*/\prod_{v\notin S} U_v\to\mathbf{Q}_p$ a continuous homomorphism, whose local factor at v is denoted by $\lambda_v\colon K_v^*\to\mathbf{Q}_p$.

Proposition. *There is a unique bilinear symmetric pairing*

$$(E^\dagger(K)\otimes\mathbf{Q}_p)\times(E^\dagger(K)\otimes\mathbf{Q}_p)\to\mathbf{Q}_p\qquad [(P,Q)\mapsto\langle P,Q\rangle_\lambda^\dagger]$$

depending only upon $\lambda\colon K^*\backslash\mathbf{A}_K^*\to\mathbf{Q}_p$ and not upon the choice of S (the "extended analytic λ-height") such that, with a_v as above,

$$\langle\tilde{P},\tilde{Q}\rangle_\lambda^\dagger=\langle P,Q\rangle_\lambda\qquad \textit{for}\quad P,Q\in E_S(K)$$

$$\langle a_v,P\rangle_\lambda^\dagger=\lambda_v(w_v(P))/\mathrm{ord}_v(q_v)\qquad \textit{for}\quad v\ \textit{of type}\ \mathrm{I}\quad \textit{and}\quad P\in E_S(K)$$

$$\langle a_v,a_{v'}\rangle_\lambda^\dagger=\begin{cases}\lambda_v(q_v)/\mathrm{ord}_v(q_v), & \textit{if}\ \ v=v'\\ 0, \quad \textit{if}\ \ v\neq v', & \textit{for}\ \ v,v'\ \textit{of type}\ \mathrm{I}.\end{cases}$$

Proof. Straightforward.

Definition. The *λ-sparsity of $E_{/K}$*, $\mathcal{S}_\lambda(E_{/K})$, is defined to be

$$\mathcal{S}_\lambda(E_{/K}):=\det\langle P_i,P_j\rangle_\lambda^\dagger/t^2\in\mathbf{Q}_p,$$

where $P_1,\ldots,P_{r+N}$ is a maximal system of linearly independent points in $E^\dagger(K)$ and t is the index of the subgroup they generate in $E^\dagger(K)$.

One immediately checks that the definition of λ-sparsity is independent of the system $\{P_i\}$ chosen. When $\lambda=\log_p$, put $\mathcal{S}_p(E_{/K}):=\mathcal{S}_\lambda(E_{/K})$. Note that when $N=0$, $\mathcal{S}_\lambda(E_{/K})$ is given by

$$\mathcal{S}_\lambda(E_{/K})=\frac{R_\lambda(E_{/K})}{|E(K)_{\mathrm{tors}}|^2}$$

where $R_\lambda(E_{/K})$ is the discriminant of the lattice $(E(K)/\mathrm{torsion})$ in $E(K)\otimes\mathbf{Q}_p$ computed with respect to the analytic λ-height pairing.

One can also express the λ-sparsity in terms of a slight modification of the analytic λ-height, under certain circumstances:

Definition. Suppose that $\lambda_v(q_v)$ is nonzero for all v of type I. The *Schneider λ-height,*

$$E(K)\times E(K)\to\mathbf{Q}_p,\qquad (P,Q)\mapsto\langle P,Q\rangle_\lambda^{Sch}$$

is then defined to be the bilinear symmetric pairing which for $P,Q\in E_S(K)$ is given by the formula:

$$\langle P,Q\rangle_\lambda^{Sch}:=\langle\tilde{P},\tilde{Q}\rangle_\lambda-\sum_{v\ \mathrm{of\ type\ I}}\frac{\lambda_v(w_v(P))\cdot\lambda_v(w_v(Q))}{\lambda_v(q_v)\cdot\mathrm{ord}_v(q_v)}.$$

Remark. We call this the Schneider height because it is Schneider's "norm-adapted" height [Sch] in the special case where $\lambda_v=\log_p\mathbf{N}_{K_v/\mathbf{Q}_p}$ for $v\,|\,p$. Note that Schneider height and analytic height coincide when λ_v is unramified for all v of type I.

Define $R_\lambda^{Sch}(E_{/K})$ to be the discriminant of the lattice $E(K)$/torsion in $E(K)\otimes\mathbf{Q}_p$ computed with respect to the pairing defined by Schneider λ-height.

Proposition. *Suppose that $\lambda_v(q_v)$ is nonzero for all v of type* I. *Then*

$$\mathscr{S}_\lambda(E_{/K})=\Big(\prod_{v\text{ of type I}}\mathscr{L}_\lambda(E_{/K_v})\Big)\cdot R_\lambda^{Sch}(E_{/K})\cdot|E(K)_{\text{tors}}|^{-2}.$$

Proof. Given a square matrix, with entries in any commutative ring, decomposed into block matrices,

$$M=\begin{bmatrix} A & B\\ C & D\end{bmatrix}$$

where A and D are square matrices, with D invertible, the identity

$$M=\begin{bmatrix} A-BD^{-1}C & BD^{-1}\\ 0 & I\end{bmatrix}\cdot\begin{bmatrix} I & 0\\ C & D\end{bmatrix}$$

shows that $\det(A-BD^{-1}C)\cdot\det D=\det M$. Applying this remark to the block matrix representation for the discriminant of the lattice $E^\dagger(K)$/torsion in $E^\dagger(K)\otimes\mathbf{Q}_p$ computed with respect to the extended analytic height, where the block matrix representation corresponds to the direct sum decomposition

$$E^\dagger(K)\otimes\mathbf{Q}_p=(\mathbf{Z}^N\otimes\mathbf{Q}_p)\oplus(E(K)\otimes\mathbf{Q}_p)$$

(the direct sum decomposition being induced from the canonical lifting of $E_S(K)$ to $E^\dagger(K)$), yields our proposition.

§7. Weil curves

The theory of Weil curves (i.e., elliptic curves E over $\mathbf{Q}$ parametrized by modular functions) has been amply documented [Man, Maz, M-S-D, St]. By definition, a *Weil parametrization* $\pi\colon X_0(N)\to E$ is a mapping defined over $\mathbf{Q}$ such that the pullback of a holomorphic differential of E is a nontrivial multiple of a newform f (on $\Gamma_0(N)$, of weight 2). If E admits a Weil parametrization then it is called a Weil curve. One can always normalize the parametrization to take the cusp ∞ to the origin in E. Changing E by a rational isogeny, if necessary, one can also suppose that the map induced by π on the jacobian of $X_0(N)$ has connected kernel. Now that the isogeny theorem is proved, we know that E is a Weil curve if and only if its Hasse-Weil L-functions $L(E,\chi,s)$ have analytic extensions to the entire complex plane, and possess functional equations of the appropriate type, for all Dirichlet characters χ (or for sufficiently many of them; see [W]). The conjecture of Weil and Taniyama asserts that every elliptic curve over $\mathbf{Q}$ is a Weil curve.

Fix a Weil curve $E_{/\mathbf{Q}}$ and let $f=1\cdot q+a_2q^2+a_3q^3+\dots$ be the newform in $\mathscr{C}(N,\varepsilon,2)$ ($\varepsilon=$ the trivial character) attached to E in the manner described above.

§ 8. Arithmetic invariants of Weil curves

Let $E_{/\mathbf{Z}}$ denote the Néron model of $E_{/\mathbf{Q}}$, and $E_{/\mathbf{F}_p}$ the fiber of $E_{/\mathbf{Z}}$ over $\mathbf{F}_p$. Choose a Néron differential ω_E of $E_{/\mathbf{Q}}$, i.e., a rational differential 1-form on E which specializes to an invariant differential (neither zero nor infinite) on every fiber $E_{/\mathbf{F}_p}$. The choice of Néron differential ω_E is unique, up to sign. If

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \tag{1}$$

is a Weierstrass minimal model for $E_{/\mathbf{Z}}$ ($a_i \in \mathbf{Z}$) then a choice of ω_E is given by $dx/(2y+a_1x+a_3)$.

For each rational prime l denote by $m_l = m_l(E)$ the number of $\mathbf{F}_l$-rational components of the Néron fiber.

Let $E(\mathbf{C})^{\pm}$ denote the ± 1 eigen-subgroups of $E(\mathbf{C})$ under the action of the complex conjugation involution. Thus $E(\mathbf{C})^{+}=E(\mathbf{R})$ and $E(\mathbf{C})^{-}=E'(\mathbf{R})$, where E' is the result of twisting E by $\mathbf{C}/\mathbf{R}$. The choice of ω_E determines (invariant) orientations on $E(\mathbf{C})^{\pm}$ such that the integrals

$$\Omega_E^+ := \int_{E(\mathbf{C})^+} \omega_E \quad \text{and} \quad \Omega_E^- := \int_{E(\mathbf{C})^-} \omega_E$$

are positive, and positive imaginary, respectively.

In the notation of Chap. 1, § 3, let $\lambda(f, z^0; a, m)$ denote the modular symbols attached to f, and $L_f \subset \mathbf{C}$ the "module of integral values". Define:

$$\lambda_E(a,m) = \lambda(f, z^0; a, m) = -\int_{\infty}^{-\frac{a}{m}} f(z)\,dz \in L_f.$$

If $L_f^+ = L_f \cap \mathbf{R}$, $L_f^- = L_f \cap i\mathbf{R}$ then $L_f^+ \cdot \mathbf{Q}$ is a one-dimensional vector space over $\mathbf{Q}$ generated by $\Omega_{E'}^+$ and $L_f^- \cdot \mathbf{Q}$ is one-dimensional generated by Ω_E^-.

We may symmetrize and anti-symmetrize the modular symbols:

$$\lambda_E^{\pm}(a,m) := \lambda_E(a,m) \pm \lambda_E(-a,m) \in L_f^{\pm} \cdot \mathbf{Q}.$$

If ψ is a Dirichlet character, we define the *modular symbol of E twisted by* ψ to be

$$\Lambda_E(\psi) := \sum_{a \bmod m} \psi(a)\,\lambda_E(a,m) = (1/2) \cdot \sum_{a \bmod m} \psi(a)\,\lambda_E^{\mathrm{sign}(\psi)}(a,m),$$

where $m = \mathrm{cond}(\psi)$. Then $\Lambda_E(\psi)$ lies in $L_f^{\mathrm{sign}(\psi)} \cdot \bar{\mathbf{Q}}$.

Let $Ш$ denote the Shafarevich group of $E_{/\mathbf{Q}}$. *We suppose* $Ш$ to be finite; then its order is known to be a perfect square.

§ 9. Exceptional zeros

As before, $E_{/\mathbf{Q}}$ is a Weil curve associated to the newform f on $\Gamma_0(N)$ of weight 2. Suppose p is a prime for which E has either good ordinary reduction, or multiplicative reduction. In either case there is a unique allowable p-root α for f. We shall say that $L_p(E, \psi, s)$ *has an exceptional zero at* $s=1$ if $e_p(\alpha, j, \psi)=0$

where $j=0$. This happens (cf. Chap. I, § 15) if and only if $p \| N$, i.e., the reduction is multiplicative, and $\alpha=\psi(p)$.

We say that $E_{/\mathbf{Q}}$ has *split multiplicative reduction* at p if the connected component of the Néron fiber of E at p is isomorphic to $\mathbf{G}_{m/\mathbf{F}_p}$, i.e., if the cubic curve (1), viewed over $\mathbf{F}_p$, has a node with tangents rational over $\mathbf{F}_p$.

Proposition. *$L_p(E, \psi, s)$ has an exceptional zero at $s=1$ if and only if either:*

(a) *E has split multiplicative reduction at p and $\psi(p)=1$*

or

(b) *E has nonsplit multiplicative reduction at p, and $\psi(p)=-1$.*

If ψ is a quadratic character of conductor prime to p, then $L_p(E, \psi, s)$ has an exceptional zero at $s=1$ if and only if E^{ψ} has split multiplicative reduction at p, where E^{ψ} denotes the twist of E by ψ.

§ 10. The conjecture of Birch and Swinnerton-Dyer, and p-adic analogues

Let $E_{/\mathbf{Q}}$ be a Weil curve. Its Hasse-Weil L-function $L(E, s)$ is then equal to the Mellin transform of the newform f related to E:

$$L(E, s)=L(f, s)$$

and is therefore an entire analytic function. Put

$$L^{(k)}(E):=(1/k!)\cdot \frac{d^k}{ds^k} L(E, s)|_{s=1}.$$

The classical conjecture reads:

Conjecture ($BSD(\infty)$).

(i) $L^{(k)}(E)=0$ *for* $k<r=\operatorname{rank} E(\mathbf{Q})$.

(ii) $L^{(r)}(E)=|Ш(E_{/\mathbf{Q}})|\cdot \dfrac{R_{\infty}(E_{/\mathbf{Q}})}{|E(\mathbf{Q})_{\text{tors}}|^2}\left(\prod_l m_l\right)\Omega_E^{+}$,

where $R_{\infty}(E_{/\mathbf{Q}})$ is the classical regulator of E, i.e., the discriminant of the lattice $(\mathrm{E}(\mathbf{Q})/\text{torsion})$ in $E(\mathbf{Q})\otimes\mathbf{R})$ computed via the (classical) canonical height pairing.

Now let p be a prime of good, ordinary reduction for E, or a prime such that the Néron fiber $E_{/\mathbf{F}_p}$ is multiplicative (equivalently, $p \| N$). Let α denote the unique allowable p-root for f. Define, for Dirichlet characters ψ:

$$L_p(E, \psi, s):=L_p(f, \alpha, \psi, s-1)$$

and, if $\psi=1$, put $L_p(E, \psi, s)=L_p(E, s)$.

Let $L_p^{(k)}(E, \psi):=(1/k!)\dfrac{d^k}{ds^k} L_p(E, \psi, s)|_{s=1}$, and again if $\psi=1$ put $L_p^{(k)}(E, \psi)=L_p^{(k)}(E)$.

The p-adic analogue of the classical Birch-Swinnerton-Dyer conjecture is the following:

Conjecture ($BSD(p)$). I. (*Nonexceptional case*). *If* $\alpha \neq 1$, *i.e., if* E *has good ordinary or non-split multiplicative reduction at* p, *then:*

(i) $L_p^{(k)}(E)=0$ *for* $k<r=\operatorname{rank} E(\mathbf{Q})$

and

(ii) $L_p^{(r)}(E)=\left(1-\frac{1}{\alpha}\right)^b \cdot |Ш(E_{/\mathbf{Q}})| \cdot \mathscr{S}_p(E_{/\mathbf{Q}}) \cdot (\prod_l m_l)\, \Omega_E^+,$

where

$$b=\begin{cases} 2 \text{ if } E \text{ has good reduction at } p \\ 1 \text{ if } E \text{ has non-split multiplicative reduction at } p. \end{cases}$$

II. (*Exceptional case*). *If* $\alpha=1$, *i.e., if* E *has split multiplicative reduction at* p, *then:*

(i) $L_p^{(k)}(E)=0$ *for* $k<r+1$

and

(ii) $L_p^{(r+1)}(E)=|Ш(E_{/\mathbf{Q}})| \cdot \mathscr{S}_p(E_{/\mathbf{Q}}) \cdot (\prod_l m_l)\, \Omega_E^+.$

Remarks. The p-adic sparsity $\mathscr{S}_p(E_{/\mathbf{Q}})$ is conjectured to be nonzero, so that in either of the above cases the quantity in formula (ii) is conjecturally nonzero. The factor $\left(1-\frac{1}{\alpha}\right)^b$ is just the p-adic multiplier $e_p(\alpha, j, \psi)$ with $j=0$ and $\psi=1$. Hence, when $r=0$ and we are not in the exceptional case, $BSD(p)$ is equivalent to $BSD(\infty)$ by Chap. I, § 14. If, however, $r>0$, or if we are in the exceptional case, $BSD(p)$ is not implied by $BSD(\infty)$. If we are in the exceptional case, and, as is conjectured, $\mathscr{L}_p(E_{/\mathbf{Q}_p})$ doesn't vanish, then Schneider's height pairing is defined (cf. end of §6), and the right-hand side of (ii) can be expressed in terms of it, giving us an alternate expression for the conjectured formula (ii):

Conjecture $BSD(p)$*-exceptional case:*

(i) $L_p^{(k)}(E)=0$ *for* $k<r+1$

and

(ii) $L_p^{(r+1)}(E)=\mathscr{L}_p(E_{/\mathbf{Q}_p}) \cdot |Ш(E_{/\mathbf{Q}})| \dfrac{R_p^{Sch}(E_{/\mathbf{Q}})}{|E(\mathbf{Q})_{\text{tors}}|^2} (\prod_l m_l)\, \Omega_E^+.$

It is a theorem of Cassel's that $BSD(\infty)$ is stable under $\mathbf{Q}$-rational isogeny of F in the sense that the right-hand side of the conjectured equality (ii) does not change if E is replaced by an elliptic curve which is $\mathbf{Q}$-isogenous to E (the left-hand side clearly doesn't change). It follows as an easy exercise that $BSD(p)$ is likewise stable under $\mathbf{Q}$-rational isogeny of E. It is also the case that the p-adic and classical Birch-Swinnerton-Dyer conjectures are compatible with the conjectures given in Chap. I, § 16 on orders of vanishing.

Note also that $BSD(p)$ is "homogeneous" in the choice of logarithm, in the following sense: The right-hand-side of (ii) depends inherently on our having chosen $\log_p$ for λ. Had we chosen $\lambda=c\cdot\log_p$ instead (for c some arbitrary constant), the right-hand-side would change by the multiplicative factor c^r in the nonexceptional case and c^{r+1} in the exceptional case. But the left-hand-sides are similarly homogeneous in the choice of logarithm, and of the same degree, for:

$$L_p^{(k)}(E) = \int_{\mathbf{Z}_p^*} (\log_p x)^k \, d\mu_{f,\alpha}(x)$$

where k is any positive integer, and f is the newform associated to the Weil curve E, and the notation is as in Chap. I, § 11.

The reader might also wonder what justification there is in putting the "same" p-adic multiplier in the formula, irrespective of the size of r, as if the p-adic multiplier acts as an Euler factor. We see little theoretical justification since we are rather perplexed by the p-adic multiplier; it is just what seems to work in our numerical experiments.

§ 11. Twisted conjectures

We retain the hypotheses and notation of § 10.

Now let ψ be a Dirichlet character attached to a quadratic number field of discriminant D.

Let $E^{\psi}_{/\mathbf{Q}}$ denote the elliptic curve over $\mathbf{Q}$ twisted by the quadratic character ψ. Thus we have a canonical isomorphism between E and E^{ψ} over the quadratic field to which the character ψ belongs.

We make the following

Hypothesis on D. The prime p does not divide D, and we can write $N = QQ'$ with $(Q, D) = 1$, and $Q' \mid D$.

Then, by the remark after (18.3) in Chap. I, f_{ψ} is a newform of level $Q|D|^2$. Hence E^{ψ} is a Weil curve belonging to the form f_{ψ}. (Now that the isogeny theorem is proved, this is obvious.) Consequently, by the proposition at the end of § 13 of Chap. I we have

$$L_p(E, \psi, s) = \langle |D| \rangle^{s-1} \psi(-1) \, \tau(\psi) \, L_p(E^{\psi}, s).$$

Therefore, for $k \leqq$ the order of zero of $L_p(E^{\psi}, s)$ at $s = 1$, we have

$$L_p^{(k)}(E, \psi) = \psi(-1) \, \tau(\psi) \, L_p^{(k)}(E^{\psi}). \tag{1}$$

On the other hand, if we identify $E_{/\mathbf{C}}$ and $E^{\psi}_{/\mathbf{C}}$ by means of the canonical isomorphism between E and E^{ψ} which is defined over $\mathbf{Q}(\sqrt{D})$, then

$$E^{\psi}(\mathbf{C})^{\pm} = E(\mathbf{C})^{\pm(\operatorname{sign}\psi)}.$$

Moreover, a Néron differential on E^{ψ} is given by

$$\omega_{E^{\psi}} = \frac{\eta}{\sqrt{D}} \, \omega_E, \tag{2}$$

where η (made explicit at the end of this section) is either 1 or 2 and where by $\sqrt{D}$ we mean the positive or positive imaginary square root. The real period of E^{ψ} is given by:

$$\Omega^{+}_{E^{\psi}} = \frac{\eta}{\sqrt{D}} \, \Omega_E^{\operatorname{sign}\psi}. \tag{3}$$

If α is the unique allowable p-root for E, then that for E^{ψ} is

$$\alpha(E^{\psi}) = \psi(p)\,\alpha. \tag{4}$$

Finally, recalling the fact that

$$\tau(\psi) = \sqrt{D}, \tag{5}$$

which (cf. [H], §58) is equivalent to the classical quadratic reciprocity law, together with (5) for prime D's, we find

Proposition. *The conjecture $BSD(p)$ for E^{ψ} is equivalent to the following*

Conjecture ($BSD(p, \psi)$). *Let* $r^{\psi} = \operatorname{rank}(E^{\psi}(\mathbf{Q}))$. *Then*

I. (*Nonexceptional case*). *If* $\psi(p) \neq \alpha$, *then*

(i) $L_p^{(k)}(E, \psi) = 0$ *for* $k < r^{\psi}$

and

(ii) $$L_p^{(r^{\psi})}(E, \psi) = \eta \cdot \left(1 - \frac{\psi(p)}{\alpha}\right)^b |Ш(E^{\psi}_{/\mathbf{Q}})|\, \mathscr{S}_p(E^{\psi}_{/\mathbf{Q}}) (\prod_l m_l(E^{\psi})) \cdot \Omega_E^{\operatorname{sign}(\psi)},$$

where

$$b = \begin{cases} 1, & \text{if } E^{\psi} \text{ has non-split multiplicative reduction at } p \\ 2, & \text{if } E \text{ has good ordinary reduction at } p. \end{cases}$$

II. (*Exceptional case*). *If* $\psi(p) = \alpha$, *then*

(i) $L_p^{(k)}(E, \psi) = 0$ *for* $k < r^{\psi} + 1$

and

(ii) $$L_p^{(r^{\psi}+1)}(E, \psi) = \eta \cdot |Ш(E^{\psi}_{/\mathbf{Q}})| \cdot \mathscr{S}_p(E^{\psi}_{/\mathbf{Q}}) \cdot \prod_l m_l(E^{\psi}) \cdot \Omega_E^{\operatorname{sign}(\psi)},$$

where η *is as given below.*

We have $\eta = 1$ unless D is even. If D is even and E has semi-stable reduction at 2, then $\eta = 1$ unless $8 \mid D$ and the coefficient a_1 in formula (1) of §8 is even, in which case $\eta = 2$. If D is even and E is additive at 2, we think $\eta = 2$.

§12. Numerical evidence

We have accumulated numerical evidence for the twisted conjecture $BSD(p, \psi)$ by studying the curve $E = X_0(11)$, with equation $y^2 + y = x^3 - x^2 - 10x - 20$ over $\mathbf{Z}$. For each of the primes $p = 3$, 5, and 11, we approximated both sides of the conjectured equalities mod small powers of p for 27 quadratic characters ψ such that $r^{\psi} = 1$ and 2 characters such that $r^{\psi} = 2$. Both 3 and 5 are primes of ordinary reduction for E, while 11 is a prime of multiplicative reduction, so that both the exceptional and non-exceptional cases were covered. We also computed $L_{11}(1, \psi)$ for 9 characters which have $r^{\psi} = 0$, but which fall under the exceptional case.

The accuracy levels for which we verified the conjectures are listed in Table 12.1. An accuracy level of n means that the *ratio* of the two sides of the conjectured equality in $BSD(p, \psi)$ is in fact a unit $\equiv 1 \bmod p^n$ – with the following two caveats. First, we assumed throughout that $|Ш(E^{\psi}/\mathbf{Q})|=1$. Second, where a height regulator was involved we computed it with respect to a set of points of small naive height listed in Table 12.2. In view of the conjectures, we take the data as evidence that our points are generators and the Ш's involved are trivial.

Some of our calculations were done on $X_0(11)$, some on $X_1(11)$ as indicated in the tables – this is because points of small height were more

Table 12.1. Accuracy levels

Prime	Conductor (ψ)	r^{ψ}	Case	Accuracy level
11	5, 37, 53, 56, 60, 69, 89, 97, 104	0	exceptional	2
3, 5, 11	−7, −8, −19, −24 −39, −40, −43, −52 −68, −79, −95, −127	1	exceptional if $p=11$ non-exceptional if $p=3, 5$	$p=11:2$ $p=3:3$; $p=5:2$
3, 5, 11	8, 13, 17, 21, 24, 28, 33 41, 44, 57, 65, 73, 76, 77, 88	1	non-exceptional	2
3, 5, 11	−47, −103	2	non-exceptional	2

Table 12.2a. Height data

Our elliptic curve $E=X_0(11)$ is given by the equation $y^2=4x^3-4x^2-40x-79$, $\omega=\frac{dx}{y}$ and we have twisted E by the thirteen quadratic characters ψ listed.

In each instance, the rank r^{ψ} of the twisted curve is 1. We tabulate the x-coordinate of a rational point P (a presumed generator) and compute its λ-height $\langle P, P\rangle_{\lambda}$ to an accuracy level of 3, where $\lambda(x)=\frac{1}{p}\log_p(x)$. We have done this for $p=3, 5, 11$ in the tabulated instances below. [We use that, for $p=3$, $e_2(X_0(11),\omega)\equiv -37 \bmod 81$ and, for $p=5$, $e_2(X_0(11),\omega)\equiv -23 \bmod 125$].

HEIGHT $=\langle P, P\rangle_{\lambda}$ to accuracy 3

Conductor of ψ	$x(P)$	$p=3$	$p=5$	$p=11$ (Exceptional case)
− 7	− 6	23/9	83/5	779
− 8	− 1/2	22	143/5	748
− 19	9/4	20/9	−23/5	536
− 24	−25/6	−31	−28/5	824
− 39	− 7/3	−35	−36/5	101
− 40	39/10	−22/9	−38/5	320
− 43	69/16	−19/9	33/5	557
− 52	−57/4	8/9	42/5	709
− 68	−13/4	−24	−27/5	196
− 79	0	38/9	97	1109
− 87	4/3			872
− 95	−41/5	−31	47/5	
−127	3	−31/9	25 · 78	

Table 12.2b. Height data

$E = X_1(11)$: $y^2 = 4x^3 - 4x - 1$; $\omega = dx/y$; $\lambda(x) = \frac{1}{p}\log_p(x)$;

$$e_2(X_1(11), \omega) \equiv \begin{cases} -22 \bmod 81 \\ 47 \bmod 125 \end{cases} \qquad r^{\psi} = 1$$

Height $= \langle P, P \rangle_\lambda$

Conductor of ψ	$x(P)$	$p=3$ (accuracy 4)	$p=5$ (accuracy 2)	$p=11$ (accuracy 2)
8	1/2	13/9	11	81
13	1/4	40	13	59
17	2	37/9	20	58
21	−5/12	29	4/5	14
24	1/6	18	9/5	48
28	3/4	33	16	63
33	−1/3	27	2	18
41	5/4	34/9	8/5	73
44	−1/4	38/9	21/5	88
57	1/3	51	6	71
65	−2/5	67/9	4	113
73	3	25	22	87
77	17/4	−17/9	0	65
88	3/2	22/9	24	24

Table 12.2c. Height data

Curve $E = X_0(11)$; $r_\psi = 2$. See 12.2a for further information.

$$R = \begin{pmatrix} \langle P, P \rangle_\lambda & \langle P, Q \rangle_\lambda \\ \langle P, Q \rangle_\lambda & \langle Q, Q \rangle_\lambda \end{pmatrix}$$

Conductor of ψ	Points P, Q on E^{ψ}	$p=3$ (accuracy $=3$)	$p=5$ (accuracy $=2$)	$p=11$ (accuracy $=2$)
−47	$x(P)$: −1 $x(Q)$: −2	$R = \begin{pmatrix} 18 & 13 \\ 13 & 15 \end{pmatrix}$ det $R = 20$	$R = \begin{pmatrix} 14 & 2 \\ 2 & 12 \end{pmatrix}$ det $R = 14$	$R = \begin{pmatrix} 58 & 67 \\ 67 & 5 \end{pmatrix}$ det $R = 36$
−103	$x(P) = -3$ $x(Q) = -36$	$R = \begin{pmatrix} 8/9 & -13/9 \\ -13/9 & -2/9 \end{pmatrix}$ det $R = -11/9$	$R = \begin{pmatrix} 17 & 15 \\ 15 & 17 \end{pmatrix}$ det $R = 14$	$R = \begin{pmatrix} 30 & 51 \\ 51 & 64 \end{pmatrix}$ det $R = 45$

common on one curve or the other, depending on ψ. Of course, the two curves are isogenous, so their L-functions are identical. The techniques for making the computations are implicit in the discussion of height in II.1–5 and all the results are listed in Tables 12.2a, b, and c. In those tables, an "accuracy n" means that the *ratio* of the tabulated height (or regulator in case c) to the true height (or regulator) is a unit congruent to 1 modulo p^n. In those tables we use the same "x-coordinate" to describe points P (up to sign, which is all that matters for heights) on an elliptic curve $y^2=4x^3+ax^2+bx+c$ and on all of its twists $Dy^2=4x^3+ax^2+bx+c$ by quadratic extensions $\mathbf{Q}(\sqrt{D})$; the D is listed under "conductor of ψ" in the tables.

§ 13. The p-adic exceptional zero conjecture (preliminary version)

In the exceptional case when $r=0$ one can put the p-adic conjecture $BSD(p)$ together with the classical $BSD(\infty)$ to produce a conjectural formula linking modular symbols to the multiplicative period $q_p=q_p(E)$. One is led to the following.

Exceptional zero conjecture (for Weil curves)

Let $E_{/\mathbf{Q}}$ be a Weil curve and p a prime of split multiplicative reduction for E. For any Dirichlet character ψ of conductor prime to p and such that $\psi(p)=1$, we have:

$$L_p^{(1)}(E,\psi)=\mathscr{L}_p(E_{/\mathbf{Q}_p})\cdot \Lambda_E(\psi).$$

In this case, the left-hand side of the above conjectured equality can be expressed quite simply as a limit, leading to the following equivalent conjecture (under the same hypotheses).

Conjecture 1. For $M=\operatorname{cond}(\psi)$ *we have*

$$\lim_{(n\to\infty)} \sum_{a \bmod p^n M} \psi(a)\log_p(a)\,\lambda_E(a,p^nM)=\mathscr{L}_p(E_{/\mathbf{Q}_p})\cdot \sum_{a \bmod M} \psi(a)\,\lambda_E(a,M).$$

The remarkable nature of the above conjecture is that the modular symbols λ_E are computed as path integrals on a Riemann surface which provides a *complex analytic modular parametrization* of E, while the term $\mathscr{L}_p(E_{/\mathbf{Q}_p})$ is a p-adic number (presumably even transcendental) obtained from the *p-adic uniformization* of E.

For a numerical example, we may return to the curve $X=X_0(11)$ discussed in § 12 whose multiplicative period q_{11} is computed to be $11^5\cdot 8744$ (cf. § 3). One finds

$$\mathscr{L}_{11}(E_{/\mathbf{Q}_{11}})\equiv 11\cdot 547 \bmod 11^4.$$

Now define

$$\sigma_E^+(a,m)=\lambda_E^+(a,m)/\Omega_E^+,\qquad \sigma_E^-(a,m)=\lambda_E^-(a,m)/\Omega_E^-,$$

so that $\sigma_E^\pm(a,m)$ are rational numbers of bounded denominator and are 11-adically integral.

Conjecture 1 can be verified to "2 significant 11-adic places" (for our given E, p, and ψ) if we can establish the following congruence mod 11^2.

Conjecture 2

$$\sum_{a' \bmod 11^5 M} \psi(a')[\log_{11}(a')/11]\,\sigma_E^{\mathrm{sign}(\psi)}(a', 11^5\cdot M)$$
$$\equiv 547\cdot \sum_{a \bmod M} \psi(a)\,\sigma_E^{\mathrm{sign}(\psi)}(a, M) \mod 11^2$$

where $\psi(11)=1$ *and* $M=\mathrm{cond}(\psi)$.

We have established this congruence for the 9 quadratic characters associated to the quadratic fields of discriminant D, where $D=5$, 37, 53, 56, 60, 69, 89, 97, and 104. (Compare the case $r^{\psi}=0$ of § 12).

§ 14. The p-adic "exceptional zero conjecture" (more general version)

Let f be a newform in $\mathscr{C}(N, \varepsilon, 2)$. Let p be a prime number such that $p \| N$ and the character ε has conductor prime to p. Assume (for simplicity) that ε is real. Let $A_{f/\mathbf{Q}}$ be the abelian subvariety of the jacobian of $X_1(N)_{/\mathbf{Q}}$ attached to the newform f (cf. [Sh], Theorem 7.14). Then it is known that A_f has purely multiplicative reduction at p (that is, the Néron model of A_f over the base $\mathbf{Z}_p$ has a special fibre whose connected component is a torus over $\mathbf{F}_p$. This follows easily from [D-R] VI Theorem 6.9 and Raynaud's Theorem (cf. [Ra] or [M-W], Chap. 2, Prop. 1). We may use the theory of [McC, Mo] to obtain an analytic parametrization of $A=A_f$ and of its dual $B=B_f$. Namely, there is a Galois pairing (determined up to canonical isomorphism)

$$X\times Y \xrightarrow[j]{} \bar{\mathbf{Q}}_p^*,$$

where X and Y are free abelian groups of finite rank on which $G=\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ operates, and where j is a bi-multiplicative mapping such that the composition $\mathrm{ord}_p\circ j$ tensored with $\mathbf{Q}$ gives a perfect duality of finite-dimensional $\mathbf{Q}$-vector spaces

$$X\otimes\mathbf{Q}\times Y\otimes\mathbf{Q} \xrightarrow{(\mathrm{ord}_p\circ j)} \mathbf{Q} \tag{1}$$

and, moreover, such that there is a pair of exact sequences of G-modules

$$0\to X\to \mathrm{Hom}(Y, \bar{\mathbf{Q}}_p^*) \xrightarrow[t_A]{} A(\bar{\mathbf{Q}}_p)\to 0$$
$$0\to Y\to \mathrm{Hom}(X, \bar{\mathbf{Q}}_p^*) \xrightarrow[t_B]{} B(\bar{\mathbf{Q}}_p)\to 0$$

where the unlabelled maps with domain X and Y in the above diagram are induced by j.

Now let $\mathbf{T}_f\subseteq\mathrm{End}(A_{f/\mathbf{Q}})$ denote the subring generated by the Hecke operators T_l (all l). By functoriality, $\mathbf{T}_f$ operates on the $\mathbf{Z}$-modules X and Y in a manner compatible with the pairing j. That is,

$$j(\tau x, y)=j(x, \tau y), \quad \text{for } \tau\in\mathbf{T}_f.$$

Let $F=\mathbf{T}_f\otimes\mathbf{Q}$ be the algebraic number field generated by the Hecke operators. Then the $\mathbf{Q}$-vector spaces $X\otimes\mathbf{Q}$ and $Y\otimes\mathbf{Q}$ are naturally endowed with the structure of F-vector spaces, of dimension one over F. The nondegenerate pairing (1) induces an isomorphism of (1-dimensional) F-vector spaces

$$\alpha: Y \otimes \mathbf{Q} \to \mathrm{Hom}(X \otimes \mathbf{Q}, \mathbf{Q}).$$

Now let $F_p = F \otimes \mathbf{Q}_p$; it is a finite product of local fields. The $\mathbf{Q}_p$-modules $X \otimes \mathbf{Q}_p$ and $Y \otimes \mathbf{Q}_p$ are free F_p-modules of rank 1. Consider the composition of the pairing j with $\log_p$; it induces a bilinear pairing,

$$(X \otimes \mathbf{Q}_p) \times (Y \otimes \mathbf{Q}_p) \to \mathbf{Q}_p$$

an hence a homomorphism of F_p-modules (free of rank 1)

$$\beta_p: Y \otimes \mathbf{Q}_p \to \mathrm{Hom}_{\mathbf{Q}_p}(X \otimes \mathbf{Q}_p, \mathbf{Q}_p).$$

Let $\alpha_p = \alpha \otimes 1: Y \otimes \mathbf{Q}_p \to \mathrm{Hom}_{\mathbf{Q}_p}(X \otimes \mathbf{Q}_p, \mathbf{Q}_p)$.

Since α_p is an isomorphism, there is a unique element in F_p, call it $\mathscr{L}_p(f) \in F_p$, such that

$$\beta_p = \mathscr{L}_p(f) \cdot \alpha_p.$$

By construction, $\mathscr{L}_p(f)$ (the *$\mathscr{L}$-invariant of the modular form f*) is seen to lie naturally in $F_p = \mathbf{T}_f \otimes \mathbf{Q}_p$ and depends only upon the newform f.

The mapping of Hecke operators to their eigenvalues ($T_l \mapsto a_l$) establishes an imbedding of $\mathbf{T}_f$ in $\bar{\mathbf{Q}}$. Composing this imbedding with the imbedding $\bar{\mathbf{Q}} \xrightarrow{\iota} \mathbf{Q}_p$ fixed in Chap. 1, § 11 provides a homomorphism $F_p \to \mathbf{C}_p$. Let $\mathscr{L}_p^{\iota}(f) \in \mathbf{C}_p$ denote the image of $\mathscr{L}_p(f)$ under this homomorphism.

Exceptional zero conjecture (for newforms of weight 2)

Let f be a newform of weight 2 on $\Gamma_0(N)$ with character ε such that ε is real and $\mathrm{cond}(\varepsilon)$ is prime to p. Suppose $p \| N$. Let ψ be a finite Dirichlet character of conductor M prime to p such that $e_p(\alpha, 0, \psi) = 0$, where $\alpha = a_p$ is the unique allowable p-root for f, and such that N has a factorization $N = QQ'$ with $(Q, M) = 1$ and $Q' | M$, and such that $\varepsilon_{Q'} \psi^{-1}$ has conductor M. Then:

$$L_p'(f, \alpha, \psi, s)|_{s=0} = \mathscr{L}_p^{\iota}(f) \cdot \sum_{\substack{a \bmod M \\ M = \mathrm{cond}(\psi)}} \psi(a) \cdot \lambda(f, z^0; a, M).$$

Remark. The above conjecture implies that when $k = 2$ the exceptional zero is of local type (cf. Chap. I, § 19).

§ 15. Are there $\mathscr{L}$-invariants attached to modular forms of higher weight?

The $\mathscr{L}$-invariant $\mathscr{L}_p^{\iota}(f)$ defined in the previous section depends only upon the p-adic representation, $\rho_p(f)$, of $\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ attached to f. In fact, the crucial property required of the p-adic representation $\rho_p(f)$ in order that $\mathscr{L}_p^{\iota}(f)$ be defined is that it be a two-dimensional p-adic representation whose image is contained in a Borel subgroup of $GL_2(\mathbf{C}_p)$.

There are, however, a number of examples of cuspidal newforms f of even weight $k \geqq 4$ whose p-adic L-function possesses an exceptional zero (at the central point) and yet whose attached local $(\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p))$ representation does not factor through a Borel subgroup. Indeed, an idea of Serre enables one to easily produce examples where the image of the inertial subgroup under $\rho_p(f)$ is an open subgroup in $GL_2(\mathbf{Z}_p)$. We shall provide a small list of such examples below. The disparity between weight 2 and even weights $k \geqq 4$ seems all the greater insofar as we have *no* example of the above type for weight $k \geqq 4$ where $\rho_p(f)$ *does* factor through a Borel subgroup. We are led to ask the question which forms the title of this section, despite the fact that the definition of $\mathscr{L}_p(f)$ which we have given in the case of weight 2 does not seem to generalize to higher weights, because we have amassed numerical data in support of the following version of the *Exceptional Zero Conjecture for newforms of weight two* (§ 14), already alluded to in Chap. I, § 19.

Exceptional zero conjecture (for newforms of even weight)

Let f be a newform of even weight $k \geqq 2$ on $\Gamma_0(N)$ with character ε such that ε is real and $\mathrm{cond}(\varepsilon)$ is prime to p. Suppose $p \| N$.

Then there is a nonzero element $\mathscr{L}_p^{\iota}(f) \in \mathbf{C}_p$ such that *for all* finite Dirichlet characters ψ which have the property that:

(*) $e_p(\alpha, (k-2)/2, \psi) = 0$, where $\alpha = a_p$ is the unique allowable p-root for f,

we have:

$$L'_p(f, \alpha, \psi, s)|_{s=(k-2)/2} = \mathscr{L}_p^{\iota}(f) \cdot \sum_{a \bmod M} \psi(a) \cdot \lambda(f, z^{(k-2)/2}; a, M).$$

Note that this conjecture is, of course, weaker than the corresponding conjecture made in § 14 for weight 2 forms, insofar as *we have no conjectural interpretation* of the local factor $\mathscr{L}_p^{\iota}(f)$ if $k \geqq 4$. The strength of the above conjecture lies in the fact that it is required to hold for all characters ψ satisfying (*). If there is one such character, there are an infinity of them, and consequently we can test the conjecture by finding a single such character ψ_0 for which

$$\sum_{a \bmod M} \psi_0(a)\, \lambda(f, z^{(k-2)/2}; a, M)$$

is nonzero, and then by *defining* $\mathscr{L}_p^{\iota}(f)$ to be such that the above conjecture holds for $\psi = \psi_0$. We have done precisely this in the following instances. For $p = 3$, $f = \eta(\tau)^6 \eta(3\tau)^6$, $k = 6$, and quadratic characters of conductors 7, 10, 13, 19, 22, 31, 34, and 37, take $\mathscr{L}_3(f) \equiv 3 \cdot 44 \bmod 3^5$. For $p = 5$, $f = \eta(\tau)^4 \eta(5\tau)^4$, $k = 4$ and quadratic characters of conductors -2, -3, -7, -13, -17, and -22, take $\mathscr{L}_5(\mathrm{f}) \equiv \dfrac{31372}{5} \bmod 5^7$.

Examples where the image of inertia is large

Let f be a cuspidal newform with Fourier coefficients in $\mathbf{Z}$. Let us say that f is *inertially large at* p if the image of the inertia group at p under $\rho_p(f)$ is an open subgroup of $GL_2(\mathbf{Z}_p)$.

In [S2], Serre showed why $\omega_{12}=\Delta$ is inertially large at p for $p \leqq 7$. Serre's argument applies immediately to show that the newforms $f=\omega_k$ (cf. Chap. I, § 12) are inertially large at p for the following values of k and p:

k	p						
12	2	3	5	7			
16	2	3	5	7	11		
18	2	3	5	7	11	13	
20	2	3	5	7	11	13	
22	2	3	5	7	13	17	
26	2	3	5	7	11	17	19

More germane to the discussion above is the fact that his argument also applies in the following three instances:

k	f	$p=N$	ε
4	$\omega_4=(\eta\eta_5)^4$	5	1
6	$\omega_6=(\eta\eta_3)^6$	3	1
8	$\omega_8=(\eta\eta_2)^8$	2	1

and with a bit of work it can be made to apply for the primes $p=2$ and 3 to the case of

$$f=(\eta\eta_2\eta_3\eta_6)^2$$

which is a cuspidal newform of weight 4 on $\Gamma_0(6)$, $\varepsilon=1$.

For these example, then, we are at a loss to provide (even conjecturally) a 'local' definition of $\mathscr{L}'_p(f)$.

References

[A] Arnaud, B.: Interpolation p-adique d'un produit de Rankin. University of Orsay, 1984 (Preprint)

[A-V] Amice, Y., Vélu, J.: Distributions p-adiques associées aux séries de Hecke. Astérisque, No. 24/25. Soc. Math. Fr., Paris, 119–131 (1975)

[A-L] Atkin, O., Li, W.: Twists of newforms and pseudo-eigenvalues of W-operators. Invent. Math. **48**, 221–243 (1978)

[D-R] Deligne, P., Rapoport, M.: Schémas de modules de courbes elliptiques. Lect. Notes Math., vol. 349. Berlin-Heidelberg-New York: Springer 1973

[H] Hecke, E.: Vorlesungen über die Theorie der algebraische Zahlen. New York: Chelsea 1948

[I] Iwasawa, K.: Lectures on p-adic L-functions. Ann. Math. Stud., vol. 74. Princeton: Princeton University Press 1972

[K] Katz, N.: p-adic properties of modular schemes and forms. In: Modular Functions of One Variable, III. Lect. Notes Math., vol. 350, pp. 69–191. Berlin-Heidelberg-New York: Springer 1973

[La] Lang, S.: Elliptic Functions. Reading, MA: Addison-Wesley 1973

[L-T] Lang, S., Trotter, H.: Frobenius Distributions in GL_2-Extensions. Lect. Notes Math., vol. 504. Berlin-Heidelberg-New York: Springer 1976

[L] Li, W.: Newforms and functional equations. Math. Ann. **212**, 285–315 (1975)

[Man] Manin, J.: Parabolic points and zeta functions of modular curves. Izv. Akad. Nauk SSSR (AMS translation) **6**(1) 19–64 (1972)

[Maz] Mazur, B.: Courbes elliptiques et symboles modulaires. Sémin. Bourbaki exp. No. 414; Lect. Notes Math., vol. 317. Berlin-Heidelberg-New York: Springer 1973

[M-S-D] Mazur, B., Swinnerton-Dyer, P.: Arithmetic of Weil curves. Invent. Math. **25**, 1–61 (1974)

[M-T1] Mazur, B., Tate, J.: The p-adic sigma function. (In preparation)

[M-T2] Mazur, B., Tate, J.: Canonical Height Pairings via Biextensions. In: Arithmetic and Geometry, Progr. Math., vol. 35, pp. 195–237. Boston-Basel-Stuttgart: Birkhäuser 1983

[M-W] Mazur, B., Wiles, A.: Class fields of abelian extensions of **Q**. Invent. Math. **76**, 179–330 (1984)

[M^{c}C] M^{c}Cabe, J.: p-adic Theta Functions. Harvard Ph.D. Thesis 1968

[Mo] Morikawa, H.: On theta functions and abelian varieties over valuation fields of rank one, I and II. Nagoya Math. J. **20**, 1–27 and 231–250 (1962)

[N] Norman, P.: p-adic theta functions. Am. J. Math. **107**, 617–661 (1985)

[O] Ogg, A.: On the eigenvalues of Hecke operators. Math. Ann. **179**, 101–108 (1969)

[P] Panciskin, A.: Le prolongement p-adique analytiques des fonctions L de Rankin. C.R. Acad. Sci. Paris, I **295**, 51–53 and 227–230 (1982)

[P-R] Perrin-Riou, B.: Descente infinie et hauteur p-adique sur les courbes elliptiques à multiplication complexe. Invent. Math. **70**, 369–398 (1983)

[Ra] Raynaud, M.: Spécialisation du foncteur de Picard. Publ. Math. I.H.E.S. **38**, 27–76 (1970)

[R] Roquette, P.: Analytic theory of elliptic functions over local fields. Hamb. Math. Einzelschriften, Neu Folgen, Heft 1, 1970

[Sch] Schneider, P.: p-adic heights. Invent. Math. **69**, 401–409 (1982)

[S] Serre, J.-P.: Quelques applications de théorème de densité de Chebotarev. I.H.E.S. Publ. Math. **54**, 323–401 (1981)

[S2] Serre, J.-P.: Une interprétation des congruences relatives à la fonction τ de Ramanujan. Séminaire Delange-Pisot-Poitou: Théorie des nombres Exposé 14 (1967/68)

[S3] Serre, J.-P.: Sur la lacunarité des puissances de η. Glasgow Math. J. **27**, 203–221 (1985)

[Sh] Shimura, G.: Introduction to the arithmetic theory of automorphic forms. Publ. Math. Soc. Japan, vol. 11. Iwanami. Shoten and Princeton Univ. Press 1971

[St] Stevens, G.: Arithmetic on Modular Curves. Progr. Math., vol. 20. Boston-Basel-Stuttgart: Birkhäuser 1982

[V] Vishik, M.: Nonarchimedean measures connected with Dirichlet series. Math. USSR Sb. **28**, 216–228 (1976)

[W] Weil, A.: Uber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. Math. Ann. **168**, 149–156 (1967); (Oeuvres, vol. III, pp. 165–172)

Oblatum 5-VII-1985