Modular Symbols and p-adic L-functions

Karim Belabas, Bernadette Perrin-Riou

after Pollack and Stevens

Acknowledgements

This talk is expository with little original content. I am closely following papers and talks by Bernadette Perrin-Riou, Robert Pollack and Glenn Stevens.

Modular curves

Let $G \subset \mathrm{PSL}_2(\mathbb{Z})$ be a subgroup of finite index. It acts on Poincaré's upper half plane $\mathfrak{h} := \{z \in \mathbb{C}\colon\ \mathrm{Im}\, z > 0\}$ by fractional linear transformations:

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z := \frac{az+b}{cz+d},$$

as well as on its boundary, the real projective line $\mathbb{P}^1(\mathbb{R})$

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot (p:q) := \frac{ap+bq}{cp+dq}.$$

N.B. We identify the point at infinity $(1:0)$ with $i\infty$ on the Riemann sphere.

Let $\mathfrak{h}^* = \mathfrak{h} \cup \mathbb{P}^1(\mathbb{Q})$ be the completed upper half plane. The quotient space $G\backslash\mathfrak{h}$ is compactified by adding a finite number of *cusps* from $G\backslash\mathbb{P}^1(\mathbb{Q})$. The result is the *modular curve* $X(G) = G\backslash\mathfrak{h}^*$, a compact Riemann surface.

Motivating example:

$$G = \Gamma_0(N) := \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})\colon c \equiv 0 \pmod{N}\right\};$$

in this case, $X(G)$ is the classical modular curve $X_0(N)$.

Modular forms (1/2)

For a given integer k, the group G *acts in weight k* on functions on $\mathfrak{h}$

$$f \mid_k \gamma := (cz+d)^{-k} f(\gamma \cdot z), \quad \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G.$$

A *modular function* of weight k for G is a *meromorphic* function on $\mathfrak{h}^*$ (on $\mathfrak{h}$ and at all cusps) satisfying

$$f \mid_k \gamma = f, \quad \forall \gamma \in G.$$

For instance, a modular function of weight 0 is a function on $X(G)$; a form of weight 2 is a differential on $X(G)$: since $d(\gamma \cdot z) = (cz+d)^{-2} dz$, we have

$$\gamma^*(f(z)\,dz) := f(\gamma \cdot z)\,d(\gamma \cdot z) = (f \mid_2 \gamma)(z)\,dz = f(z)\,dz.$$

Forms of higher (even) weights $2k$ are sections of appropriate line bundles on $X(G)$ (k-fold differentials).

Modular forms (2/2)

A *modular form* for G is a *holomorphic* modular function on $\mathfrak{h}^*$. Let $M_k(G)$ be the $\mathbb{C}$-vector space of modular forms of weight k for G.

Theorem . $\dim_{\mathbb{C}} M_k(G) < +\infty$.

For instance, for $G = \Gamma_0(N)$, we have $\dim_{\mathbb{C}} M_k(G) \approx \frac{kN}{12}$.

Cusp forms, L-series

Assume for the moment that $G = \Gamma_0(N)$: the definitions implies that $f \in M_k(G)$ satisfies $f(z+1) = f(z)$ and has a Fourier expansion at infinity $f(z) = \sum_{n \geqslant 0} a_n q^n$, where $q = \exp(2i\pi z)$. (For a general congruence subgroup and a general cusp, there is an expansion in $q^{1/H}$, depending on the width $H \geqslant 1$ of the cusp, for an appropriate local parameter q.)

Let $S_k(G) \subset M_k(G)$ be the subspace of *cusp forms*: vanishing at all cusps. In particular, $a_0 = 0$ and we can define associated L-series, for $f \in S_k(G)$:

$$L(f,s) = \sum_{n \geqslant 1} a_n n^{-s}, \quad L(f,\chi,s) = \sum_{n \geqslant 1} a_n \chi(n) n^{-s},$$

where χ is a Dirichlet character. The $a_n = O(n^C)$ are polynomially bounded $\Rightarrow$ those functions are in principle defined for $\operatorname{Re} s$ big enough, in a right half-plane. In fact, they are *entire functions*. Completing them by a gamma factor, we obtain $\Lambda(f,s)$ satisfying a functional equation relating s to $k-s$. *Critical values* $L(f,j)$, for integers $0 < j < k$, are of particular interest.

Hecke operators, Atkin-Lehner theory (1/2)

Still assume that $G = \Gamma_0(N)$. (Analogous results hold for $\Gamma_1(N)$.) There is a canonical decomposition

$$S_k(G) = S_k(G)_{\text{old}} \oplus S_k(G)_{\text{new}},$$

where S_{old} contains the forms from $S_k(\Gamma_0(M))$, M a strict divisor of N; and S_{new} is the interesting part. (A basis of S_{new} can be computed via the intersection of kernels of explicit linear operators associated to divisors of N.)

For any integer $n \geqslant 1$ we have a Hecke operator T_n on $M_k(G)$. These linear "averaging" operators commute and satisfy nice multiplicativity relations, e.g. $T_{mn} = T_m T_n$ when $(m, n) = 1$ and $(mn, N) = 1$, or formulas expressing T_{p^i} in terms of T_p for p prime. Formally,

$$T_n f := \sum_{\gamma \in \Gamma_0(N) \backslash D_n} f \mid_k \gamma,$$

where D_n is the set of matrices of determinant n in $M_2(\mathbb{Z}) / \{-\mathrm{Id}, \mathrm{Id}\}$. (The sum is finite. We extend the action $f \mid_k \gamma$ from $\mathrm{PSL}_2(\mathbb{Z})$ to D_n by multiplying our formula for $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$ by n^{k-1}.)

Hecke operators, Atkin-Lehner theory (2/2)

Nice properties of Hecke operators:

- all T_n with $(n, N) = 1$ are diagonalizable, their eigenvalues are algebraic integers;
- they stabilize $S_k(G)$, in fact both S_{new} and S_{old} separately;
- there exist a $\mathbb{C}$-basis of S_{new} of *simultaneous eigenvectors* for all T_n;
- if $f = \sum_{n\geqslant 1} a_n q^n \in S_{\text{new}}$ is an eigenvector for all T_n, then $a_1 \neq 0$ and we can normalize f so that $a_1 = 1$; then $T_n f = a_n f$. Such a form is called *primitive*.
- a primitive form satisfies a *product formula*

$$L(f, s) = \prod_{p\mid N} (1 - a_p p^{-s})^{-1} \prod_{p\nmid N} \left(1 - a_p p^{-s} + p^{k-1-2s}\right)^{-1}.$$

- if $f = \sum a_n q^n$ is primitive, then $\mathbb{Q}(f) := \mathbb{Q}(a_2, a_3, \dots)$ is a number field.

Example

The simplest example is

$$\Delta(q) = q \prod_{n \geqslant 1} (1 - q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 \ldots,$$

the only primitive form in $S_{12}(\mathrm{PSL}_2(\mathbb{Z}))$.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and $L(E, s) = \sum_{n \geqslant 1} a_n n^{-s}$ its L-series. Then

$$\sum_{n \geqslant 1} a_n q^n \in S_2(\Gamma_0(N))_{\text{new}} \quad \text{is primitive.}$$

For instance, let

$$E : y^2 + y = x^3 - x^2 - 10x - 20 \quad (= \mathtt{11a1}),$$

then the corresponding primitive form is

$$q \prod_{n \geqslant 1} (1 - q^n)^2 (1 - q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + q^5 \ldots.$$

Periods and critical L-values (1/2)

Let $f \in S_k(G)$, the *period*

$$\int_r^s f(z) z^j dz, \quad j \in \mathbb{Z}_{\geqslant 0},$$

is well-defined for any $r, s \in \mathbb{P}^1(\mathbb{Q})$. (The integral does not depend on the path in $\mathfrak{h}$ joining the cusps since f is holomorphic in $\mathfrak{h}$, and it converges since f decreases exponentially at cusps.)

Let $f = \sum_n a_n q^n \in S_2(G)$; heuristically, periods should be related to L-values, barring convergence issues…

$$2i\pi \int_{i\infty}^0 f(z) z^j dz \approx \sum_n a_n \underbrace{\int_{i\infty}^0 2i\pi \exp(2i\pi n z) z^j \, dz}_{= (-2i\pi n)^{-j} \cdot \frac{1}{n} \cdot \Gamma(j+1)} \approx \frac{j!}{(-2i\pi)^j} L(f, j+1).$$

Periods and critical L-values (2/2)

It can actually be proven rigorously in a more general form:

Theorem . *Let $f \in S_k(G)$, G a congruence subgroup. Then*

$$2i\pi \int_{i\infty}^{0} f(z) z^j \, dz = \frac{j!}{(-2i\pi)^j} L(f, j+1),$$

for all critical $0 \leqslant j \leqslant k-2$.

Similarly for twists by a primitive Dirichlet character of conductor $D > 1$, in weight 2:

$$\frac{\tau(\chi)}{D} \sum_{a \bmod D} \overline{\chi}(a) 2i\pi \int_{i\infty}^{-a/D} f(z) \, dz = L(f, \chi, 1),$$

as well as more complicated generalizations in higher weight.

Periods know all about (twisted) critical L-values.

Complex modular symbols, weight 2

Let $\Delta_0 := \mathrm{Div}^0(\mathbb{P}^1(\mathbb{Q}))$: given $s, r \in \mathbb{P}^1(\mathbb{Q})$, think of the divisor $[s] - [r]$, as an oriented path in $\mathfrak{h}$ connecting $r \to s$. E.g., the semicircle connecting s to r, or a vertical line through r if $s = i\infty$. Those divisors generate Δ_0. Note that Δ_0 is a $\mathrm{GL}_2(\mathbb{Q})$-module : for $g \in \mathrm{GL}_2(\mathbb{Q})$,

$$g \cdot ([s] - [r]) := [g \cdot s] - [g \cdot r].$$

In matrix form, if $r = (a : c)$, $s = (b : d)$, the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ codes the path $[s] - [r]$: then the path $g \cdot ([s] - [r])$ is identified with the matrix $g \times \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

Let $f \in S_2(G)$, we define a map ψ_f from Δ_0 to $\mathbb{C}$ by

$$[s] - [r] \mapsto 2i\pi \int_r^s f(z)\, dz$$

(Well-defined: Chasles relation.) Since $f \in S_2(G)$, we have

$$\int_{\gamma \cdot r}^{\gamma \cdot s} f(z)\, dz = \int_{\gamma \cdot r}^{\gamma \cdot s} f(\gamma \cdot z)\, d(\gamma \cdot z) = \int_r^s f(z)\, dz.$$

Thus $\psi_f \in \mathrm{Hom}_G(\Delta_0, \mathbb{C})$: $\psi(\gamma \cdot D) = \psi(D)$ for all $\gamma \in G$.

Complex modular symbols, general weight k

The relevant period integrals attached to $f \in S_k(G)$ are the

$$\int_r^s f(z) z^j \, dz, \quad 0 \leqslant j \leqslant k-2.$$

Let $V := \mathrm{Sym}^{k-2}(\mathbb{C}^2)$, realized as the space of homogeneous polynomials of degree $k-2$ in $\mathbb{C}[X,Y]$, together with the *right* $\mathrm{SL}_2(\mathbb{Z})$ action: $(P \mid \gamma)(X,Y) := P((X,Y) \times \gamma^{-1})$.
There is a natural right action on $\mathrm{Hom}(\Delta_0, V)$: for $\phi \in \mathrm{Hom}(\Delta_0, V)$, define $\phi \mid \gamma$ by

$$(\phi \mid \gamma)(D) := \phi(\gamma \cdot D) \mid \gamma, \quad \forall D \in \Delta_0.$$

Define $\psi_f \in \mathrm{Hom}(\Delta_0, V)$ by

$$\psi_f([s]-[r]) := 2i\pi \int_r^s f(z)(zX+Y)^{k-2} \, dz \ \in V.$$

Then $\psi_f \mid \gamma = \psi_f$ for any $\gamma \in G$! Again, $\psi_f \in \mathrm{Hom}_G(\Delta_0, V)$.

Proof of $\psi_f \in \mathrm{Hom}_G(\Delta_0, V)$

Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$. Recall that

$$f \mid_k \gamma = f,$$

$$(P \mid \gamma)(X, Y) := P((X, Y) \times \gamma^{-1}), \quad P \in V,$$

$$(\phi \mid \gamma)(D) := \phi(\gamma \cdot D) \mid \gamma,$$

$$\psi_f([s] - [r]) := 2i\pi \int_r^s f(z)(zX + Y)^{k-2}\, dz \ \in V.$$

We have

$$\begin{aligned}
\psi_f([s] - [r]) \mid \gamma^{-1} &= 2i\pi \int_r^s f(z)\Big((X, Y)\gamma \left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right)\Big)^{k-2} dz \\
&= 2i\pi \int_r^s f(\gamma \cdot z)/(cz + d)^k \Big((X, Y) \left(\begin{smallmatrix} az+b \\ cz+d \end{smallmatrix}\right)\Big)^{k-2} dz \\
&= 2i\pi \int_r^s f(\gamma \cdot z)\Big((X, Y) \left(\begin{smallmatrix} \gamma \cdot z \\ 1 \end{smallmatrix}\right)\Big)^{k-2} d(\gamma \cdot z) \\
&= 2i\pi \int_{\gamma \cdot r}^{\gamma \cdot s} f(z)\Big((X, Y) \left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right)\Big)^{k-2} dz = \psi_f(\gamma \cdot ([s] - [r])) \qquad \square
\end{aligned}$$

Cohomological interpretation

Let $G \subset \mathrm{PSL}(2, \mathbb{Z})$ be a congruence subgroup, and V be a right G-module. One defines the cohomology of the modular curve $X(G)$ with coefficients in V, the group of interest being $H^1_c(X(G), V)$; one can again define Hecke operators in this context.

Back to previous example: $G = \Gamma_0(N), V = \mathrm{Sym}^{k-2}\,\mathbb{C}^2$,

$$(P \mid \gamma)(X, Y) = P((X, Y)\gamma^{-1}), \quad P \in V.$$

We recover classical $\mathbb{C}$-vector spaces of holomorphic modular forms for G:

Theorem (Eichler-Shimura)**.**

$$H^1_c(X(G), V) \simeq_{Hecke} S_k(G) \oplus M_k(G)$$

Cohomology classes are not that explicit…

Abstract modular symbols (1/3)

Classical modular symbols for $G = \Gamma_0(N)$ provide

- an algebraic version of periods of holomorphic forms,
- a way to describe (and compute!) $M_k(G)$ as a Hecke-module from finite rational data,

For general G (congruence subgroup) and V (over $\mathbb{C}$, $\mathbb{F}_p$, $\mathbb{Q}_p$, $\mathbb{Z}$, infinite dimensional...), they also are

- a concrete realization of cohomology classes $H^1_c(X(G), V)$ that afford a painless way to define (and compute!) general spaces of “modular forms”, or rather systems of Hecke eigenvalues, using basic linear algebra.

Abstract modular symbols (2/3)

Let $\Delta_0 := \mathrm{Div}^0(\mathbb{P}^1(\mathbb{Q}))$, generated by the divisors $[\beta] - [\alpha]$, which we denote by $\{\alpha, \beta\}$ and see as a path through the completed upper half plane $\mathfrak{h}^*$ linking the two cusps $\alpha \to \beta$. This is a left $\mathrm{GL}(2, \mathbb{Q})$-module via fractional linear transformations:

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot [(u : v)] := [(au + bv : cu + dv)].$$

Let $G \subset \mathrm{PSL}_2(\mathbb{Z})$ be a subgroup of finite index and let V be a right G-module. $\mathrm{Hom}(\Delta_0, V)$ becomes a right G-module via

$$(\phi \mid \gamma)(D) := \phi(\gamma \cdot D) \mid \gamma$$

We define the *V-valued modular symbols on G* by

$$\mathrm{Symb}_G(V) := \mathrm{Hom}_G(\Delta_0, V), \quad \phi \mid \gamma = \phi, \forall \phi \in G.$$

N.B. Δ_0 is “almost free” as a $\mathbb{Z}[G]$-module, of finite type ! A symbol is defined by the set of values (satisfying simple relations) it takes on chosen generators.

Abstract modular symbols (3/3)

Theorem (Ash-Stevens). *Let G be a congruence subgroup and V a right G-module. Provided that the orders of torsion elements of G act invertibly on V (e.g. if V is a vector space), we have a canonical isomorphism*

$$\mathrm{Symb}_G(V) \simeq H^1_c(X(G), V).$$

Assume V also allows a right action by the semi-group $\mathrm{GL}(2,\mathbb{Q}) \cap M_2(\mathbb{Z})$, then we can define a Hecke action on $\mathrm{Symb}_G(V)$. E.g. if $G = \Gamma_0(N)$ and ℓ is prime, then

$$T_\ell \phi := \underbrace{\phi \mid \left(\begin{smallmatrix} \ell & 0 \\ 0 & 1 \end{smallmatrix}\right)}_{\text{if } \ell \nmid N} + \sum_{a=0}^{\ell-1} \phi \mid \left(\begin{smallmatrix} 1 & a \\ 0 & \ell \end{smallmatrix}\right).$$

If $\sigma := \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ normalizes G, then it acts as an involution on $\mathrm{Symb}_G(V)$; if 2 acts invertibly on V, this yields a decomposition

$$\mathrm{Symb}_G(V) = \mathrm{Symb}_G(V)^+ \oplus \mathrm{Symb}_G(V)^-$$

into eigenspaces for this action.

Computing Δ_0 as a $\mathbb{Z}[G]$-module (1/5)

Let $G \subset \Gamma = \mathrm{PSL}(2,\mathbb{Z})$ and $B = [\Gamma : G] < +\infty$. The subgroup G is given via an enumeration $(m_1, \dots, m_B)$ of matrices representing $G \backslash \mathrm{PSL}(2,\mathbb{Z})$. Assume that

- the coset representatives m_i have size $O(\log B)^C$,
- the map $(\gamma \in \Gamma \mapsto \text{its coset})$, i.e. the unique i such that $G\gamma = Gm_i$, is computed in polynomial time $O(\log \|\gamma\| + \log B)^C$.

In particular, both the membership problem ($\gamma \in G$?) and test for equivalence ($\gamma_1 \sim_G \gamma_2$?) are solved in polynomial time in the size of the $\gamma_i \in \Gamma$.

Theorem (Manin). *If $B = 1$ ($G = \Gamma$), then*

$$\Delta_0 \simeq_\Gamma \mathbb{Z}[\Gamma]/I, \quad \textit{where} \quad I := \mathbb{Z}[\Gamma](1+\sigma) + \mathbb{Z}[\Gamma](1+\tau+\tau^2),$$

where $\sigma = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $\tau = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ *and* $\Gamma = \langle \sigma, \tau \rangle$.

In this case a V-valued modular symbol $\phi \in \mathrm{Hom}_\Gamma(\Delta_0, V)$ is defined by $v_\sigma, v_\tau \in V$ s.t.

$$v_\sigma \mid (1+\sigma) = v_\tau \mid (1+\tau+\tau^2) = 0.$$

Computing Δ_0 as a $\mathbb{Z}[G]$-module (2/5)

In principle, Manin's theorem yields a presentation of Δ_0 as a $\mathbb{Z}[G]$ module: $\mathbb{Z}[\Gamma]$ is free (generated by the m_i), and quotienting out yields relations of the form

$$m_i(1+\sigma) = m_i + m_i\sigma = m_i + \gamma_{i,j} m_j \in I,$$

for some j and $\gamma_{i,j} \in G$. There's a neater, simpler, way.

Fact: the torsion elements in $\mathrm{PSL}_2(\mathbb{Z})$ have order 2 or 3.

Theorem (Pollack-Stevens). *Let $G \subset \mathrm{PSL}_2(\mathbb{Z})$ be a subgroup of finite index B* without 3-torsion. *There exist a connected fundamental domain $\mathcal{F}$ for the action of G on $\mathfrak{h}^*$ all of whose vertices are cusps and whose boundary is a union of* unimodular paths.

Computing Δ_0 as a $\mathbb{Z}[G]$-module (3/5)

Proof. Start from the hyperbolic triangle $R = (0, 1, i\infty)$, a fundamental domain for $\Gamma_0(2)$. We use Farey dissection to add further triangles until we obtain the full domain : given 2 cusps $(a : b) < (c : d)$ on the boundary of current domain

$$\alpha_1 R \cup \cdots \cup \alpha_r R,$$

such that $ad - bc = 1$, the third vertex of the triangle $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) R$ is the mediant $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$. Add the new triangle to the domain if and only if $\alpha_i \tau^j \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)^{-1} \notin \Gamma$, $\forall 1 \leqslant i \leqslant r$, $0 \leqslant j \leqslant 2$. The algorithm stops after at most B triangles are added. $\square$

If G has 3-torsion : assentially the same, but we must split triangles in 3: $R = T \cup \tau T \cup \tau^2 T$, where $T = (0, e^{i\pi/3}, i\infty)$, and we sometimes add only $1/3$ of a triangle (αT instead of αR).

Theorem . *Under our asumptions on G, the fundamental domain $\mathcal{F}$ can be computed in time $\widetilde{O}(B)$.*

N.B. some complexity estimates only depend on the number of cusps rather than B, which is advantageous: $G = \Gamma_0(p)$ has index $p + 1$ but only 2 cusps.

Computing Δ_0 as a $\mathbb{Z}[G]$-module (4/5)

- If G has *no torsion* then Δ_0 is generated by the $g_i := [c_{i+1}] - [c_i]$, paths between consecutive vertices of $\mathcal{F}$, with the *single relation* $\sum_i g_i = 0$!
- If G has 2-*torsion*, then it can happen that $\gamma_i g_i = -g_i$ for some $\gamma_i \in G$ swapping c_i and c_{i+1} (implies γ_i has order 2). Then $(1 + \gamma_i) \cdot g_i = 0$ and g_i is torsion.
- If G has 3-*torsion*, then we have extra torsion relations corresponding to going around a triangle αR fixed by an element of order 3.

Computing Δ_0 as a $\mathbb{Z}[G]$-module (5/5)

Summary: In general, we obtain

- a "minimal" system of generators (g_i), $i \leqslant n$, $g_n = [\infty] - [0]$.
- relations explicitly written down (without computation):
  - one relation for each conjugacy class of 2-torsion elements in G: $(1 + \gamma_i) \cdot g_i = 0$, $1 \leqslant i \leqslant s$
  - one for each pairs of conjugacy classes of 3-torsion elements: $(1 + \gamma_i + \gamma_i^2) \cdot g_i = 0$, $s + 1 \leqslant i \leqslant s + r$.
  - and one "boundary relation" (walk around the fundamental domain and come back to starting point).

Corollary . *Given G a finite index subgroup and V a right G-module. Choose any $n-1$ elements $v_i \in V$, compatible with the torsion relations when $i \leqslant s+r$ (e.g. $v_i(1+\gamma_i) = 0$, i.e restrict v_i to an eigenspace $V_i \subset V$). Solve for v_n so that the boundary relation is satisfied. Then $\phi(g_i) = v_i$ uniquely defines a modular symbol ϕ, and all modular symbols arise in this way.*

Discrete logarithm in Δ_0 as $\mathbb{Z}[G]$-module

Recall that a (non-trivial) path $(a:c) \to (b:d)$ is encoded by the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q})^+$. A *unimodular* path has determinant 1.

Recall that the subgroup G is given via an enumeration $(m_1, \ldots, m_B)$ of matrices representing $G \backslash \mathrm{PSL}(2, \mathbb{Z})$.

- the discrete logs $m_i = \sum \lambda_{i,j} g_j$, $i \leqslant B$, are precomputed: $\widetilde{O}(B^2)$ time and space.
- a path $\infty \to (b:d)$ can be written as a sum of $O(\log \max(|b|, |d|))$ *unimodular paths*. Proof: write the finite continued fraction of b/d. The successive convergents satisfy $(p_{-1} : q_{-1}) = (1:0), \ldots, (p_n : q_n) = (b:d)$ and $\det \left(\begin{smallmatrix} p_i & p_{i+1} \\ q_i & q_{i+1} \end{smallmatrix}\right) = \pm 1$. $\square$
- a path $(a:c) \to (b:d)$ can be written as a sum of $O(\log \max(|a|, |b|, |c|, |d|))$ unimodular paths. Proof: $(a:c) \to (1:0) \to (b:d)$. Better (halve number of paths on average), $U^{-1} \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \begin{pmatrix} 1 & b' \\ 0 & d' \end{pmatrix}$ (HNF), then $U \cdot \gamma_i$. $\square$
- a unimodular path is uniquely written as $\gamma \cdot m_i$ for some $\gamma \in G$.

p-adic L functions (1/4)

Let $f \in S_k(G)$, $V = \mathbb{C}[X,Y]_{k-2}$. Recall that $\psi_f \in \mathrm{Symb}_G(V)$ defined by

$$\psi_f([s]-[r]) := 2i\pi \int_r^s f(z)(zX+Y)^{k-2}\,dz \ \in V$$

knows about critical L-values:

$$\psi_f([0]-[i\infty]) = \sum_{0\leqslant j\leqslant k-2} X^j Y^{k-2-j} \binom{k-2}{j} \frac{j!}{(-2i\pi)^j} L(f,j+1).$$

Theorem (Manin, Shimura). *There exist $\Omega_f^{\pm} \in \mathbb{C}$ such that*

$$\frac{L(f,\chi,j+1)}{(-2i\pi)^j} \in \Omega_f^{\pm}\overline{\mathbb{Q}},$$

for all Dirichlet characters χ and $j \leqslant k-2$. (Precisely in $\Omega_f^{(-1)^j\chi(-1)}\overline{\mathbb{Q}}$.)

By fixing an embedding of $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}_p}$, we can consider those renormalized $\mathcal{L}(f,\chi,j+1)$ as p-adic numbers!

p-adic L functions (2/4)

Fix a prime p. Let Γ be a congruence sugroup of level prime to p and $G := \Gamma \cap \Gamma_0(p)$. Let $f \in S_k(G)$ be a normalized eigenform, with $T_p f = \alpha f$.

The p-adic L-function μ_f associated to f should be a way to associate $(j, \chi) \mapsto \mathcal{L}(f, \chi, j+1)$. It's going to be a *$p$-adic distribution*, mapping "nice functions" (characters, polynomials) to p-adic numbers. Precisely, assume that $v_p(\alpha) < k-1$; for any finite order character χ of $\mathbb{Z}_p^\times$ of conductor p^n and any integer $0 \leqslant j \leqslant k-2$, we want

$$\mu_f(z^j \cdot \chi) := \alpha^{-n} p^{n(j+1)} \frac{j!}{\tau(\chi^{-1})} \mathcal{L}(f, \chi^{-1}, j+1) \in \overline{\mathbb{Q}_p}.$$

This defines μ_f uniquely, for a given choice of complex periods $\Omega_f^\pm$. The distribution μ_f can be evaluated on locally analytic functions (χ is locally constant but not analytic!); we write $\int g(t)\, d\mu_f(t)$ for $\mu_f(g)$.

Hard to compute when defined this way: Riemann sums with (at least) p^n terms to evaluate modulo p^n.

p-adic L functions (3/4)

Let $V = \mathcal{D}_k(\mathbb{Z}_p) =: \mathcal{D}$, the space of locally analytic p-adic distributions on $\mathbb{Z}_p$, with weight $k-2$ action of G:

$$(\mu \mid_k \gamma)(g) := \mu(\gamma \cdot g), \quad \text{where} \quad (\gamma \cdot g)(z) := (a+cz)^{k-2} f\left(\frac{b+dz}{a+cz}\right).$$

This defines $\mathrm{Symb}_G(\mathcal{D})$, the space of overconvergent modular symbols.

Composing with the p-adic period map $\rho_k \colon \mathcal{D} \to \mathrm{Sym}^{k-2}\,\mathbb{Q}_p^2$, given by

$$\mu \mapsto \int (Y - tX)^{k-2} d\mu(t),$$

defines specializations

$$\mathrm{Symb}_G(\mathcal{D}) \to \mathrm{Symb}_G(\mathrm{Sym}^{k-2}\,\mathbb{Q}_p^2).$$

The target of this map is finite dimensional while the source has infinite dimension!

Nevertheless, by restricting to natural subspaces, Pollack and Stevens obtain a Hecke-equivariant isomorphism.

p-adic L functions (4/4)

The p-adic *slope* of a primitive form $f \in S_k(G)$ is $v_p(a_p)$, it is $\leqslant k-1$. (*Critical slope* when equality.)

Theorem (Stevens). *The map*

$$\mathrm{Symb}_G(\mathcal{D})^{(<k-1)} \to \mathrm{Symb}_G(\mathrm{Sym}^{k-2}\,\mathbb{Q}_p)^{(<k-1)}$$

is an isomorphism, compatible with Hecke action.

Theorem . *Let f be primitive for G of non-critical slope and $\phi_f \in \mathrm{Symb}_G(\mathrm{Sym}^{k-2}\,\mathbb{Q}_p)$ be the corresponding classical modular eigensymbol. Let Φ_f be the unique overconvergent eigensymbol lifting ϕ_f. Then* $\Phi_f([0]-[i\infty])$ is the p-adic L-function of g.

The case of critical slope can also be dealt with in a similar way.

Theorem . *The $\Phi_f([0]-[i\infty])(z^j)$ modulo p^{M-j}, $j \leqslant M$ can be computed in time $pM^{O(1)}$: polynomial time for fixed p.*