p-adic distributions associated to

Heegner points on modular curves

Winfried Kohnen

Universität Augsburg
Mathematisch-Naturwissenschaftliche Fakultät
Memmingerstr. 6
8900 Augsburg, FRG

Max-Planck-Institut für Mathematik
Gottfried-Claren-Str. 26
5300 Bonn 3, FRG

MPI 86-46

Introduction

Let f be a normalized newform of weight 2 on $\Gamma_0(N)$ ($N \in \mathbb{N}$) and let $A_f/\mathbb{Q}$ be the abelian subvariety of the jacobian of the modular curve $X_0(N)/\mathbb{Q}$ corresponding to f. Let p be a rational prime with $p \nmid N$ and denote by $\mathbb{C}_p$ a completion of an algebraic closure of the field of p-adic numbers.

Let K be an imaginary quadratic field and let K_∞/K be the anti-cyclotomic $\mathbb{Z}_p$-extension of K.

Suppose that every rational prime ℓ dividing N is split or ramified in K, and every rational prime ℓ with ℓ^2 dividing N is split in K. The main purpose of this paper then is to construct a distribution μ_f on $Gal(K_\infty/K)$ with values in the subspace of the $\mathbb{C}_p$-vector space $\mathbb{C}_p \otimes_{\mathbb{Z}} A_f(K_\infty)$ which is generated by the Heegner points for K. This distribution is of moderate growth w.r.t. an appropriate norm (§3.). Choosing an anti-cyclotomic p-adic logarithm τ over K we then obtain a p-adic function $h_{f,\tau}(\chi, s)$ for every finite character χ on $Gal(K_\infty/K)$ in the usual way as a Mellin-Mazur integral (§4.). In the final section of the paper (§5.) we give a simple relation (kindly suggested to me by P. Schneider) between μ_f and the measure constructed by Mazur in [9], §22., which plays an important rôle in recent work of Perrin-Riou ([12]) on a p-adic analogue of the theory of Gross-Zagier ([3]). We also make some further remarks on μ_f and $h_{f,\tau}$, respectively.

As P. Schneider pointed out to me, Heegner points -like cyclotomic units- behave almost like universal norms, and then by a rather formal argument this property can be translated into a distribution relation (Heegner points as universal norms are also treated in [9], §19. and in [11]). In this context -as is true for many distributions occurring in practice- μ_f is a special case of P. Schneider's fundamental notion of a distribution of Galois type arising from norm-finite elements ([16]).

Acknowledgements: I would like to thank B. Mazur for some useful discussions; in particular, after I talked to him about a first version of this article, he showed me a preprint of his paper [9], from which I profitted very much. -I also would like to thank P. Schneider for several useful suggestions and improvements on this paper.

§1. Modules in imaginary quadratic fields

Let K be an imaginary quadratic field. For $n \geq 0$ we denote by $\mathcal{O}_n$ the order of K of conductor p^n, where p is a fixed rational prime. We write $\mathcal{O}=\mathcal{O}_0$. We let D be the discriminant of K.

There is a homomorphism from the monoid of proper $\mathcal{O}_n$-lattices onto the monoid of proper $\mathcal{O}$-lattices given by

(1) $$\mathfrak{a} \longmapsto \mathfrak{a}\mathcal{O}.$$

The group $(\mathcal{O}/p^n\mathcal{O})^* / (\mathbb{Z}/p^n\mathbb{Z})^*$ is isomorphic to its kernel under the map

$$x \longmapsto \mathfrak{c}_{n,x},$$

where

(2) $$\mathfrak{c}_{n,x} = p^n\mathcal{O}+\mathbb{Z}x.$$

Denote by I_n the group of proper $\mathcal{O}_n$-lattices modulo equivalence and put

$$A_n = \left((\mathcal{O}/p^n\mathcal{O})^* / (\mathbb{Z}/p^n\mathbb{Z})^*\right) \Big/ (\mathcal{O}^*/\mathcal{O}_n^*).$$

Then (1) induces an exact sequence of finite abelian groups

$$0 \to A_n \to I_n \to I_0 \to 0$$

(note that $\mathcal{O}_n^*=\{\pm 1\}$ for $n \geq 1$ and that $\mathcal{O}^*/\mathcal{O}_n^*$ is non-trivial only for $D=-3$ and $D=-4$, in which cases its order is 3 and 2, respectively). In particular

$$|I_n| = |I_0| \, [\mathcal{O}^*:\mathcal{O}_n^*]^{-1} p^n \left(1-\left(\frac{D}{p}\right)\frac{1}{p}\right).$$

Note that (1) also induces a bijection between proper $\mathcal{O}_n$-ideals prime to p and proper $\mathcal{O}$-ideals prime to p (the inverse map is given by $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}_n$).

Let

$$\pi_n : A_n \to A_{n-1} \quad (n \geq 1)$$

be the canonical projection. The order of $\ker \pi_n$ is p for $n \geq 2$ and is $[\mathcal{O}^* : \mathcal{O}_1^*]^{-1}(p - (\frac{D}{p}))$ for n=1.

Lemma. <u>Let</u> $\mathfrak{c}$ <u>be a proper</u> $\mathcal{O}$-<u>ideal prime to</u> p. <u>Let</u> $x \in A_n$. <u>Then for all</u> $x' \in \pi_{n+1}^{-1} x$ <u>the lattice</u> $(\mathfrak{c} \cap \mathcal{O}_{n+1})\mathfrak{c}_{n+1,x'}$ <u>has index</u> p <u>in</u> $(\mathfrak{c} \cap \mathcal{O}_n)\mathfrak{c}_{n,x}$.

Proof. Write $\mathfrak{c}_n = \mathfrak{c} \cap \mathcal{O}_n$. We shall prove that

(3) $$p\mathfrak{c}_n \mathfrak{c}_{n,x} \subset \mathfrak{c}_{n+1}\mathfrak{c}_{n+1,x'}.$$

The Lemma will follow from this. Indeed, the inclusion

$$\mathfrak{c}_{n+1}\mathfrak{c}_{n+1,x'} \subset \mathfrak{c}_n \mathfrak{c}_{n,x}$$

must be strict, since $(\mathfrak{c}, p) = 1$ and so the coefficient ring of $\mathfrak{c}_n \mathfrak{c}_{n,x}$ is $\mathcal{O}_n$ and that of $\mathfrak{c}_{n+1}\mathfrak{c}_{n+1,x'}$ is $\mathcal{O}_{n+1}$.

Let us now prove (3) which is equivalent to

(4) $$p^2(\mathfrak{c}_n \cdot p^n \mathfrak{c}_{n,x}) \subset \mathfrak{c}_{n+1} \cdot p^{n+1} \mathfrak{c}_{n+1,x'}.$$

The lattices $\mathfrak{c}_n$ and $p^n \mathfrak{c}_{n,x}$ are $\mathcal{O}_n$-ideals with $(\mathfrak{c}_n, p^n \mathfrak{c}_{n,x}) = 1$, since $(\mathfrak{c}, p) = 1$
Therefore

$$\mathfrak{c}_n \cdot p^n \mathfrak{c}_{n,x} = \mathfrak{c}_n \cap p^n \mathfrak{c}_{n,x}.$$

Therefore (4) is equivalent to

$$p^2(\mathfrak{c}_n \cap p^n \mathfrak{c}_{n,x}) \subset \mathfrak{c}_{n+1} \cap p^{n+1} \mathfrak{c}_{n+1,x'}$$

or to

$$p^2(\mathfrak{c} \cap p^n \mathfrak{c}_{n,x}) \subset \mathfrak{c} \cap p^{n+1} \mathfrak{c}_{n+1,x'}.$$

The latter inclusion, however, is obvious since $p\mathfrak{c}_{n,x} \subset \mathfrak{c}_{n+1,x'}$, by definition of x'.

§2. Heegner points

For basic facts on Heegner points we refer to [2] (our notation will be consistent with that of [2]). Let $N \in \mathbb{N}$ and suppose that every rational prime ℓ dividing N is split or ramified in the imaginary quadratic field K, and every rational prime ℓ with $\ell^2 | N$ is split in K. Let $\mathfrak{n}$ be a proper $\mathcal{O}$-ideal with $\mathcal{O}/\mathfrak{n}\mathcal{O} \cong \mathbb{Z}/N\mathbb{Z}$ (such an ideal n exists if and only if the above conditions on N and ℓ are satisfied). We put $\mathfrak{n}_n = \mathfrak{n} \cap \mathcal{O}_n$, where $\mathcal{O}_n$ is the order of K of conductor p^n and p is a fixed rational prime with $p \nmid N$.

We let $Y_0(N)$ be the open modular curve of level N, which classifies triples (E, E', φ) consisting of two elliptic curves E and E′ and a cyclic isogeny $E \xrightarrow{\varphi} E'$ of degree N.

If $\mathfrak{a}$ is a proper $\mathcal{O}_n$-ideal and $[\mathfrak{a}] \in I_n$ its class we denote by

$$(\mathcal{O}_n, \mathfrak{n}_n, [\mathfrak{a}])$$

the corresponding Heegner point $(\mathcal{O}/\mathfrak{a} \hookrightarrow \mathcal{O}/\mathfrak{a}\mathfrak{n}_n^{-1})$ on $Y_0(N)$. It is rational over the ring class field $H_n = K(j(\mathcal{O}_n))$ obtained from K by adjoining the j-invariant of $\mathcal{O}_n$. The extension H_n/K is anti-cyclotomic with Galois group canonically isomorphic to I_n by class field theory (recall that an abelian extension L/K is called anti-cyclotomic if $L/\mathbb{Q}$ is Galois and if the non-trivial element of $Gal(K/\mathbb{Q})$ acts on $Gal(L/K)$ by complex conjugation).

The Galois group of H_n over K acts on Heegner points according to the formula

$$(\mathcal{O}_n, \mathfrak{n}_n, [\mathfrak{a}])^{\sigma[\mathfrak{b}]} = (\mathcal{O}_n, \mathfrak{n}_n, [\mathfrak{a}\mathfrak{b}^{-1}])$$

($\mathfrak{b}$ a proper $\mathcal{O}_n$-ideal, $(\mathfrak{b}, p) = 1$, $\sigma[\mathfrak{b}]$ the Artin symbol of $[\mathfrak{b}]$ in $Gal(H_n/K)$; cf. [2], 4.2.).

Let $J_0(N)/\mathbb{Q}$ be the jacobian of the complete modular curve $X_0(N)/\mathbb{Q}$. The divisor

$$(\mathcal{O}_n, \mathfrak{n}_n, [\mathfrak{a}]) - (i\infty)$$

is rational over H_n, and we shall write

$$y(\mathcal{O}_n, \mathfrak{n}_n, [\mathfrak{a}])$$

for its image in $J_0(N)(H_n)$.

Let

$$H = \bigcup_{n\geq 0} H_n$$

and put

$$V = \mathbb{C}\otimes_{\mathbb{Z}} J_0(N)(H_\infty) = \bigcup_{n\geq 0} \mathbb{C}\otimes_{\mathbb{Z}} J_0(N)(H_n).$$

By the Mordell-Weil Theorem the group $J_0(N)(H_n)$ is finitely generated for every $n\geq 0$. The complex vector space V has an hermitian inner product given by

$$\langle ze, z'e'\rangle = z\overline{z'}\langle e,e'\rangle_J.$$

Here $e,e'\in J_0(N)(H_\infty)$ and $\langle\ ,\ \rangle_J$ is the normalized height pairing on $J_0(N)(H_\infty)$.

Let $\mathbb{T}$ be the commutative subalgebra of $\mathrm{End}_{\mathbb{Q}}(J_0(N))$ generated over $\mathbb{Z}$ by the Hecke operators T_ℓ with $\ell\nmid N$ and the Atkin-Lehner involutions w_ℓ with $\ell|N$. Then $\mathbb{T}$ acts on V in a natural way. Since this action is self-adjoint w.r.t. $\langle\ ,\ \rangle$, we have a spectral decomposition

$$V = \bigoplus_F V_F,$$

where $F:\mathbb{T}\to\overline{\mathbb{Q}}$ runs through the finite set of characters of $\mathbb{T}$ and V_F denotes the corresponding eigenspace.

Let

$$f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z} \qquad (z\in\mathbb{C},\ \mathrm{Im}z>0)$$

be a normalized newform ($a_1=1$) of weight 2 on $\Gamma_0(N)$ and let $A_f/\mathbb{Q}$ be the abelian subvariety of $J_0(N)/\mathbb{Q}$ corresponding to f ([17], chap.7). Then

$$\mathbb{C}\otimes_{\mathbb{Z}} A_f(H_\infty) = \bigoplus_\sigma V_{f^\sigma},$$

where σ runs through the distinct complex embeddings of $\mathbb{Q}(\{a_n\}_{n\geq 1})/\mathbb{Q}$ and $f^\sigma = \sum_{n\geq 1} a_n^\sigma e^{2\pi i n z}$. Moreover, we have identified the newform f^σ with the corresponding character $\mathbb{T}\to\overline{\mathbb{Q}}$, $T\to\lambda^\sigma(T)$ $(Tf^\sigma=\lambda^\sigma(T)f^\sigma)$.

In order to obtain a spectral decomposition w.r.t. $\mathbb{T}$ also for $\mathbb{C}_p\otimes_{\mathbb{Z}} J_0(N)(H_\infty)$ we now choose a $\mathbb{Q}$-isomorphism $\mathbb{C}\cong\mathbb{C}_p$. Then $V\cong\mathbb{C}_p\otimes_{\mathbb{Z}} J_0(N)(H_\infty)$, and V and V_f become $\mathbb{C}_p$-vector spaces.

If $\mathfrak{a}$ is a proper $\mathcal{O}_n$-module we write

$$y_f(\mathcal{O}_n, \mathfrak{n}_n, [\mathfrak{a}])$$

for the image of the Heegner point $y(\mathcal{O}_n, \mathfrak{n}_n, [\mathfrak{a}])$ in V_f.

§3. p-adic distributions associated to Heegner points

We keep all notations of §1. and §2. In particular, we let I_n be the group of classes of proper $\mathcal{O}_n$-lattices. For $n \geq 1$ there is a surjective homomorphism

$$\pi_n : I_n \rightarrow I_{n-1}, \quad [\mathfrak{a}] \mapsto [\mathfrak{a}\mathcal{O}_{n-1}]$$

which extends the projection $\pi_n : A_n \rightarrow A_{n-1}$. We let

$$I_\infty = \varprojlim (I_n, \pi_n).$$

By class field theory I_n resp. I_∞ is canonically isomorphic to $\mathrm{Gal}(H_n/K)$ resp. $\mathrm{Gal}(H_\infty/K)$, and the diagram

$$\begin{array}{ccc} I_n & \xrightarrow{\pi_n} & I_{n-1} \\ \wr\| & & \wr\| \\ \mathrm{Gal}(H_n/K) & \xrightarrow{\mathrm{res}} & \mathrm{Gal}(H_{n-1}/K) \end{array}$$

is commutative, where res is the restriction map.

Recall that a p-adic distribution ν on I_∞ with values in an abelian group Y is given by a family $\{\nu_n\}_{n \geq 1}$ of maps

$$\nu_n : I_n \rightarrow Y$$

which satisfy the compatibility relations

(5) $$\nu_n(A) = \sum_{\pi_{n+1} B = A} \nu_{n+1}(B)$$

for all $n \geq 1$.

Now let us suppose that

(6)

i) $f(z) = \sum_{n \geq 1} a_n e^{2\pi i n z}$ is a normalized newform of weight 2 on $\Gamma_0(N)$;

ii) every rational prime ℓ with $\ell | N$ is split or ramified in the imaginary quadratic field K, and $\ell^2 | N$ implies that ℓ is split in K;

iii) $\mathfrak{n}$ is a proper $\mathcal{O}$-ideal with $\mathcal{O}/\mathfrak{n} = \mathbb{Z}/N\mathbb{Z}$ (such an $\mathfrak{n}$ exists by ii) we keep $\varkappa$ fixed throughout the following and therefore mostly omit it from the notation);

iv) p is a rational prime with $p\nmid N$ and $\rho=\rho_p$ is a root of $x^2-a_px+p=0$ which satisfies $|\rho|_p>|p|_p=p^{-1}$, where $|.|_p$ is the normalized p-adic absolute value on $\mathbb{C}_p$.

From now on we will always assume that the conditions in (6) are satisfied.

For $n\geq 1$ we define a map

$$\nu_{f,n}: I_n \longrightarrow V_f$$

by

$$\nu_{f,n}(A) = \rho^{-n} y_f(\mathcal{O}_n,\varkappa_n,A) - \rho^{-n-1} y_f(\mathcal{O}_{n-1},\varkappa_{n-1},\pi_n A).$$

We put

(7) $$\nu_f = \{\nu_{f,n}\}_{n\geq 1}.$$

Theorem 1. Under the assumptions in (6) the family ν_f defined by (7) is a p-adic distribution on I_∞.

Proof. We must verify (5). Write ν_n instead of $\nu_{f,n}$. We have

(8) $$\left\{\begin{aligned} \sum_{\pi_{n+1}B=A} \nu_{n+1}(B) = \rho^{-n-1} &\sum_{\pi_{n+1}B=A} y_f(\mathcal{O}_{n+1},\varkappa_{n+1},B) \\ - \rho^{-n-2} &\sum_{\pi_{n+1}B=A} y_f(\mathcal{O}_n,\varkappa_n,\pi_{n+1}B). \end{aligned}\right.$$

For $p\nmid N$ let T_p be the Hecke operator of degree p viewed as a correspondence on $X_0(N)$. Then T_p acts on Heegner points according to

$$T_p(R,\mathfrak{n},[\mathfrak{m}]) = \sum_{\mathfrak{m}/\mathfrak{m}'\cong\mathbb{Z}/p\mathbb{Z}} (R_{\mathfrak{m}'},\mathfrak{n}_{\mathfrak{m}'},[\mathfrak{m}'])$$

(formula 6.1. in [2]; here R is an arbitrary order in K, $\mathfrak{n}$ and $\mathfrak{m}$ are proper R-modules, $R/\mathfrak{n}\cong\mathbb{Z}/N\mathbb{Z}$, the sum is taken over the p+1 sublattices $\mathfrak{m}'$ of index p in $\mathfrak{m}$, $R_{\mathfrak{m}'}=\mathrm{End}(\mathfrak{m}')$ and $\mathfrak{n}_{\mathfrak{m}'}=\mathfrak{n}R_{\mathfrak{m}'}\cap R_{\mathfrak{m}'}$).

Let $A\in I_n$. Write $A=[\mathfrak{a}]$, where $\mathfrak{a}$ is a proper $\mathcal{O}_n$-ideal with $(\mathfrak{a},p)=1$. Then

$$\pi_{n+1}^{-1}A = \left\{[\mathfrak{a}\cap\mathcal{O}_{n+1}][\mathfrak{c}_{n+1,x'}] \mid x'\in\ker\pi_{n+1}\right\}$$

with $\mathfrak{c}_{n,x}$ defined by (2), and the lattice $(\mathfrak{a}\cap\mathcal{O}_{n+1})\mathfrak{c}_{n+1,x'}$ has index p in

$\mathfrak{a}$ by the Lemma in §1. (take $\mathfrak{c}=\mathfrak{a}\mathcal{O}$, so $\mathfrak{c}\cap\mathcal{O}_n=\mathfrak{a}$). Therefore for $n\geq 1$ the p lattices $(\mathfrak{a}\cap\mathcal{O}_{n+1})\mathfrak{c}_{n+1,x'}$ $(x'\in\ker\pi_{n+1})$ together with $p\mathfrak{a}\mathcal{O}_{n-1}$ give all the p+1 different sublattices of $\mathfrak{a}$ of index p. Since T_p commutes with the projection onto V_f we conclude

$$\begin{aligned} a_p y_f(\mathcal{O}_n,\varkappa_n,A) &= T_p y_f(\mathcal{O}_n,\varkappa_n,A) \\ &= \sum_{\pi_{n+1}B=A} y_f(\mathcal{O}_{n+1},\varkappa_{n+1},B) + y_f(\mathcal{O}_{n-1},\varkappa_{n-1},[p\mathfrak{a}\mathcal{O}_{n-1}]) \end{aligned}$$

and so

$$(9) \qquad \sum_{\pi_{n+1}B=A} y_f(\mathcal{O}_{n+1},\varkappa_{n+1},B) = a_p y_f(\mathcal{O}_n,\varkappa_n,A) - y_f(\mathcal{O}_{n-1},\varkappa_{n-1},\pi_n A).$$

Substituting (9) into the first term on the right of (8) and observing that $|\ker\pi_n|=p$ for $n\geq 2$ we obtain

$$\begin{aligned} \sum_{\pi_{n+1}B=A} \nu_{n+1}(B) &= \varrho^{-n-1}a_p y_f(\mathcal{O}_n,\varkappa_n,A) - \varrho^{-n-1}y_f(\mathcal{O}_{n-1},\varkappa_{n-1},\pi_n A) \\ &\qquad - \varrho^{-n-2}p y_f(\mathcal{O}_n,\varkappa_n,A) \\ &= \varrho^{-n-2}(\varrho a_p - p)y_f(\mathcal{O}_n,\varkappa_n,A) - \varrho^{-n-1}y_f(\mathcal{O}_{n-1},\varkappa_{n-1},\pi_n A) \\ &= \varrho^{-n}y_f(\mathcal{O}_n,\varkappa_n,A) - \varrho^{-n-1}y_f(\mathcal{O}_{n-1},\varkappa_{n-1},\pi_n A) \\ &= \nu_n(A), \end{aligned}$$

where in the third line we have used $\varrho^2-a_p\varrho+p=0$. This completes the proof.

We remark that formally ν_f is an analogue for the "modular symbols distribution" introduced in [6] and [7] to construct the cyclotomic p-adic L-function of f.

Now recall that the group I_∞ is isomorphic to $F\times\mathbf{Z}_p$, where F is a finite group. Let K_∞ be the fixed field of F. Then K_∞/K is the anti-cyclotomic $\mathbf{Z}_p$-extension of K. Let F_n be the image of F under the canonical projection $I_\infty\to I_n^-$, and let

$$\overline{I_\infty} = \varprojlim (I_n/F_n,\bar{\pi}_n)$$

where $\bar{\pi}_n$ is the reduction of π_n. We have canonical isomorphisms

$$(10) \quad \mathrm{Gal}(K_\infty/K) \cong I_\infty/F \cong \overline{I_\infty}.$$

Let W_f be the f-subeigenspace of the $\mathbf{C}_p$-vector space $\mathbf{C}_p\otimes_{\mathbf{Z}}J_0(N)(K_\infty)$. The group $\mathrm{Gal}(H_\infty/K)$ acts on $\mathbf{C}_p\otimes_{\mathbf{Z}}J_0(N)(H_\infty)$ in a natural way, and the Galois average

$$\sum_{\sigma\in F_n} \nu_{f,n}(A)^{\sigma} \qquad (A\in I_n)$$

of $\nu_{f,n}(A)$ is in W_f; from the action of the Galois group on Heegner points (§2.) we see that it only depends on the coset of A modF_n. We define a distribution

$$\mu_f = \{\mu_{f,n}\}_{n\geq 1}$$

on I_∞ by

(11) $\quad \mu_{f,n}: I_n/F_n \to W_f, \quad \mu_{f,n}(\bar{A}) = \sum_{\sigma\in F_n} \nu_{f,n}(A)^{\sigma} \qquad (A\in I_n,\ \bar{A}=A \bmod F_n).$

That this, in fact, is a distribution follows from the equation

$$|F_n| \sum_{\sigma\in F_{n+1}} \sum_{\pi_{n+1}B=A} \nu_{f,n+1}(B)^{\sigma}$$

$$= |F_{n+1}| \sum_{\bar{\pi}_{n+1}\bar{B}=\bar{A}} \Big(\sum_{\sigma\in F_{n+1}} \nu_{f,n+1}(B)^{\sigma} \Big) .$$

Thus we have obtained

Corollary. Let K_∞/K be the anti-cyclotomic $\mathbb{Z}_p$-extension of K and let W_f be the f-subeigenspace of $\mathbb{C}_p\otimes_{\mathbb{Z}}J_0(N)(K_\infty)$. Assume that the conditions in (6) are satisfied. Then via the identifications given in (10) the family $\mu_f=\{\mu_{f,n}\}_{n\geq 1}$ defined by (11) is a distribution on $\mathrm{Gal}(K_\infty/K)$ taking values in W_f.

§4. Mellin-Mazur transform of μ_f

We will now define an ultrametric norm $\|\cdot\|$ on the $\mathbb{C}_p$-vector space $\mathbb{C}_p\otimes_{\mathbb{Z}}A_f(K_\infty)$ and hence on the subspace W_f, for which μ_f is of moderate growth, i.e. there is $r\in[0,1)$ and $c\in\mathbb{R}$ such that $\|\mu_{f,n}(\bar{A})\| \leq p^{rn+c}$ for all $A\in I_n$ and all n (cf. [6],[8]); in fact, μ_f will be bounded if a_p is a p-adic unit.

Lemma. Let A be an abelian variety over a number field k. Then for any $\mathbb{Z}_p$-extension k_∞/k the group $A(k_\infty)$ modulo torsion is a free $\mathbb{Z}$-module.

The above result is essentially due to B. Perrin-Riou and was proved for A an elliptic curve in [10], II,1.3.,Thm.4; it was pointed out to me by P. Schneider that the proof carries over to the general situation if one replaces Lemma 6 in [10] by the following argument (we use the same notation as in [10]): since $\Theta=\mathrm{Gal}(k_\infty/k)$ is a pro-cyclic pro-p-group, we have an isomorphism between $H^1(\Theta,\Omega(k_\infty)) = H^1(\Theta,\Omega(k_\infty)(p))$ and the Θ-coinvariants of $\Omega(k_\infty/k)$. Now $\Omega(k_\infty)(p)$ is a $\mathbb{Z}_p$-module of cofinite type, hence the Θ-coinvariants of $\Omega(k_\infty)(p)$ are finite if and only if the Θ-invariants of $\Omega(k_\infty)(p)$ are finite; the latter, however, is $\Omega(k)(p)$, which obviously is finite.

Now let $w \in \mathbb{C}_p \otimes_{\mathbb{Z}} A_f(K_\infty)$ and let $\lambda_1, \lambda_2, \ldots$ be the $\mathbb{C}_p$-coordinates of w w.r.t. any $\mathbb{Z}$-basis of $A_f(K_\infty)$ modulo torsion. We put

(12) $$\|w\| = \max_{n\geq 1}\{|\lambda_n|_p\}.$$

Using the non-archimedean property of $|\cdot|_p$ one readily sees that this definition is independent of the chosen basis. Thus we have

Proposition 1. <u>Let $\|\cdot\|$ be defined by (12). Then</u> $(\mathbb{C}_p \otimes_{\mathbb{Z}} A_f(K_\infty), \|.\|)$ is a <u>normed $\mathbb{C}_p$-vector space, and the norm is ultrametric</u>.

Theorem 2. <u>The distribution μ_f is of moderate growth w.r.t.</u> $\|\cdot\|$. <u>Moreover, if a_p is a p-adic unit, then μ_f is bounded</u>.

Proof. Let $X = \bigoplus_\sigma \mathbb{C}f^\sigma$ with the sum over all embeddings σ of $\mathbb{Q}(\{a_n\}_{n\geq 1})/\mathbb{Q}$ in $\mathbb{C}$ and let $r=\dim_{\mathbb{C}}X$. If $F\in X$ and $F(z) = \sum_{\alpha\geq 1} c_\alpha(F)e^{2\pi i\alpha z}$ we may view c_α as an element of the $\mathbb{C}$-dual X' of X. Let $c_{i_1},\ldots,c_{i_r}$ be a basis of X'. Then the matrix

$$M = \left(c_\alpha(f^{\sigma_\beta})\right)_{1\leq\alpha,\beta\leq r}$$

is invertible.

If $A \in I_n$ we put

$$x(\sigma_n, \varkappa_n, A) = \sum_{\sigma \in F_n} y(\sigma_n, \varkappa_n, A)^{\sigma}.$$

Thus $x(\sigma_n, \varkappa_n, A) \in J_0(N)(K_\infty)$. Let $x_{A_f}(\sigma_n, \varkappa_n, A)$ resp. $x_f(\sigma_n, \varkappa_n, A)$ be the images of $x(\sigma_n, \varkappa_n, A)$ in $A_f(K_\infty)$ resp. W_f. Then

$$(13) \qquad x_{A_f}(\sigma_n, \varkappa_n, A) = \sum_{1 \le \beta \le r} x_{f^{\sigma_\beta}}(\sigma_n, \varkappa_n, A).$$

Since $T_\alpha x_{A_f}(\sigma_n, \varkappa_n, A)$ is rational over K_n, it is of norm ≤ 1. Applying T_α on both sides of (13) we obtain

$$(T_\alpha x_{A_f}(\sigma_n, \varkappa_n, A))_{\alpha = i_1, \ldots, i_r} = (x_{f^{\sigma_\beta}}(\sigma_n, \varkappa_n, A))_{\beta = 1, \ldots, r} M^t,$$

where M^t is the transpose of M. Since the column on the left has entries bounded w.r.t. $\|.\|$, and since M is invertible and has integral algebraic entries, we see that $x_{f^\sigma}(\sigma_n, \varkappa_n, A)$ has bounded norm, and the bound is independent of A.

Since furthermore, by assumption, $|\varrho|_p > |p|_p = p^{-1}$ and $|\varrho|_p = 1$ if $|a_p|_p = 1$, we conclude that μ_f is of moderate growth and is even bounded for $|a_p|_p = 1$.

The conjectures of Birch and Swinnerton-Dyer for abelian varieties predict that the groups $A_f(H_\infty)$ and $A_f(K_\infty)$ (and so the vector spaces V_f and W_f) are not finitely generated. In fact, let $L(f \otimes \psi, s)$ be the complex L-series attached to the tensor product of the ℓ-adic representations of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ corresponding to f and $ind\psi$, where $\psi: Gal(H_n/K) \to \mathbb{C}^*$ is any ring class character ([2]). Then by [2] and [4] $L(f \otimes \psi, s)$ satisfies a functional equation under $s \mapsto 2-s$, and under the assumption that every prime dividing N is split or ramified in K, and every prime whose square divides N is split in K, its root number is -1, and so in particular $L(f \otimes \psi, 1) = 0$. Let $L(A_f/H_n, s)$ be the Hasse-Weil L-function of A_f/H_n. Then

$$L(A_f/H_n,s) = \prod_{\sigma,\psi} L(f^\sigma \otimes \psi, s)$$

with ψ running over all characters of $Gal(H_n/K)$ and σ running over the distinct complex embeddings over $\mathbb{Q}$ of $\mathbb{Q}(\{a_n\}_{n\geq 1})$, and with f^σ defined as in §2. Therefore $ord_{s=1}L(A_f/H_n,s)$ goes to infinity with $n \to \infty$ and hence -by the conjectures of Birch and Swinnerton Dyer- so should do $rank_{\mathbb{Z}} A_f(H_n)$. Similar remarks apply if we replace H_n by $H_n \cap K_\infty$.

Note that if the results of Rohrlich ([13,14]) and Greenberg ([1]) could be generalized to give $L'(f\otimes\psi,1)\neq 0$ for almost all primitive ψ and n, then it would be a consequence of the work of Gross and Zagier ([3]) that V_f and W_f are, in fact, infinite-dimensional.

Let $(\overline{W}_f, \|.\|)$ be the completion of $(W_f, \|.\|)$. We can integrate any continuous function $g: I_\infty/F \to \mathbb{C}_p$ w.r.t. μ_f in the usual manner: if g_n is a sequence of locally constant functions converging uniformly to g, we put

$$\int_{I_\infty/F} g \, d\mu_f = \lim_{n\to\infty} \sum_{\bar{A}\in I_n/F_n} g(\bar{A})\mu_{f,n}(\bar{A}),$$

where the right-hand side is an element of $\overline{W}_f$.

Now let τ be an anti-cyclotomic p-adic logarithm over K, i.e. a non-trivial homomorphism from $Gal(\bar{\mathbb{Q}}/K)$ to the additive group of $\mathbb{Q}_p$, whose K/$\mathbb{Q}$ conjugate is equal to its inverse (cf. [9], §15.). Any two anti-cyclotomic p-adic logarithms over K are proportional by an element of $\mathbb{Q}_p^*$. The fixed field of $\ker\tau$ is K .

Denote by $\overline{W}_f[[s]]$ the $\mathbb{C}_p[[s]]$-module of power series in s with coefficients in $\overline{W}_f$.

Definition. Let χ: $Gal(K_\infty/K) \to \mathbb{C}_p^*$ be a character of finite order, and let τ be an anti-cyclotomic p-adic logarithm over K. Assume that the conditions in (6) hold. Then we define the Mellin-Mazur transform of μ_f associated to τ and χ as the power series

$$h_{f,\tau}(\chi,s) = \sum_{n\geq 0} \frac{1}{n!} \left(\int_{I_\infty/F} \chi\tau^n \, d\mu_f \right) s^n$$

in $\overline{W}_f[[s]]$.

Proposition 2. Let $n\geq 1$ and let $\chi: I_n/F_n \to \mathbb{C}_p^*$ be a character such that the inflation $\tilde{\chi}: I_n \to \mathbb{C}_p^*$ of χ is primitive (i.e. not induced by a character of I_m with $m<n$). Then

$$h_{f,\tau}(\chi,0) = \varrho^{-n} \sum_{A\in I_n} \tilde{\chi}(A)y_f(O_n,n_n,A).$$

The proof is standard and will be left to the reader.

Proposition 3. Let χ_0 be the trivial character, let $p>3$ and assume that $(\frac{D}{p})=-1$. Then

$$h_{f,\tau}(\chi_0,0) = \frac{1}{|F_0|} (1-\varrho^{-2}) \sum_{A\in I_0} y_f(\sigma,\varkappa,A).$$

This is proved by arguments similar to those used in the proof of Theorem 1. In general, the value $h_{f,\tau}(\chi_0,0)$ is given as the sum of

$$\frac{\alpha}{|F_0|} (\alpha^{-1}+p\varrho^{-2}(\alpha-1)+\varrho^{-2}(\tfrac{D}{p})) \sum_{A\in I_0} y_f(\sigma,\varkappa,A) \qquad (\alpha=[O^*:O_1^*])$$

and a certain correction term (vanishing for $(\frac{D}{p})=-1$) which arises from the fact that the order of $\ker\pi_1$ is $\alpha^{-1}(p-(\frac{D}{p}))$ and so depends on the value of $(\frac{D}{p})$.

§5. Complements

5.1. Relation of μ_f to Mazur's distribution

The following observations were kindly suggested to me by P. Schneider.

Assume that A_f is of dimension 1, let σ be a p-adic cyclotomic logarithm over K and let $\langle\ ,\ \rangle_\sigma$ be the p-adic height pairing on $A_f(K_\infty)$ associated to σ ([9], §20.). Let $\check{\mu}_f = \{\check{\mu}_{f,n}\}_{n\geq 1}$ be the distribution on I_∞/F defined by

$$\check{\mu}_{f,n}(\bar{A}) = \mu_{f,n}(\overline{A^{-1}})$$

and define the convolution product

$$(\mu_f * \check{\mu}_f)_n(\bar{A}) = \sum_{\bar{B}\bar{C}=\bar{A}} \langle \mu_{f,n}(\bar{B}), \check{\mu}_{f,n}(\bar{C})\rangle_\sigma .$$

Then $\mu_f * \check{\mu}_f$ is a $\mathbb{C}_p$-valued distribution. Since ν_f is of Galois type in the sense of [16], i.e.

$$\nu_{f,n}([\alpha]) = \nu_{f,n}([\theta_n])^{\sigma[\alpha^{-1}]}$$

(cf. §2. for notation), we can easily check (using the invariance of $\langle\ ,\ \rangle_\sigma$ under the action of $\mathrm{Gal}(K_\infty/K)$) that

$$(\mu_f * \check{\mu}_f)_n(\bar{A}) = p^n \langle \mu_{f,n}(\overline{[\theta_n]}), \mu_{f,n}(\bar{A})\rangle_\sigma .$$

The distribution $\mu_f * \check{\mu}_f$ therefore is of the same kind as the distribution constructed by Mazur in [9], §22. Mazur's distribution plays an important role in the work of Perrin-Riou ([12]) on a p-adic version of the theory of Gross-Zagier.

5.2. Zeros of $h_{f,\tau}(\chi,s)$

For simplicity suppose p>2. If we fix an isomorphism κ: $\mathrm{Gal}(K_\infty/K) \xrightarrow{\sim} 1+p\mathbb{Z}_p$, then $\tau = c\log_p \circ \kappa$ with $c \in \mathbb{Q}_p^*$ and therefore

$$h_{f,\tau}(\chi,s) = \int_{I_\infty/F} \chi\, \exp_p(cs\cdot\log_p\circ\kappa)\, d\mu_f$$

($\log_p$ and $\exp_p$ denote the p-adic logarithm and exponential, respectively) Clearly, the integral converges for $|s|_p < r := p^\delta |c|_p^{-1}$ $(\delta = 1-\frac{1}{p-1})$. If we fix a topological generator γ of I_∞/F, then

$$h_{f,\tau}(\chi,s) = H_{f,\tau}(\chi, \exp_p(cs\log_p(\kappa(\gamma))-1) \qquad (|s|_p < r)$$

with a power series $H_{f,\tau}(\chi,T) \in \bar{W}_f[[T]]$. Now if $|a_p|_p = 1$, then μ_f is a measure and hence the coefficients of $H_{f,\tau}(\chi,T)$ are bounded. One may then ask whether $H_{f,\tau}(\chi,s)$ -if not identically zero- has only finitely many zeros for $|s|_p < r$. This is in fact true. The argument which was pointed out to me by P. Schneider, runs as follows.

Let L be a finite extension of $\mathbb{Q}_p$ containing ϱ and all the Fourier coefficients a_n of f. Let U be the completion w.r.t. $\|\cdot\|$ of the f-eigenspace in $L\otimes_{\mathbf{Z}} J_0(N)(K_\infty)$. According to [15], Cor. 2.4. and Thm. 4.15. the space U is pseudo-reflexive and hence, in particular, the natural map of U to its topological bidual is injective (loc.cit. p.60). Therefore if we set $H(T) = H_{f,\tau}(\chi,T)$ and write

$$H(T) = \sum_{n\geq n_0} u_n T^n$$

with $u_{n_0} \neq 0$, then there is a bounded linear map $\ell: U \to L$ with $\ell(u_{n_0}) \neq 0$. It follows that the power series

$$H_\ell(T) = \sum_{n\geq n_0} \ell(u_n) T^n \in L[[T]]$$

is not identically zero and has bounded coefficients, and that

$$H_\ell(s) = (1\hat{\otimes}\ell)(H)(s) \qquad (|s|_p < r),$$

where $1\hat{\otimes}\ell$ is the natural extension of ℓ to $\overline{W}_f = \mathbb{C}_p \otimes_L U$ (for the precise meaning of the symbol "$\check{\otimes}$" cf. [15]). Since by the Weierstrass Preparation Theorem $H_\ell(s)$ has only finitely many zeros for $|s|_p < r$, the result follows for H(T).

According to the above we can write

$$H_{f,\tau}(\chi,T) = P_{f,\tau}(\chi,T)\, H^{(0)}_{f,\tau}(\chi,T),$$

where $P_{f,\tau}(\chi,T)$ is a polynomial <u>with coefficients in</u> $\mathbb{C}_p$ whose zeros coincide with those of $h_{f,\tau}(\chi,s)$ for $|s|_p < r$ and $H^{(0)}_{f,\tau}(\chi,T) \in \overline{W}_f[[T]]$, $H^{(0)}_{f,\tau}(\chi,s) \neq 0$ for all s with $|s|_p < r$. Does the polynomial $P_{f,\tau}(\chi,T)$ have any arithmetical meaning?

5.3. A distribution induced by μ_f

We would like to describe how μ_f induces a distribution in a somewhat different way. Suppose again that $A_f = E$ is an elliptic curve defined over $\mathbb{Q}$ and assume that E is given by a Néron minimal equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_\nu \in \mathbf{Z}).$$

Let $\mathfrak{p}$ be a prime of K lying above p and let $\mathfrak{P}$ be a prime of K_∞ lying above $\mathfrak{p}$. Denote by $\tilde{K}_\infty$ the completion of K_∞ at $\mathfrak{P}$. Reduction mod $\mathfrak{P}$ induces an isomorphism

$$E(\tilde{K}_\infty)/E_0(\tilde{K}_\infty) \cong \bar{E}(k_\infty)$$

where $E_0(\tilde{K}_\infty)$ is the kernel of the reduction map, $\bar{E}$ is the reduced curve mod $\mathfrak{P}$ and k_∞ is the residue field. Since K_∞/K is totally ramified at $\mathfrak{p}$ we have $k_\infty=\mathcal{O}/\mathfrak{p}$. Put

(14) $$r=|\bar{E}(k_\infty)|\ .$$

View x and y as rational functions on E having poles of orders 2 and 3, respectively, at the origin O of E and put $t=-\frac{x}{y}$. Let

$$\omega = \frac{dx}{2y+a_1x+a_3}$$

be a differential of the first kind on E and write

$$\omega(t) = \sum_{n\geq 0} h_n t^n$$

with $h_n \in \mathbf{Z}[a_1,\ldots,a_6]$ and $h_0=1$. Let

$$L(t) = \int \omega(t)dt = \sum_{n\geq 1} h_{n-1}\frac{t^n}{n}$$

be the elliptic logarithm of the formal group of E, and let

$$E_{\mathfrak{P}} = \{P\in E_0(\tilde{K}_\infty) \mid |t(P)|_p<1\}.$$

Then $E_{\mathfrak{P}}$ is a subgroup of $E_0(\tilde{K}_\infty)$, and the map

$$P\mapsto L(t(P))$$

is a homomorphism of $E_{\mathfrak{P}}$ to the additive group of $\tilde{K}_\infty$ (cf. e.g. [5], chap.III,§3.).

The distribution μ_f now gives rise to a $\tilde{K}_\infty$-valued distribution $\tilde{\mu}_f = \{\tilde{\mu}_{f,n}\}_{n\geq 1}$ defined by

$$\tilde{\mu}_{f,n} = (id\otimes L\circ t)\circ(id\otimes \bar{r})\circ\mu_{f,n},$$

where r denotes multiplication by r (cf. (14)) and id is the identity map of $\mathbf{Z}_p$. Elementary estimates for the rate of growth of L only show that $\tilde{\mu}_f$ is of growth 1 in the sense of [8], i.e. $|\tilde{\mu}_{f,n}|_p\leq p^{n+c}$ where c is a constant, and so it is not clear if analytic functions could be integrated.

Nevertheless, if χ is a primitive character on I_n/F_n ($n \geq 1$) we might ask for the meaning of the sum

$$\sum_{A \in I_n/F_n} \chi(A)\tilde{\mu}_{f,n}(A).$$

Is there any analogy with Leopoldt's analytic formula giving the value of the Kubota-Leopoldt p-adic L-function of a primitive non-principal Dirichlet character at s=1 in terms of the p-adic logarithm?

References

[1] R.Greenberg, On the Birch and Swinnerton-Dyer conjecture, Invent. math. 72, 241-265 (1983)

[2] B.H.Gross, Heegner points on $X_0(N)$, in: Modular Forms, ed. R.A. Rankin, Ellis Horwood Series Mathematics and its Applications, Chichester, 87-105 (1985)

[3] B.H.Gross, D.Zagier, Heegner points and derivatives of L-series, to appear in Invent. math.

[4] P.K.Kurcanov, The zeta functions of elliptic curves over certain abelian extensions of imaginary quadratic fields, Math. USSR Sbornik 31, 49-62 (1977)

[5] S.Lang, Elliptic Curves: Diophantine Analysis, Grundlehren der Math. Wiss., No.231, Springer, Berlin-Heidelberg-New York

[6] J.I.Manin, Periods of modular forms and p-adic Hecke series, Math. USSR Sbornik 21, 371-393 (1973)

[7] B.Mazur, H.P.F.Swinnerton-Dyer, Arithmetic of Weil curves, Invent. math. 25, 1-61 (1974)

[8] B.Mazur, A meromorphic continuation of the Gauss sum, manuscript, unpublished

[9] B.Mazur, Modular curves and arithmetic, Proceedings of the International Congress of Mathematicians, Warszawa August 16-24, 1983, Vol. 1, PWN, North Holland (1984)

[10] B.Perrin-Riou, Arithmétique des courbes elliptiques et théorie d' Iwasawa, Mem. Soc. Math. France 17 (1984)

[11] B.Perrin-Riou, Fonctions L p-adiques, théorie d' Iwasawa et points de Heegner, preprint (1985)

[12] B.Perrin-Riou, Fonctions L p-adiques et points de Heegner, preprint (1985)

[13] D.E.Rohrlich, On L-functions of elliptic curves and anti-cyclotomic towers, Invent. math. 75, 383-408 (1984)

[14] D.E.Rohrlich, On L-functions of elliptic curves and cyclotomic towers, Invent. math. 75, 409-423 (1984)

[15] A.van Rooij, Non-archimedean functional analysis, Marcel Dekker (1985)

[16] P.Schneider, letter to the author, September 19, 1985

[17] G.Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Iwanami Shoten, Princeton 1971