Proceedings of Symposia in Pure Mathematics
Volume 29, 1975

P-ADIC INTERPOLATION VIA HILBERT MODULAR FORMS

Kenneth A. Ribet

Katz's article [3] was primarily concerned with the question of constructing p-adic measures $\mu^{(a)}$ on $\mathbb{Z}_p$ whose moments are the values at negative integers of the Riemann zeta function. Here we shall try to generalize one of the approaches discussed by Katz, the technique involving modular forms, to study instead the values at negative integers of the zeta function attached to any number field.

I. Deligne's Integrality Theorem

To begin, let K be a number field and let $\zeta_K(s)$ be its Dedekind zeta function. Since the values ζ_K at negative integers are all zero if K is not totally real, we shall assume that K is a totally real field. The values of ζ_K at negative even integers are in any case zero, and $\zeta_K(0) = 0$ except when $K = \mathbb{Q}$ $(\zeta_{\mathbb{Q}}(0) = -1/2)$. Moreover, according to a result of Siegel ([6], p. 136), the numbers

$$\zeta_K(1-k), \quad k \geq 1$$

are rational.

It is therefore natural to ask whether or not the function

$$k \to \zeta_K(1-k)$$

has p-adic properties analogous to those of the Riemann zeta function. Given the situation for $\zeta_{\mathbb{Q}}$, in fact, we might try to construct p-adic measures $\mu^{(a)}$ on $\mathbb{Z}_p$ whose moments satisfy

$$\int x^{k-1}\, d\mu^{(a)} = f(k,\mu^{(a)})\cdot \zeta_K(1-k),$$

where $f(k,\mu^{(a)})$ is a simple "fudge factor" analogous to the factor $1-a^k$ that comes up when $K = \mathbb{Q}$. Again (to continue the analogy) we might look for Eisenstein series g_k which have q-expansions

$$\sum_{n \geq 0} a_{nk}\, q^n$$

such that $a_{nk} \in \mathbb{Z}$ for $n \geq 1$ and such that a_{0k} is essentially $\zeta_K(1-k)$. These are provided by the following result.

Theorem (Siegel, Serre [5]). For each $k \geq 1$, there exists a modular form g_k of weight $kr = k\cdot[K:\mathbb{Q}]$ whose q-expansion has constant term

$$a_{0k} = 2^{-r}\cdot\zeta_K(1-k)$$

and higher terms

$$a_{nk} = \begin{cases} 0 & \text{if } k \text{ is odd} \\ \displaystyle\sum_{\substack{Tr(x) = n \\ x \in \mathfrak{d}^{-1} \\ x \gg 0}} \; \sum_{\mathfrak{N} \mid (x)\mathfrak{d}} (N\mathfrak{N})^{k-1} & \text{if } k \text{ is even.} \end{cases}$$

(In the double sum we sum first over a finite set of elements x of the inverse different $\mathfrak{d}^{-1}$ of K, and for each x we then sum over the (finite) set of integral ideals $\mathfrak{N}$ which divide the ideal $(x)\mathfrak{d}$.)

Now let p be a prime. By combining the above theorem with the technique of ([3],§XII) we get measures $\mu^{(a)}$ with the desired property:

Theorem 1. For each $a \in \mathbb{Z}_p^*$ there exists a $\mathbb{V}$-valued measure $\mu^{(a)}$ on $\mathbb{Z}_p$ whose moments are given by the formula

$$\int_{\mathbb{Z}_p} x^{k-1}\, d\mu^{(a)} = (1-a^{kr})g_k.$$

Corollary. For each $a \in \mathbb{Z}_p^*$ there exists a $\mathbb{Z}_p$-valued measure $\mu^{(a)}$ on $\mathbb{Z}_p$ such that

$$\int_{\mathbb{Z}_p} x^{k-1}\, d\mu^{(a)} = (1-a^{kr})\, 2^{-r}\, \zeta_K(1-k)$$

for $k \geq 1$. Consequently, the number $2^{-r}\zeta_K(1-k)$ is p-integral if $kr \not\equiv 0 \pmod{p-1}$.

As Serre pointed out in his Antwerp lectures, this corollary does not give the "best" integrality statement for values of ζ_K at negative integers (cf. [4], p. 164). Indeed, we have the following result of Deligne.

Theorem 2([2]). The quantity $2^{-r}\zeta_K(1-k)$ is p-integral whenever $kd \not\equiv 0$ (mod p-1), where d is the degree over $\mathbb{Q}$ of the intersection of K with the field $\mathbb{Q}(\mu_{p^\infty})$ of p-power roots of unity.

The idea behind this theorem is Serre's suggestion that g_k be viewed not merely as a function on the $\mathcal{M}^{triv}$ of [3] but instead as the restriction to $\mathcal{M}^{triv}$ of a function G_k defined on a larger moduli scheme, the Hilbert-Blumenthal scheme $\mathcal{M}_K^{triv}$ discussed below. This is possible since functions on $\mathcal{M}_K^{triv}$ are p-adic Hilbert modular functions (just as functions on Katz's $\mathcal{M}^{triv}$ are generalized one-variable p-adic modular functions), whereas g_k by its very construction over $\mathbb{C}$ is the restriction to the usual upper half plane of a Hilbert modular form G_k whose (generalized) q-expansion is rational [7]. The point, in other words, is to make algebraic sense out of Siegel's G_k. Doing this allows us to construct a new family of measures μ on $\mathbb{Z}_p$ so that for each k satisfying $kd \not\equiv 0$ (mod p-1) there is a measure μ for which the fudge factor $f(k,\mu)$ is a unit.

II. The Hilbert-Blumenthal Scheme $\mathcal{M}_K^{triv}$

We first need a notion replacing that of an elliptic curve /R. Let O be the integer ring of K. A Hilbert-Blumenthal structure over a ring R is an abelian scheme X/R together with an inclusion

$$m: \mathcal{O} \hookrightarrow \mathrm{End}_R\, X$$

which makes Lie (X), the tangent space to X at the origin, free of rank 1 over $\mathcal{O} \otimes R$. A trivialization of such a structure over a p-adically complete and separated R is an isomorphism of formal groups

$$\varphi: \mathcal{O} \otimes_{\mathbb{Z}} \hat{\mathbb{G}}_m \xrightarrow{\sim} \hat{X}.$$

If X admits such a trivialization, then X is (fibre-by-fibre) ordinary. Given an ordinary Hilbert-Blumenthal structure over R (i.e., a structure with X ordinary) there will in general be no trivialization over R. However, if φ is one trivialization, then we can get other trivializations $\underline{a}\varphi$ by "twisting" φ by elements $\underline{a}$ of

$$\mathrm{Aut}(\mathcal{O} \otimes \hat{\mathbb{G}}_m) = (\mathcal{O} \otimes \mathbb{Z}_p)^*.$$

Now we define two stacks on the category of p-adically complete and separated rings:

$$\begin{cases} \mathcal{M}_K^{\mathrm{triv}}(R) = \text{the trivialized Hilbert-Blumenthal structures } /R \\ \mathcal{M}_K^{\mathrm{ord}}(R) = \text{the ordinary Hilbert-Blumenthal structures } /R. \end{cases}$$

These are direct generalizations of the stacks $\mathcal{M}^{\mathrm{triv}}$ and $\mathcal{M}^{\mathrm{ord}}$ of elliptic curves associated to the "one-variable case," and they are connected by a "Galois" covering

$$\begin{array}{c} \mathcal{M}_K^{\mathrm{triv}} \\ \downarrow \\ \mathcal{M}_K^{\mathrm{ord}} \end{array}$$

with structural group $(\mathcal{O} \otimes \mathbb{Z}_p)^*$. As before, the stack $\mathcal{M}_K^{\mathrm{triv}}$ "is" the formal affine scheme over $\mathbb{Z}_p$ which represents the functor

$$R \mapsto \begin{array}{l}\text{isomorphism classes of trivialized}\\ \text{Hilbert-Blumenthal structures } /R .\end{array}$$

In analogy with the elliptic curve case, we call elements of the coordinate ring $\mathbb{V}_K$ of $\mathcal{M}_K^{\mathrm{triv}}$ p-adic Hilbert modular functions (over $\mathbb{Z}_p$). Given any trivialized structure (X,m,φ) over a p-adically complete and separated R, we can evaluate any $f \in \mathbb{V}_K$ at (X,m,φ) to get a number $f(X,m,\varphi)$ in R.

Now let $N:(\mathcal{O} \otimes \mathbb{Z}_p)^* \to \mathbb{Z}_p^*$ be the norm. Also, given $a \in (\mathcal{O} \otimes \mathbb{Z}_p)^*$ and $f \in \mathbb{V}_K$, let $[a]f$ be the function satisfying for each (X,m,φ):

$$([a]f)(X,m,\varphi) \quad = \quad f(X,m,a^{-1}\varphi)$$

This rule defines an operation $[a]$ on $\mathbb{V}_K$, which we extend by linearity to $V_K\left[\frac{1}{p}\right]$.

<u>Definition</u>. A function $f \in \mathbb{V}_K\left[\frac{1}{p}\right]$ has <u>weight</u> <u>k</u> if

$$[a]\, f \quad = \quad (Na)^k f.$$

for every $a \in (\mathcal{O} \otimes \mathbb{Z}_p)^*$.

<u>Theorem</u> (Siegel). For each $k \geq 1$ there exists a function $G_k \in \mathbb{V}_K\left[\frac{1}{p}\right]$ which has weight k and a (generalized) q-expansion whose constant term is $2^{-r}\zeta_K(1-k)$ and whose higher coefficients are all integers.

As mentioned earlier, this is the "key point." To prove this result, one constructs G_k as a classical Hilbert modular form [7] and observes that the "q-expansion" of G_k is rational. By the analogue of the q-expansion principle, G_k is a Hilbert modular form which is "defined over $\mathbb{Q}$." Thus it is a (negative) power of p times a Hilbert modular form over $\mathbb{Z}_p$. But on the other hand, we can view a true modular form as a p-adic modular function just as in the one-variable case; this gives exactly what is desired.

The legitimacy of this chain of reasoning rests on our knowing what the q-expansion of a Hilbert modular form actually is and our knowing that a function is determined by its q-expansion (at least in characteristic 0). We will return soon to the latter point, although we will ignore the former point from now on. Incidentally, the theory of q-expansions for Hilbert modular forms is contained in the (unpublished) work of M. Rapoport on the Hilbert modular scheme.

Assuming a satisfactory theory of q-expansions we will prove for $\mathbb{V}_K$ a

Key Lemma. Let $h \in \mathbb{V}_K\left[\frac{1}{p}\right]$ be a function whose q-expansion is p-integral except perhaps for its constant term. Then for each $a \in (\mathcal{O} \otimes \mathbb{Z}_p)^*$ the difference

$$h - [a]h$$

belongs to $\mathbb{V}_K$.

Proof. Let c be the constant term of the q-expansion of h. Then $h - c$ belongs to $\mathbb{V}_K$ because it is an element of $\mathbb{V}_K\left[\frac{1}{p}\right]$ with integral q-expansion. Since $[a]c = c$, we have

$$h - [a]h = (h-c) - [a](h-c) \in \mathbb{V}_K.$$

Theorem 3. For each $a \in (\mathcal{O} \otimes \mathbb{Z}_p)^*$, the number

$$\{1 - (\mathrm{N}a)^k\}\, 2^{-r}\zeta_K(1-k)$$

is p-integral.

Proof. Since G_K has weight k,

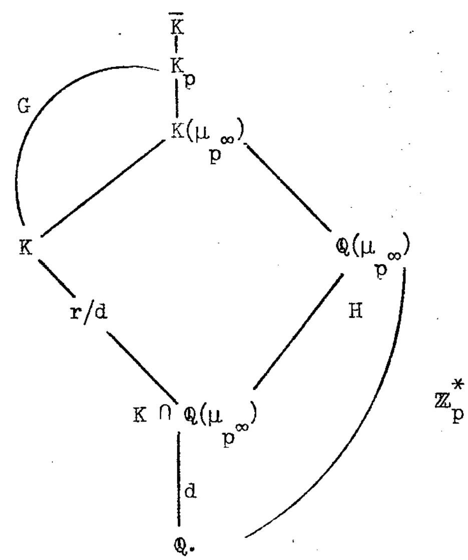
$$G_k - [a]G_k = \{1 - (\mathrm{N}a)^k\}G_k.$$

The former is an element of $\mathbb{V}_K$ by the Key Lemma, so in particular it has an integral q-expansion. Therefore the constant term of $\{1 - (\mathrm{N}a)^k\}G_k$ is integral; this is exactly what we want.

Now if a is in $\mathbb{Z}_p^*$, then $\mathrm{N}a = a^r$. Hence Theorem 3 tells us in particular that

$$(1-a^{rk})2^{-r}\zeta(1-k)$$

is p-integral whenever $a \in \mathbb{Z}_p^*$; this is Theorem 1 (or more precisely its corollary). On the other hand, Theorem 3 is a consequence of Theorem 2. Indeed, let K_p be the largest abelian extension of K which is unramified away from p, and let $G = \mathrm{Gal}(K_p/K)$. Let μ_{p^∞} be the group of p-power roots of unity in $\overline{K}$. Then we have a diagram



Restriction provides a norm map $N: G \to \mathbb{Z}_p^*$ whose image H is

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty}) : K \cap \mathbb{Q}(\mu_{p^\infty})).$$

Thus the image of G in $\mathbb{Z}_p^*$ has index $d = [K \cap \mathbb{Q}(\mu_{p^\infty}) : \mathbb{Q}]$. If j is the composition of the natural inclusion

$$(\mathcal{O} \otimes \mathbb{Z}_p)^* \hookrightarrow (\text{Idèles of } K)$$

with the Artin map

$$(\text{Idèles of } K) \to \mathrm{Gal}(K_p/K),$$

then j is a map $(\mathcal{O} \otimes \mathbb{Z}_p)^* \to G$, and the diagram

$$\begin{array}{ccc} (\mathcal{O} \otimes \mathbb{Z}_p)^* & \xrightarrow{\ j\ } & G \\ & {\scriptstyle N}\searrow \quad \swarrow{\scriptstyle N} & \\ & \mathbb{Z}_p^* & \end{array}$$

is (anti-) commutative. It follows that

$$(\mathbb{Z}_p^*)^d = H \supseteq N[(\mathcal{O} \otimes \mathbb{Z}_p)^*]$$

and this shows that Theorem 2 implies Theorem 3. In other words, we have obtained a result intermediate between the one-variable theorem (Theorem 1) and the "good" theorem (Theorem 2) essentially by shifting our perspective and working with $\mathcal{M}_K^{\mathrm{triv}}$ instead of $\mathcal{M}^{\mathrm{triv}} = \mathcal{M}_{\mathbb{Q}}^{\mathrm{triv}}$.

III. Irreducibility of the Covering $\mathcal{M}_K^{\mathrm{triv}} \to \mathcal{M}_K^{\mathrm{ord}}$.

In the case of modular functions of one variable, Katz obtained the main facts concerning q-expansions as a corollary of the irreducibility of $\mathcal{M}^{\mathrm{triv}}$ ([3], § XI). Here we will discuss the question of irreducibility for $\mathcal{M}_K^{\mathrm{triv}}$.

The first difficulty is that in general the base $\mathcal{M}_K^{\mathrm{ord}}$ is not connected. Indeed, if X/k is a Hilbert-Blumenthal structure over an algebraically closed field, we define its polarization module $\mathcal{P} = \mathcal{P}(X)$, a certain invertible $\mathcal{O}$-module "with positivity," as follows: $\mathcal{P}$ is the set of $\mathcal{O}$-homomorphisms $f \in \mathrm{Hom}_k(X,\hat{X})$ which are symmetric in the sense that $f = \hat{f}$ (note that $\hat{f}$ is a map $X = \hat{\hat{X}} \to \hat{X}$ just as f is); $f \in \mathcal{P}$ is positive if f is a polarization of X, i.e., an isogeny $X \to \hat{X}$ associated to some ample line bundle on X. Now just as the isomorphism classes of invertible $\mathcal{O}$-modules are the ideal classes of K, so the isomorphism classes of invertible $\mathcal{O}$-modules with positivity are the strict ideal classes of K. Thus, taking $\mathcal{P}(X)$ to its isomorphism class enables us to associate to the Hilbert-Blumenthal structure X a strict ideal class of K. It turns out that this association decomposes $\mathcal{M}_K^{\text{ord}}$ into components $\mathcal{M}_{K,\mathfrak{G}}^{\text{ord}}$ parameterized by the strict ideal classes of K and that each component $\mathcal{M}_{K,\mathfrak{G}}^{\text{ord}}$ is geometrically irreducible.

For each $\mathfrak{G}$, let $\mathcal{M}_{K,\mathfrak{G}}^{\text{triv}}$ be the fibre of $\mathcal{M}_K^{\text{triv}}$ over $\mathcal{M}_{K,\mathfrak{G}}^{\text{ord}}$. We still have for each $\mathfrak{G}$ a covering

$$\begin{array}{c}\mathcal{M}_{K,\mathfrak{G}}^{\text{triv}}\\ \big\downarrow\\ \mathcal{M}_{K,\mathfrak{G}}^{\text{ord}}\end{array}$$

with structural group $(0 \otimes \mathbb{Z}_p)^*$

<u>Theorem</u>. The scheme $\mathcal{M}_{K,\mathfrak{G}}^{\text{triv}}$ is geometrically irreducible.

As explained by Katz, the covering gives rise to a character

$$\chi: \pi_1(\mathcal{M}_{K,\mathfrak{G}}^{\text{ord}}) \to (0 \otimes \mathbb{Z}_p)^*$$

and (given the irreducibility of the base) the theorem is equivalent to the surjectivity of

$$\chi \mid \pi_1(\mathcal{M}_{K,\mathfrak{G}}^{\text{ord}} \otimes \bar{\mathbb{F}}_p)$$

For simplicity, we will prove this only when $\mathfrak{G}$ is the class of the inverse different $\mathfrak{d}^{-1}$ of K.

For convenience, let us adopt the following notation:

$$\mathcal{M}^{\text{triv}} = \mathcal{M}_{K,\mathfrak{G}}^{\text{triv}} \otimes \mathbb{F}_p,$$

$$\mathcal{M} = \mathcal{M}_{K,\mathfrak{G}}^{\text{ord}} \otimes \mathbb{F}_p,$$

$$0_p = 0 \otimes \mathbb{Z}_p.$$

Also, let χ now be the character

$$\pi_1(\mathcal{M}) \to O_p^*$$

arising from the covering

$$\mathcal{M}^{\text{triv}} \to \mathcal{M}.$$

What we want to prove is the surjectivity of

$$\chi \mid \pi_1(\mathcal{M} \otimes \bar{\mathbb{F}}_p).$$

Since π_1 is compact and χ is continuous, it is enough to prove for each positive integer k that the image G of $\pi_1(\mathcal{M} \otimes \bar{\mathbb{F}}_p)$ in $(O/p^kO)^*$ is all of $(O/p^kO)^*$. But on the other hand, G is clearly the intersection

$$\bigcap_n G_n,$$

where G_n is the image in $(O/p^kO)^*$ of $\pi_1(\mathcal{M} \otimes \mathbb{F}_{p^n})$. So it suffices to prove that $G_n = (O/p^kO)^*$ for all n sufficiently large.

Suppose that $\alpha \in (O/p^kO)^*$. Choose $a \in O$ congruent to α mod p^k. Let $n \geq k$ be an integer large enough so that $a^2 - 4p^n$ is totally negative. Let T be the free $\mathbb{Z}$-module

$$O[x]/(x^2 - ax + p^n)$$

of rank $2\cdot[K:\mathbb{Q}]$ and let F be the endomorphism "multiplication by x" on T. One checks easily that the pair (T,F) satisfies hypotheses (a), (b), and (c) of the main theorem of [1]. Let X be the ordinary abelian variety over $\mathbb{F}_{p^n}$ associated to (T,F) by that main theorem, and let

$$m: O \hookrightarrow \mathrm{End}_{\mathbb{F}_{p^n}}(X)$$

be the map arising from the F-linear action of O on T. To check that (X,m) is a Hilbert-Blumenthal structure, we note that Lie(x) is dual to the kernel of F on $T \otimes_{\mathbb{Z}} \mathbb{F}_{p^n}$ and observe that this kernel is free of rank 1 over $O \otimes \mathbb{F}_{p^n}$.

Also, I claim that the polarization module attached to X is $\mathfrak{d}^{-1}$. For this, let

$$\hat{T} = T \otimes_O \mathfrak{d}^{-1}$$

and define a pairing $\langle \ , \ \rangle : T \times \hat{T} \to 2\pi i\, \mathbb{Z}$ by the formula

$$\langle a+bx,\ c+dx\rangle \;=\; 2\pi i \cdot tr_{O/\mathbb{Z}}(ad - bc).$$

Then the pair consisting of $\hat{T}$ and its map "multiplication by x" represents the dual variety $\hat{X}$ to X. Therefore the O-module of O-homomorphisms from $X/\mathbb{F}_{p^n}$ to its dual is given by

$$\mathrm{Hom}_{O[x]}(T,\hat{T}) \xrightarrow{\sim} \hat{T},$$

the isomorphism being the map $f \mapsto f(1)$. Now if f belongs to this module, then its dual is the map $\hat{f} \in \mathrm{Hom}_{O[x]}(T,\hat{T})$ which satisfies

$$\langle f(t),u\rangle^{\wedge} \;=\; \langle t,\hat{f}(u)\rangle$$

for all $t,\ u \in T$, where $\langle \ , \ \rangle^{\wedge}$ is the pairing on $\hat{T} \times T \;=\; \hat{T} \times \hat{\hat{T}}$ analogous to $\langle \ , \ \rangle$. (Thus $\langle w,z\rangle^{\wedge} = -\langle z,w\rangle$.) Thus f is symmetric (i.e., f is an element of $\mathcal{P}(X)$) if and only if $\langle f(t),u\rangle^{\wedge} = \langle t,f(u)\rangle$. This equation holds exactly when $f(1) \in \mathfrak{d}^{-1}$ as follows immediately from the definition of $\langle \ , \ \rangle$; thus $\mathcal{P}(X)$ is the O-submodule $\mathfrak{d}^{-1}\cdot 1$ of $\hat{T}$.

Now if T'_p is the Tate module attached to X, viewed as an O_p-module, then Deligne's recipe tells us that the Frobenius endomorphism of X acts on T'_p by multiplication by ξ, where ξ is the unique element of $(O \otimes \mathbb{Z}_p)^*$ which satisfies

$$\xi^2 - a\xi + p^n = 0$$

So if x is the point of $\mathcal{M} \otimes \mathbb{F}_{p^n}$ defined by X and if $F_x \in \pi_1(\mathcal{M} \otimes \mathbb{F}_{p^n})$ is its Frobenius element (well-defined up to conjugation), then

$$\chi(F_x) \;=\; \xi.$$

Since

$$\xi^2 \equiv a\,\xi \mod p^n$$

we have

$$\xi \equiv a \mod p^k$$

because $k \leq n$. Thus the image of F_x in G_n is $(a \bmod p^k)$, or in other words α. So $\alpha \in G_n$. Therefore $(O/p^k O)^* = G_n$ provided that n is sufficiently large.

Bibliography

1. P. Deligne, Variétés abéliennes ordinaires sur un corps fini. Inventiones Math. 8 (1969), 238-243.

2. P. Deligne and K. Ribet, Values of abelian L-functions at negative integers. To appear.

3. N. Katz, p-adic L-functions via moduli of elliptic curves. In this volume.

4. J-P. Serre, Cohomologie des groupes discretes. In Prospects in Mathematics, Ann. Math. Studies 70, Princeton University Press (1971).

5. J-P. Serre, Formes modulaires et fonctions zêta p-adiques. Proceedings Antwerp Summer School, 1972. Springer Lecture Notes in Mathematics 350 (1973).

6. C. L. Siegel, Lectures on the analytical theory of quadratic forms (1934-35). Institute for Advanced Study Lecture Notes, Reprinted 1955.

7. C. L. Siegel, Berechnung von Zetafunktionen au ganzzahligen Stellen. Gött. Nach., (1969), 87-102.

PRINCETON UNIVERSITY