[20] KATZ N.- The regularity theorem in algebraic geometry, Actes Congrès Intern. Math. 1970, I, pp. 437-443, Gauthier-Villars.

[21] KATZ N.- Introduction aux travaux récents de Dwork, 1970.

[22] KATZ N. and MESSING W.- Some Consequences of the Riemann Hypothesis for Varieties over Finite Fields, Inventiones Math. 23, 73-77 (1974).

[23] KATZ N. and ODA T.- On the differentiation of De Rham cohomology classes with respect to parameters, Kyoto Math. J., Vol. 8, n° 2, 1968.

[24] MAZUR B.- Frobenius and the Hodge filtration, Bull. Amer. Math. Soc., Vol. 78, n° 5, 1972.

[25] MAZUR B.- Frobenius and the Hodge filtration (estimates), Ann. of Math., 98 (1973), pp. 58-95.

[26] MAZUR B.- Eigenvalues of Frobenius acting on algebraic varieties over finite fields, this volume.

[27] MAZUR B. and MESSING W.- Universal Extensions and One Dimensional Crystalline Cohomology, Lecture Notes n° 370.

[28] MESSING W.- The Crystals associated to Barsotti-Tate Groups, Lecture Notes n° 264.

[29] MESSING W.- The Universal Extension of an Abelian Variety by a Vector Group, Istituto Nazionale di Alta Matematica, Symposia Mathematica, Vol. XI (1973).

[30] MONSKY P. and WASHNITZER G.- Formal Cohomology I, Annals of Math. 88 (1968), pp. 181-217.

[31] ROBY N.- Lois polynômes et lois formelles en théorie des modules, Ann. de l'ENS, 80, 1963, pp. 213-348.

[32] ROBY N.- Les algèbres à puissances divisées, Bull. Soc. Math. France, 89, pp. 75-91, 1965.

[33] SERRE J.P.- Sur la topologie des variétés algébriques en caractéristique p, Symposium Internacional de Topologia algebraica, Mexico 1958.

CNRS PARIS

Proceedings of Symposia in Pure Mathematics
Volume 29, 1975

P-ADIC L-FUNCTIONS VIA MODULI OF ELLIPTIC CURVES

Nicholas M. Katz

The first half of the paper is quite elementary. We explain the relation between p-adic congruences for zeta-values and p-adic measures, and then we give an Eulerian construction of the p-adic measure required for zeta and L-functions of $\mathbb{Q}$. Unfortunately, such elementary constructions are unknown for other number fields.

The second half is less elementary. We explain the basic facts about the moduli of p-adic elliptic curves. We then show how to use the resulting theory of "generalized modular functions" to construct p-adic measures and explain how these measures lead to the p-adic interpolation of certain "L-series with grossencharacter" of quadratic imaginary fields.

I would like to thank Neal Koblitz for preparing a preliminary version of this paper based on my lecture at the conference.

I. p-adic congruences for zeta (Euler, Kummer, Kubota-Leopoldt)

The theory of p-adic zeta functions may be said to have begun when Euler discovered that the Riemann zeta function $\zeta(s)$ assumes rational values (essentially Bernoulli numbers) at negative integers.

Some two centuries later, Kummer was led to look at Bernoulli numbers when he discovered that the question of whether a given prime p was "regular" depended upon the p-adic shape of certain Bernoulli numbers. He

discovered the "Kummer congruences" between Bernoulli numbers, which we will record here as congruences between ζ-values.

Kummer Congruence If $k \geq 1$ is an integer not divisible by $p - 1$, then $\zeta(1-k)$ is p-integral, and the value of $\zeta(1-k)$ mod p depends only on the value of k mod $p - 1$. (If k is divisible by $p - 1$, $\zeta(1-k)$ is not p-integral).

In the late 1950's, Kubota and Leopoldt, in trying to understand this, discovered that much more was true. To state their results, it is convenient to introduce the auxiliary functions

$$\zeta^*(s) = (1 - p^{-s})\zeta(s)$$

and, for each integer $a \geq 2$ prime to p,

$$\zeta^{*,a}(s) = (1 - a^{1-s})\,\zeta^*(s).$$

Kubota-Leopoldt congruences:

I. If $k \geq 1$ is an integer, then $\zeta^{*,a}(1-k)$ is p-integral, and the value of $\zeta^{*,a}(1-k)$ mod p^{n+1} depends only on the value of k mod $(p-1)p^n$.

II. If $k \geq 1$ is an integer not divisible by $p - 1$, then $\zeta^*(1-k)$ is p-integral, and its value mod p^{n+1} depends only on the value of k mod $(p-1)p^n$.

In fact, II may be directly deduced from I by choosing a to be a primitive root mod p. Notice that we recover the Kummer congruences as the special case $n = o$ of II.

The viewpoint of Kubota-Leopoldt is this. For each integer b mod $p - 1$, let $S(b)$ denote the set of strictly positive integers $\equiv b$ mod $p - 1$. Then $S(b)$ is dense in $\mathbb{Z}_p$. By congruence I, the $\mathbb{Z}_p$-valued function on $S(b)$ defined by $k \mapsto \zeta^{*,a}(1-k)$ extends to a continous $\mathbb{Z}_p$-valued function on all of $\mathbb{Z}_p$. Such functions on $\mathbb{Z}_p$ are called p-adic zeta and L functions. In what follows, we will supress this point of view, and emphasize the actual

congruences which underlie it.

II. p-adic congruences from p-adic measures (Mazur)

Let us begin by recalling the notion of a p-adic measure. Let X be a compact and totally disconnected space. In the applications, it will always be either $\mathbb{Z}_p$, $\mathbb{Z}_p^\times$, a finite space, a galois group, or a finite product of the preceding. Let R be any ring which is complete and separated in its p-adic topology. For the time being, R will be $\mathbb{Z}_p$ itself, but later R will be very large.

Consider the ring $\mathrm{Contin}(X, \mathbb{Z}_p)$ of all continuous $\mathbb{Z}_p$-valued functions on the space X. A $\mathbb{Z}_p$-linear map (not necessarily a ring homomorphism)

$$\mu : \mathrm{Contin}(X, \mathbb{Z}_p) \to R$$

is called an R-valued p-adic measure on X. The identity $\mathrm{Contin}(X,R) = \mathrm{Contin}(X, \mathbb{Z}_p) \hat{\otimes} R$ shows that we can also view μ as an R-linear map $\mathrm{Contin}(X,R) \to R$. For $f : X \to \mathbb{Z}_p$ an element of $\mathrm{Contin}(X, \mathbb{Z}_p)$, we denote its image $\mu(f) \in R$ symbolically as

$$\int_X f d\mu \text{ , or } \int_X f(x)d\mu(x)$$

Obvious lemma Suppose that $f,g : X \to \mathbb{Z}_p$ are continuous functions, and that $f(x) \equiv g(x)$ mod p^n for all $x \in X$. Then

$$\int_X f d\mu \equiv \int_X g d\mu \quad \text{mod } p^n R$$

proof We have $f - g = p^n h$, with $h \in \mathrm{Contin}(X, \mathbb{Z}_p)$. Thus

$$\int_X f d\mu - \int_X g d\mu = p^n \int_X h d\mu$$

QED

Let us specialize to the case $X = \mathbb{Z}_p^x$, and the power functions x^k. A congruence $k \equiv k' \mod (p-1)p^n$ between exponents implies a congruence $x^k \equiv x^{k'} \mod p^{n+1}$ for all $x \in \mathbb{Z}_p^x$ (since $(\mathbb{Z}/p^{n+1}\mathbb{Z})^x$ has order $(p-1)p^n$). Then the obvious lemma gives

$$\int_{\mathbb{Z}_p^x} x^k d\mu \equiv \int_{\mathbb{Z}^x} x^{k'} d\mu \mod p^{n+1} \text{ if } k \equiv k' \mod (p-1)p^n$$

for any p-adic measure on $\mathbb{Z}_p^x$.

These are <u>exactly</u> the congruences that the function $k \mapsto \zeta^{*,a}(-k)$ satisfies. So it is natural to expect that we can explain the Kubota-Leopoldt congruences by constructing a $\mathbb{Z}_p$-valued measure $\mu^{(a)}$ on $\mathbb{Z}_p^x$, one for each integer $a \geq 2$ prime to p, such that

$$\int_{\mathbb{Z}_p^x} x^k d\mu^{(a)} = \zeta^{*,a}(-k) = (1-a^{k+1})(1-p^k)\zeta(-k) \; ; \; k = 0,1,2,\ldots$$

In fact, we will first construct a measure $\mu^{(a)}$ on all of $\mathbb{Z}_p$ which satisfies

$$\int_{\mathbb{Z}_o} x^k d\mu^{(a)} = (1-a^{k+1})\zeta(-k) \quad \text{for } k = 0,1,2,\ldots$$

[Notice that we cannot expect the moments $\int_{\mathbb{Z}_p} x^k d\mu$ of a measure on $\mathbb{Z}_p$ to satisfy the same sharp congruences. The point is that if k and k' are congruent modulo $(p-1)p^n$, then the functions x^k and $x^{k'}$ are congruent mod p^{n+1} on $\mathbb{Z}_p^x$, but on $p\mathbb{Z}_p$ they are only congruent modulo $p^{\min(k,k')}$.] The measure $\mu^{(a)}$ on $\mathbb{Z}_p^x$ is then obtained by restriction:

$$\int_{\mathbb{Z}_p^x} f(x)d\mu^{(a)} \underline{\underline{\text{dfn}}} \int_{\mathbb{Z}_p} \left(\text{the contin. fct. } x \to \begin{cases} f(x) & \text{if } x \in \mathbb{Z}_p^x \\ 0 & \text{if not} \end{cases} \right) d\mu^{(a)}$$

(It is a general phenomenon in interpolating L functions that the first step is to construct a measure on $\mathbb{Z}_p$ whose "moments" give the entire L-function. When the measure is restricted to $\mathbb{Z}_p^x$, the effect upon the moments is to remove the p-Euler factor of the corresponding L-value.)

This brings us to another point. Once we have constructed a measure $\mu^{(a)}$ on $\mathbb{Z}_p^x$, we can integrate any continuous function. Thus let $\chi(x)$ be a Dirichlet character mod p^n, which we view as a locally constant function on $\mathbb{Z}_p^x$. It turns out (though it is by no means obvious), that

$$(*) \qquad \int_{\mathbb{Z}_p^x} \chi(x) \cdot x^k d\mu^{(a)} = (1 - a^{k+1}\chi(a))\, L(-k,\chi)$$

where $L(s,\chi)$ is the Dirichlet series

$$L(s,\chi) = \sum_{\substack{n \geq 1 \\ (n,p)=1}} \chi(n) \cdot n^{-s}$$

[The value $L(-k,\chi)$ lies in the field $\mathbb{Q}$(values of χ). In order to view χ as a continuous p-adic function on $\mathbb{Z}_p^x$, we must choose a prime $\mathcal{y}$ of this field lying over p, and view χ as having values in its $\mathcal{y}$-adic completion. The integral then lies in this completion, and it is in that completion that the equality (*) holds.]

III. <u>p-adic measures on $\mathbb{Z}_p$</u>

To understand what a p-adic measure on $\mathbb{Z}_p$ is, we must understand what the ring Contin($\mathbb{Z}_p$, $\mathbb{Z}_p$) looks like. For example, the binomial coefficient functions

$$\binom{x}{n} = \frac{x(x-1)\ \dots\ (x-n+1)}{n!} = \sum_{i=0}^{n} C_{i,n} x^i$$

assume $\mathbb{Z}_p$-values on $\mathbb{Z}_p$ (by continuity : they take $\mathbb{Z}$-values on $\mathbb{Z}$).

Theorem (Mahler) Let R be p-adically complete and separated. Then any $f \in \mathrm{Contin}(\mathbb{Z}_p, R)$ can be uniquely written

$$f(x) = \sum_{n \geq 0} a_n \binom{x}{n} \quad , \quad a_n \in R, \quad a_n \to 0$$

The a_n may be recovered as the higher differences of f :

$$a_n = (\Delta^n f)(0) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} f(i).$$

Conversely, any series

$$\sum_{n \geq 0} a_n \binom{x}{n} \quad , \quad a_n \in R \ , \ a_n \to 0$$

converges to an element of $\mathrm{Contin}(\mathbb{Z}_p, R)$.

Corollary An R-valued measure μ on $\mathbb{Z}_p$ is uniquely determined by the sequence $b_n(\mu) = \int_{\mathbb{Z}_p} \binom{x}{n} d\mu$ of elements of R, and any sequence b_n determines an R-valued measure μ by the formula

$$\int_{\mathbb{Z}_p} f(x) d\mu = \sum_{n \geq 0} a_n b_n = \sum_{n \geq 0} b_n (\Delta^n f)(0)$$

Corollary Suppose that p is not a zero divisor in R. Then an R-valued measure μ on $\mathbb{Z}_p$ is uniquely determined by the sequence $m_n(\mu) \in R$ of its moments

$$m_n(\mu) = \int_{\mathbb{Z}_p} x^n d\mu.$$

A sequence m_n of elements of R arises as the moments of an R-valued

measure μ if and only if the quantities

$$b_n \overset{\text{dfn}}{=\!=} \sum_{i=0}^{n} C_{i,n} m_i \quad , \text{ a priori in } R[1/p]$$

all lie in R, in which case we have

$$\int_{\mathbb{Z}_p} \binom{x}{n} d\mu = b_n$$

IV. Elementary construction of the zeta measure $\mu^{(a)}$ (Euler, Leibniz)

We begin by recalling Euler's computation of $(1-2^{k+1})\zeta(-k)$.

Euler writes

$$(1-2^{k+1})\zeta(-k) = (1-2^{k+1}) \sum_{n \geq 1} n^k = \sum_{n \geq 1} n^k - 2 \sum_{n \geq 1} (2n)^k$$

$$= \sum_{\substack{n \geq 1 \\ \text{odd}}} n^k - \sum_{\substack{n \geq 1 \\ n \text{ even}}} n^k = - \sum_{n \geq 1} (-1)^n \cdot n^k$$

and applies Abel summation to this last expression:

$$- \sum_{n \geq 1} (-1)^n n^k = - \sum_{n \geq 1} (-1)^n n^k T^n \big|_{T=1} = \left(T \frac{d}{dT}\right)^k \left(\frac{T}{1+T}\right) \Big|_{T=1}.$$

If we make the substitution $T \to 1/T$ in this last formula, we see that $\zeta(-k) = 0$ if $k \geq 2$ is even. If we make the substitution $T = e^x$ then a short calculation gives the usual expression in terms of Bernoulli numbers.

More generally, let $a \geq 2$ be any integer. Then

$$(1 - a^{k+1})\zeta(-k) = \sum_{n \geq 1} n^k - a \sum_{n \geq 1} (an)^k = \sum_{n \geq 1} f(n) \cdot n^k$$

where

$$f(n) = \begin{cases} 1 & \text{if } n \not\equiv 0 \mod a \\ 1 - a & \text{if } n \equiv 0 \mod a \end{cases}$$

The important points are that f is periodic mod a, and $\sum_{n \bmod a} f(n) = 0$.

Thus

$$(1 - a^{k+1})\zeta(-k) = (T\frac{d}{dT})^k\left(\sum_{n \geq 1} f(n)T^n\right)|_{T=1}$$

$$= (T\frac{d}{T})^k\left(\frac{\sum_{n=1}^{a} f(n)T^n}{1 - T^a}\right)|_{T=1}$$

$$= (T\frac{d}{dT})^k\left(\frac{\sum_{n=1}^{a} f(n)(T^n - 1)}{1 - T^a}\right)|_{T=1}$$

$$= (T\frac{d}{dT})^k\left(\frac{\sum_{n=1}^{a} f(n)(1+T+\ldots+T^{n-1})}{1+T+\ldots+T^{a-1}}\right)|_{T=1}$$

$$= \frac{\text{element of } \mathbb{Z}[T]}{(1+T+\ldots+T^{a-1})^{k+1}}\ |_{T=1}$$

This last expression shows that $a^{k+1}(1 - a^{k+1})\zeta(-k) \in \mathbb{Z}$, a fact equivalent to the Lipschitz-Sylvester theorem on Bernoulli numbers (cf [15]).

We are now ready to prove

Theorem For each integer $a \geq 2$ prime to p, there exists a $\mathbb{Z}_p$-valued measure $\mu^{(a)}$ whose moments are given by

$$\int_{\mathbb{Z}_p} x^k d\mu^{(a)} = (1 - a^{k+1})\zeta(-k) \quad , \quad k = 0,1,\ldots$$

Proof Our Eulerian calculation showed that

$$(1 - a^{k+1})\zeta(-k) = (T\frac{d}{dT})^k\left(\frac{\text{elt. of } \mathbb{Z}[T]}{1+T+\ldots+T^{a-1}}\right)|_{T=1}$$

What is important here is that the denominator is an integral polynomial which assumes a p-adic unit value (namely a) at $T = 1$.

Let us denote by A the subring of $\mathbb{Q}_p(T)$ consisting of all ratios $P(T)/Q(T)$ with $P,Q \in \mathbb{Z}_p[T]$, and $Q(1) \in \mathbb{Z}_p^{\times}$. Since this is an algebraic geometry conference, let me point out that A is the local ring of $\mathbb{Z}_p[T]$ at the maximal ideal $(p,T-1)$.

Theorem (bis) Given any element $F(T) \in A$, there is a $\mathbb{Z}_p$-valued measure μ_F on $\mathbb{Z}_p$ whose moments are given by the formula

$$\int_{\mathbb{Z}_p} x^k d\mu_F = (T\frac{d}{dT})^k(F)\,|_{T=1}$$

Proof What must be shown is that

$$\sum_{i=o}^{n} C_{i,n}\,(T\frac{d}{dT})^i(F)|_{T=1} \text{ lies in } \mathbb{Z}_p \quad \text{for } n = 0,1,\ldots$$

or equivalently that

$$\binom{T\frac{d}{dT}}{n}(F)|_{T=1} \in \mathbb{Z}_p \quad \text{for } n = 0,1,\ldots$$

In fact, we have

Lemma The operators $\binom{T\frac{d}{dT}}{n}$ act stably on the ring A, i.e.,

$$\binom{T\frac{d}{dT}}{n}(F) \in A$$

Proof If we notice that

$$\binom{T\frac{d}{dT}}{n}(T^a) = \binom{a}{n}T^a$$

then we see that they act stably on $\mathbb{Z}_p[T]$.

If we notice that

$$\binom{T\frac{d}{dT}}{n} = T^n\frac{(\frac{d}{dT})^n}{n!}$$

then we see that Leibniz's formula is satisfied.

$$\binom{T\frac{d}{dT}}{n}(F\cdot G) = \sum_{i+j=n}\binom{T\frac{d}{dT}}{i}(F)\cdot\binom{T\frac{d}{dT}}{j}(G).$$

Let $Q \in \mathbb{Z}_p[T]$ have $Q(1) \in \mathbb{Z}_p^\times$. Applying Leibniz's formula to the product $Q\cdot\frac{1}{Q} = 1$, we find inductively that $\binom{T\frac{d}{dT}}{n}(\frac{1}{Q}) \in A$. Applying the same formula to the product $P\cdot\frac{1}{Q}$ then shows that A is stable by the $\binom{T\frac{d}{dT}}{n}$.

QED

V. Examples of μ_F, and relations to Iwasawa's approach

$$F = T^n \quad : \quad \int f d\mu_F = f(n)$$

$$F = (T-1)^n \quad : \quad \int f d\mu_F = (\Delta^n f)(o)$$

This second example permits us to identify $\mathbb{Z}_p$-valued measures on $\mathbb{Z}_p$ with the elements of $\mathbb{Z}_p[[T-1]]$, the measure μ corresponding to the series $\Sigma\, b_n(T-1)^n$, where $b_n = \int \binom{x}{n}d\mu$. The measures μ_F we considered above correspond exactly to the rational functions in $\mathbb{Z}_p[[T-1]]$ (the "rationality of the zeta function"!). The multiplication of power series corresponds to convolution of measures on the additive group $\mathbb{Z}_p$:

$$\int f(x)d(\mu * \nu) \overset{\text{dfn}}{=\!=} \iint f(x+t)d\mu(x)d\nu(t).$$

This identification of measures is the link to Iwasawa's approach. Let f_s, for $s \in \mathbb{Z}_p$, denote the function $f_s(x) = (1+p)^{sx}$; then

$$(\Delta^n f_s)(o) = ((1+p)^s - 1)^n,$$

so that

$$\int f_s(x)d\mu = \sum_{n\geq o} b_n\,((1+p)^s-1)^n$$

when the measure μ corresponds to the series $\Sigma\, b_n(T-1)^n$.

VI. Relation to L-functions

Let Ψ be a locally constant function on $\mathbb{Z}_p$, say constant on cosets modulo p^n. For $F \in A$, we define the function $[\Psi](F)$ by

$$[\Psi](F)(T) \overset{\text{dfn}}{=\!=} \frac{1}{p^n}\sum_{b \bmod p^n}\Psi(b)\sum_{\zeta^{p^n}=1}\zeta^{-b}F(\zeta T)$$

Let us check that $[\Psi]F$ lies again in A. We have

$$[\Psi](T^n) = \Psi(n)T^n$$

and

$$[\Psi](GF) = G\cdot[\Psi](F) \text{ if } G(T) = G(\zeta T) \text{ for all } \zeta^{p^n} = 1.$$

The first formula shows that $[\Psi]$ preserves $\mathbb{Z}_p[T]$. If we notice that every element of A may be written with a denominator which is invariant by $T \to \zeta T$ for $\zeta^{p^n} = 1$ (simply multiply numerator and denominator of $P(T)/Q(T)$ by $\prod Q(\zeta T)$, the product extended to the non-trivial p^n'th roots of unity), then the second formula shows that $[\Psi]$ is stable on A.

This operation $[\Psi]$ gives A the structure of module over the ring of locally constant functions on $\mathbb{Z}_p$. On the other hand, the set of all measures on $\mathbb{Z}_p$ is a module over the ring of all continuous functions, the module structure defined by $\int g(x)d(f\mu) = \int f(x)g(x)d\mu$. These structures are compatible, for we have the

Integration Formula $\quad \int f(x)d\mu_{[\Psi]F} = \int \Psi(x)f(x)\cdot d\mu_F$

Proof Suppose first that $F = T^n$. Then $[\Psi](T^n) = \Psi(n)T^n$, and both integrals

are $\psi(n)f(n)$. By linearity, the two integrals then coincide for all $F \in \mathbb{Z}_p[T]$.

Now consider the general case $F \in A$. Suppose that ψ is constant on cosets mod p^n. By the already used trick of writing elements of A with denominators which are polynomials in T^{p^n}, we may suppose F is so written. Separating the exponents occurring in its numerator into congruence classes mod p^n, we may suppose (by additivity in F) that F is of the form $T^a G(T^{p^n})$, where $G(T) \in A$.

Since the $(p,T-1)$-adic completion of A is $\mathbb{Z}_p[[T-1]]$, the subring $\mathbb{Z}_p[T]$ is dense in A. Thus we may write $G(T) = \lim G_k(T)$, with $G_k \in \mathbb{Z}_p[T]$. Putting $F_k = T^a G_k(T^{p^n})$, we obtain

$$\begin{cases} F_k \in \mathbb{Z}_p[T],\ F = \lim F_k \\ [\psi](F_k) = \psi(a)F_k \\ [\psi](F) = \psi(a)F \end{cases}$$

Because the $(p,T-1)$-adic topology on $\mathbb{Z}_p[[T-1]]$ is the strong topology on measures, we may compute

$$\begin{aligned} \int \psi(x)f(x)d\mu_F = \lim \int \psi(x)f(x)d\mu_{F_k} &= \lim \int f(x)d\mu_{[\psi]F_k} \\ &= \lim \psi(a) \int f(x)d\mu_{F_k} \\ &= \psi(a) \int f(x)d\mu_F \\ &= \int f(x)d\mu_{[\psi]F} \end{aligned}$$

QED

Corollary For any locally constant function ψ on $\mathbb{Z}_p$, we have

$$\int_{\mathbb{Z}_p} \psi(x)x^k d\mu^{(a)} = L(-k, \psi \cdot a^{k+1}\psi_a)$$

where ψ_a is the function $\psi_a(x) = \psi(ax)$.

In particular, if ψ is a multiplicative function on $\mathbb{Z}_p$,

$$\int_{\mathbb{Z}_p} \psi(x)x^k d\mu^{(a)} = (1 - a^{k+1}\psi(a)) \cdot L(-k,\psi).$$

(Notice that for ψ = the characteristic function of $\mathbb{Z}_p^\times$, $L(s,\psi)$ is $\zeta^*(s)$).

Proof Recall that $\mu^{(a)}$ is of the form μ_F for $F \in A$ the rational function

$$F = \frac{\sum_{n=1}^{a} f(n)\, T^n}{1 - T^a} \qquad f(n) = \begin{cases} 1 & n \not\equiv 0 \bmod a \\ 1-a & n \equiv 0 \bmod a \end{cases}$$

written here in "non-A" form.

Suppose that ψ is constant on cosets modulo p^M. Then we can rewrite F in another "non-A" form,

$$F = \frac{\sum_{n=1}^{ap^M} f(n)\, T^n}{1 - T^{ap^M}}.$$

The denominator is now invariant under $T \to \zeta T$ for $\zeta^{p^M} = 1$, so we get a "non-A" representation of $[\psi]F$:

$$[\psi]F = \frac{\sum_{n=1}^{ap^M} \psi(n)f(n)T^n}{1 - T^{ap^M}} = \sum_{n \geq 1} \psi(n)f(n)T^n$$

$$= \sum_{n \geq 1} \psi(n)T^n - a \sum_{n \geq 1} \psi(an) \cdot T^{an}$$

$$= \frac{\sum_{n=1}^{p^M} \psi(n)T^n}{1 - T^{p^M}} - a \frac{\sum_{n=1}^{p^M} \psi(an)T^{an}}{1 - T^{ap^M}}$$

By the integration formula, we have

$$\int \psi(x)x^k d\mu^{(a)} = \int \psi(x)x^k d\mu_F = \int x^k d\mu_{[\psi]F} = (T\frac{d}{dT})^k([\psi]F)|_{T=1}.$$

If we now substitute into this last formula the expression we found above for the rational function $[\psi]F$, we obtain the desired value à la Euler, namely $L(-k,\psi - a^{k+1}\psi_a)$.

VII. The relation with modular forms (Siegel, Serre)

We will now begin an extremely indirect approach to the values of ζ at negative integers. We will first obtain these values as the constant terms of the q-expansions of certain modular forms. We will then interpret these modular forms as functions on a certain moduli problem for p-adic elliptic curves. Finally, we will explain how geometric information about this moduli problem gives information about zeta values, culminating in a new construction of the measure $\mu^{(a)}$.

The point of this method, as opposed to the elementary one, is that it works equally well for studying the values at negative integers of the Dedekind zeta function of any totally real number field (if the number field K is not totally real, its zeta function vanishes at all negative integers). See Ribet's talk in this volume for more details. In fact, it is at present the only method known for general totally real fields (but cf [1] for an explicit approach to real quadratic fields). As a bonus, it also gives information on the values of certain L-series with "grossencharacter of type A_o" attached to quadratic imaginary fields.

VIII. Modular forms and their q-expansions

Over any ring R, we have the notion of an elliptic curve E/R (an abelian scheme of dimension one), together with the notion of a nowhere vanishing invariant differential $\omega \in H^o(E,\Omega^1_{E/R})$. Given E/R, such an ω always exists at least locally on R, and if ω is one such, any other is of

the form $\lambda\omega$ for some $\lambda \in R^x$.

When $R = \mathbb{C}$, such a pair (E,ω) is equivalent to the giving of a lattice $L \subset \mathbb{C}$: to (E,ω) we associate the lattice of all periods of ω over the elements of $H_1(E^{an}, \mathbb{Z})$, and to the lattice $L \subset \mathbb{C}$ we associate the complex torus $\mathbb{C}/L$ with the invariant differential dz (z the parameter on $\mathbb{C}$). This pair $(\mathbb{C}/L, dz)$ is given algebraically by $(y^2 = 4x^3 - g_2x - g_3, dx/y)$, where x is the Weierstrass $\wp$-function $\wp(z;L)$ associated to the lattice L, $y = \wp'(z;L)$, and the constants g_2 and g_3 are given by the formulas

$$g_2 = 60 \sum_{\substack{\ell \in L \\ \ell \neq o}} 1/\ell^4 \quad , \quad g_3 = 140 \sum_{\substack{\ell \in L \\ \ell \neq o}} 1/\ell^6.$$

Under this correspondence, the replacement of (E,ω) by $(E,\lambda\omega)$ corresponds to the replacement of L by λL.

An (unrestricted) modular form of weight k over $\mathbb{C}$ is classically defined to be a holomorphic function of lattices F(L) satisfying $F(\lambda L) = \lambda^{-k}F(L)$. Since any lattice is multiple of one of the form $\mathbb{Z} + \mathbb{Z}\tau$ with $\mathrm{Im}(\tau) > o$, F is uniquely determined by the holomorphic function on the upper half-plane $f(\tau) = F(\mathbb{Z} + \mathbb{Z}\tau)$. The function f arises from an F of weight k if and only if it satisfies the functional equation

$$f(\frac{a\tau + b}{c\tau + d}) = (c\tau + d)^k f(\tau) \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

An example of such a modular form is

$$A_k(L) = \sum_{\substack{\ell \in L \\ \ell \neq o}} 1/\ell^k \qquad \text{for } k \geq 3; \text{ it is zero for } k \text{ odd.}$$

The q-expansion of a classical modular form is the possibly infinite-tailed Laurent series expansion in $q = e^{2\pi i\tau}$ of the (periodic with period one) function $\tau \mapsto F(2\pi i\,\mathbb{Z} + 2\pi i\,\mathbb{Z}\tau) = (2\pi i)^{-k}f(\tau)$. For example, the q-expansion of

$$G_k = \frac{(-1)^k (k-1)!}{2} A_k \quad , \quad k \geq 4$$

is given by

$$G_k(q) = \begin{cases} \frac{1}{2}\zeta(1-k) + \sum_{n \geq 1} q^n \sum_{d|n} d^{k-1} & \text{for } k \geq 4 \text{ even} \\ 0 \text{ for } k \text{ odd} \end{cases}$$

This formula is the basis of the connection between modular forms and ζ-values.

We may algebraically define an (unrestricted) modular form of weight k over any ring R to be a rule which assigns to <u>any</u> pair (E,ω) over <u>any</u> R-algebra R' a value $F(E,\omega) \in R'$, in such a way that

$$\begin{cases} F(E,\lambda\omega) = \lambda^{-k} F(E,\omega) \quad \forall\, \lambda \in (R')^{\times} \\ F \text{ commutes with all extensions of scalars } R' \to R'' \\ F(E,\omega) \text{ depends only on the } R'\text{-isomorphism class of } (E,\omega) \end{cases}$$

The q-expansion of a modular form F over R is a finite-tailed Laurent series $F(q) \in R((q))$ obtained as follows. Over $\mathbb{C}$, the lattice $2\pi i\,\mathbb{Z} + 2\pi i\,\mathbb{Z}\tau$ defines the elliptic curve with differential

$$\left(\mathbb{C} \Big/ 2\pi i\,\mathbb{Z} + 2\pi i\,\mathbb{Z}\tau \;,\; dz\right)$$

which is isomorphic, by the exponental map $z \to t = \exp(z)$, to

$$\left(\mathbb{C}^{\times} \Big/ q^{\mathbb{Z}} \;,\; \frac{dt}{t}\right)$$

The Weierstrass equation defining this curve has coefficients in the ring $\mathbb{Z}[1/6][[q]]$, and with a bit of rearranging can be turned into an equation over $\mathbb{Z}[[q]]$ which defines an elliptic curve with differential over $\mathbb{Z}((q))$. This curve we call the Tate-Jacobi curve $\mathrm{Tate}(q)$ with its canonical

differential ω_{can}. By extension of scalars, we obtain $(\mathrm{Tate}(q), \omega_{can})$ over $R((q))$. The q-expansion of a modular forms over R is defined to be its <u>value</u> on this curve:

$$f(q) \overset{\text{dfn}}{=\!=} F(\mathrm{Tate}(q), \omega_{can}).$$

Let us state without proof the GAGA-type relations between these different concepts of modular forms (cf [4], [7]).

1. A classical modular form $F^{c\ell}$ over $\mathbb{C}$ of weight k comes from an algebraic one F over $\mathbb{C}$ of weight k if and only if $F^{c\ell}$ has a <u>finite-tailed</u> q-expansion. In this case $F(q) = F^{c\ell}(q)$, and F is uniquely determined.
2. (q-expansion principle) If the q-expansion of a modular form F over R of weight k has all of its coefficients in a subring $R_o \subset R$, then there exists a unique modular form F_o of weight k over R_o which gives rise to F by extension of scalars. In particular, a modular form of given weight k is uniquely determined by its q-expansion.

The modular forms with holomorphic q-expansions are really rather down to earth objects. For example, over a ring R in which both 2 and 3 are invertible, the graded ring of all (holomorphic) modular forms is just $R[g_2, g_3]$, with g_2 of weight four and g_3 of weight six.

IX. <u>Heuristic</u>

As a corollary of the GAGA principle, the modular forms $2G_k$ are defined over $\mathbb{Q}$, in fact over $\mathbb{Z}[\zeta(1-k)]$. By looking at their coefficients, we obtain many measures on $\mathbb{Z}_p$, as follows. For $n \geq 1$, the coefficient of q^n in G_k, $k \geq 3$, is given by

$$\text{coef of } q^n \text{ in } 2G_k = \sum_{d|n} (d^{k-1} - (-d)^{k-1})$$

This suggests that we define a measure μ_n on $\mathbb{Z}_p$ by the formula

$$\int_{\mathbb{Z}_p} f(x)d\mu_n = \sum_{d|n} (f(d) - f(-d))$$

Thus we have

$$\int_{\mathbb{Z}_p} x^{k-1}d\mu_n = \text{coef. of } q^n \text{ in } 2G_k$$

So we would like to "let n go to zero" and define a measure μ_o on $\mathbb{Z}_p$ such that

$$\int_{\mathbb{Z}_p} x^{k-1}d\mu_o = \text{constant term in } 2G_k = \zeta(1-k).$$

Of course this is not possible as stated, simply because $\zeta(1-k)$ need not be p-integral. We could at best hope to obtain $\mu^{(a)}$ as the "limit" in some sense of the measures $\mu_n^{(a)}$ defined by

$$\int_{\mathbb{Z}_p} f(x)d\mu_n^{(a)} = \int_{\mathbb{Z}_p} (f(x) - af(ax))d\mu_n.$$

Let us explain how to realize this hope, by studying a moduli problem on which the series $G_k - \frac{1}{2}\zeta(1-k)$ themselves have an intrinsic meaning.

X. Generalized p-adic modular functions and trivialized elliptic curves

Henceforth, p is a fixed prime number, and we consider only rings R which are p-adically complete and separated. Rather than consider pairs (E,ω) over R, we will now consider "trivialized elliptic curves" (E,φ) over R:

$$\begin{cases} E \text{ an elliptic curve over } R \\ \varphi : \hat{E} \xrightarrow{\sim} \hat{\mathbb{G}}_m \text{ an isomorphism between the formal} \\ \quad \text{group of } E \text{ and the formal multiplicative group.} \end{cases}$$

Given an elliptic curve E/R, it cannot admit a trivialization φ unless all the fibres of E/R are ordinary elliptic curves. If the fibres are all ordinary, then in order to construct a trivialization we will in general have to extend scalars from R to a vast pro-ind-etale over-ring R_∞ (i.e., R_∞ will be p-adically complete and separated, and for each n, R_∞/p^nR_∞ will be an increasing union of finite etale over-rings of R/p^nR).

Once we have one trivialization φ, then any other is of the form $\alpha\varphi$ for some $\alpha \in \mathbb{Z}_p^\times = \mathrm{Aut}(\hat{\mathbb{G}}_m)$, at least over a ring R such that $\mathrm{Spec}(R/pR)$ is connected.

Notice that a trivialized elliptic curve (E,φ) over R gives rise to an elliptic curve with differential $(E, \varphi^*(\frac{dt}{t}))$, simply by pulling back the standard invariant differential dt/t on $\hat{\mathbb{G}}_m$. Notice also that the Tate curve Tate (q), considered over $\hat{\mathbb{Z}}_p((q))$, the p-adic completion of $\mathbb{Z}_p((q))$, admits a canonical trivialization φ_{can}, simply because Tate(q) was obtained as the quotient of $\hat{\mathbb{G}}_m$ by the discrete subgroup $q^{\mathbb{Z}}$. Under this trivialization, we have $\varphi_{can}^*(dt/t) = \omega_{can}$.

We now define a generalized p-adic modular function over a p-adically complete and separated R to be rule F which assigns to any trivialized elliptic curve (E,φ) over any p-adically complete and separated R-algebra R' a value $F(E,\varphi) \in R'$ in such a way that

$$\begin{cases} F \text{ commutes with extension of scalars } R' \to R'' \\ \quad \text{of p-adically complete and separated } R\text{-algebras} \\ F(E,\varphi) \text{ depends only upon the } R'\text{-isomorphism class} \\ \quad \text{of } (E,\varphi) \end{cases}$$

It is of the utmost importance that we do not require that F have a weight, i.e., a transformation property under the action of $\mathbb{Z}_p^\times$, defined by

$$[\alpha]F(E,\varphi) = F(E,\alpha^{-1}\varphi)$$

The ring of all generalized p-adic modular functions defined over R, noted $\mathbb{V}_R$, is itself a p-adically complete and separated R-algebra. It represents the functor

$$M^{triv}(R') = \text{isomorphism classes of trivialized elliptic curves } (E,\varphi) \text{ over } R'$$

on the category of p-adically complete and separated R-algebras.

Geometrically, the functor M^{triv} is formed from the stack of trivialized elliptic curves $\mathcal{M}^{triv}$ by passing to isomorphism classes. The stack $\mathcal{M}^{triv}$ sits over the stack $\mathcal{M}^{ord}$ of ordinary elliptic curves as an ind-etale covering, with structural group $\mathbb{Z}_p^\times$ (we need stacks because the functor M^{ord} is not representable):

$$\begin{array}{c}\mathcal{M}^{triv}\\ \Big\downarrow \quad \text{ind-etale with structural group } \mathbb{Z}_p^\times.\\ \mathcal{M}^{ord}\end{array}$$

Indeed, if $E \xrightarrow{\pi} \mathcal{M}^{ord}$ is the tautological "universal elliptic curve" over the stack $\mathcal{M}^{ord}$, then $\mathcal{M}^{triv}$ is obtained as the bundle of frames of the locally free rank one $\mathbb{Z}_p$-etale sheaf $R^1\pi_*\mathbb{Z}_p$ on $\mathcal{M}^{ord}$.

This sheaf corresponds to a character χ of the fundamental group of $\mathcal{M}^{ord}$ with values in $\mathbb{Z}_p^\times$. The surjectivity of this character is equivalent to the irreducibility of $\mathcal{M}^{triv}$ (since $\mathcal{M}^{ord}$ is itself irreducible). There are two proofs of this surjectivity. The first, due to Igusa, studies what happens in the neighborhood of a "missing point", corresponding to a supersingular elliptic curve. Igusa proves that even after restricting χ to the local monodromy group (inertia group) at such a point, χ remains

surjective. The second proof, found recently by Ribet, is arithmetic in nature, based on the interpretation of the value of χ on the Frobenius element attached to a closed point of $\mathcal{M}^{ord}$ (i.e., to an ordinary elliptic curve over a finite field) as the unit root of the zeta function of that elliptic curve. Ribet's proof works also for Hilbert modular varieties, and is discussed, along with its applications, in his article in these Proceedings.

Remark To avoid stacks, we could instead choose an integer $N \geq 3$ prime to p and rigidify our moduli problems with level N structures. Then $M^{ord}(N)$ is itself representable, though no longer geometrically irreducible, and the covering $M^{triv}(N) \to M^{ord}(N)$ is irreducible over each irreducible component of $M^{ord}(N)$. The coordinate ring $\mathbb{V}(N)$ of $M^{triv}(N)$ has a canonical action of $GL(2, \mathbb{Z}/N\mathbb{Z})$ on it, under which the subring of invariants is $\mathbb{V}$.

XI. Consequences of the irreducibility of M^{triv}

Evaluation at $(\mathrm{Tate}(q), \varphi_{can})$ defines the q-expansion homomorphism $\mathbb{V}_R \to \hat{R}((q))$ for any R. Suppose first that R is a field k of characteristic p. Then $\mathbb{V}_k$ is the coordinate ring of $M^{triv} \otimes k$, which is (essentially) a smooth irreducible affine curve over k. Then $(\mathrm{Tate}(q), \varphi_{can})$ defines a $k((q))$-valued point of this curve which obviously does not lie over any closed point, so therefore must lie over the generic point. Thus we have proven

Lemma When k is a field of characteristic p, the q-expansion homomorphism $\mathbb{V}_k \to k((q))$ is injective.

As an immediate corollary, we get

Lemma Let R be a complete discrete valuation ring with uniformizing parameter π, and residue field k of characteristic p. Then the q-expansion homomorphism

$$\mathbb{V}_R \to \hat{R}((q))$$

is injective, and its cokernel $\widehat{R((q))}/\mathbb{V}_R$ is R-flat, i.e., has no p-torsion.

Proof Since $\mathbb{V}_R$ is flat over R (being formally ind-smooth over R), and $\mathbb{V}_R \otimes k = \mathbb{V}_k$ (because $M_k^{triv} = M_R^{triv} \otimes k$), the injectivity of $\mathbb{V}_R \to \widehat{R((q))}$ follows from its injectivity modulo π, and the fact that $\mathbb{V}_R$ is p-adically separated. Given the injectivity of $\mathbb{V}_R \to \widehat{R((q))}$, the flatness of its cokernel results from (and is equivalent to) its injectivity modulo π.

QED

Technical as it looks, this last lemma is the key to everything, for it allows us to construct a large number of elements of $\mathbb{V}$ $(= \mathbb{V}_{\mathbb{Z}_p})$:

1. Let f be an (unrestricted) modular form of weight k, defined over $\mathbb{Z}_p$. Then f may be viewed as an element of $\mathbb{V}$, as being the rule

$$(E,\varphi) \to f(E,\varphi^*(dt/t)).$$

The q-expansion of f remains the same before and after we view f as lying in V. Under the action of $\mathbb{Z}_p^\times$ on $\mathbb{V}$ defined by $[\alpha]F(E,\varphi) = F(E,\alpha^{-1}\varphi)$, f transforms by

$$[\alpha]f = \alpha^k f$$

2. Let $\{f_i\}$ be a finite set of modular forms, f_i of weight i, defined over $\mathbb{Z}_p$, and suppose that $\sum f_i(q) \in p^N \mathbb{Z}_p[[q]]$, say $\sum f_i(q) = p^N h(q)$. Then there is a unique element $h \in \mathbb{V}$ whose q-expansion is h(q). (For by hypothesis, the series h(q) is a p^M-torsion element in $\widehat{\mathbb{Z}_p((q))}/\mathbb{V}$, hence itself is the q-expansion of a necessarily unique element $h \in V$).

For example, $G_k - \frac{1}{2}\zeta(1-k)$ lies in $\mathbb{V}$. Elements of this sort are called divided congruences, and form a subring of $\mathbb{V}$ which can be proven to be dense in all of $\mathbb{V}$ (cf [8]).

3. Let h_i be a sequence of elements of $\mathbb{V}$ such that $\lim h_i(q)$ exists in $\widehat{\mathbb{Z}_p((q))}$. Then there is an element $h_\infty \in \mathbb{V}$ such that $h_\infty(q) = \lim h_i(q)$. (Because $p^n \mathbb{V} = \mathbb{V} \cap p^n \widehat{\mathbb{Z}_p((q))}$, the h^i are a Cauchy sequence in $\mathbb{V}$).

Thus $\mathbb{V}$ contains all "p-adic modular forms" in the sense of Serre [17] and all divided congruences between them. In fact, Serre's "p-adic modular forms of weight χ" are exactly the elements $F \in V$ satisfying $[a]F = \chi(a)F$ for all $a \in \mathbb{Z}_p^\times$ (cf [8]).

4. Let θ denote the differential operator $q\frac{d}{dq}$. If $h \in \mathbb{V}$, then $\theta h \in \mathbb{V}$ in the sense that $\theta(h(q))$ is the q-expansion of an element of $\mathbb{V}$. (Use the fact that θ operates stably on Serre's p-adic modular forms, stably on all divided congruences between them, and then invoke 3. above together with the density of divided congruences in $\mathbb{V}$).

XII. Construction of the $\mathbb{V}$-valued measure $\mu^{(a)}$ on $\mathbb{Z}_p$

The modular forms G_k, $k \geq 3$, have already been defined over $\mathbb{Q}_p$ albeit by a transcendental summation followed by an appeal to the q-expansion principle. Serre [17] has shown that the series

$$G_2(q) = \frac{1}{2}\zeta(-1) + \sum_{n \geq 1} q^n \sum_{d \mid n} d \qquad ; \zeta(-1) = \frac{-1}{24}.$$

is the q-expansion of a p-adic modular form of weight two over $\mathbb{Q}_p$. We define G_1 to be zero. We view all the G_k, $k = 1,2,\ldots$, as elements of $\mathbb{V}[\frac{1}{p}]$. The fundamental theorem is

Theorem For $a \in \mathbb{Z}_p^\times$, there exists a $\mathbb{V}$-valued measure on $\mathbb{Z}_p$ whose moments are given by

$$\int_{\mathbb{Z}_p} x^k d\mu^{(a)} = 2(1 - a^{k+1})G_{k+1} = 2G_{k+1} - 2[a]G_{k+1} \qquad \text{for } k = 0,1,2,..$$

Proof Let us begin by noting that $G_{k+1} - [a]G_{k+1}$ does indeed lie in $\mathbb{V}$: Certainly we have $G_{k+1} \in \mathbb{V}[\frac{1}{p}]$, and G_{k+1} has integral q-expansion except possibly for its constant term. Thus we may apply the

Key Lemma Suppose $h \in \mathbb{V}[\frac{1}{p}]$, and h has p-integral q-expansion except possibly for its constant term. Then for any $a \in \mathbb{Z}_p^x$, $h - [a]h \in \mathbb{V}$.

Proof of Key Lemma Let us write $h(q) = A + f(q)$, with $A \in \mathbb{Q}_p$ and $f(q) \in \mathbb{Z}_p\hat{}((q))$. Suppose that $p^M h \in \mathbb{V}$. Then $p^M A \in \mathbb{Z}_p$, and $p^M f(q) = (p^M h)(q) + p^M A$, which shows that $p^M f(q)$, and hence $f(q)$ itself, is the q-expansion of an element of $\mathbb{V}$. Thus

$$h = A + \text{an elt. of } \mathbb{V} \quad \text{in } \mathbb{V}[\tfrac{1}{p}]$$

Applying [a] yields

$$[a]h = A + [a](\text{an elt. of } \mathbb{V}) = A + \text{an elt. of } \mathbb{V}.$$

Subtracting gives $h - [a]h \in \mathbb{V}$. QED

Let us conclude the construction. We must show that

$$\sum_{i=o}^{m} C_{i,m} \int_{\mathbb{Z}_p} x^i d\mu^{(a)} \in \mathbb{V} \quad \text{for } m = 0,1,\ldots$$

where the coefficients $C_{i,m}$ are defined by

$$\binom{x}{m} = \sum_i C_{i,m} x^i.$$

Thus we must show that

$$2\sum_i C_{i,m} G_{i+1} - [a]\left(2\sum_i C_{i,m} G_{i+1}\right) \in V.$$

By the Key Lemma, it suffices to check that the element

$$2\sum_{i=o}^{m} C_{i,m} G_{i+1} \in \mathbb{V}[\tfrac{1}{p}]$$

has integral q-expansion except for its constant term. But we have already computed the coefficient of q^n in $2G_{i+1}$: it was

$$\int_{\mathbb{Z}_p} x^i d\mu_n \text{ , where } \int_{\mathbb{Z}_p} f(x) d\mu_n = \sum_{d|n} (f(d) - f(-d)).$$

Thus

$$2\sum_{1=o}^{m} C_{i,m} G_{i+1}(q) = \text{constant} + \sum_{n \geq 1} q^n \int_{\mathbb{Z}_p} \binom{x}{m} d\mu_n. \qquad \text{QED}$$

XIII. Applications to quadratic imaginary fields: Hurwitz numbers

The constant term of the q-expansion of the $\mathbb{V}$-valued measure $\mu^{(a)}$ is a $\mathbb{Z}_p$-valued measure on $\mathbb{Z}_p$, which for $a \in \mathbb{Z}$, $a > o$, differs from the measure we constructed by elementary means, only by a single point mass at the origin (because the G_k's ignore the "accident" that $\zeta(o) = -\frac{1}{2}$ is $\neq o$, while $G_1 = o$).

However, as we have a $\mathbb{V}$-valued measure, we may evaluate it at any trivialized elliptic curve (E,φ) over any p-adically complete and separated ring R, and obtain an R-valued measure on $\mathbb{Z}_p$.

To fix ideas, consider the gaussian curve $y^2 = 4x^3 - 4x$, which has complex multiplication by the gaussian integers; i acts as $(x,y) \to (-x,iy)$. We view this curve as defined over $\mathbb{Z}_p$, but because we want it to be ordinary mod p, we must suppose that $p \equiv 1 \mod 4$.

What about a trivialization? None exists over $\mathbb{Z}_p$. If we extend scalars to W, the Witt vectors of the algebraic closure of $\mathbb{F}_p$, then there will be trivializations. In fact, if φ is a trivialization, then $\varphi^*(dt/t) = c \cdot dx/y$ with $c \in W^x$, and c satisfies the equation

$$c^\sigma/c = u$$

where σ is the Frobenius automorphism of W, and $u \in \mathbb{Z}_p^x$ is the unit root

of Frobenius. Conversely, if $c \in W^x$ satisfies $c^\sigma = uc$, there exists a unique trivialization φ with $\varphi^*(dt/t) = cdx/y$. In fact, the discovery by Tate of the relationship between trivializations and unit roots of Frobenius was the starting point of the application of p-adic analysis to any sort of zeta function (cf [3], p. 257).

Let us fix a choice of c, and denote by φ_c the corresponding trivialization. Then by evaluating $\mu^{(a)}$ at $(y^2 = 4x^3 - 4x, \varphi_c)$ we obtain:

Theorem There exists a W-valued measure $\mu^{(a)}$ on $\mathbb{Z}_p$ whose moments are given by

$$\int_{\mathbb{Z}_p} x^{k-1} d\mu^{(a)} = (1 - a^k)\, G_k(y^2 = 4x^3 - 4x,\ cdx/y) \quad \text{for } k = 1,2\ldots$$

Let us make explicit the interpretation of these moments as values of L-series with grossencharacter. For $k \geq 4$, we can write

$$G_k(y^2 = 4x^3 - 4x,\ cdx/y) = c^{-k} G_k(y^2 = 4x^3 - 4x,\ dx/y)$$

$$= \frac{(-1)^k (k-1)!}{2}\, c^{-k}\, A_k(y^2 = 4x^3 - 4x,\ dx/y).$$

Over $\mathbb{C}$, the lattice corresponding to $(y^2 = 4x^3 - 4x, dx/y)$ is easily seen to be $\Omega\, \mathbb{Z}[i]$, where

$$\Omega = 2\int_0^1 \frac{dt}{\sqrt{1-t^4}} = 2.622057\ldots$$

Thus we obtain an equality of complex numbers

$$A_k(y^2 = 4x^3 - 4x,\ dx/y) = A_k(\Omega\, \mathbb{Z}[i]) = \Omega^{-k} A_k(\mathbb{Z}[i]) = \Omega^{-k} \sum_{(a,b) \neq (o,o)} \frac{1}{(a+bi)^k}$$

which shows that the A_k are essentially the Hurwitz numbers [5].

The series $\sum_{(a,b) \neq (o,o)} \frac{1}{(a+bi)^k}$ converges absolutely for $k \geq 3$, but sums to zero unless $k = 4\ell$, in which case it is

$$4 \sum_{\text{ideals } \mathfrak{n}} \chi^{-k}(\mathfrak{n}) = L(0,\chi^{-k})$$

where χ^{-k} is the grossencharacter of $\mathbb{Z}[i]$ defined by

$$\chi^{-k}(\mathfrak{n}) = 1/\alpha^k \quad \text{if } \mathfrak{n} = (\alpha)$$

Thus we obtain the p-adic interpolation the function $k \to L(0,\chi^{-k})$.

XIV. Manin's function of two variables

By quite different techniques, Manin and Vishik [12] have shown that series of the form

$$\sum_{(a,b) \neq (o,o)} \frac{(a-bi)^r}{(a+bi)^{k+r}} = \begin{cases} L(0,\bar{\chi}^r \chi^{-k-r}) & \text{if } k + 2r \equiv 0(4) \\ 0 & \text{if not} \end{cases}$$

once their transcendental factors are removed, can be p-adically interpolated to continuous p-adic functions of two variables (k,r), provided that $p \equiv 1\ (4)$.

By using the techniques explained here, we are able to construct a V-valued measure $\mu^{(a)}$ on $\mathbb{Z}_p \times \mathbb{Z}_p$ whose moments

$$\int_{\mathbb{Z}_p} \int_{\mathbb{Z}_p} x^{k-1} y^r\, d\mu^{(a)}(x,y) \in \mathbf{V}$$

when evaluated on $(y^2 = 4x^3 - 4x, \varphi_c)$, give essentially these same L-values. The proofs are long, and will appear elsewhere.

A Short Bibliography

The following list is very far from being complete. The interested reader should also consult the bibliographies of the works cited here.

1. J. Coates and W. Sinnott, On p-adic L-functions over real quadratic fields. Inv. Math. 25 (1974), 253-279.
2. Z. I. Borevich and I. R. Shafarevich, Number Theory, esp. pp. 355-389. Academic Press, New York and London, 1966.
3. B. Dwork, A deformation theory for the zeta function of a hypersurface. Proc. Intl. Cong. Math. (1962), Stockholm, 247-259.
4. P. Deligne and M. Rapoport, Les schemas de modules de courbes élliptiques. Proceedings of the 1972 Antwerp Summer School, Springer Lecture Notes in Mathematics 349 (1973), 143-316.
5. A. Hurwitz, Uber die Entwicklungskoeffizienten der lemniscatischen Functionen. Math. Ann. 51 (1899), 196-226.
6. K. Iwasawa, Lectures on P-adic L-Functions, Annals of Math. Studies 74, Princeton Univ. Press, 1972.
7. N. Katz, P-adic properties of modular schemes and modular forms, Proceedings of the 1972 Antwerp Summer School, Springer Lecture Notes in Mathematics 350 (1973), 70-189.
8. N. Katz, Higher congruences between modular forms, to appear in Annals of Math.
9. N. Katz, The Eisenstein measure and p-adic interpolation, to appear in Amer. J. Math.
10. T. Kubota and H. W. Leopoldt, Eine p-adische Theorie der Zetawerte I, J. Reine Ang. Math. 214/215 (1964), 328-339.
11. K. Mahler, An interpolation series for a continuous function of a p-adic variable. J. Reine Ang. Math. 199 (1958), 23-34.
12. J. Manin and S. Vishik, P-adic Hecke series for quadratic imaginary fields (in Russian), to appear in Math. Sbornik.
13. B. Mazur, Analyse p-adique. secret Bourbaki redaction, 1973.
14. B. Mazur and H. P. F. Swinnerton-Dyer, Arithmetic of Weil curves. Inv. Math. 25 (1974), 1-61.
15. J. Milnor and J. Stasheff, Characteristic Classes, esp. Appendix B, Annals of Math. Studies 76, Princeton Univ. Press, 1974.
16. K. Ribet, P-adic interpolation via Hilbert modular forms, this volume.
17. J.-P. Serre, Formes modulaires et fonctions zeta p-adiques. Proceedings of the 1972 Antwerp Summer School, Springer Lecture Notes in Mathematics 350 (1973), 191-268.

PRINCETON UNIVERSITY

Proceedings of Symposia in Pure Mathematics
Volume 29, 1975

TOPOLOGICAL USE OF POLAR CURVES

Lê Dũng Tráng

In his lectures B. Teissier has mainly spoken about the use of polar curves in the case of isolated singularities of complex hypersurfaces. Then in the case of complex plane curves, M.Merle has shown the relations between the topology of generic polar curves and that of the related plane curve. In this lecture we shall deal with polar curves in the case of hypersurfaces with not necessarily isolated singularities and we shall give the different theorems one can prove involving polar curves.

1. DEFINITION

Let $f: U \subset \mathbb{C}^{n+1} \longrightarrow \mathbb{C}$ be an analytic function defined on the open neighbourhood U of $0 \in \mathbb{C}^{n+1}$. Let $\phi: U \longrightarrow \mathbb{C}^2$ be the mapping defined by $\phi(z) = (x_0, f(z))$, where x_0 is a linear form of $\mathbb{C}^{n+1}$. We call $c(\phi)$ the critical locus of ϕ. We may suppose x_0 is a coordinate of $\mathbb{C}^{n+1}$ and that $x_1, \cdots, x_n$ are the others, then:

$$c(\phi) := \{z \in U \mid \partial f/\partial x_1 = \cdots = \partial f/\partial x_n = 0\}.$$

(1.1) Notice that $c(\phi)$ always contains the critical locus $\Sigma(f)$ of f, when U is sufficiently small:

$$\Sigma(f) := \{z \in c(\phi) \mid \partial f/\partial x_0 = 0\}.$$

In [4] we have proved:

LEMMA (1.2) There is a Zariski open dense set Ω of the projective space of linear hyperplanes of $\mathbb{C}^{n+1}$ passing through 0, such that for any $L \in \Omega$, say defined by some $x_0 = 0$, choosing U sufficiently small, one has

$$c(\phi) = \Sigma(f) \cup \Gamma$$

where Γ is either void or a curve not contained in $H := \{f = 0\}$.

Moreover if $\Gamma \neq \phi$, at any $x \in \Gamma - \{0\}$ the ideal $(\partial f/\partial x_1, \cdots, \partial f/\partial x_n)$ defines a reduced curve.