p-adic L-functions and modular forms

Alexei PANCHISHKIN
Institut Fourier, Université Grenoble-1
B.P.74, 38402 St.–Martin d'Hères, FRANCE

Lectures for the International Summer School and Conference
p-adic Analysis and its Applications
August 31th to September 18th, 2009 (Trieste - ITALY)

September, 2009

Abstract

1) Congruences and p-adic numbers. Hensel's lemma. The Tate field

2) Continuous and p-adic analytic functions. Mahler's criterion. Newton polygons
Zeroes of analytic functions. The Weierstrass preparation theorem and its generalizations.

3) Distributions, measures, and the abstract Kummer congruences.
The Kubota and Leopoldt p-adic L-functions and the Iwasawa algebra

4) Modular forms and L-functions.
Congruences and families of modular forms.

5) Method of canonical projection of modular distributions.
Examples of construction of p-adic L-functions

Related topics (for discussions, not included in the text of these materials)

6) Other approaches of constructing p-adic L-functions by Mazur-Tate-Teitelbaum, J.Coates, P.Colmez, H.Hida ... (using modular symbols by Manin-Mazur and their generalizations; Euler systems, work of D.Delbourgo, T.Ochiai, L.Berger, ..., overconvergent modular symbols by R.Pollack, G.Stevens, H.Darmon, ...)

7) Relations to the Iwasawa Theory

8) Applications of p-adic L-functions to Diophantine geometry

9) Open questions and problems in the theory of p-adic L-functions (Basic sources: Coates 60th Birthday Volume, Bourbaki talks by P.Colmez, J.Coates ...)

Lecture N°1. p-adic numbers and congruences

Originally p-adic numbers were invented by Hensel as a tool of solving congruences modulo powers of a prime number p.

Example. $p = 7$. Solve the congruence $x^2 \equiv 2 \bmod 7^n$.

Solution. If $n = 1$, put $x_0 = \pm 3$ then $x_0^2 \equiv 2 \mod 7$.
If $n = 2$, put $x_1 = x_0 + 7t_1, x_0 = 3$ then $(x_0 + 7t_1)^2 \equiv 2 \mod 7^2$ gives:
$9 + 6 \cdot 7t_1 + 7^2 t_1^2 \equiv 2 \mod 7^2 \Rightarrow 9 + 6t_1 \equiv 0 \mod 7 \Rightarrow t_1 = 1$
$\Rightarrow x_1 = 3 + 7 \cdot 1 = 10$.
If $n = 3$, put $x_2 = x_1 + 7^2 t_2, x_1 = 10$ then $(10 + 7^2 t_2)^2 \equiv 2 \mod 7^3$ gives:
$100 + 20 \cdot 7^2 t_2 + 7^4 t_2^2 \equiv 2 \mod 7^3 \Rightarrow t_2 \equiv -2/20 \mod 7 \Rightarrow t_2 \equiv 2 \mod 7$
$\Rightarrow x_2 = 3 + 7 \cdot 1 + 2 \cdot 7^2 = 108$.
In this way we obtain a sequence $x_0, x_1, x_2, \ldots$, so that $x_n \equiv x_{n+1} \bmod p^n$.
This is in strong analogy with approximation of a real number by rationls, for example:
$\sqrt{2} = 1.41421356237309504880168872 4 \cdots$
$= 1 + 4 \cdot 10^{-1} + 1 \cdot 10^{-2} + 4 \cdot 10^{-3} + 2 \cdot 10^{-4} + \cdots$

p-adic numbers as a completion of rationals

The idea of extending the field $\mathbb{Q}$ appears in algebraic number theory in various different guises. For example, the embedding $\mathbb{Q} \subset \mathbb{R}$ often gives useful necessary conditions for the existence of solutions to Diophantine equations over $\mathbb{Q}$ or $\mathbb{Z}$. The important feature of $\mathbb{R}$ is its completeness: every Cauchy sequence $\{\alpha_n\}_{n=1}^{\infty}$ in $\mathbb{R}$ has a limit α (a sequence is called Cauchy if for any $\varepsilon > 0$ we have $|\alpha_n - \alpha_m| < \varepsilon$ whenever n and m are greater than some large $N = N(\varepsilon)$). Also, every element of $\mathbb{R}$ is the limit of some Cauchy sequence $\{\alpha_n\}_{n=1}^{\infty}$ with $\alpha_n \in \mathbb{Q}$.
An analogous construction exists using the p–adic absolute value $|\cdot|_p$ of $\mathbb{Q}$:

$$|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0} = \{x \in \mathbb{R} \,|x \ \geq 0\}$$
$$|a/b|_p = p^{\mathrm{ord}_p b - \mathrm{ord}_p a}, \quad |0|_p = 0,$$

where $\mathrm{ord}_p a$ is the highest power of p dividing the integer a.

This general construction of "adjoining the limits of Cauchy sequences" to a field k with an absolute value $|\cdot|$ leads to a completion of k. This completion, often denoted $\hat{k}$, is complete, and contains k as a dense subfield with respect to the extended absolute value $|\cdot|$, [?], [?].
As was noted at the end of §2, all absolute values of $\mathbb{Q}$ are equivalent either to the usual Archimedean absolute value, or to the p–adic absolute value. Thus any completion of $\mathbb{Q}$ is either $\mathbb{R}$, or $\mathbb{Q}_p$, the field of p-adic numbers, i.e. the completion of the field of rational numbers $\mathbb{Q}$ with respect to the p-adic absolute value. Using the embeddings $\mathbb{Q} \hookrightarrow \mathbb{R}$ and $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ (for all primes p) many arithmetical problems can be simplified. An important example is given by the following *Minkowski–Hasse theorem* [?], Ch.1. the equation

$$Q(x_1, x_2, \ldots, x_n) = 0, \tag{2.1}$$

given by a quadratic form $Q(x_1, x_2, \ldots, x_n) = \sum_{i,j} a_{ij} x_i x_j$, $a_{ij} \in \mathbb{Q}$ has a non–trivial solution in rational numbers, iff it is non–trivially solvable over $\mathbb{R}$ and over all $\mathbb{Q}_p$. There are very effective tools for finding solutions in $\mathbb{Q}_p$. These tools are somewhat analogous to those for $\mathbb{R}$ such as the "Newton - Raphson algorithm", which in the p–adic case becomes *Hensel's lemma*.

The simplest way to define the p–adic numbers is to consider expressions of the type

$$\alpha = a_m p^m + a_{m+1} p^{m+1} + \dots, \tag{2.2}$$

where $a_i \in \{0, 1, \dots . p-1\}$ are digits to the base p, and $m \in \mathbb{Z}$. It is convenient to write down α as a sequence of digits, infinite to the left:

$$\alpha = \begin{cases} \cdots a_{m+1} a_m \overbrace{000\dots0}^{m-1 \text{ zeros}}{}_{(p)}, & \text{if } m \geq 0, \\ \cdots a_1 a_0 . a_{-1} \cdots a_{m(p)}, & \text{if } m < 0. \end{cases}$$

These expressions form a field, in which algebraic operations are executed in the same way as for natural numbers $n = a_0 + a_1 p + \dots a_r p^r$, written as sequences of digits to the base p. Consequently, this field contains all the natural numbers and hence all rational numbers.

Expression of rational numbers as p-adic numbers

For example,

$$-1 = \frac{p-1}{1-p} = (p-1) + (p-1)p + (p-1)p^2 + \cdots = \cdots (p-1)(p-1)_{(p)};$$

$$\frac{-a_0}{p-1} = a_0 + a_0 p + a_0 p^2 + \cdots = \cdots a_0 a_0 a_{0(p)}.$$

For $n \in \mathbb{N}$ the expression for $-n = n \cdot (-1)$ of type (??) is obtained if we multiply the above expressions for n and for -1. Generally, for $\alpha \in \mathbb{Q}$ write $\alpha = c - \frac{a}{b}$, where $a, c \in \mathbb{Z}$, $b \in N$, $0 \leq a < b$, i.e. a/b is a proper fraction. Then by an elementary theorem of Euler, $p^{\varphi(b)} - 1 = bu$, $u \in \mathbb{N}$. Hence

$$-\frac{a}{b} = \frac{au}{p^{\varphi(b)} - 1},$$

and $au < bu = p^r - 1$, $r = \varphi(b)$. Now let au be written to the base p as $a_{r-1} \cdots a_{0(p)}$, then the expression of type (??) for α is obtained as the sum of the expression for $c \in \mathbb{N}$ and

$$-\frac{a}{b} = \cdots a_0 \overbrace{a_{r-1} \cdots a_0}^{r \text{ digits}} \overbrace{a_{r-1} \cdots a_0}^{r \text{ digits}}{}_{(p)}.$$

For example, if $p = 5$,

$$\frac{9}{7} = 2 - \frac{5}{7} = 2 + \frac{5 \cdot 2232}{1 - 5^6} \quad c = 2 \; a = 5, \; b = 7,$$

so that

$$2232 = 32412_{(5)} = 3 \cdot 5^4 + 2 \cdot 5^3 + 4 \cdot 5^2 + 1 \cdot 5 + 2,$$

thus

$$\frac{9}{7} = \cdots \overbrace{3241203241203}^{} 24122_{(5)}.$$

It is easy to verify that the completion of $\mathbb{Q}$ with respect to the p–adic metric $|\cdot|_p$ can be identified with the described field of p–adic expansions (??), where $|\alpha|_p = p^m$ for α as in (??) with $a_m \neq 0$ (see Koblitz N. (1980)).

It is curious to compare the expansions (??) infinite to the left with the ordinary expansions of real numbers $\alpha \in \mathbb{R}$, infinite to the right:

$$\alpha = a_m a_{m-1} \cdots a_0 . a_{-1} \cdots = a_m 10^m + a_{m-1} 10^{m-1} + \cdots a_0 + a_{-1} 10^{-1} + \cdots ,$$

where $a_i \in \{0, 1, \cdots , 9\}$ are digits, $a_m \neq 0$. These expansions to any natural base lead to the same field $\mathbb{R}$. Also, a given α can possess various expressions of this type, e.g. $2.000 \cdots = 1.999 \cdots$. However, in the p–adic case the expressions (??) are uniquely determined by α. This fact provides additional comfort when calculating with p–adic numbers.

Computation with PARI/GP (see [?])

```
gp > forprime(p=2,131,print("p="p,","9/7="9/7+O(p^6)))
p=2,9/7=1 + 2 + 2^2 + 2^3 + 2^5 + O(2^6)
p=3,9/7=3^2 + 3^3 + 2*3^5 + O(3^6)
p=5,9/7=2 + 2*5 + 5^2 + 4*5^3 + 2*5^4 + 3*5^5 + O(5^6)
p=7,9/7=2*7^-1 + 1 + O(7^6)
p=11,9/7=6 + 9*11 + 7*11^2 + 4*11^3 + 9*11^4 + 7*11^5 + O(11^6)
p=13,9/7=5 + 9*13 + 3*13^2 + 9*13^3 + 3*13^4 + 9*13^5 + O(13^6)
p=17,9/7=11 + 14*17 + 4*17^2 + 7*17^3 + 2*17^4 + 12*17^5 + O(17^6)
p=19,9/7=4 + 8*19 + 5*19^2 + 16*19^3 + 10*19^4 + 13*19^5 + O(19^6)
p=23,9/7=21 + 9*23 + 16*23^2 + 19*23^3 + 9*23^4 + 16*23^5 + O(23^6)
p=29,9/7=22 + 20*29 + 20*29^2 + 20*29^3 + 20*29^4 + 20*29^5 + O(29^6)
p=31,9/7=19 + 26*31 + 8*31^2 + 13*31^3 + 4*31^4 + 22*31^5 + O(31^6)
p=37,9/7=33 + 15*37 + 26*37^2 + 31*37^3 + 15*37^4 + 26*37^5 + O(37^6)
p=41,9/7=13 + 29*41 + 11*41^2 + 29*41^3 + 11*41^4 + 29*41^5 + O(41^6)
p=43,9/7=32 + 30*43 + 30*43^2 + 30*43^3 + 30*43^4 + 30*43^5 + O(43^6)
p=47,9/7=8 + 20*47 + 13*47^2 + 40*47^3 + 26*47^4 + 33*47^5 + O(47^6)
p=53,9/7=24 + 45*53 + 37*53^2 + 22*53^3 + 45*53^4 + 37*53^5 + O(53^6)
p=59,9/7=35 + 50*59 + 16*59^2 + 25*59^3 + 8*59^4 + 42*59^5 + O(59^6)
p=61,9/7=10 + 26*61 + 17*61^2 + 52*61^3 + 34*61^4 + 43*61^5 + O(61^6)
p=67,9/7=30 + 57*67 + 47*67^2 + 28*67^3 + 57*67^4 + 47*67^5 + O(67^6)
p=71,9/7=52 + 50*71 + 50*71^2 + 50*71^3 + 50*71^4 + 50*71^5 + O(71^6)
p=73,9/7=43 + 62*73 + 20*73^2 + 31*73^3 + 10*73^4 + 52*73^5 + O(73^6)
p=79,9/7=69 + 33*79 + 56*79^2 + 67*79^3 + 33*79^4 + 56*79^5 + O(79^6)
p=83,9/7=25 + 59*83 + 23*83^2 + 59*83^3 + 23*83^4 + 59*83^5 + O(83^6)
p=89,9/7=14 + 38*89 + 25*89^2 + 76*89^3 + 50*89^4 + 63*89^5 + O(89^6)
p=97,9/7=29 + 69*97 + 27*97^2 + 69*97^3 + 27*97^4 + 69*97^5 + O(97^6)
p=101,9/7=59 + 86*101 + 28*101^2 + 43*101^3 + 14*101^4 + 72*101^5 + O(101^6)
p=103,9/7=16 + 44*103 + 29*103^2 + 88*103^3 + 58*103^4 + 73*103^5 + O(103^6)
p=107,9/7=93 + 45*107 + 76*107^2 + 91*107^3 + 45*107^4 + 76*107^5 + O(107^6)
p=109,9/7=48 + 93*109 + 77*109^2 + 46*109^3 + 93*109^4 + 77*109^5 + O(109^6)
p=113,9/7=82 + 80*113 + 80*113^2 + 80*113^3 + 80*113^4 + 80*113^5 + O(113^6)
p=127,9/7=92 + 90*127 + 90*127^2 + 90*127^3 + 90*127^4 + 90*127^5 + O(127^6)
p=131,9/7=20 + 56*131 + 37*131^2 + 112*131^3 + 74*131^4 + 93*131^5 + O(131^6)
```

Topology of p-adic numbers

The field $\mathbb{Q}_p$ is a *complete metric space* with the topology generated by the "open discs":

$$U_a(r) = \{x \mid |x-a| < r\} \quad (x,\ a \in \mathbb{Q}_p,\ r > 0)$$

(or "closed discs" $D_a(r) = \{x \mid |x-a| \leq r\}$). From the topological point of view, the sets $U_a(r)$ and $D_a(r)$ are both open and closed in $\mathbb{Q}_p$.
An important topological property of $\mathbb{Q}_p$ is its *local compactness*: all discs of finite radius are compact. The easiest way to show this is to consider any sequence $\{\alpha_n\}_{n=1}^{\infty}$ of elements $\alpha_n \in D_a(r)$ and to construct a limit point. Such a point may be found step–by–step using the *p–adic digits* (??). One knows that the number of digits "after the point" is bounded on any finite disc. In particular, the disc

$$\mathbb{Z}_p = D_0(1) = \{x \mid |x|_p \leq 1\} = \left\{x = a_0 + a_1 p + a_2 p^2 + \cdots\right\}$$

is a compact topological ring, whose elements are called p–adic integers. $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$. The ring $\mathbb{Z}_p$ is local, i.e. it has only one maximal ideal $p\mathbb{Z}_p = U_0(1)$ with residue field $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$. The set of invertible elements (units) of $\mathbb{Z}_p$ is

$$\mathbb{Z}_p^{\times} = \mathbb{Z}_p \backslash p\mathbb{Z}_p = \{x \mid |x|_p = 1\} = \left\{x = a_0 + a_1 p + a_2 p^2 + \cdots \mid a_0 \neq 0\right\}.$$

Applications of p–adic Numbers to Solving Congruences.

The first appearances of p–adic numbers, in papers by Hensel, were related to the problem of finding solutions to congruences modulo p^n. An application of this method by his student H.Hasse to the theory of quadratic forms has lead to an elegant reformulation of this theory, without the use of considerations over the residue rings $\mathbb{Z}/p^n\mathbb{Z}$. These considerations are tiring because of the zero–divisors in $\mathbb{Z}/p^n\mathbb{Z}$. From the above presentation of $\mathbb{Z}_p$ as the projective limit

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

it follows that for $f(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n]$, the congruences

$$f(x_1, \ldots, x_n) \equiv 0 (\mathrm{mod}\ p^n)$$

are solvable for all $n \geq 1$ iff the equation

$$f(x_1, \ldots, x_n) = 0$$

is solvable in p–adic integers. Solutions in $\mathbb{Z}_p$ can be obtained using the following p–adic version of the *"Newton - Raphson algorithm"*.

Theorem (Hensel's Lemma)

Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial in one variable x, $f'(x) \in \mathbb{Z}_p[x]$ its formal derivative, and suppose that for some $\alpha_0 \in \mathbb{Z}_p$ the initial condition

$$|f(\alpha_0)/f'(\alpha_0)^2|_p < 1 \tag{2.3}$$

is satisfied.
Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that

$$f(\alpha) = 0, \quad |\alpha - \alpha_0| < 1.$$

We prove this by induction using the sequence of "successive approximations":

$$\alpha_n = \alpha_{n-1} - \frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}.$$

Taking into account the formal Taylor expansion of $f(x)$ at $x = \alpha_{n-1}$ one shows that this sequence is Cauchy, and its limit α has all the desired properties (cf. [**?**], [**?**]).
For example, if $f(x) = x^{p-1} - 1$, then any $\alpha_0 \in \{1, 2, \ldots, p-1\}$ satisfies the condition $|f(\alpha_0)|_p < 1$ At the same time
$f'(\alpha_0) = (p-1)\alpha_0^{p-2} \not\equiv 0 \mod p$, hence the initial condition (**??**) is satisfied. The root α coincides then with the uniquely defined Teichmüller representative of α_0: $\alpha = \omega(\alpha_0)$.

Lecture N°2. Continuous and analytic functions over a non-Archimedean field

Let K be a closed subfield of the Tate field $\mathbb{C}_p$. For a subset $W \subset K$ we consider continuous functions $f : W \to \mathbb{C}_p$. The standard examples of continuous functions are provided by polynomials, by rational functions (at points where they are finite), and also by locally constant functions. If W is compact then for any continuous function $f : W \to \mathbb{C}_p$ and for any $\varepsilon > 0$ there exists a polynomial $h(x) \in \mathbb{C}_p[x]$ such that $|f(x) - h(x)|_p < \varepsilon$ for all $x \in W$. If $f(W) \subset L$ for a closed subfield L of $\mathbb{C}_p$ then $h(x)$ can be chosen so that $h(x) \in L[x]$ (see [?], [?]).

Interesting examples of continuous p-adic functions are provided by interpolation of functions, defined on certain subsets, such as $W = \mathbb{Z}$ or $\mathbb{N}$ with $K = \mathbb{Q}_p$. Let f be any function on non-negative integers with values in $\mathbb{Q}_p$ or in some (complete) $\mathbb{Q}_p$-Banach space. In order to extend $f(x)$ to all $x \in \mathbb{Z}_p$ we can use the interpolation polynomials

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}.$$

Then we have that $\binom{x}{n}$ is a polynomial of degree n of x, which for $x \in \mathbb{Z}$, $x \geq 0$ gives the binomial coefficient. If $x \in \mathbb{Z}_p$ then x is close (in the p-adic topology) to a positive integer, hence the value of $\binom{x}{n}$ is also close to an integer, therefore $\binom{x}{n} \in \mathbb{Z}_p$.

Mahler's criterion

The classical Mahler's interpolation theorem says that any continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ can be written in the form (see [?], [?]):

$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}, \tag{3.4}$$

with $a_n \to 0$ (p-adically) for $n \to \infty$. For a function $f(x)$ defined for $x \in \mathbb{Z}$, $x \geq 0$ one can write formally

$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n},$$

where the coefficients can be founded from the system of linear equations

$$f(n) = \sum_{m=0}^{n} a_m \binom{n}{m},$$

that is

$$a_m = \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} f(j).$$

The series for $f(x)$ is always reduced to a finite sum for each $x \in \mathbb{Z}$, $x \geq 0$. If $a_n \to 0$ then this series is convergent for all $x \in \mathbb{Z}_p$. As was noticed above, the inverse statement is also valid ("*Mahler's criterion*"). If convergence of a_n to zero is so fast that the series defining the coefficients of the x-expansion of $f(x)$ also converge, then $f(x)$ can be extended to an *analytic function*. Unfortunately, for an arbitrary sequence a_n with $a_n \to 0$ the attempt to use (**??**) for continuation of $f(x)$ out of the subset $\mathbb{Z}_p$ in $\mathbb{C}_p$ may fail. However, in the sequel we mostly consider anlytic functions, that are defined as sums of power series.

Distributions and measures.

Let us consider a commutative associative ring R, an R-module $\mathcal{A}$ and a profinite (i.e. compact and totally disconnected) topological space Y. Then Y is a projective limit of finite sets:

$$Y = \varprojlim_{I} Y_i$$

where I is a (partially ordered) inductive set and for $i \geq j$, $i, j \in I$ there are surjective homomorphisms $\pi_{i,j} : Y_i \to Y_j$ with the condition $\pi_{i,j} \circ \pi_{j,k} = \pi_{i,k}$ for $i \geq j \geq k$. The inductivity of I means that for any $i, j \in I$ there exists $k \in I$ with the condition $k \geq i$, $k \geq j$. By the universal property we have that for each $i \in I$ a unique map $\pi_i : Y \to Y_i$ is defined, which satisfies the property $\pi_{i,j} \circ \pi_i = \pi_j$ (for each $i, j \in I$).

Let $\mathrm{Step}(Y,R)$ be the R-module consisting of all R-valued locally constant functions $\phi : Y \to R$.

Definition

A distribution on Y with values in a R-module $\mathcal{A}$ is a R-linear homomorphism

$$\mu : \mathrm{Step}(Y,R) \longrightarrow \mathcal{A}.$$

For $\varphi \in \mathrm{Step}(Y,R)$ we use the notations

$$\mu(\varphi) = \int_Y \varphi \mathrm{d}\mu = \int_Y \varphi(y)\mathrm{d}\mu(y).$$

Each distribution μ can be defined by a system of functions $\mu^{(i)} : Y_i \to \mathcal{A}$, satisfying the following finite-additivity condition

$$\mu^{(j)}(y) = \sum_{x \in \pi_{i,j}^{-1}(y)} \mu^{(i)}(x) \quad (y \in Y_j, \quad x \in Y_i). \tag{4.5}$$

In order to construct such a system it suffices to put

$$\mu^{(i)}(x) = \mu(\delta_{i,x}) \in \mathcal{A} \quad (x \in Y_i),$$

where $\delta_{i,x}$ is the characteritic function of the inverse image $\pi_i^{-1}(x) \subset Y$ with respect to the natural projection $Y \to Y_i$. For an arbitrary function $\varphi_j : Y_j \to R$ and $i \geq j$ we define the functions

$$\varphi_i = \varphi_j \circ \pi_{i,j}, \quad \varphi = \varphi_j \circ \pi_j, \quad \varphi \in \mathrm{Step}(Y,R), \quad \varphi_i : Y_i \xrightarrow{\pi_{i,j}} Y_j \longrightarrow R.$$

A convenient criterion of the fact that a system of functions $\mu^{(i)} : Y_i \to \mathcal{A}$ satisfies the finite additivity condition (??) (and hence is associated to some distribution) is given by the following condition (*compatibility criterion*): for all $j \in I$, and $\varphi_j : Y_j \to R$ the value of the sums

$$\mu(\varphi) = \mu^{(i)}(\varphi_i) = \sum_{y \in Y_i} \varphi_i(y)\mu^{(i)}(y), \tag{4.6}$$

is independent of i for all large enough $i \geq j$. When using (??), it suffices to verify the condition (??) for some "basic" system of functions. For example, if

$$Y = G = \varprojlim_i G_i$$

is a profinite abelian group, and R is a domain containing all roots of unity of the order dividing the order of Y (which is a "supernatural number") then it suffices to check the condition (??) for all characters of finite order $\chi : G \to R$, since their $R \otimes \mathbb{Q}$ -linear span coincides with the whole ring $\mathrm{Step}(Y, R \otimes \mathbb{Q})$ by the orthogonality properties for characters of a finite group (see [?], [?]).

Example: Bernoulli distributions

Let M be a positive integer, $f : \mathbb{Z} \to \mathbb{C}$ is a periodic function with the period M (i.e. $f(x+M) = f(x)$, $f : \mathbb{Z}/M\mathbb{Z} \to \mathbb{C}$). The generalized Bernoulli number (see [?]) $B_{k,f}$ is defined as $k!$ times the coefficient by t^k in the expansion in t of the following rational quotient

$$\sum_{a=0}^{M-1} \frac{f(a)te^{at}}{e^{Mt}-1},$$

that is,

$$\sum_{k=0}^{\infty} \frac{B_{k,f}}{k!} t^k = \sum_{a=0}^{M-1} \frac{f(a)te^{at}}{e^{Mt}-1}. \tag{4.7}$$

Now let us consider the profinite ring

$$Y = \mathbb{Z}_S = \varprojlim_M (\mathbb{Z}/M\mathbb{Z})$$

$(S(M) \subset S)$, the projective limit being taken over the set of all positive integers M with support $S(M)$ in a fixed finite set S of prime numbers. Then the periodic function $f : \mathbb{Z}/M\mathbb{Z} \to \mathbb{C}$ with $S(M) \subset S$ may be viewed as an element of $\mathrm{Step}(Y, \mathbb{C})$. We claim that there exists a distribution $E_k : \mathrm{Step}(Y, \mathbb{C}) \to \mathbb{C}$ which is uniquely determined by the condition

$$E_k(f) = B_{k,f} \text{ for all } f \in \mathrm{Step}(Y, \mathbb{C}). \tag{4.8}$$

In order to prove the existence of this distribution we use the above criterion (??) and check that for every $f \in \mathrm{Step}(Y, \mathbb{C})$ the right hand side in (??) (i.e. $B_{k,f}$) does not depend on the choice of a period M of the function f. It follows directly from the definition (??); however we give here a different proof which is based on an interpretation of the numbers $B_{k,f}$ as certain special values of L-functions.

For a function $f : \mathbb{Z}/M\mathbb{Z} \to \mathbb{C}$ let

$$L(s,f) = \sum_{n=1}^{\infty} f(n) n^{-s}$$

be the corresponding L-series which is absolutely convergent for all s with $\mathrm{Re}(s) > 1$ and admits an analytic continuation over all $s \in \mathbb{C}$. For this series we have that

$$L(1-k,f) = -\frac{B_{k,f}}{k}. \tag{4.9}$$

For example, if $f \equiv 1$ is the constant function with the period $M = 1$ then we have that

$$\zeta(1-k) = -\frac{B_k}{k}, \qquad \sum_{k=0}^{\infty} \frac{B_k}{k!} t^k = \frac{t}{e^t - 1},$$

B_k being the Bernoulli number. The formula (??) is established by means of the contour integral discovered by Riemann. formula apparently implies the desired independence of $B_{k,f}$ on the choice of M. We note also that if $K \subset \mathbb{C}$ is an arbitrary subfield, and $f(Y) \subset K$ then we have from the formula (??) that $B_{k,f} \in K$ hence the distribution E_k is a K-valued distribution on Y.

Measures

Let R be a topological ring, and $\mathcal{C}(Y, R)$ be the topological module of all R-valued functions on a profinite set Y.

Definition

A measure on Y with values in the topological R-module $\mathcal{A}$ is a continuous homomorphism of R-modules

$$\mu : \mathcal{C}(Y, R) \longrightarrow \mathcal{A}.$$

The restriction of μ to the R-submodule $\mathrm{Step}(Y, R) \subset \mathcal{C}(Y, R)$ defines a distribution which we denote by the same letter μ, and the measure μ is uniquely determined by the corresponding distribution since the R-submodule $\mathrm{Step}(Y, R)$ is dense in $\mathcal{C}(Y, R)$. The last statement expresses the well known fact about the uniform continuity of a continuous function over a compact topological space.

Now we consider any closed subring R of the Tate field $\mathbb{C}_p$, $R \subset \mathbb{C}_p$, and let $\mathcal{A}$ be a complete R-module with topology given by a norm $|\cdot|_{\mathcal{A}}$ on $\mathcal{A}$ compatible with the norm $|\cdot|_p$ on $\mathbb{C}_p$ so that the following conditions are satisfie:

- for $x \in \mathcal{A}$ the equality $|x|_{\mathcal{A}} = 0$ is equivalent to $x = 0$,
- for $a \in R$, $x \in \mathcal{A}$: $|ax|_{\mathcal{A}} = |a|_p |x|_{\mathcal{A}}$,
- for all $x, y \in \mathcal{A}$: $|x + y|_{\mathcal{A}} < \max(|x|_{\mathcal{A}}, |y|_{\mathcal{A}})$.

Then the fact that a distribution (a system of functions $\mu^{(i)} : Y_i \to \mathcal{A}$) gives rise to a $\mathcal{A}$-valued measure on Y is equivalent to the condition that the system $\mu^{(i)}$ is bounded, i.e. for some constant $B > 0$ and for all $i \in I$, $x \in Y_i$ the following uniform estimate holds:

$$|\mu^{(i)}(x)|_{\mathcal{A}} < B. \tag{4.10}$$

This criterion is an easy consequence of the non-Archimedean property

$$|x + y|_{\mathcal{A}} \leq \max(|x|_{\mathcal{A}}, |y|_{\mathcal{A}})$$

of the norm $|\cdot|_{\mathcal{A}}$ (see [?], [?]). In particular if $\mathcal{A} = R = \mathrm{O}_p = \{x \in \mathbb{C}_p \quad | \quad |x|_p \leq 1\}$ is the subring of integers in the Tate field $\mathbb{C}_p$ then the set of O_p-valued distributions on Y coincides with O_p-valued measures (in fact, both sets are R-algebras with multiplication defined by convolution.

Lecture N°3. The abstract Kummer congruences and the p-adic Mellin transform

A useful criterion for the existence of a measure with given properties is:

Proposition (The abstract Kummer congruences)

(see [?]). Let $\{f_i\}$ be a system of continuous functions $f_i \in \mathcal{C}(Y, \mathrm{O}_p)$ in the ring $\mathcal{C}(Y, \mathrm{O}_p)$ of all continuous functions on the compact totally disconnected group Y with values in the ring of integers O_p of $\mathbb{C}_p$ such that $\mathbb{C}_p$-linear span of $\{f_i\}$ is dense in $\mathcal{C}(Y, \mathbb{C}_p)$. Let also $\{a_i\}$ be any system of elements $a_i \in \mathrm{O}_p$. Then the existence of an O_p-valued measure μ on Y with the property

$$\int_Y f_i d\mu = a_i$$

is equivalent to the following congruences, for an arbitrary choice of elements $b_i \in \mathbb{C}_p$ almost all of which vanish

$$\sum_i b_i f_i(y) \in p^n \mathrm{O}_p \text{ for all } y \in Y \text{ implies } \sum_i b_i a_i \in p^n \mathrm{O}_p. \qquad (4.11)$$

Remark

Since $\mathbb{C}_p$-measures are characterised as bounded $\mathbb{C}_p$-valued distributions, every $\mathbb{C}_p$-measures on Y becomes a O_p-valued measure after multiplication by some non-zero constant.

Proof of proposition **??**. The necessity is obvious since

$$\begin{aligned}\sum_i b_i a_i &= \int_Y (p^n \mathrm{O}_p - \text{valued function}) d\mu = \\ &= p^n \int_Y (\mathrm{O}_p - \text{valued function}) d\mu \in p^n \mathrm{O}_p.\end{aligned}$$

In order to prove the sufficiency we need to construct a measure μ from the numbers a_i. For a function $f \in \mathcal{C}_(Y, \mathrm{O}_p)$ and a positive integer n there exist elements $b_i \in \mathbb{C}_p$ such that only a finite number of b_i does not vanish, and

$$f - \sum_i b_i f_i \in p^n \mathcal{C}(Y, \mathrm{O}_p),$$

according to the density of the $\mathbb{C}_p$-span of $\{f_i\}$ in $\mathcal{C}(Y, \mathbb{C}_p)$. By the assumption (**??**) the value $\sum_i a_i b_i$ belongs to O_p and is well defined modulo p^n (i.e. does not depend on the choice of b_i). Following N.M. Katz ([**?**]), we denote this value by "$\int_Y f d\mu \bmod p^n$ ". Then we have that the limit procedure

$$\int_Y f d\mu = \lim_{n\to\infty} \text{“} \int_Y f d\mu \bmod p^n \text{ ”} \in \varprojlim_n \mathrm{O}_p/p^n\mathrm{O}_p = \mathrm{O}_p,$$

gives the measure μ.

Mazur's measure

Let $c > 1$ be a positive integer coprime to

$$M_0 = \prod_{q \in S} q$$

with S being a fixed set of prime numbers. Using the criterion of the proposition **??** we show that the $\mathbb{Q}$ -valued distribution defined by the formula

$$E_k^c(f) = E_k(f) - c^k E_k(f_c), \qquad f_c(x) = f(cx), \tag{4.12}$$

turns out to be a measure where $E_k(f)$ are defined by (**??**), $f \in \mathrm{Step}(Y, \mathbb{Q}_p)$ and the field $\mathbb{Q}$ is viewed as a subfield of $\mathbb{C}_p$.
Define the generelized Bernoulli polynomials $B_{k,f}^{(M)}(X)$ as

$$\sum_{k=0}^{\infty} B_{k,f}^{(M)}(X) \frac{t^k}{k!} = \sum_{a=0}^{M-1} f(a) \frac{te^{(a+X)t}}{e^{Mt} - 1}, \tag{4.13}$$

and the generalized sums of powers

$$S_{k,f}(M) = \sum_{a=0}^{M-1} f(a) a^k.$$

Then the definition (??) formally implies that

$$\frac{1}{k}[B_{k,f}^{(M)}(M) - B_{k,f}^{(M)}(0)] = S_{k-1,f}(M), \tag{4.14}$$

and also we see that

$$B_{k,f}^{(M)}(X) = \sum_{i=0}^{k} \binom{k}{i} B_{i,f} X^{k-i} = B_{k,f} + kB_{k-1,f}X + \cdots + B_{0,f}X^k. \tag{4.15}$$

The last identity can be rewritten symbolically as

$$B_{k,f}(X) = (B_f + X)^k.$$

The equality (??) enables us to calculate the (generalized) sums of powers in terms of the (generalized) Bernoulli numbers. In particular this equality implies that the Bernoulli numbers $B_{k,f}$ can be obtained by the following p-adic limit procedure (see [?]):

$$B_{k,f} = \lim_{n\to\infty} \frac{1}{Mp^n} S_{k,f}(Mp^n) \quad \text{(a } p\text{-adic limit)}, \tag{4.16}$$

where f is a $\mathbb{C}_p$-valued function on $Y = \mathbb{Z}_S$. Indeed, if we replace M in (??) by Mp^n with growing n and let D be the common denominator of all coefficients of the polynomial $B_{k,f}^{(M)}(X)$. Then we have from (??) that

$$\frac{1}{k}\left[B_{k,f}^{(Mp^n)}(M) - B_{k,f}^{(M)}(0)\right] \equiv B_{k-1,f}(Mp^n) \pmod{\frac{1}{kD}p^2 n}. \tag{4.17}$$

The proof of (??) is accomplished by division of (??) by Mp^n and by application of the formula (??).

Now we can directly show that the distribution E_k^c defined by (??) are in fact bounded measures. If we use (??) and take the functions $\{f_i\}$ to be all of the functions in $\mathrm{Step}(Y, \mathrm{O}_p)$. Let $\{b_i\}$ be a system of elements $b_i \in \mathbb{C}_p$ such that for all $y \in Y$ the congruence

$$\sum_i b_i f_i(y) \equiv 0 \pmod{p^n} \tag{4.18}$$

holds. Set $f = \sum_i b_i f_i$ and assume (without loss of generality) that the number n is large enough so that for all i with $b_i \neq 0$ the congruence

$$B_{k,f_i} \equiv \frac{1}{Mp^n} S_{k,f_i}(Mp^n) \pmod{p^n} \tag{4.19}$$

is valid in accordance with (??). Then we see that

$$B_{k,f} \equiv (Mp^n)^{-1} \sum_i \sum_{a=0}^{Mp^n-1} b_i f_i(a) a^k \pmod{p^n}, \tag{4.20}$$

hence we get by definition (??):

$$\begin{aligned} E_k^c(f) &= B_{k,f} - c^k B_{k,f_c} \qquad (4.21)\\ &\equiv (Mp^n)^{-1} \sum_i \sum_{a=0}^{Mp^n-1} b_i \left[f_i(a) a^k - f_i(ac)(ac)^k \right] \pmod{p^n}. \end{aligned}$$

Let $a_c \in \{0, 1, \cdots, Mp^n - 1\}$, such that $a_c \equiv ac \pmod{Mp^n}$, then the map $a \longmapsto a_c$ is well defined and acts as a permutation of the set $\{0, 1, \cdots, Mp^n - 1\}$, hence (??) is equivalent to the congruence

$$E_k^c(f) = B_{k,f} - c^k B_{k,f_c} \equiv \sum_i \frac{a_c^k - (ac)^k}{Mp^n} \sum_{a=0}^{Mp^n-1} b_i f_i(a) a^k \pmod{p^n}. \quad (4.22)$$

Now the assumption (??) formally inplies that $E_k^c(f) \equiv 0 \pmod{p^n}$, completing the proof of the abstact congruences and the construction of measures E_k^c.

Remark

The formula (??) also implies that for all $f \in \mathcal{C}(Y, \mathbb{C}_p)$ the following holds

$$E_k^c(f) = kE_1^c(x_p^{k-1} f) \quad (4.23)$$

where $x_p : Y \longrightarrow \mathbb{C}_p \in \mathcal{C}(Y, \mathbb{C}_p)$ is the composition of the projection $Y \longrightarrow \mathbb{Z}_p$ and the embedding $\mathbb{Z}_p \hookrightarrow \mathbb{C}_p$.

Indeed if we put $a_c = ac + Mp^n t$ for some $t \in \mathbb{Z}$ then we see that

$$a_c^k - (ac)^k = (ac + Mp^n t)^k - (ac)^k \equiv kMp^n t(ac)^{k-1} \pmod{(Mp^n)^2},$$

and we get that in (??):

$$\frac{a_c^k - (ac)^k}{Mp^n} \equiv k(ac)^{k-1} \frac{a_c - ac}{Mp^n} \pmod{Mp^n}.$$

The last congruence is equivalent to saying that the abstract Kummer congruences (??) are satisfied by all functions of the type $x_p^{k-1} f_i$ for the measure E_1^c with $f_i \in \mathrm{Step}(Y, \mathbb{C}_p)$ establishing the identity (??).

The domain of definition of the non-Archimedean zeta functions

In the classical case the set on which zeta functions are defined is the set of complex numbers $\mathbb{C}$ which may be viewed equally as the set of all continuous characters (more precisely, quasicharacters) via the following isomorphism:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\sim} & \mathrm{Hom}_{\mathrm{cont}}(\mathbb{R}_+^\times, \mathbb{C}^\times) \\ s & \longmapsto & (y \longmapsto y^s) \end{array} \tag{4.24}$$

The construction which associates to a function $h(y)$ on $\mathbb{R}_+^\times$ (with certain growth conditions as $y \to \infty$ and $y \to 0$) the following integral

$$L_h(s) = \int_{\mathbb{R}_+^\times} h(y) y^s \frac{dy}{y}$$

(which converges probably not for all values of s) is called the *Mellin transform*.

For example, if $\zeta(s) = \sum_{n\geq 1} n^{-s}$ is the Riemann zeta function, then the function $\zeta(s)\Gamma(s)$ is the Mellin transform of the function $h(y) = 1/(1-e^{-y})$:

$$\zeta(s)\Gamma(s) = \sum_0^\infty \frac{1}{1-e^{-y}} y^s \frac{dy}{y}, \tag{4.25}$$

so that the integral and the series are absolutely convergent for $\mathrm{Re}(s) > 1$. For an arbitrary function of type

$$f(z) = \sum_{n=1}^\infty a(n) e^{2i\pi nz}$$

with $z = x + iy \in \mathbb{H}$ in the upper half plane $\mathbb{H}$ and with the growth condition $a(n) = \mathrm{O}(n^c)$ $(c > 0)$ on its Fourier coefficients, we see that the zeta function

$$L(s, f) = \sum_{n=1}^\infty a(n) n^{-s},$$

essentially coincides with the Mellin transform of $f(z)$, that is

$$\frac{\Gamma(s)}{(2\pi)^s} L(s, f) = \int_0^\infty f(iy) y^s \frac{dy}{y}. \tag{4.26}$$

Both sides of the equality (??) converge absolutely for $\mathrm{Re}(s) > 1 + c$. The identities (??) and (??) are immediately deduced from the well known integral representation for the gamma-function

$$\Gamma(s) = \int_0^\infty e^{-y} y^s \frac{dy}{y}, \tag{4.27}$$

where $\frac{dy}{y}$ is a measure on the group $\mathbb{R}_+^\times$ which is invariant under the group translations (Haar measure). The integral (??) is absolutely convergent for $\mathrm{Re}(s) > 0$ and it can be interpreted as the integral of the product of an additive character $y \mapsto e^{-y}$ of the group $\mathbb{R}^{(+)}$ restricted to $\mathbb{R}_+^\times$, and of the multiplicative character $y \mapsto y^s$, integration is taken with respect to the Haar measure $\mathrm{d}y/y$ on the group $\mathbb{R}_+^\times$.

In the theory of the non-Archimedean integration one considers the group $\mathbb{Z}_S^\times$ (the group of units of the S-adic completion of the ring of integers $\mathbb{Z}$) instead of the group $\mathbb{R}_+^\times$, and the Tate field $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}}_p$ (the completion of an algebraic closure of $\mathbb{Q}_p$) instead of the complex field $\mathbb{C}$. The domain of definition of the p-adic zeta functions is the p-adic analytic group

$$X_S = \mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}_S^\times, \mathbb{C}_p^\times) = X(\mathbb{Z}_S^\times), \tag{4.28}$$

where:

$$\mathbb{Z}_S^\times \cong \oplus_{q \in S} \mathbb{Z}_q^\times,$$

and the symbol

$$X(G) = \mathrm{Hom}_{\mathrm{cont}}(G, \mathbb{C}_p^\times) \tag{4.29}$$

denotes the functor of all p-adic characters of a topological group G (see [?]).

The analytic structure of X_S

Let us consider in detail the structure of the topological group X_S. Define

$$U_p = \{x \in \mathbb{Z}_p^\times \quad | \quad x \equiv 1 \pmod{p^\nu}\},$$

where $\nu = 1$ or $\nu = 2$ according as $p > 2$ or $p = 2$. Then we have the natural decomposition

$$X_S = X\left((\mathbb{Z}/p^\nu\mathbb{Z})^\times \times \prod_{q \neq p} \mathbb{Z}_q^\times\right) \times X(U_p). \tag{4.30}$$

The analytic dstructure on $X(U_p)$ is defined by the following isomorphism (which is equivalent to a special choice of a local parameter):

$$\varphi : X(U_p) \xrightarrow{\sim} T = \{z \in \mathbb{C}_p^\times \quad | \quad |z-1|_p < 1\},$$

where $\varphi(x) = x(1+p^\nu)$, $1+p^\nu$ being a topoplogical generator of the multiplicative group $U_p \cong \mathbb{Z}_p$. An arbitrary character $\chi \in X_S$ can be uniquely represented in the form $\chi = \chi_0\chi_1$ where χ_0 is trivial on the component U_p, and χ_1 is trivial on the other component

$$(\mathbb{Z}/p^\nu\mathbb{Z})^\times \times \prod_{q \neq p} \mathbb{Z}_q^\times.$$

The character χ_0 is called the *tame component*, and χ_1 the *wild component* of the character χ. We denote by the symbol $\chi_{(t)}$ the (wild) character which is uniquely determined by the condition

$$\chi_{(t)}(1+p^\nu) = t$$

with $t \in \mathbb{C}_p$, $|t|_p < 1$.
In some cases it is convenient to use another local coordinate s which is analogous to the classical argument s of the Dirichlet series:

$$\begin{array}{rcl} \mathrm{O}_p & \longrightarrow & X_S \\ s & \longmapsto & \chi^{(s)}, \end{array}$$

where $\chi^{(s)}$ is given by $\chi^{(s)}((1+p^\nu)^\alpha) = (1+p^\nu)^{\alpha s} = \exp(\alpha s \log(1+p^\nu))$. The character $\chi^{(s)}$ is defined only for such s for which the series exp is p-adically convergent (i.e. for $|s|_p < p^{\nu - 1/(p-1)}$). In this domain of values of the argument we have that $t = (1+p^\nu)^s - 1$. But, for example, for $(1+t)^{p^n} = 1$ there is certainly no such value of s (because $t \neq 1$), so that the s-coordonate parametrizes a smaller neighborhood of the trivial character than the t-coordinate (which parametrizes all wild characters) (see [?], [?]).

p-adic analytic functions on X_S

Recall that an analytic function $F : T \longrightarrow \mathbb{C}_p$ ($T = \{z \in \mathbb{C}_p^\times \quad | \quad |z-1|_p < 1\}$), is defined as the sum of a series of the type $\sum_{i \geq 0} a_i (t-1)^i$ ($a_i \in \mathbb{C}_p$), which is assumed to be absolutely convergent for all $t \in T$. The notion of an analytic function is then obviously extended to the whole group X_S by shifts. The function

$$F(t) = \sum_{i=0}^{\infty} a_i (t-1)^i$$

is bounded on T iff all its coefficients a_i are universally bounded. This last fact can be easily deduced for example from the basic properties of the Newton polygon of the series $F(t)$ (see [?], [?]). If we apply to these series the Weierstrass preparation theorem (see [?], [?]), we see that in this case the function F has only a finite number of zeroes on T (if it is not identically zero).

In particular, consider the torsion subgroup $X_S^{\mathrm{tors}} \subset X_S$. This subgroup is discrete in X_S and its elements $\chi \in X_S^{\mathrm{tors}}$ can be obviously identified with primitive Dirichlet characters $\chi \mod M$ such that the support $S(\chi) = S(M)$ of the conductor of χ is containded in S. This identification is provided by a fixed embedding denoted

$$i_p : \overline{\mathbb{Q}}^\times \hookrightarrow \mathbb{C}_p^\times$$

if we note that each character $\chi \in X_S^{\mathrm{tors}}$ can be factored through some finite factor group $(\mathbb{Z}/M\mathbb{Z})^\times$:

$$\chi : \mathbb{Z}_S^\times \to (\mathbb{Z}/M\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times \overset{i_p}{\hookrightarrow} \mathbb{C}_p^\times,$$

and the smallest number M with the above condition is the conductor of $\chi \in X_S^{\mathrm{tors}}$.
The symbol x_p will denote the composition of the natural projection $\mathbb{Z}_S^\times \to \mathbb{Z}_p^\times$ and of the natural embedding $\mathbb{Z}_p^\times \to \mathbb{C}_p^\times$, so that $x_p \in X_S$ and all integers k can be considered as the characters $x_p^k : y \longmapsto y^k$.

Let us consider a bounded $\mathbb{C}_p$-analytic function F on X_S. The above statement about zeroes of bounded $\mathbb{C}_p$-analytic functions implies now that the function F is uniquely determined by its values $F(\chi_0\chi)$, where χ_0 is a fixed character and χ runs through all elements $\chi \in X_S^{\mathrm{tors}}$ with possible exclusion of a finite number of characters in each analyticity component of the decomposition (**??**). This condition is satisfied, for example, by the set of characters $\chi \in X_S^{\mathrm{tors}}$ with the S-complete conductor (i.e. such that $S(\chi) = S$), and even for a smaller set of characters, for example for the set obtained by imposing the additional assumption that the character χ^2 is not trivial (see [**?**], [**?**], [**?**]).

p-adic Mellin transform

Let μ be a (bounded) $\mathbb{C}_p$-valued measure on $\mathbb{Z}_S^\times$. Then the *non-Archimedean Mellin transform* of the measure μ is defined by

$$L_\mu(x) = \mu(x) = \int_{\mathbb{Z}_S^\times} x \mathrm{d}\mu, \qquad (x \in X_S), \tag{4.31}$$

which represents a bounded $\mathbb{C}_p$-analytic function

$$L_\mu : X_S \longrightarrow \mathbb{C}_p. \tag{4.32}$$

Indeed, the boundedness of the function L_μ is obvious since all characters $x \in X_S$ take values in O_p and μ also is bounded. The analyticity of this function expresses a general property of the integral (**??**), namely that it depends analytically on the parameter $x \in X_S$. However, we give below a pure algebraic proof of this fact which is based on a description of the Iwasawa algebra. This description will also imply that every bounded $\mathbb{C}_p$-analytic function on X_S is the Mellin transform of a certain measure μ.

The Iwasawa algebra

Let O be a closed subring in $\mathrm{O}_p = \{z \in \mathbb{C}_p \quad | \quad |z|_p \leq 1\}$,

$$G = \varprojlim_i G_i, \qquad (i \in I),$$

a profinite group. Then the canonical homomorphism $G_i \xleftarrow{\pi_{ij}} G_j$ induces a homomorphism of the corresponding group rings

$$\mathrm{O}[G_i] \longleftarrow \mathrm{O}[G_j].$$

Then the *completed group ring* $\mathrm{O}[[G]]$ is defined as the projective limit

$$\mathrm{O}[[G]] = \varprojlim_i \mathrm{O}[[G_i]], \qquad (i \in I).$$

Let us consider also the set $\mathrm{Dist}(G, \mathrm{O})$ of all O-valued distributions on G which itself is an O-module and a ring with respect to multiplication given by the *convolution of distributions*, which is defined in terms of families of functions

$$\mu_1^{(i)}, \mu_2^{(i)} : G_i \longrightarrow \mathrm{O},$$

(see the previous section) as follows:

We noticed above that the theorem ?? would imply a description of $\mathbb{C}_p$-analytic bounded functions on X_S in terms of measures. Indeed, these functions are defined on analyticity components of the decomposition (??) as certain power series with p-adically bounded coefficients, that is, power series, whose coefficients belong to O_p after multiplication by some constant from $\mathbb{C}_p^\times$. Formulas for coefficients of these series can be also deduced from the proof of the theorem. However, we give a more direct computation of these coefficients in terms of the corresponding measures. Let us consider the component aU_p of the set $\mathbb{Z}_S^\times$ where

$$a \in (\mathbb{Z}/p^\nu\mathbb{Z})^\times \times \prod_{q\neq} \mathbb{Z}_q^\times,$$

and let $\mu_a(x) = \mu(ax)$ be the corresponding measure on U_p defined by restriction of μ to the subset $aU_p \subset \mathbb{Z}_S^\times$.

Consider the isomorphism $U_p \cong \mathbb{Z}_p$ given by:

$$y = \gamma^x \quad (x \in \mathbb{Z}_p, y \in U_p),$$

with some choice of the generator γ of U_p (for example, we can take $\gamma = 1 + p^\nu$). Let μ'_a be the corresponding measure on $\mathbb{Z}_p$. Then this measure is uniquely determined by values of the integrals

$$\int_{\mathbb{Z}_p} \binom{x}{i} d\mu'_a(x) = a_i, \tag{4.36}$$

with the interpolation polynomials $\binom{x}{i}$, since the $\mathbb{C}_p$-span of the family

$$\left\{ \binom{x}{i} \right\} \quad (i \in \mathbb{Z}, i \geq 0)$$

is dense in $\mathcal{C}(\mathbb{Z}_p, \mathrm{O}_p)$ according to Mahler's interpolation theorem for continuous functions on $\mathbb{Z}_p$). Indeed, from the basic properties of the interpolation polynomials it follows that

$$\sum_i b_i \binom{x}{i} \equiv 0 \pmod{p^n} \quad (\text{for all } x \in \mathbb{Z}_p) \Longrightarrow b_i \equiv 0 \pmod{p^n}.$$

We can now apply the abstract Kummer congruences (see proposition **??**), which imply that for arbitrary choice of numbers $a_i \in \mathrm{O}_p$ there exists a measure with the property (**??**).

Coefficients of power series and the Iwasawa isomorphism

We state that the Mellin transform L_{μ_a} of the measure μ_a is given by the power series $F_a(t)$ with coefficients as in (??), that is

$$\int_{U_p} \chi_{(t)}(y)\mathrm{d}\mu(ay) = \sum_{i=0}^{\infty} \left(\int_{\mathbb{Z}_p} \binom{x}{i} \mathrm{d}\mu'_a(x) \right) (t-1)^i \qquad (4.37)$$

for all wild characters of the form $\chi_{(t)}$, $\chi_{(t)}(\gamma) = t$, $|t-1|_p < 1$. It suffices to show that (??) is valid for all characters of the type $y \longmapsto y^m$, where m is a positive integer. In order to do this we use the binomial expansion

$$\gamma^{mx} = (1 + (\gamma^m - 1))^x = \sum_{i=0}^{\infty} \binom{x}{i} (\gamma^m - 1)^i,$$

which implies that

$$\int_{u_p} y^m \mathrm{d}\mu(ay) = \int_{\mathbb{Z}_p} \gamma^{mx} \mathrm{d}\mu'_a(x) = \sum_{i=0}^{\infty} \left(\int_{\mathbb{Z}_p} \binom{x}{i} \mathrm{d}\mu'_a(x) \right) (\gamma^m - 1)^i,$$

establishing (??).

Example: Mazur's measure and the non-Archimedean Kubota-Leopoldt zeta function

Let us first consider a positive integer $c \in \mathbb{Z}_S^\times \cap \mathbb{Z}$, $c > 1$ coprime to all primes in S. Then for each complex number $s \in \mathbb{C}$ there exists a complex distribution μ_s^c on $G_S = \mathbb{Z}_S^\times$ which is uniquely determined by the following condition

$$\mu_s^c(\chi) = (1 - \chi^{-1}(c)c^{-1-s})L_{M_0}(-s, \chi), \tag{4.38}$$

where $M_0 = \prod_{q \in S} q$. Moreover, the right hand side of (**??**) is holomorphic for all $s \in \mathbb{C}$ including $s = -1$. If s is an integer and $s \geq 0$ then according to criterion of proposition **??** the right hand side of (**??**) belongs to the field

$$\mathbb{Q}(\chi) \subset \mathbb{Q}^{\mathrm{ab}} \subset \overline{\mathbb{Q}}$$

generated by values of the character χ.

Thus we get a distribution with values in $\mathbb{Q}^{\mathrm{ab}}$. If we now apply to (??) the fixed embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ we get a $\mathbb{C}_p$-valued distribution $\mu^{(c)} = i_p(\mu_0^c)$ which turns out to be an O_p-measure in view of proposition ??, and the following equality holds

$$\mu^{(c)}(\chi x_p^r) = i_p(\mu_r^c(\chi)).$$

This identity relates the special values of the Dirichlet L-functions at different non-positive points. The function

$$L(x) = \left(1 - c^{-1}x(c)^{-1}\right)^{-1} L_{\mu^{(c)}}(x) \quad (x \in X_S) \tag{4.39}$$

is well defined and it is holomorphic on X_S with the exception of a simple pole at the point $x = x_p \in X_S$. This function is called the *non-Archimedean zeta-function of Kubota-Leopoldt*. The corresponding measure $\mu^{(c)}$ will be called the *S-adic Mazur measure*.

Lecture N°4. Method of canonical projection of modular distributions.

1. Modular forms, L-functions and congruences between modular forms
2. A traditional method of p-adic interpolation and the method of canonical projection of modular distributions
3. The use of the Eisenstein series and of the Rankin-Selberg method The Eisenstein measure by N.M.Katz, ... Convolutions of Eisenstein distributions with other distributions
4. Examples of construction of p-adic L-functions
5. Families of modular forms and L-functions.

Modular forms as a tool in arithmetic

We view modular forms as:

1) q-power series

$f = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{C}[[q]]$ and as

2) holomorphic functions

on the upper half plane

$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\ z > 0\}$

where $q = \exp(2\pi i z)$,

$z \in \mathbb{H}$, and define

L-function

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

for a Dirichlet character

$\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ (its Mellin transform)

A famous example: the Ramanujan function $\tau(n)$

The function Δ (of the variable z) is defined by the formal expansion

$\Delta = \sum_{n=1}^{\infty} \tau(n) q^n$

$= q \prod_{m=1}^{\infty} (1 - q^m)^{24}$

$= q - 24q^2 + 252q^3 + \cdots$

is a cusp form of weight $k = 12$ for the group $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

$\tau(1) = 1, \tau(2) = -24,$

$\tau(3) = 252, \tau(4) = -1472$

$\tau(m)\tau(n) = \tau(mn)$

for $(n, m) = 1$,

$|\tau(p)| \leq 2p^{11/2}$

for all primes p .

Classical modular forms

are introduced as certain holomorphic functions on the upper half plane $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\ z > 0\}$, which can be regarded as a homogeneous space for the group $G(\mathbb{R}) = \mathrm{GL}_2(\mathbb{R})$:

$$\mathbb{H} = \mathrm{GL}_2(\mathbb{R})/\mathrm{O}(2) \cdot Z, \tag{4.40}$$

where $Z = \{\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \ | x \in \mathbb{R}^\times\}$ is the center of $G(\mathbb{R})$ and $\mathrm{O}(2)$ is the orthogonal group. The group $\mathrm{GL}_2^+(\mathbb{R})$ of matrices $\gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix}$ with positive determinant acts on $\mathbb{H}$ by fractional linear transformations; on cosets (**??**) this action transforms into the natural action by group shifts. Let Γ be a subgroup of finite index in the modular group $\mathrm{SL}_2(\mathbb{Z})$.

Definition of a modular form

A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called a modular form of (integral) weight k with respect to Γ iff the conditions a) and b) are satisfied:

- a) *Automorphy condition*

$$f((a_\gamma z + b_\gamma)/(c_\gamma z + d_\gamma)) = (c_\gamma z + d_\gamma)^k f(z) \qquad (4.41)$$

  for all elements $\gamma \in \Gamma$;
- b) *Regularity at cusps*: f is regular at cusps $z \in \mathbb{Q} \cup i\infty$ (the cusps can be viewed as fixed points of parabolic elements of Γ); this means that for each element $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ the function $(cz + d)^{-k} f\left(\frac{az+b}{cz+d}\right)$ admits a Fourier expansion over non–negative powers of $q^{1/N} = e(z/N)$ for a natural number N. One writes traditionally

$$q = e(z) = \exp(2\pi i z).$$

  A modular form

$$f(z) = \sum_{n=0}^{\infty} a(n) e(nz/N)$$

  is called a cusp form if f vanishes at all cusps (i.e. if the above Fourier expansion contains only positive powers of $q^{1/N}$), see [?], [?]

The complex vector space of all modular (resp. cusp) forms of weight k with respect to Γ is denoted by $\mathcal{M}_k(\Gamma)$ (resp. $\mathcal{S}_k(\Gamma)$).
A basic fact from the theory of modular forms is that the spaces of modular forms are finite dimensional. Also, one has $\mathcal{M}_k(\Gamma)\mathcal{M}_l(\Gamma) \subset \mathcal{M}_{k+l}(\Gamma)$. The direct sum

$$\mathcal{M}(\Gamma) = \bigoplus_{k=0}^{\infty} \mathcal{M}_k(\Gamma)$$

turns out to be a graded algebra over $\mathbb{C}$ with a finite number of generators.
An example of a modular form with respect to $\mathrm{SL}_2(\mathbb{Z})$ of weight $k \geq 4$ is given by the *Eisenstein series*

$$G_k(z) = \sum_{m_1,m_2\in\mathbb{Z}}{}' (m_1 + m_2 z)^{-k} \tag{4.42}$$

(prime denoting $(m_1, m_2) \neq (0, 0)$). For these series the automorphy condition (??) can be deduced straight from the definition. One has $G_k(z) \equiv 0$ for odd k and

$$G_k(z) = \frac{2(2\pi i)^k}{(k-1)!}\left[-\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n)e(nz)\right], \tag{4.43}$$

where $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$ and B_k is the k^{th} *Bernoulli number*.
The graded algebra $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$ is isomorphic to the polynomial ring of the (independent) variables G_4 and G_6.

Examples

Recall that B_k denote the Bernoullli numbers defined by the development

$$\frac{x}{e^x-1}=\sum_{k=0}^{\infty}B_k\frac{x^k}{k!}$$

(Numerical table:

$$B_0=1,\ B_1=-\frac{1}{2},\ B_2=\frac{1}{6},\ B_3=B_5=\cdots=0,\ B_4=-\frac{1}{30},\ B_6=\frac{1}{42},$$
$$B_8=-\frac{5}{66},\ B_{12}=\frac{691}{2730}\ B_{14}=-\frac{7}{6},\ B_{16}=\frac{3617}{510}\ B_{18}=-\frac{43867}{798}\ ,\dots).$$

One has

$$\zeta(k)=-\frac{(2\pi i)^k}{2}\ ,G_k(z)=\frac{(2\pi i)^k}{(k-1)!}\left[-\frac{B_k}{2k}+\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\right].$$

$$E_4(z)=1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n\in\mathcal{M}_4(\mathrm{SL}(2,\mathbb{Z})),$$
$$E_6(z)=1-504\sum_{n=1}^{\infty}\sigma_5(n)q^n\in\mathcal{M}_6(\mathrm{SL}(2,\mathbb{Z})),$$
$$E_8(z)=1+480\sum_{n=1}^{\infty}\sigma_7(n)q^n\in\mathcal{M}_8(\mathrm{SL}(2,\mathbb{Z})),$$
$$E_{10}(z)=1-264\sum_{n=1}^{\infty}\sigma_9(n)q^n\in\mathcal{M}_{10}(\mathrm{SL}(2,\mathbb{Z})),$$
$$E_{12}(z)=1+\frac{65520}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)q^n\in\mathcal{M}_{12}(\mathrm{SL}(2,\mathbb{Z})),$$
$$E_{14}(z)=1-24\sum_{n=1}^{\infty}\sigma_{13}(n)q^n\in\mathcal{M}_{14}(\mathrm{SL}(2,\mathbb{Z})).$$

Proof see in [?].

Fast computation of the Ramanujan function:

Put $h_k := \sum_{n=1}^{\infty} \sum_{d|n} d^{k-1} q^n = \sum_{d=1}^{\infty} \frac{d^{k-1} q^d}{1-q^d}$. The classical fact is that $\Delta = (E_4^3 - E_6^2)/1728$ where $E_4 = 1 + 240 h_4$ and $E_6 = 1 - 504 h_6$.

Computing with PARI-GP see [?], The PARI/GP number theory system), `http://pari.math.u-bordeaux.fr`

$$h_k := \sum_{n=1}^{\infty} \sum_{d|n} d^{k-1} q^n = \sum_{d=1}^{\infty} \frac{d^{k-1} q^d}{1-q^d} \Longrightarrow$$

```
gp > h6=sum(d=1,20,d^5*q^d/(1-q^d)+O(q^20))
gp > h4=sum(d=1,20,d^3*q^d/(1-q^d)+O(q^20)
gp > Delta=((1+240*h4)^3-(1-504*h6)^2)/1728

q - 24*q^2 + 252*q^3 - 1472*q^4 + 4830*q^5 - 6048*q^6 - 16744*q^7
+ 84480*q^8 - 113643*q^9 - 115920*q^10 + 534612*q^11
- 370944*q^12 - 577738*q^13 + 401856*q^14 + 1217160*q^15
+ 987136*q^16 - 6905934*q^17+ 2727432*q^18 + 10661420*q^19
 + O(q^20)
```

Congruence of Ramanujan

$\tau(n) \equiv \sum_{d|n} d^{11} \mod 691$:

```
gp > (Delta-h12)/691
%10 = -3*q^2 - 256*q^3 - 6075*q^4 - 70656*q^5 - 525300*q^6
 - 2861568*q^7 - 12437115*q^8 - 45414400*q^9
 - 144788634*q^10 - 412896000*q^11 - 1075797268*q^12
 - 2593575936*q^13 - 5863302600*q^14 - 12517805568*q^15
 - 25471460475*q^16 - 49597544448*q^17
 - 93053764671*q^18 - 168582124800*q^19 + O(q^20)
```

More programs of computing $\tau(n)$ (see [?])

```
 PROGRAM

(MAGMA) M12:=ModularForms(Gamma0(1), 12); t1:=Basis(M12)[2];
PowerSeries(t1[1], 100); Coefficients($1);

(PARI) a(n)=if(n<1, 0, polcoeff(x*eta(x+x*O(x^n))^24, n))

(PARI) {tau(n)=if(n<1, 0, polcoeff(x*(sum(i=1, (sqrtint(8*n-7)+1)\2,
(-1)^i*(2*i-1)*x^((i^2-i)/2), O(x^n)))^8, n));}
gp > tau(6911)
%3 = -615012709514736031488
gp > ##
  ***   last result computed in 3,735 ms.
```

Bibliography


Andrianov, A.N., *Quadratic Forms and Hecke Operators*, Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, 1987.


Batut, C., Belabas, D., Bernardi, H., Cohen, H., Olivier, M.: The PARI/GP number theory system. `http://pari.math.u-bordeaux.fr`


Borevich, Z.I., Shafarevich, I.R. (1985): Number Theory. (in Russian). 3rd ed. Nauka, Moscow (1985). English transl.: New York/London: Academic Press, 1966.


Böcherer, S., Panchishkin, A.A., *Admissible p-adic measures attached to triple products of elliptic cusp forms*, Extra volume : John H.Coates' Sixtieth Birthday (2006), 77-132.


Chandrasekharan, K. Arithmetical functions. Berlin–Heidelberg–New York, Springer–Verlag (1970).


Coates, J. *On p–adic L–functions.* Sem. Bourbaki, 40eme annee, 1987-88, n° 701, Asterisque (1989) 177–178.

- Coates, J. and Perrin-Riou, B., *On p-adic L-functions attached to motives over* $\mathbb{Q}$, Advanced Studies in Pure Math. 17, 23–54 (1989)
- H.Cohen, *Sums Involving the Values at Negative Integers of L-Functions of Quadratic Characters*, Math. Ann. 217 (1975), p. 271-285.
- R. Coleman, *p-adic Banach spaces and families of modular forms*. Invent. Math. 127, N°3, 417-479 (1997)
- R. Coleman, B. Mazur, *The eigencurve. Galois representations in arithmetic algebraic geometry* (Durham, 1996), 1–113, London Math. Soc. Lecture Note Ser., 254,
- R. Coleman, G. Stevens, J. Teitelbaum, *Numerical experiments on families of p-adic modular forms*, in: Computational perspectives in Number Theory, ed. by D.A. Buell, J.T. Teitelbaum, Amer. Math. Soc., 143-158 (1998).

P.Colmez, *Fonctions L p-adiques*, Séminaire Bourbaki, 51 ème année, 1998–99, N°851. Novembre 1998. Cambridge Univ. Press, Cambridge, 1998.

Courtieu,M., Panchishkin ,A.A., *Non-Archimedean L-Functions and Arithmetical Siegel Modular Forms*, Lecture Notes in Mathematics 1471, Springer-Verlag, 2004 (2nd augmented ed.)

Deligne P., *Valeurs de fonctions L et périodes d'intégrales,* Proc.Sympos.Pure Math. vol. 55. Amer. Math. Soc., Providence, RI, 1979 , 313-346.

G. Faltings, Ching-Li Chai, *Degeneration of abelian varieties.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, 22. Berlin etc.: Springer-Verlag. xii, 316 p. (1990).

F.Gouvêa, B.Mazur, *On the density of modular representations*, in: Computational perspectives in Number Theory, ed. by D.A. Buell, J.T. Teitelbaum, Amer. Math. Soc., 127–142 (1998).

- Khoai Ha Huy, *p-adic interpolation and the Mellin-Mazur transform* , Acta Math. Viet. 5, 77-99 (1980).
- M. Harris, *The Rationality of Holomorphic Eisenstein Series*, Invent. Math. 63, 305-310 (1981).
- M. Harris, *Special Values of Zeta-Functions attached to Siegel Modular Forms*, Ann. Sci. Ec. Norm. Sup. 14, 77-120 (1981).
- M. Harris, *Eisenstein Series on Shimura Varieties*, Ann. of Math. 119 (1984), p. 59-94.
- Harris, M., Li, Jian-Shu., Skinner, Ch.M., *p-adic L-functions for unitary Shimura varieties.* Preprint, 2006.
- E. Hecke, *Theorie der Eisensteinscher Reihen und ihre Anwebdung auf Fonktionnentheorie und Arithmetik*, Abh. Math. Sem. Hamburg 5 (1927), p. 199-224.
- H. Hida, *Congruence of cusp forms and special values of their zeta functions.* Invent. Math. 63 (1981), no. 2, 225–261.

 H. Hida, *A p-Adic Measure attached to the Zeta Functions associated with two Elliptic Cusp Forms. I*, Invent. Math. 79 (1985), p 159-195.

 H. Hida, *Galois representations into $GL_2(\mathbb{Z}_p[\![X]\!])$ attached to ordinary cusp forms*, Invent. Math. 85 (1986) 545–613.

 H. Hida, *Le produit de Petersson et de Rankin p-adique*, Séminaire de Théorie des Nombres, Paris 1988–1989, 87–102, Progr. Math., 91, Birkhäuser Boston, Boston, MA, 1990.

 H. Hida, *On p-adic L-functions of $GL(2) \times GL(2)$ over totally real fields*, Ann. Inst. Fourier, (Grenoble) 40, no.2 (1991) 311–391.

 H. Hida, *Elementary theory of L-functions and Eisenstein series*, London Mathematical Society Student Texts. 26 Cambridge University Press

 H. Hida, *p-adic automorphic forms on Shimura varieties.* Springer Monographs in Mathematics. Springer-Verlag, New York, 2004. xii+390 pp.


Hulsbergen, W.W.J.: Conjectures in Arithmetic Algebraic Geometry. A Survey. Second revised ed., AMS, 1994


K. Iwasawa, *Lectures on p-Adic L-Functions*, Ann. of Math. Studies, N° 74. Princeton Univ. Press (1972).


N.M. Katz, *p-Adic L-Functions for CM-Fields*, Invent. Math. 48 (1978), p 199-297.


D. Kazhdan, B. Mazur, C.-G. Schmidt, *Relative modular symbols and Rankin-Selberg convolutions*. J. Reine Angew. Math. 519, 97-141 (2000).


Koblitz, N. (1980): $p-$adic analysis: a short course on recent work. London Math. Soc. Lecture Note Ser., London: Cambridge Univ. Press (1980).


Neal Koblitz, *A course of number theory and cryptography*, Graduate texts in mathematics 114, New York: Springer Verlag, 1987.


A. W. Knapp, *Elliptic curves*, Math. notes, v.40 Princeton University Press, Princeton, 1993


T. Kubota, H.W. Leopoldt, *Eine p-Adische Theorie der Zetawerte*, J. Reine Angew. Math. 214/215 (1964), p 328-339.


Lang S. (1976): Introduction to Modular Forms. New York - Berlin - Heidelberg: Springer–Verlag, 1976.


Manin, Yu.I. (1971): Cyclotomic fields and modular curves. (in Russian). Uspekhi, **26**, no.6 (1971), 7-78. English transl.: Russ.Math.Surv. **26**, No.6 (1972), 7-78.


Yu.I. Manin, *Periods of cusp forms and p-adic Hecke series*, Mat. Sbornik, 92 , 1973, pp. 378-401


Y.I. Manin, *Non-Archimedean Integration and p-Adic L-Functions of Jacquet-Langlands*, Uspekhi Mat. Nauk 31 (1976), p 5-54 (in Russian).


Yu.I. Manin, M. M.Vishik, *p-adic Hecke series of imaginary quadratic fields*, (Russian) Mat. Sb. (N.S.) 95(137) (1974), 357-383.


Manin, Yu. I., *Selected papers of Yu. I. Manin*, World Scientific Series in 20th Century Mathematics, 3. World Scientific Publishing Co., Inc., River Edge, NJ, 1996. xii+600 pp.


Manin, Yu.I. and Panchishkin, A.A., *Introduction to Modern Number Theory*, Encyclopaedia of Mathematical Sciences, vol. 49 (2nd ed.), Springer-Verlag, 2005, 514 p.


Toshitsune Miyake, *Modular forms. Transl. from the Japanese by Yoshitaka Maeda.*, Berlin etc.: Springer-Verlag. viii, 335 p. (1989).


Mazur, B. (1986): Arithmetic on curves. Bull. AMS, **14**, No.2, 207-259 (1986)


Mazur, B., Swinnerton–Dyer, H.P.F. (1974): Arithmetic of Weil curves. Inv. Math., **25**, 1-61 (1974).


B. Mazur; J. Tate; J. Teitelbaum: On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. Invent. Math. 84, 1-48 (1986).


A.A. Panchishkin, *Admissible Non-Archimedean Standard Zeta Functions of Siegel Modular Forms*, Proceedings of the joint AMS Summer Conference on Motives, Seatle, July 20 - August 2 1991, Seatle, Providence, R.I. vol. 2 (1994), p 251-292.


A.A. Panchishkin, *On the Siegel-Eisenstein measure and its applications*, Israel Journal of Mathemetics, 120, Part B (2000) 467-509.


A.A. Panchishkin, *On p-adic integration in spaces of modular forms and its applications*, J. Math. Sci., New York 115, No.3, 2357-2377 (2003).


A.A.Panchishkin, *A new method of constructing p-adic L-functions associated with modular forms*, Moscow Mathematical Journal, 2 (2002), Number 2, 1-16


A.A.Panchishkin, *Two variable p-adic L functions attached to eigenfamilies of positive slope*, Invent. Math. v. 154, N3 (2003), pp. 551 - 615


A.A. Panchishkin, *p-adic Banach modules of arithmetical modular forms and triple products of Coleman's families*, (for a special volume of Quarterly Journal of Pure and Applied Mathematics dedicated to Jean-Pierre Serre), 2006.


J.– P. Serre, *Cours d'arithmétique*. Paris: Presses Univ. France, 1970.


J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972) 191–268, Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973.


Shimura, G., *On modular correspondences for Sp(n, Z) and their congruence relations*, Proc. Nat. Acad. Sci. U.S.A. 49 (1963), 824-828.


Shimura G., *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press, 1971.


G. Shimura, *Arithmeticity in the theory of automorphic forms*, Mathematical Surveys and Monographs. 82. Providence, RI: American Mathematical Society (AMS). x, 302 p. (2000)


Silverman J.H. , *The Arithmetic of Elliptic Curves.* Berlin–Heidelberg–New York: Springer–Verlag, 1986.


Neil J. A. Sloane: Home Page The On-Line Encyclopedia of Integer. Contains 131774 sequences [Thu Aug 23 15:09:40 EDT 2007] `http://www.research.att.com/ njas/sequences/A000594`


S. A. Stepanov, *Arithmetic of algebraic curves*. Monographs in Contemporary Mathematics, New–York and London: Consultants Bureau, 1994


G. Stevens, *Overconvergent modular symbols and a conjecture of Mazur, Tate and Teitelbaum.* Unpublished notes


J. Sturm, *Special Values of Zeta Functions and Eisenstein Series of half integral weight*, Amer. J. Math. **102**, 219-240 (1980).


Tate, J., The Arithmetic of Elliptic Curves. Inv. Math., 23, 179-206 (1974)

Tilouine, J. and Urban, E., *Several variable p-adic families of Siegel-Hilbert cusp eigenforms and their Galois representations*, Ann. scient. Éc. Norm. Sup. 4^{e} série, 32 (1999) 499–574.

M.M. Višik, *Non-Archimedean Measures associated with Dirichlet series*, Mat. Sbornik 99 (1976), p 248-260.

Washington L.C. (1982): Introduction to Cyclotomic Fields. New York–Berlin–Heidelberg: Springer–Verlag, 1982.

A.Weil, *On a certain type of characters of the idèle-class group of an algebraic number-field*, Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955, pp. 1–7, Science Council of Japan, Tokyo, 1956.

Weil A. (1974a): Basic Number Theory. 3rd ed. Berlin–Heidelberg–New York: Springer–Verlag, 1974.

A.Wiles, *Modular elliptic curves and Fermat's Last Theorem.* Ann. Math., II. Ser. 141, No.3, 443-551 (1995)


Yoshida, H., *Siegel's Modular Forms and the Arithmetic of Quadratic Forms*, Inventiones math. 60, 193–248 (1980)


Yoshida, H., *Motives and Siegel modular forms*, American Journal of Mathematics, 123 (2001), 1171–1197.


D.B. Zagier, *Modular Forms whose Fourier Coefficients involve Zeta-Functions of Quadratic Fields*, In : Modular Functions. V, Springer-Verlag, Lect. Notes in Math. N° 627 (1977), p 106-168.