The Abdus Salam
International Centre for Theoretical Physics

United Nations
Educational, Scientific and
Cultural Organization

IAEA
International Atomic Energy Agency

2056-2

Advanced School and Workshop on p-adic Analysis and Applications

31 August - 18 September, 2009

p-adic L-functions and modular forms

Alexei PANCHISHKIN
Institut Fourier
Universite' Grenoble-1
B.P. 74, 38402 St. Martin d'Heres
FRANCE

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 Septemer 18th, 2008 (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 $|\cdot|$, [BS85], [Kob80]. 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* [BS85], 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. 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 (2.2) is obtained if we

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

$$\frac{9}{7} = \cdots \overbrace{324120}\overbrace{324120}324122_{(5)}.$$

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 (2.2), where $|\alpha|_p = p^m$ for α as in (2.2) with $a_m \neq 0$ (see Koblitz N. (1980)).

It is curious to compare the expansions (2.2) 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 (2.2) are uniquely determined by α. This fact provides additional comfort when calculating with p–adic numbers.

Computation with PARI/GP (see [BBBCO])

```
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* (2.2). 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

$$|f(\alpha_0)/f'(\alpha_0)^2|_p < 1 \qquad (2.3)$$

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. [BS85], [Serre70]).
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 (2.3) is satisfied. The root α coincides then with the uniquely defined Teichmüller representative of α_0: $\alpha = \omega(\alpha_0)$.

4. Ω

So far we've been dealing only with algebraic extensions of $\mathbb{Q}_p$. But, as mentioned before, this is not yet enough to give us the p-adic analogy of the complex numbers.

Theorem 12. $\overline{\mathbb{Q}}_p$ *is not complete.*

PROOF. We must give an example of a Cauchy sentence $\{a_i\}$ in $\overline{\mathbb{Q}}_p$ such that there cannot exist a number $a \in \overline{\mathbb{Q}}_p$ which is the limit of the a_i.

Let b_i be a primitive $(p^{2^i} - 1)$th root of 1 in $\overline{\mathbb{Q}}_p$, i.e., $b_i^{p^{2^i}-1} = 1$, but $b_i^m \neq 1$ if $m < p^{2^i} - 1$. Note that $b_i^{p^{2^{i'}}-1} = 1$ if $i' > i$, because $2^i|2^{i'}$ implies $p^{2^i} - 1 \mid p^{2^{i'}} - 1$. (In fact, instead of 2^i we could replace the exponent of p by any increasing sequence whose ith term divides its $(i + 1)$th, e.g., 3^i, $i!$, etc.) Thus, if $i' > i$, b_i is a power of $b_{i'}$. Let

$$a_i = \sum_{j=0}^{i} b_j p^{N_j},$$

where $0 = N_0 < N_1 < N_2 < \cdots$ is an increasing sequence of nonnegative integers that will be chosen later. Note that the b_j, $j = 0, 1, \ldots, i$, are the digits in the p-adic expansion of a_i in the unramified extension $\mathbb{Q}_p(b_i)$, since the b_j are Teichmüller representatives. Clearly $\{a_i\}$ is Cauchy.

We now choose the N_j, $j > 0$, by induction. Suppose we have defined N_j for $j \leq i$, so that we have our $a_i = \sum_{j=0}^{i} b_j p^{N_j}$. Let $K = \mathbb{Q}_p(b_i)$. In §3 we proved that K is a Galois unramified extension of degree 2^i. First note that $\mathbb{Q}_p(a_i) = K$, because otherwise there would be an automorphism σ of K which leaves a_i fixed (see paragraph (11) in §1). But $\sigma(a_i)$ has p-adic expansion $\sum_{j=0}^{i} \sigma(b_j) p^{N_j}$, and $\sigma(b_i) \neq b_i$, so that $\sigma(a_i) \neq a_i$ because they have different p-adic expansions.

Next, by exercise 9 of §III.1, there exists $N_{i+1} > N_i$ such that a_i does not satisfy any congruence

$$\alpha_n a_i^n + \alpha_{n-1} a_i^{n-1} + \cdots + \alpha_1 a_i + \alpha_0 \equiv 0 \pmod{p^{N_{i+1}}}$$

for $n < 2^i$ and $\alpha_j \in \mathbb{Z}_p$ not all divisible by p.

This gives us our sequence $\{a_i\}$.

Suppose that $a \in \overline{\mathbb{Q}}_p$ were a limit of $\{a_i\}$. Then a satisfies an equation

$$\alpha_n a^n + \alpha_{n-1} a^{n-1} + \cdots + \alpha_1 a + \alpha_0 = 0,$$

where we may assume that all of the $\alpha_i \in \mathbb{Z}_p$ and not all are divisible by p. Choose i so that $2^i > n$. Since $a \equiv a_i \pmod{p^{N_{i+1}}}$, we have

$$\alpha_n a_i^n + \alpha_{n-1} a_i^{n-1} + \cdots + \alpha_1 a_i + \alpha_0 \equiv 0 \pmod{p^{N_{i+1}}},$$

a contradiction. This proves the theorem. □

Note that we have actually proved that $\mathbb{Q}_p^{\text{unram}}$, not only $\overline{\mathbb{Q}}_p = \mathbb{Q}_p^{\text{alg cl}}$, is not complete.

So we now want to "fill in the holes," and define a new field Ω to be the *completion* of $\overline{\mathbb{Q}}_p$. Strictly speaking, this means looking at equivalence classes of Cauchy sequences of elements in $\overline{\mathbb{Q}}_p$ and proceeding in exactly the same way as how $\mathbb{Q}_p$ was constructed from $\mathbb{Q}$ (or how $\mathbb{R}$ was constructed from $\mathbb{Q}$, or how a completion can be constructed for *any* metric space). Intuitively speaking, we're creating a new field Ω by throwing in all numbers which are convergent infinite sums of numbers in $\overline{\mathbb{Q}}_p$, for example, of the type considered in the proof of Theorem 12.

Just as in going from $\mathbb{Q}$ to $\mathbb{Q}_p$, in going from $\overline{\mathbb{Q}}_p$ to Ω we can extend the norm $|\ |_p$ on $\overline{\mathbb{Q}}_p$ to a norm on Ω be defining $|x|_p = \lim_{i\to\infty}|x_i|_p$, where $\{x_i\}$ is a Cauchy sequence of elements in $\overline{\mathbb{Q}}_p$ that is in the equivalence class of x (see §I.4). As in going from $\mathbb{Q}$ to $\mathbb{Q}_p$, it is easy to see that if $x \neq 0$ this limit $|x|_p$ is actually equal to $|x_i|_p$ for i sufficiently large.

We also extend ord_p to Ω:

$$\text{ord}_p\, x = -\log_p|x|_p.$$

Let $A = \{x \in \Omega \mid |x|_p \leq 1\}$ be the "valuation ring" of Ω, let $M = \{x \in \Omega \mid |x|_p < 1\}$ be its maximal ideal, and let $A^\times = \{x \in \Omega \mid |x|_p = 1\} = A - M$ be the set of invertible elements of A. Suppose that $x \in A^\times$, i.e., $|x|_p = 1$. Since $\overline{\mathbb{Q}}_p$ is dense in Ω, we can find an algebraic x' such that $x - x' \in M$, i.e., $|x - x'|_p < 1$. Since then $|x'|_p = 1$, it follows that x' is integral over $\mathbb{Z}_p$, i.e., it satisfies a monic polynomial with coefficients in $\mathbb{Z}_p$. Reducing that polynomial modulo p, we find that the coset $x + M = x' + M$ *is algebraic over* $\mathbb{F}_p$, i.e., lies in some $\mathbb{F}_{p^f}$. Now let $\omega(x)$ be the $(p^f - 1)$th root of 1 which is the Teichmüller representative of $x + M \in \mathbb{F}_{p^f}$, and set $\langle x \rangle = x/\omega(x)$. Then $\langle x \rangle \in 1 + M$. In other words, any $x \in A^\times$ is the product of a root of unity $\omega(x)$ and an element $\langle x \rangle$ which is in the open unit disc about 1. (If $x \in \mathbb{Z}_p$ has first digit a_0, this simply says that x is the product of the Teichmüller representative of a_0 and an element of $1 + p\mathbb{Z}_p$.) Finally, an arbitrary nonzero $x \in \Omega$ can be written as a fractional power of p times an element $x_1 \in \Omega$ of absolute value 1. Namely, if $\text{ord}_p\, x = r = a/b$ (see Exercise 1 below), then let p^r denote any root of $X^b - p^a = 0$. Then $x = p^r x_1 = p^r\omega(x_1)\langle x_1 \rangle$ for some x_1 of norm 1. In other words, *any nonzero element of* Ω *is a product of a fractional power of* p, *a root of unity, and an element in the open unit disc about* 1.

The next theorem tells us that we are done: Ω will serve as the p-adic analogue of the complex numbers.

Theorem 13. *Ω is algebraically closed.*

PROOF. Let: $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, $a_i \in \Omega$. We must show that $f(X)$ has a root in Ω. For each $i = 0, 1, \ldots, n - 1$, let $\{a_{ij}\}_j$ be a sequence of elements of $\bar{\mathbb{Q}}_p$ which converge to a_i. Let $g_j(X) = X^n + a_{n-1,j}X^{n-1} + \cdots + a_{1,j}X + a_{0,j}$. Let r_{ij} be the roots of $g_j(X)$ ($i = 1, 2, \ldots, n$). We claim that we can find i_j ($1 \le i_j \le n$) for $j = 1, 2, 3, \ldots$ such that the sequence $\{r_{i_j,j}\}$ is Cauchy. Namely, suppose we have $r_{i_j,j}$ and we want to find $r_{i_{j+1},j+1}$. Let $\delta_j = |g_j - g_{j+1}|_p = \max_i(|a_{i,j} - a_{i,j+1}|_p)$ (which approaches 0 as $j \to \infty$). Let $A_j = \max(1, |r_{i_j,j}|_p{}^n)$. Clearly there is a uniform constant A such that $A_j \le A$ for all j (see Exercise 3 below). Then we have

$$\begin{aligned}\prod_i |r_{i_j,j} - r_{i,j+1}|_p &= |g_{j+1}(r_{i_j,j})|_p \\ &= |g_{j+1}(r_{i_j,j}) - g_j(r_{i_j,j})|_p \\ &\le \delta_j A.\end{aligned}$$

Hence at least one of the $|r_{i_j,j} - r_{i,j+1}|_p$ on the left is $\le \sqrt[n]{\delta_j A}$. Let $r_{i_{j+1},j+1}$ be any such $r_{i,j+1}$. Clearly this sequence of $r_{i_j,j}$ is Cauchy.

Now let $r = \lim_{j\to\infty} r_{i_j,j} \in \Omega$. Then $f(r) = \lim_{j\to\infty} f(r_{i_j,j}) = \lim_{j\to\infty} g_j(r_{i_j,j}) = 0$. □

Summarizing Chapters I and III, we can say that we have constructed Ω, which is the smallest field which contains $\mathbb{Q}$ and is both algebraically closed and complete with respect to $|\ |_p$. (Strictly speaking, this can be seen as follows: let Ω' be any such field; since Ω' is complete, it must contain a field isomorphic to the p-adic completion of $\mathbb{Q}$, which we can call $\mathbb{Q}_p$; then, since Ω' contains $\mathbb{Q}_p$ and is algebraically closed, it must contain a field isomorphic to the algebraic closure of $\mathbb{Q}_p$, which we can call $\bar{\mathbb{Q}}_p$; and, since Ω' contains $\bar{\mathbb{Q}}_p$ and is complete, it must contain a field isomorphic to the completion of $\bar{\mathbb{Q}}_p$, which we call Ω. Thus any field with these properties must contain a field isomorphic to Ω. The point is that both completion and algebraic closure are unique processes up to isomorphism.)

Actually, Ω should be denoted Ω_p, so as to remind us that everything we're doing depends on the prime number p we fixed at the start. But for brevity of notation we shall omit the subscript p.

The field Ω is a beautiful, gigantic realm, in which p-adic analysis lives.

Exercises

1. Prove that the possible values of $|\ |_p$ on $\bar{\mathbb{Q}}_p$ is the set of all rational powers of p (in the positive real numbers). What about on Ω? Recall that we let the ord_p function extend to Ω by defining $\text{ord}_p\, x = -\log_p |x|_p$ (i.e., the power $1/p$ is raised to get $|x|_p$). What is the set of all possible values of ord_p on Ω? Now prove that $\bar{\mathbb{Q}}_p$ and Ω are *not* locally compact. This is one striking difference with $\mathbb{C}$, which is locally compact under the Archimedean metric (the usual definition of distance on the complex plane).

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 [Kob80], [Wash82]).

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 [Hi91], [Wash82]):

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

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 (3.4) 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.

CHAPTER IV

p-adic power series

1. Elementary functions

Recall that in a metric space whose metric comes from a non-Archimedean norm $\| \ \|$, a sequence is Cauchy if and only if the difference between adjacent terms approaches zero; and if the metric space is complete, an infinite sum converges if and only if its general term approaches zero. So if we consider expressions of the form

$$f(X) = \sum_{n=0}^{\infty} a_n X^n, \qquad a_n \in \Omega,$$

we can give a value $\sum_{n=0}^{\infty} a_n x^n$ to $f(x)$ whenever an x is substituted for X for which $|a_n x^n|_p \to 0$.

Just as in the Archimedean case (power series over $\mathbb{R}$ or $\mathbb{C}$), we define the "radius of convergence"

$$r = \frac{1}{\limsup |a_n|_p^{1/n}},$$

where the terminology "$1/r = \limsup |a_n|_p^{1/n}$" means that $1/r$ is the *least* real number such that for *any* $C > 1/r$ there are only finitely many $|a_n|_p^{1/n}$ greater than C. Equivalently, $1/r$ is the greatest "point of accumulation," i.e., the greatest real number which can occur as the limit of a subsequence of $\{|a_n|_p^{1/n}\}$. If, for example, $\lim_{n\to\infty} |a_n|_p^{1/n}$ exists, then $1/r$ is simply this limit.

We justify the use of the term "radius of convergence" by showing that the series converges if $|x|_p < r$ and diverges if $|x|_p > r$. First, if $|x|_p < r$, then, letting $|x|_p = (1 - \varepsilon)r$, we have: $|a_n x^n|_p = (r|a_n|_p^{1/n})^n(1 - \varepsilon)^n$. Since there are only finitely many n for which $|a_n|_p^{1/n} > 1/(r - \frac{1}{2}\varepsilon r)$, we have

$$\lim_{n\to\infty} |a_n x^n|_p \leq \lim_{n\to\infty} \left(\frac{(1 - \varepsilon)r}{(1 - \frac{1}{2}\varepsilon)r}\right)^n = \lim_{n\to\infty} \left(\frac{1 - \varepsilon}{1 - \frac{1}{2}\varepsilon}\right)^n = 0.$$

Similarly, we easily see that if $|x|_p > r$, then $a_n x^n$ does not approach 0 as $n \to \infty$.

What if $|x|_p = r$? In the Archimedean case the story on the boundary of the interval or disc of convergence can be a little complicated. For example, $\log(1 + x) = \sum_{n=1}^{\infty} (-1)^{n+1} x^n/n$ has radius of convergence 1. When $|x| = 1$, it diverges for $x = -1$ and converges ("conditionally," not "absolutely") for other values of x (i.e., for $x = 1$ in the case of the reals and on the unit circle minus the point $x = -1$ in the case of the complexes).

But in the non-Archimedean case there's a single answer for all points $|x|_p = r$. This is because a series converges if and only if its terms approach zero, i.e., if and only if $|a_n|_p |x|_p^n \to 0$, and this depends only on the norm $|x|_p$ and not on the particular value of x with a given norm—there's no such thing as "conditional" convergence ($\sum \pm a_n$ converging or diverging depending on the choices of $\pm$'s).

If we take the same example $\sum_{n=1}^{\infty} (-1)^{n+1} X^n/n$, we find that $|a_n|_p = p^{\mathrm{ord}_p n}$, and $\lim_{n\to\infty} |a_n|_p^{1/n} = 1$. The series converges for $|x|_p < 1$ and diverges for $|x|_p > 1$. If $|x|_p = 1$, then $|a_n x^n|_p = p^{\mathrm{ord}_p n} \geq 1$, and the series diverges for all such x.

Now let's introduce some notation. If R is a ring, we let $R[[X]]$ be the ring of formal power series in X with coefficients in R, i.e., expressions $\sum_{n=0}^{\infty} a_n X^n$, $a_n \in R$, which add and multiply together in the usual way. For us, R will usually be $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_p$, $\mathbb{Q}_p$, or Ω. We often abbreviate other sets using this notation, for example,

$$1 + XR[[X]] \underset{\text{def}}{=} \{f \in R[[X]] \mid \text{constant term } a_0 \text{ of } f \text{ is } 1\}.$$

We define the "closed disc of radius $r \in \mathbb{R}$ about a point $a \in \Omega$" to be

$$D_a(r) \underset{\text{def}}{=} \{x \in \Omega \mid |x - a|_p \leq r\},$$

and we define the "open disc of radius r about a" to be

$$D_a(r^-) \underset{\text{def}}{=} \{x \in \Omega \mid |x - a|_p < r\}.$$

We let $D(r) \underset{\text{def}}{=} D_0(r)$ and $D(r^-) \underset{\text{def}}{=} D_0(r^-)$. (Note: whenever we refer to the closed disc $D(r)$ in Ω, we understand r to be a possible value of $| \ |_p$, i.e., a rational power of p; we always write $D(r^-)$ if there are no $x \in \Omega$ with $|x|_p = r$.)

(A word of caution. The terms "closed" and "open" are used only out of analogy with the Archimedean case. From a topological point of view the terminology is bad. Namely, the set $C_c = \{x \in \Omega \mid |x - a|_p = c\}$ is open in the topological sense, because every point $x \in C_c$ has a disc about it, for example $D_x(c^-)$, all points of which belong to C_c. But then any union of C_c's is open. Both $D_a(r)$ and $D_a(r^-)$, as well as their complements, are such unions: for example, $D_a(r^-) = \bigcup_{c<a} C_c$. Hence both $D_a(r)$ and $D_a(r^-)$ are simultaneously *open and closed* sets. The term for this peculiar state of affairs in Ω is "totally disconnected topological space.")

Just to get used to the notation, we prove a trivial lemma.

Lemma 1. *Every* $f(X) \in \mathbb{Z}_p[[X]]$ *converges in* $D(1^-)$.

PROOF. Let $f(X) = \sum_{n=0}^{\infty} a_n X^n$, $a_n \in \mathbb{Z}_p$, and let $x \in D(1^-)$. Thus, $|x|_p < 1$. Also $|a_n|_p \leq 1$ for all n. Hence $|a_n x^n|_p \leq |x|_p{}^n \to 0$ as $n \to \infty$. □

Another easy lemma is

Lemma 2. *Every* $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \Omega[[X]]$ *which converges in an (open or closed) disc* $D = D(r)$ *or* $D(r^-)$ *is continuous on* D.

PROOF. Suppose $|x' - x|_p < \delta$, where $\delta < |x|_p$ will be chosen later. Then $|x'|_p = |x|_p$. (We are assuming $x \neq 0$; the case $x = 0$ is very easy to check separately.) We have

$$\begin{aligned} |f(x) - f(x')|_p &= \left| \sum_{n=0}^{\infty} (a_n x^n - a_n x'^n) \right|_p \\ &\leq \max_n |a_n x^n - a_n x'^n|_p \\ &= \max_n (|a_n|_p |(x - x')(x^{n-1} + x^{n-2}x' + \cdots \\ &\qquad\qquad + xx'^{n-2} + x'^{n-1}|_p). \end{aligned}$$

But $|x^{n-1} + x^{n-2}x' + \cdots + xx'^{n-2} + x'^{n-1}|_p \leq \max_{1 \leq i \leq n} |x^{n-i} x'^{i-1}|_p = |x|_p^{n-1}$. Hence

$$\begin{aligned} |f(x) - f(x')|_p &\leq \max_n (|x - x'|_p |a_n|_p |x|_p^{n-1}) \\ &< \frac{\delta}{|x|_p} \max_n (|a_n|_p |x|_p{}^n). \end{aligned}$$

Since $|a_n|_p |x|_p{}^n$ is bounded as $n \to \infty$, this $|f(x) - f(x')|_p$ is $< \varepsilon$ for suitable δ. □

Now let's return to our series $\sum_{n=1}^{\infty} (-1)^{n+1} X^n/n$, which, as we've seen, has disc of convergence $D(1^-)$. That is, this series gives a function on $D(1^-)$ taking values in Ω. Let's call this function $\log_p(1 + X)$, where the subscript p reminds us of the prime which gave us the norm on $\mathbb{Q}$ used to get Ω, and also remind us not to confuse this function with the classical $\log(1 + X)$ function—which has a different domain (a subset of $\mathbb{R}$ or $\mathbb{C}$) and range ($\mathbb{R}$ or $\mathbb{C}$). Unfortunately, the notation $\log_p$ for the "p-adic logarithm" is identical to classical notation for "log to the base p." From now on, we shall assume that $\log_p$ means p-adic logarithm

$$\log_p(1 + X): D(1^-) \to \Omega, \qquad \log_p(1 + x) = \sum_{n=1}^{\infty} (-1)^{n+1} x^n/n,$$

unless *explicitly* stated otherwise.

The dangers of confusing Archimedean and p-adic functions will be illustrated below, and also in Exercises 8–10 at the end of §1.

Anyone who has studied differential equations (and many who haven't) realize that $\exp(x) = e^x = \sum_{n=0}^{\infty} x^n/n!$ is about the most important function there is in classical mathematics. So let's look at the series $\sum_{n=0}^{\infty} X^n/n!$ p-adically. The classical exponential series converges everywhere, thanks to the $n!$ in the denominator. But while big denominators are good things to have classically, they are not so good p-adically. Namely, it's not hard to compute (see Exercise 14 §I.2)

$$\mathrm{ord}_p(n!) = \frac{n - S_n}{p - 1} \quad (S_n = \text{sum of digits in } n \text{ to base } p);$$

$$|1/n!|_p = p^{(n-S_n)/(p-1)}.$$

Our formula for the radius of convergence $r = 1/(\limsup |a_n|_p^{1/n})$ gives us

$$\mathrm{ord}_p\, r = \liminf\left(\frac{1}{n}\,\mathrm{ord}_p\, a_n\right),$$

(where the "lim inf" of a sequence is its smallest point of accumulation). In the case $a_n = 1/n!$, this gives

$$\mathrm{ord}_p\, r = \liminf\left(-\frac{n - S_n}{n(p-1)}\right);$$

but $\lim_{n\to\infty}(-(n - S_n)/(n(p - 1))) = -1/(p - 1)$. Hence $\sum_{n=0}^{\infty} x^n/n!$ converges if $|x|_p < p^{-1/(p-1)}$ and diverges if $|x|_p > p^{-1/(p-1)}$. What if $|x|_p = p^{-1/(p-1)}$, i.e., $\mathrm{ord}_p\, x = 1/(p - 1)$? In that case

$$\mathrm{ord}_p(a_n x^n) = -\frac{n - S_n}{p - 1} + \frac{n}{p - 1} = \frac{S_n}{p - 1}.$$

If, say, we choose $n = p^m$ to be a power of p, so that $S_n = 1$, we have: $\mathrm{ord}_p(a_{p^m} x^{p^m}) = 1/(p - 1)$, $|a_{p^m} x^{p^m}|_p = p^{-1/(p-1)}$, and hence $a_n x^n \not\to 0$ as $n \to \infty$. Thus, $\sum_{n=0}^{\infty} X^n/n!$ has disc of convergence $D(p^{-1/(p-1)-})$ (the $^-$ denoting the open disc, as usual). Let's denote $\exp_p(X) \underset{\text{def}}{=} \sum_{n=0}^{\infty} X^n/n! \in \mathbb{Q}_p[[X]]$.

Note that $D(p^{-1/(p-1)-}) \subset D(1^-)$, so that $\exp_p$ converges in a *smaller* disc than $\log_p$!

While it is important to avoid confusion between log and exp and $\log_p$ and $\exp_p$, we can carry over some basic properties of log and exp to the p-adic case. For example, let's try to get the basic property of log that log of a product equals the sum of the logs. Note that if $x \in D(1^-)$ and $y \in D(1^-)$, then also $(1 + x)(1 + y) = 1 + (x + y + xy) \in 1 + D(1^-)$. Thus, we have:

$$\log_p[(1 + x)(1 + y)] = \sum_{n=1}^{\infty} (-1)^{n+1}(x + y + xy)^n/n.$$

Meanwhile, we have the following relation in the ring of power series over $\mathbb{Q}$ in *two* indeterminates (written $\mathbb{Q}[[X, Y]]$):

$$\sum (-1)^{n+1} X^n/n + \sum (-1)^{n+1} Y^n/n = \sum (-1)^{n+1}(X + Y + XY)^n/n.$$

This holds because over $\mathbb{R}$ or $\mathbb{C}$ we have $\log(1 + x)(1 + y) = \log(1 + x) + \log(1 + y)$, so that the difference between the two sides of the above equality—call it $F(X, Y)$—must vanish for all real values of X and Y in the interval $(-1, 1)$. So the coefficient of $X^m Y^n$ in $F(X, Y)$ must vanish for all m and n.

The argument for why $F(X, Y)$ vanishes as a formal power series is typical of a line of reasoning we shall often need. Suppose that an expression involving some power series in X and Y—e.g., $\log(1 + X)$, $\log(1 + Y)$, and $\log(1 + X + Y + XY)$—vanishes whenever real values in some interval are substituted for the variables. Then when we gather together all $X^m Y^n$-terms in this expression, its coefficient must always be zero. Since this is a general fact unrelated to p-adic numbers, we won't digress to prove it carefully here. But if you have any doubts about whether you could prove this fact, turn to Exercise 21 below for further explanations and hints on how to prove it.

Returning to the p-adic situation, we note that if a series converges in Ω, its terms can be rearranged in any order, and the resulting series converges to the same limit. (This is easy to check—it's related to there being no such thing as "conditional" convergence.) Thus, $\log_p[(1 + x)(1 + y)] = \sum_{n=1}^{\infty} (-1)^{n+1}(x + y + xy)^n/n$ can be written as $\sum_{m,n=0}^{\infty} c_{m,n}x^n y^m$. But the "formal identity" in $\mathbb{Q}[[X, Y]]$ tells us that the rational numbers $c_{m,n}$ will be 0 unless $n = 0$ or $m = 0$, in which case: $c_{0,n} = c_{n,0} = (-1)^{n+1}/n$ ($c_{0,0} = 0$). In other words, we may conclude that

$$\begin{aligned}\log_p[(1 + x)(1 + y)] &= \sum_{n=1}^{\infty} (-1)^{n+1}x^n/n + \sum_{n=1}^{\infty} (-1)^{n+1}y^n/n \\ &= \log_p(1 + x) + \log_p(1 + y).\end{aligned}$$

As a corollary of this formula, take the case when $1 + x$ is a p^mth root of 1. Then $|x|_p < 1$ (see Exercise 7 of §III.4), so that: $p^m \log_p(1 + x) = \log_p (1 + x)^{p^m} = \log_p 1 = 0$. Hence $\log_p(1 + x) = 0$.

In exactly the same way we can prove the familiar rule for exp in the p-adic situation: if $x, y \in D(p^{-1/(p-1)-})$, then $x + y \in D(p^{-1/(p-1)-})$, and $\exp_p(x + y) = \exp_p x \cdot \exp_p y$.

Moreover, we also find a result analogous to the Archimedean case as far as $\log_p$ and $\exp_p$ being inverse functions of one another. More precisely, suppose $x \in D(p^{-1/(p-1)-})$. Then $\exp_p x = 1 + \sum_{n=1}^{\infty} x^n/n!$, and $\text{ord}_p(x^n/n!) > n/(p - 1) - (n - S_n)/(p - 1) = S_n/(p - 1) > 0$. Thus, $\exp_p x - 1 \in D(1^-)$. Suppose we take

$$\begin{aligned}\log_p(1 + \exp_p x - 1) &= \sum_{n=1}^{\infty} (-1)^{n+1}(\exp_p x - 1)^n/n \\ &= \sum_{n=1}^{\infty} (-1)^{n+1}\left(\sum_{m=1}^{\infty} x^m/m!\right)^n \Big/ n.\end{aligned}$$

But this series can be rearranged to get a series of the form $\sum_{n=1}^{\infty} c_n x^n$. And reasoning as before, we have the following formal identity over $\mathbb{Q}[[X, Y]]$:

$$\sum_{n=1}^{\infty} (-1)^{n+1}\left(\sum_{m=1}^{\infty} X^m/m!\right)^n \Big/ n = X,$$

coming from the fact that $\log(\exp x) = x$ over $\mathbb{R}$ or $\mathbb{C}$. Hence $c_1 = 1$, $c_n = 0$ for $n > 1$, and

$$\log_p(1 + \exp_p x - 1) = x \quad \text{for } x \in D(p^{-1/(p-1)-}).$$

To go the other way—i.e., $\exp_p(\log_p(1 + x))$—we have to be a little careful, because even if x is in the region of convergence $D(1^-)$ of $\log_p(1 + X)$, it is *not* necessarily the case that $\log_p(1 + x)$ is in the region of convergence $D(p^{-1/(p-1)-})$ of $\exp_p X$. This *is* the case if $x \in D(p^{-1/(p-1)-})$, since then for $n \geq 1$:

$$(\text{ord}_p\, x^n/n) - \frac{1}{p-1} > \frac{n}{p-1} - \text{ord}_p\, n - \frac{1}{p-1} = \frac{n-1}{p-1} - \text{ord}_p\, n,$$

which has its minima at $n = 1$ and $n = p$, where it's zero. Thus, $\text{ord}_p \log_p (1 + x) \geq \min_n \text{ord}_p\, x^n/n > 1/(p - 1)$. Then everything goes through as before, and we have:

$$\exp_p(\log_p(1 + x)) = 1 + x \quad \text{for } x \in D(p^{-1/(p-1)-}).$$

All of the facts we have proved about $\log_p$ and $\exp_p$ can be stated succinctly in the following way.

Proposition. *The functions* $\log_p$ *and* $\exp_p$ *give mutually inverse isomorphisms between the multiplicative group of the open disc of radius* $p^{-1/(p-1)}$ *about* 1 *and the additive group of the open disc of radius* $p^{-1/(p-1)}$ *about* 0. (This means precisely the following: $\log_p$ gives a one-to-one correspondence between the two sets, under which the image of the product of two numbers is the sum of the images, and $\exp_p$ is the inverse map.)

This isomorphism is analogous to the real case, where log and exp give mutually inverse isomorphisms between the multiplicative group of positive real numbers and the additive group of all real numbers.

In particular, this proposition says that $\log_p$ is injective on $D_1(p^{-1/(p-1)-})$, i.e., no two numbers in $D_1(p^{-1/(p-1)-})$ have the same $\log_p$. It's easy to see that $D_1(p^{-1/(p-1)-})$ is the biggest disc on which this is true: namely, a primitive pth root ζ of 1 has $|\zeta - 1|_p = p^{-1/(p-1)}$ (see Exercise 7 of §III.4), and also $\log_p \zeta = 0 = \log_p 1$.

We can similarly define the functions

$$\sin_p\colon D(p^{-1/(p-1)-}) \to \Omega, \qquad \sin_p X = \sum_{n=0}^{\infty} (-1)^n X^{2n+1}/(2n+1)!;$$

$$\cos_p\colon D(p^{-1/(p-1)-}) \to \Omega, \qquad \cos_p X = \sum_{n=0}^{\infty} (-1)^n X^{2n}/(2n)!.$$

Another function which is important in classical mathematics is the binomial expansion $B_a(x) = (1 + x)^a = \sum_{n=0}^{\infty} a(a-1)\cdots(a-n+1)/n!\, x^n$. For any $a \in \mathbb{R}$ or $\mathbb{C}$, this series converges in $\mathbb{R}$ or $\mathbb{C}$ if $|x| < 1$ and diverges if $|x| > 1$ (unless a is a nonnegative integer); its behavior at $|x| = 1$ is a little complicated, and depends on the value of a.

Now for any $a \in \Omega$ let's define

$$B_{a,p}(X) \underset{\text{def}}{=} \sum_{n=0}^{\infty} \frac{a(a-1)\cdots(a-n+1)}{n!} X^n,$$

and proceed to investigate its convergence. First of all, suppose $|a|_p > 1$. Then $|a - i|_p = |a|_p$, and the nth term has $|\ |_p$ equal to $|ax|_p^n/|n!|_p$. Thus, for $|a|_p > 1$, the series $B_{a,p}(X)$ has region of convergence $D((p^{-1/(p-1)})/|a|_p^-)$.

Now suppose $|a|_p \leq 1$. The picture becomes more complicated, and depends on a. We won't derive a complete answer. In any case, for any such a we have $|a - i|_p \leq 1$, and so $|a(a-1)\cdots(a-n+1)/n!\, x^n|_p \leq |x^n/n!|_p$, so that at least $B_{a,p}(X)$ converges on $D(p^{-1/(p-1)-})$.

We'll soon need a more accurate result about the convergence of $B_{a,p}(X)$ in the case when $a \in \mathbb{Z}_p$. We claim that then $B_{a,p}(X) \in \mathbb{Z}_p[[X]]$ (and, in particular, it converges on $D(1^-)$ by Lemma 1). Thus, we want to show that $a(a-1)\cdots(a-n+1)/n! \in \mathbb{Z}_p$. Let a_0 be a positive integer greater than n such that $\text{ord}_p(a - a_0) > N$ (N will be chosen later). Then $a_0(a_0 - 1)\cdots(a_0 - n + 1)/n! = \binom{a_0}{n} \in \mathbb{Z} \subset \mathbb{Z}_p$. It now suffices to show that for suitable N the difference between $a_0(a_0-1)\cdots(a_0-n+1)/n!$ and $a(a-1)\cdots(a-n+1)/n!$ has $|\ |_p \leq 1$. But this follows because the polynomial $X(X-1)\cdots(X-n+1)$ is continuous. Thus,

$$B_{a,p}(X) \in \mathbb{Z}_p[[X]] \text{ if } a \in \mathbb{Z}_p.$$

As an important example of the case $a \in \mathbb{Z}_p$, suppose that $a = 1/m$, $m \in \mathbb{Z}$, $p \nmid m$. Let $x \in D(1^-)$. Then it follows by the same argument as used to prove $\log_p(1+x)(1+y) = \log_p(1+x) + \log_p(1+y)$ that we have

$$[B_{1/m,p}(x)]^m = 1 + x.$$

Thus, $B_{1/m,p}(x)$ is an mth root of $1 + x$ in Ω. (If $p|m$, this still holds, but now we can only substitute values of x in $D(|m|_p p^{-1/(p-1)-})$.) So, whenever a is an ordinary rational number we can adopt the shorthand: $B_{a,p}(X) = (1 + X)^a$.

But be careful! What about the following "paradox"? Consider $4/3 = (1 + 7/9)^{1/2}$; in $\mathbb{Z}_7$ we have $\text{ord}_7\, 7/9 = 1$, and so for $x = 7/9$ and $n \geq 1$:

$$\left| \frac{1/2(1/2-1)\cdots(1/2-n+1)}{n!} x^n \right|_7 \leq 7^{-n}/|n!|_7 < 1.$$

Hence

$$1 > |(1 + \tfrac{7}{9})^{1/2} - 1|_7 = |\tfrac{4}{3} - 1|_7 = |\tfrac{1}{3}|_7 = 1.$$

What's wrong??

Well, we were sloppy when we wrote $4/3 = (1 + 7/9)^{1/2}$. In both $\mathbb{R}$ and $\mathbb{Q}_7$ the number $16/9$ has two square roots $\pm 4/3$. In $\mathbb{R}$, the series for $(1 + 7/9)^{1/2}$ converges to $4/3$, i.e., the positive value is favored. But in $\mathbb{Q}_7$, the square root congruent to 1 mod 7, i.e., $-4/3 = 1 - 7/3$, is favored. Thus, the *exact same series* of rational numbers

$$\sum_{n=0}^{\infty} \frac{1/2(1/2-1)\cdots(1/2-n+1)}{n!} \left(\frac{7}{9}\right)^n$$

converges to a rational number both 7-adically and in the Archimedean absolute value; but the rational numbers it converges to are different! This is a counterexample to the following false "theorem."

Non-theorem 1. *Let $\sum_{n=1}^{\infty} a_n$ be a sum of rational numbers which converges to a rational number in $|\ |_p$ and also converges to a rational number in $|\ |_\infty$. Then the rational value of the infinite sum is the same in both metrics.*

For more "paradoxes," see Exercises 8–10.

Exercises

1. Find the exact disc of convergence (specifying whether open or closed) of the following series. In (v) and (vi), $\log_p$ means the old-fashioned log to base p, and in (vii) ζ is a primitive pth root of 1. [ ] means the greatest integer function.

   (i) $\sum n!\, X^n$ (iii) $\sum p^n X^n$ (v) $\sum p^{[\log_p n]} X^n$ (vii) $\sum (\zeta - 1)^n X^n/n!$
   (ii) $\sum p^{n[\log n]} X^n$ (iv) $\sum p^n X^{p^n}$ (vi) $\sum p^{[\log_p n]} X^n/n$

2. Prove that, if $\sum a_n$ and $\sum b_n$ converge to a and b, respectively (where $a_i, b_i, a, b \in \Omega$), then $\sum c_n$, where $c_n = \sum_{i=0}^{n} a_i b_{n-i}$, converges to ab.

3. Prove that $1 + X\mathbb{Z}_p[[X]]$ is a group with respect to multiplication. Let D be an open or a closed disc in Ω of some radius about 0. Prove that $\{f \in 1 + X\Omega[[X]] \mid f \text{ converges on } D\}$ is closed under multiplication, but is not a group. Prove that for fixed λ, the set of $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i$ such that $\text{ord}_p\, a_i - \lambda i$ is greater than 0 for all $i = 1, 2, \ldots$ and approaches ∞ as $i \to \infty$, is a multiplicative group. Next, let $f_j \in 1 + X\mathbb{Z}_p[[X]]$, $j = 1, 2, 3, \ldots$. Let $f(X) = \prod_{j=1}^{\infty} f_j(X^j)$. Check that $f(X) \in 1 + X\mathbb{Z}_p[[X]]$. Suppose that all of the f_j converge in the closed unit disc $D(1)$. Does $f(X)$ converge in $D(1)$ (proof or counterexample)? If all of the nonconstant coefficients of all of the f_j are divisible by p, does that change your answer (proof or counterexample)?

4. Let $\{a_n\} \subset \Omega$ be a sequence with $|a_n|_p$ bounded. Prove that
$$\sum_{n=0}^{\infty} a_n \frac{n!}{x(x+1)(x+2)\cdots(x+n)}$$
converges for all $x \in \Omega$ not in $\mathbb{Z}_p$. What can you say if $x \in \mathbb{Z}_p$?

5. Let i be a square root of -1 in $\bar{\mathbb{Q}}_p$ (actually, i lies in $\mathbb{Q}_p$ itself unless $p \equiv 3 \bmod 4$). Prove that: $\exp_p(ix) = \cos_p x + i \sin_p x$ for $x \in D(p^{-1/(p-1)-})$.

6. Show that $2^{p-1} \equiv 1 \pmod{p^2}$ if and only if p divides $\sum_{j=1}^{p-1} (-1)^j/j$ (of course, meaning that p divides the numerator of this fraction).

7. Show that the 2-adic ordinal of the rational number
$$2 + 2^2/2 + 2^3/3 + 2^4/4 + 2^5/5 + \cdots + 2^n/n$$
approaches infinity as n increases. Get a good estimate for this 2-adic ordinal in terms of n. Can you think of an entirely elementary proof (i.e., without using p-adic analysis) of this fact, which is actually completely elementary in its statement?

By the minimal total degree $\deg f$ of a nonzero power series f we mean the least d such that some $r_{i_1,\ldots,i_n}$ with $i_1 + i_2 + \cdots + i_n = d$ is nonzero. We can define a topology, the "X-adic topology," on $R[[X]]$ by fixing some positive real number $\rho < 1$ and defining the "X-adic norm" by

$$|f|_X \underset{\text{def}}{=} \rho^{\deg f} \qquad (|0|_X \text{ is defined to be } 0).$$

(1) Show that $|\ \ |_X$ makes $R[[X]]$ into a non-Archimedean metric space (see the first definition in §I.1; by "non-Archimedean," we mean, of course, that the third condition can be replaced by: $d(x, y) \leq \max(d(x, z), d(z, y))$). Say in words what it means for $|f|_X$ to be < 1.

(2) Show that $R[[X]]$ is complete with respect to $|\ \ |_X$.

(3) Show that an infinite product of series $f_j \in R[[X]]$ converges if and only if $|f_j - 1|_X \to 0$ (where 1 is the constant power series $\{r_{i_1,\ldots,i_n}\}$ for which $r_{0,\ldots,0} = 1$ and all other $r_{i,\ldots,i_n} = 0$). We will use this in §2 to see that the horrible power series defined at the end of that section makes sense.

(4) If $f \in R[[X]]$, define f_d to be the same as f but with all coefficients $r_{i_1,\ldots,i_n}$ with $i_1 + \cdots + i_n > d$ replaced by 0. Thus, f_d is a polynomial in n variables. Let $g_1, \ldots, g_n \in R[[X]]$. Note that $f_d(g_1(X), g_2(X), \ldots, g_n(X))$ is well-defined for every d, since it's just a finite sum of products of power series. Prove that $\{f_d(g_1(X), \ldots, g_n(X))\}_{d=0,1,2,\ldots}$ is a Cauchy sequence in $R[[X]]$ if $|g_j|_X < 1$ for $j = 1, \ldots, n$. In that case call its limit $f \circ g$.

(5) Now let R be the field $\mathbb{R}$ of real numbers, and suppose that $f, f_d, g_1, \ldots, g_n$ are as in (4), with $|g_j|_X < 1$. Further suppose that for some $\varepsilon > 0$ the series f and all of the series g_j are absolutely convergent whenever we substitute $X_i = x_i$ in the interval $[-\varepsilon, \varepsilon] \subset \mathbb{R}$. Prove that the series $f \circ g$ is absolutely convergent whenever we substitute $X_i = x_i$ in the (perhaps smaller) interval $[-\varepsilon', \varepsilon']$ for some $\varepsilon' > 0$.

(6) Under the conditions in (5), prove that if $f \circ g(x_1, \ldots, x_n)$ has value 0 for every choice of $x_1, \ldots, x_n \in [-\varepsilon', \varepsilon']$, then $f \circ g$ is the zero power series in $\mathbb{R}[[X]]$.

(7) As an example, let $n = 3$, write X, Y, Z instead of X_1, X_2, X_3, and let

$$\begin{aligned} f(X, Y, Z) &= \sum_{i=1}^{\infty} (-1)^{i+1}(X^i/i + Y^i/i - Z^i/i), \\ g_1(X, Y, Z) &= X, \\ g_2(X, Y, Z) &= Y, \\ g_3(X, Y, Z) &= X + Y + XY. \end{aligned}$$

As another example, let $n = 2$,

$$\begin{aligned} f(X, Y) &= \left(\sum_{i=1}^{\infty} (-1)^{i+1} X^i/i\right) - Y, \\ g_1(X, Y) &= \sum_{i=1}^{\infty} X^i/i!, \\ g_2(X, Y) &= X. \end{aligned}$$

Explain how your result in (6) can be used to prove the basic facts about the elementary p-adic power series. (Construct the f and g_j for one or two more cases.)

14. Prove that $\exp_p X$, $(\sin_p X)/X$, and $\cos_p X$ have no zeros in their regions of convergence, and that $E_p(X)$ has no zeros in $D(1^-)$.

15. Find the coefficients up through the X^4 term in $E_p(X)$ for $p = 2, 3$.

16. Find the coefficients in $E_p(X)$ through the X^{p-1} term. Find the coefficient of X^p. What fact from elementary number theory is reflected in the fact that the coefficient of X^p lies in $\mathbb{Z}_p$?

17. Use Dwork's lemma to give another proof that the coefficients of $E_p(X)$ are in $\mathbb{Z}_p$.

18. Use Dwork's lemma to prove: Let $f(X) = \exp(\sum_{i=0}^{\infty} b_i X^{p^i})$, $b_i \in \mathbb{Q}_p$. Then $f(X) \in 1 + X\mathbb{Z}_p[[X]]$ if and only if $b_{i-1} - pb_i \in p\mathbb{Z}_p$ for $i = 0, 1, 2, \ldots$ (where $b_{-1} \underset{\text{def}}{=} 0$).

3. Newton polygons for polynomials

Let $f(X) = 1 + \sum_{i=1}^{n} a_i X^i \in 1 + X\Omega[X]$ be a polynomial of degree n with coefficients in Ω and constant term 1. Consider the following sequence of points in the real coordinate plane:

$$(0, 0), (1, \operatorname{ord}_p a_1), (2, \operatorname{ord}_p a_2), \ldots, (i, \operatorname{ord}_p a_i), \ldots, (n, \operatorname{ord}_p a_n).$$

(If $a_i = 0$, we omit that point, or we think of it as lying "infinitely" far above the horizontal axis.) The *Newton polygon* of $f(X)$ is defined to be the "convex hull" of this set of points, i.e., the highest convex polygonal line joining $(0, 0)$ with $(n, \operatorname{ord}_p a_n)$ which passes on or below all of the points $(i, \operatorname{ord}_p a_i)$. Physically, this convex hull is constructed by taking a vertical line through $(0, 0)$ and rotating it about $(0, 0)$ counterclockwise until it hits any of the points $(i, \operatorname{ord}_p a_i)$, taking the segment joining $(0, 0)$ to the last such point $(i_1, \operatorname{ord}_p a_{i_1})$ that it hits as the first segment of the Newton polygon, then rotating the line further about $(i_1, \operatorname{ord}_p a_{i_1})$ until it hits a further point $(i, \operatorname{ord}_p a_i)$ $(i > i_1)$, taking the segment joining $(i_1, \operatorname{ord}_p a_{i_1})$ to the last such point $(i_2, \operatorname{ord}_p a_{i_2})$ as the second segment, then rotating the line about $(i_2, \operatorname{ord}_p a_{i_2})$ and so on, until you reach $(n, \operatorname{ord}_p a_n)$.

As an example, Figure 1 shows the Newton polygon for $f(X) = 1 + X^2 + \frac{1}{3}X^3 + 3X^4$ in $\mathbb{Q}_3[X]$.

By the vertices of the Newton polygon we mean the points $(i_j, \operatorname{ord}_p a_{i_j})$ where the slopes change. If a segment joins a point (i, m) to (i', m'), its slope is $(m' - m)/(i' - i)$; by the "length of the slope" we mean $i' - i$, i.e., the length of the projection of the corresponding segment onto the horizontal axis.

Lemma 4. *In the above notation, let $f(X) = (1 - X/\alpha_1) \cdots (1 - X/\alpha_n)$ be the factorization of $f(X)$ in terms of its roots $\alpha_i \in \Omega$. Let $\lambda_i = \operatorname{ord}_p 1/\alpha_i$. Then, if λ is a slope of the Newton polygon having length l, it follows that precisely l of the λ_i are equal to λ.*

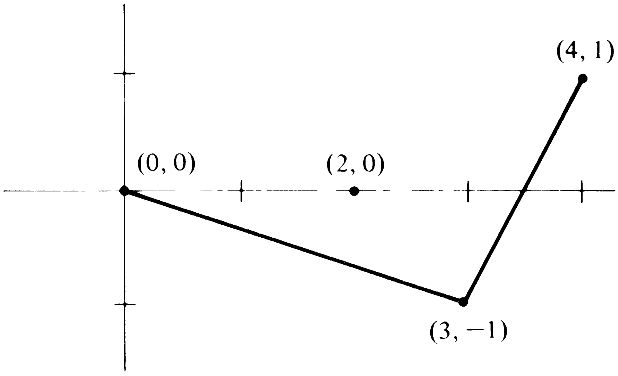


Figure IV.1

In other words, the slopes of the Newton polygon of $f(X)$ "are" (counting multiplicity) the p-adic ordinals of the reciprocal roots of $f(X)$.

PROOF. We may suppose the α_i to be arranged so that $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$. Say $\lambda_1 = \lambda_2 = \cdots = \lambda_r < \lambda_{r+1}$. We first claim that the first segment of the Newton polygon is the segment joining (0, 0) to $(r, r\lambda_1)$. Recall that each a_i is expressed in terms of $1/\alpha_1, 1/\alpha_2, \ldots, 1/\alpha_n$ as $(-1)^i$ times the ith symmetric polynomial, i.e., the sum of all possible products of i of the $1/\alpha$'s. Since the p-adic ordinal of such a product is at least $i\lambda_1$, the same is true for a_i. Thus, the point $(i, \text{ord}_p\, a_i)$ is *on or above* the point $(i, i\lambda_1)$, i.e., on or above the line joining (0, 0) to $(r, r\lambda_1)$.

Now consider a_r. Of the various products of r of the $1/\alpha$'s, exactly one has p-adic ordinal $r\lambda_1$, namely, the product $1/(\alpha_1\alpha_2\cdots\alpha_r)$. All of the other products have p-adic ordinal $> r\lambda_1$, since we must include at least one of the $\lambda_{r+1}, \lambda_{r+2}, \ldots, \lambda_n$. Thus, a_r is a sum of something with ordinal $r\lambda_1$ and something with ordinal $> r\lambda_1$, so, by the "isosceles triangle principle," $\text{ord}_p\, a_r = r\lambda_1$.

Now suppose $i > r$. In the same way as before, we see that all of the products of i of the $1/\alpha$'s have p-adic ordinal $> i\lambda_1$. Hence, $\text{ord}_p\, a_i > i\lambda_1$. If we now think of how the Newton polygon is constructed, we see that we have shown that its first segment is the line joining (0, 0) with $(r, r\lambda_1)$.

The proof that, if we have $\lambda_s < \lambda_{s+1} = \lambda_{s+2} = \cdots = \lambda_{s+r} < \lambda_{s+r+1}$, then the line joining $(s, \lambda_1 + \lambda_2 + \cdots + \lambda_s)$ to $(s + r, \lambda_1 + \lambda_2 + \cdots + \lambda_s + r\lambda_{s+1})$ is a segment of the Newton polygon, is completely analogous and will be left to the reader. □

4. Newton polygons for power series

Now let $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$ be a power series. Define $f_n(X) = 1 + \sum_{i=1}^{n} a_i X^i \in 1 + X\Omega[X]$ to be the nth partial sum of $f(X)$. In this section we suppose that $f(X)$ is not a polynomial, i.e., infinitely many

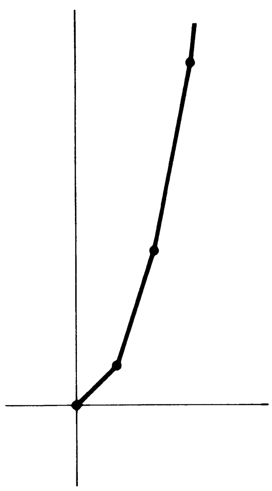


Figure IV.2

a_i are nonzero. The Newton polygon of $f(X)$ is defined to be the "limit" of the Newton polygons of the $f_n(X)$. More precisely, we follow the same recipe as in the construction of the Newton polygon of a polynomial: plot all of the points $(0, 0)$, $(1, \text{ord}_p\, a_1)$, ..., $(i, \text{ord}_p\, a_i)$, ...; rotate the vertical line through $(0, 0)$ until it hits a point $(i, \text{ord}_p\, a_i)$, then rotate it about the farthest such point it hits, and so on. But we must be careful to notice that three things can happen:

(1) We get infinitely many segments of finite length. For example, take $f(X) = 1 + \sum_{i=1}^{\infty} p^{i^2} X^i$, whose Newton polygon is a polygonal line inscribed in the right half of the parabola $y = x^2$ (see Figure 2).

(2) At some point the line we're rotating simultaneously hits points $(i, \text{ord}_p\, a_i)$ which are arbitrarily far out. In that case, the Newton polygon has a finite number of segments, the last one being infinitely long. For example, the Newton polygon of $f(X) = 1 + \sum_{i=1}^{\infty} X^i$ is simply one infinitely long horizontal segment.

(3) At some point the line we're rotating has not yet hit any of the $(i, \text{ord}_p\, a_i)$ which are farther out, but, if we rotated it any farther at all, it would rotate past such points, i.e., it would pass above some of the $(i, \text{ord}_p\, a_i)$. A simple example is $f(X) = 1 + \sum_{i=1}^{\infty} pX^i$. In that case, when the line through $(0, 0)$ has rotated to the horizontal position, it can rotate no farther without passing above some of the points $(i, 1)$. When this happens, we let the last segment of the Newton polygon have slope equal to the least upper bound of all possible slopes for which it passes below all of the $(i, \text{ord}_p\, a_i)$. In our example, the slope is 0, and the Newton polygon consists of one infinite horizontal segment (see Figure 3).

A degenerate case of possibility (3) occurs when the vertical line through $(0, 0)$ cannot be rotated at all without crossing above some points $(i, \text{ord}_p\, a_i)$. For example, this is what happens with $f(X) = \sum_{i=0}^{\infty} X^i/p^{i^2}$. In that case, $f(X)$

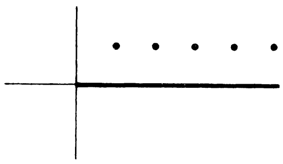


Figure IV.3

is easily seen to have zero radius of convergence, i.e., $f(x)$ diverges for any nonzero x. In what follows we shall exclude that case from consideration and shall suppose that $f(X)$ has a nontrivial disc of convergence.

In the case of polynomials, the Newton polygon is useful because it allows us to see at a glance at what radii the reciprocal roots are located. We shall prove that the Newton polygon of a power series $f(X)$ similarly tells us where the zeros of $f(X)$ lie. But first, let's make an ad hoc study of a particularly illustrative example.

Let

$$f(X) = 1 + \frac{X}{2} + \frac{X^2}{3} + \cdots + \frac{X^i}{i+1} + \cdots = -\frac{1}{X}\log_p(1 - X).$$

The Newton polygon of $f(X)$ (see Figure 4, in which $p = 3$) is the polygonal line joining the points $(0, 0)$, $(p - 1, -1)$, $(p^2 - 1, -2), \ldots, (p^j - 1, -j), \ldots$; it is of type (1) in the list at the beginning of this section. If the power series analogue of Lemma 4 of §3 is to hold, we would expect from looking at this Newton polygon that $f(X)$ has precisely $p^{j+1} - p^j$ roots of p-adic ordinal $1/(p^{j+1} - p^j)$.

But what are the roots of $-1/X \log_p(1 - X)$? First, if $x = 1 - \zeta$, where ζ is a primitive p^{j+1}th root of 1, we know by Exercise 7 of §III.4 that $\text{ord}_p\, x = 1/(p^{j+1} - p^j)$; and we know by the discussion of $\log_p$ in §IV.1 that $\log_p (1 - x) = \log_p \zeta = 0$. Since there are $p^{j+1} - p^j$ primitive p^{j+1}th roots of 1, this gives us all of the predicted roots. Are there any other zeros of $f(X)$ in $D(1^-)$?

Let $x \in D(1^-)$ be such a root. Then for any j, $x_j = 1 - (1 - x)^{p^j} \in D(1^-)$ is also a root since $\log_p(1 - x_j) = p^j \log_p(1 - x) = 0$. But for j sufficiently large, we have $x_j \in D(p^{-1/(p-1)-})$. For $x_j \in D(p^{-1/(p-1)-})$, we have $1 - x_j = \exp_p(\log_p(1 - x_j)) = \exp_p 0 = 1$. Hence $(1 - x)^{p^j} = 1$, and x must be one

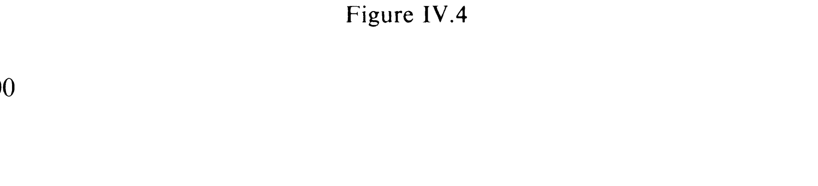


Figure IV.4

of the roots we already considered. Thus, the appearance of the Newton polygon agrees with our knowledge of all of the roots of $\log_p(1 - X)$.

We now proceed to prove that the Newton polygon plays the same role for power series as for polynomials. But first we prove a much simpler result: that the radius of convergence of a power series can be seen at a glance from its Newton polygon.

Lemma 5. *Let b be the least upper bound of all slopes of the Newton polygon of* $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$. *Then the radius of convergence is* p^b *(b may be infinite, in which case* $f(X)$ *converges on all of* Ω*).*

Proof. First let $|x|_p < p^b$, i.e., $\operatorname{ord}_p x > -b$. Say $\operatorname{ord}_p x = -b'$, where $b' < b$. Then $\operatorname{ord}_p(a_i x^i) = \operatorname{ord}_p a_i - ib'$. But it is clear (see Figure 5) that, sufficiently far out, the $(i, \operatorname{ord}_p a_i)$ lie arbitrarily far above $(i, b'i)$, in other words, $\operatorname{ord}_p(a_i x^i) \to \infty$, and $f(X)$ converges at $X = x$.

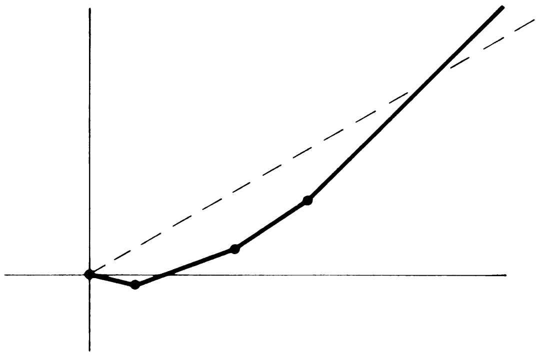


Figure IV.5

Now let $|x|_p > p^b$, i.e., $\operatorname{ord}_p x = -b' < -b$. Then we find in the same way that $\operatorname{ord}_p(a_i x^i) = \operatorname{ord}_p a_i - b'i$ is negative for infinitely many values of i. Thus $f(x)$ does not converge. We conclude that $f(X)$ has radius of convergence exactly p^b. □

Remark. This lemma says nothing about convergence or divergence when $|x|_p = p^b$. It is easy to see that convergence *at* the radius of convergence ("on the circumference") can only occur in type (3) in the list at the beginning of this section, and then if and only if the distance that $(i, \operatorname{ord}_p a_i)$ lies above the last (infinite) segment approaches ∞ as $i \to \infty$. An example of this behavior is the power series $f(X) = 1 + \sum_{i=1}^{\infty} p^i X^{p^i}$, whose Newton polygon is the horizontal line extending from $(0, 0)$. This $f(X)$ converges when $\operatorname{ord}_p x = 0$.

One final remark should be made before beginning the proof of the power series analogue of Lemma 4. If $c \in \Omega$, $\operatorname{ord}_p c = \lambda$, and $g(X) = f(X/c)$, then the Newton polygon for g is obtained from that for f by subtracting the line

$y = \lambda x$—the line through (0, 0) with slope λ—from the Newton polygon for f. This is because, if $f(X) = 1 + \sum a_i X^i$ and $g(X) = 1 + \sum b_i X^i$, then we have $\text{ord}_p\, b_i = \text{ord}_p(a_i/c^i) = \text{ord}_p\, a_i - \lambda i$.

Lemma 6. *Suppose that λ_1 is the first slope of the Newton polygon of $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$. Let $c \in \Omega$, $\text{ord}_p\, c = \lambda \leq \lambda_1$. Suppose that $f(X)$ converges on the closed disc $D(p^\lambda)$ (by Lemma 5, this automatically holds if $\lambda < \lambda_1$ or if the Newton polygon of $f(X)$ has more than one segment). Let*

$$g(X) = (1 - cX)f(X) \in 1 + X\Omega[[X]].$$

Then the Newton polygon of $g(X)$ is obtained by joining (0, 0) to $(1, \lambda)$ and then translating the Newton polygon of $f(X)$ by 1 to the right and λ upward. In other words, the Newton polygon of $g(X)$ is obtained by "joining" the Newton polygon of the polynomial $(1 - cX)$ to the Newton polygon of the power series $f(X)$. In addition, if $f(X)$ has last slope λ_f and converges on $D(p^{\lambda_f})$, then $g(X)$ also converges on $D(p^{\lambda_f})$. Conversely, if $g(X)$ converges on $D(p^{\lambda_f})$, then so does $f(X)$.

Proof. We first reduce to the special case $c = 1$, $\lambda = 0$. Suppose the lemma holds for that case, and we have $f(X)$ and $g(X)$ as in the lemma. Then $f_1(X) = f(X/c)$ and $g_1(X) = (1 - X)f_1(X)$ satisfy the conditions of the lemma with c, λ, λ_1 replaced by $1, 0, \lambda_1 - \lambda$, respectively (see the remark immediately preceding the statement of the lemma). Then the lemma, which we're assuming holds for f_1 and g_1, gives us the shape of the Newton polygon of $g_1(X)$ (and the convergence of g_1 on $D(p^{\lambda_f - \lambda})$ when f converges on $D(p^{\lambda_f})$). Since $g(X) = g_1(cX)$, if we again use the remark before the statement of the lemma, we obtain the desired information about the Newton polygon of $g(X)$. (See Figure 6.)

Thus, it suffices to prove Lemma 6 with $c = 1$, $\lambda = 0$. Let $g(X) = 1 + \sum_{i=1}^{\infty} b_i X^i$. Then, since $g(X) = (1 - X)f(X)$, we have $b_{i+1} = a_{i+1} - a_i$ for $i \geq 0$ (with $a_0 = 1$), and so

$$\text{ord}_p\, b_{i+1} \geq \min(\text{ord}_p\, a_{i+1}, \text{ord}_p\, a_i),$$

with equality holding if $\text{ord}_p\, a_{i+1} \neq \text{ord}_p\, a_i$ (by the isosceles triangle principle). Since both $(i, \text{ord}_p\, a_i)$ and $(i, \text{ord}_p\, a_{i+1})$ lie on or above the Newton polygon of $f(X)$, so does $(i, \text{ord}_p\, b_{i+1})$. If $(i, \text{ord}_p\, a_i)$ is a vertex, then $\text{ord}_p\, a_{i+1} > \text{ord}_p\, a_i$, and so $\text{ord}_p\, b_{i+1} = \text{ord}_p\, a_i$. This implies that the Newton polygon of $g(X)$ must have the shape described in the lemma as far as the last vertex of the Newton polygon of $f(X)$. It remains to show that, in the case when the Newton polygon of $f(X)$ has a final infinite slope λ_f, $g(X)$ also does; and, if $f(X)$ converges on $D(p^{\lambda_f})$, then so does $g(X)$ (and conversely). Since $\text{ord}_p\, b_{i+1} \geq \min(\text{ord}_p\, a_{i+1}, \text{ord}_p\, a_i)$, it immediately follows that $g(X)$ converges wherever $f(X)$ does. We must rule out the possibility that the Newton polygon of $g(X)$ has a slope λ_g which is *greater* than λ_f. If the Newton polygon of $g(X)$

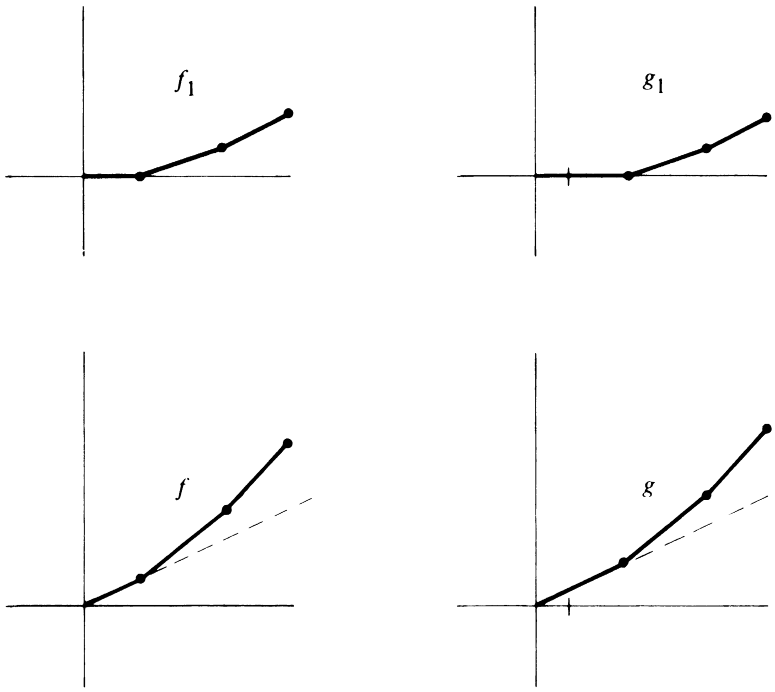


Figure IV.6

did have such a slope, then for some large i, the point $(i + 1, \text{ord}_p a_i)$ would lie below the Newton polygon of $g(X)$. Then we would have $\text{ord}_p b_j > \text{ord}_p a_i$ for all $j \geq i + 1$. This first of all implies that $\text{ord}_p a_{i+1} = \text{ord}_p a_i$, because $a_{i+1} = b_{i+1} + a_i$; then in the same way $\text{ord}_p a_{i+2} = \text{ord}_p a_{i+1}$, and so on: $\text{ord}_p a_j = \text{ord}_p a_i$ for all $j > i$. But this contradicts the assumed convergence of $f(X)$ on $D(1)$. The converse assertion (convergence of g implies convergence of f) is proved in the same way. □

Lemma 7. *Let $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$ have Newton polygon with first slope λ_1. Suppose that $f(X)$ converges on the closed disc $D(p^{\lambda_1})$, and also suppose that the line through* $(0, 0)$ *with slope λ_1 actually passes through a point* $(i, \text{ord}_p a_i)$. (*Both of these conditions automatically hold if the Newton polygon has more than one slope.*) *Then there exists an x for which* $\text{ord}_p x = -\lambda_1$ *and* $f(x) = 0$.

Proof. For simplicity, we first consider the case $\lambda_1 = 0$, and then reduce the general case to this one. In particular, $\text{ord}_p a_i \geq 0$ for all i and $\text{ord}_p a_i \to \infty$ as $i \to \infty$. Let $N \geq 1$ be the greatest i for which $\text{ord}_p a_i = 0$. (Except in the case when the Newton polygon of $f(X)$ is only one infinite horizontal line, this N is the length of the first segment, of slope $\lambda_1 = 0$.) Let $f_n(X) = 1 + \sum_{i=1}^{n} a_i X^i$. By Lemma 4, for $n \geq N$ the polynomial $f_n(X)$ has precisely N

roots $x_{n,1}, \ldots, x_{n,N}$ with $\text{ord}_p\, x_{n,i} = 0$. Let $x_N = x_{N,1}$, and for $n \geq N$ let x_{n+1} be any of the $x_{n+1,1}, \ldots, x_{n+1,N}$ with $|x_{n+1,i} - x_n|_p$ minimal. We claim that $\{x_n\}$ is Cauchy, and that its limit x has the desired properties.

For $n \geq N$ let S_n denote the set of roots of $f_n(X)$ (counted with their multiplicities). Then for $n \geq N$ we have

$$\begin{aligned} |f_{n+1}(x_n) - f_n(x_n)|_p &= |f_{n+1}(x_n)|_p \quad (\text{since } f_n(x_n) = 0) \\ &= \prod_{x \in S_{n+1}} \left|1 - \frac{x_n}{x}\right|_p \\ &= \prod_{i=1}^{N} |1 - x_n/x_{n+1,i}|_p \quad (\text{since if } x \in S_{n+1} \text{ has } \text{ord}_p\, x < 0, \\ &\qquad\qquad \text{we then have } |1 - x_n/x|_p = 1) \\ &= \prod_{i=1}^{N} |x_{n+1,i} - x_n|_p \quad (\text{since } |x_{n+1,i}|_p = 1) \\ &\geq |x_{n+1} - x_n|_p{}^N, \end{aligned}$$

by the choice of x_{n+1}. Thus,

$$|x_{n+1} - x_n|_p{}^N \leq |f_{n+1}(x_n) - f_n(x_n)|_p = |a_{n+1}x_n^{n+1}|_p = |a_{n+1}|_p.$$

Since $|a_{n+1}|_p \to 0$ as $n \to \infty$, it follows that $\{x_n\}$ is Cauchy.

If $x_n \to x \in \Omega$, we further have $f(x) = \lim_{n\to\infty} f_n(x)$, while

$$|f_n(x)|_p = |f_n(x) - f_n(x_n)|_p = |x - x_n|_p \left|\sum_{i=1}^{n} a_i \frac{x^i - x_n{}^i}{x - x_n}\right|_p \leq |x - x_n|_p,$$

since $|a_i|_p \leq 1$ and $|(x^i - x_n{}^i)/(x - x_n)|_p = |x^{i-1} + x^{i-2}x_n + x^{i-3}x_n{}^2 + \cdots + x_n^{i-1}|_p \leq 1$. Hence, $f(x) = \lim_{n\to\infty} f_n(x) = 0$. This proves the lemma when $\lambda_1 = 0$.

Now the general case follows easily. Let $\pi \in \Omega$ be any number such that $\text{ord}_p\, \pi = \lambda_1$. Note that such a π exists, for example, take an ith root of an a_i for which $(i, \text{ord}_p\, a_i)$ lies on the line through $(0, 0)$ with slope λ_1. Now let $g(X) = f(X/\pi)$. Then $g(X)$ satisfies the conditions of the lemma with $\lambda_1 = 0$. So, by what's already been proved, there exists an x_0 with $\text{ord}_p\, x_0 = 0$ and $g(x_0) = 0$. Let $x = x_0/\pi$. Then $\text{ord}_p\, x = -\lambda_1$ and $f(x) = f(x_0/\pi) = g(x_0) = 0$. □

Lemma 8. *Let $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$ converge and have value 0 at α. Let $g(X) = 1 + \sum_{i=1}^{\infty} b_i X^i$ be obtained by dividing $f(X)$ by $1 - X/\alpha$, or equivalently, by multiplying $f(X)$ by the series $1 + X/\alpha + X^2/\alpha^2 + \cdots + X^i/\alpha^i + \cdots$. Then $g(X)$ converges on $D(|\alpha|_p)$.*

Proof. Let $f_n(X) = 1 + \sum_{i=1}^{n} a_i X^i$. Clearly,

$$b_i = 1/\alpha^i + a_1/\alpha^{i-1} + a_2/\alpha^{i-2} + \cdots + a_{i-1}/\alpha + a_i,$$

so that

$$b_i\alpha^i = f_i(\alpha).$$

Hence $|b_i\alpha^i|_p = |f_i(\alpha)|_p \to 0$ as $i \to \infty$, because $f(\alpha) = 0$. □

Theorem 14 (p-adic Weierstrass Preparation Theorem). *Let $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$ converge on $D(p^\lambda)$. Let N be the total horizontal length of all segments of the Newton polygon having slope $\leq \lambda$ if this horizontal length is finite (i.e., if the Newton polygon of $f(X)$ does not have an infinitely long last segment of slope λ). If, on the other hand, the Newton polygon of $f(X)$ has last slope λ, let N be the greatest i such that $(i, \text{ord}_p\, a_i)$ lies on that last segment (there must be a greatest such i, because $f(X)$ converges on $D(p^\lambda)$). Then there exists a polynomial $h(X) \in 1 + X\Omega[X]$ of degree N and a power series $g(X) = 1 + \sum_{i=1}^{\infty} b_i X^i$ which converges and is nonzero on $D(p^\lambda)$, such that*

$$h(X) = f(X)\cdot g(X).$$

The polynomial $h(X)$ is uniquely determined by these properties, and its Newton polygon coincides with the Newton polygon of $f(X)$ out to $(N, \text{ord}_p\, a_N)$.

Proof. We use induction on N. First suppose $N = 0$. Then we must show that $g(X)$, the inverse power series of $f(X)$, converges and is nonzero on $D(p^\lambda)$. This was part of Exercise 3 of §IV.1, but, since this is an important fact, we'll prove it here in case you skipped that exercise. As usual (see the proofs of Lemma 6 and 7 and the remark right before the statement of Lemma 6), we can easily reduce to the case $\lambda = 0$.

Thus, suppose $f(X) = 1 + \sum a_i X^i$, $\text{ord}_p\, a_i > 0$, $\text{ord}_p\, a_i \to \infty$, $g(X) = 1 + \sum b_i X^i$. Since $f(X)g(X) = 1$, we obtain

$$b_i = -(b_{i-1}a_1 + b_{i-2}a_2 + \cdots + b_1 a_{i-1} + a_i) \text{ for } i \geq 1,$$

from which it readily follows by induction on i that $\text{ord}_p\, b_i > 0$. Next, we must show that $\text{ord}_p\, b_i \to \infty$ as $i \to \infty$. Suppose we are given some large M. Choose m so that $i > m$ implies $\text{ord}_p\, a_i > M$. Let

$$\varepsilon = \min(\text{ord}_p\, a_1, \text{ord}_p\, a_2, \ldots, \text{ord}_p\, a_m) > 0.$$

We claim that $i > nm$ implies that $\text{ord}_p\, b_i > \min(M, n\varepsilon)$, from which it will follow that $\text{ord}_p\, b_i \to \infty$. We prove this claim by induction on n. It's trivial for $n = 0$. Suppose $n \geq 1$ and $i > nm$. We have

$$b_i = -(b_{i-1}a_1 + \cdots + b_{i-m}a_m + b_{i-(m+1)}a_{m+1} + \cdots + a_i).$$

The terms $b_{i-j}a_j$ with $j > m$ have $\text{ord}_p(b_{i-j}a_j) \geq \text{ord}_p\, a_j > M$, while the terms with $j \leq m$ have $\text{ord}_p(b_{i-j}a_j) \geq \text{ord}_p\, b_{i-j} + \varepsilon > \min(M, (n-1)\varepsilon) + \varepsilon$ by the induction assumption (since $i - j > (n-1)m$) and the definition of ε. Hence all summands in the expression for b_i have $\text{ord}_p > \min(M, n\varepsilon)$. This proves the claim, and hence the theorem for $N = 0$.

Now suppose $N \geq 1$, and the theorem holds for $N - 1$. Let $\lambda_1 \leq \lambda$ be the first slope of the Newton polygon of $f(X)$. Using Lemma 7, we find an α such that $f(\alpha) = 0$ and $\text{ord}_p\, \alpha = -\lambda_1$. Let

$$f_1(X) = f(X)\left(1 + \frac{X}{\alpha} + \frac{X^2}{\alpha^2} + \cdots + \frac{X^i}{\alpha^i} + \cdots\right)$$
$$= 1 + \sum a_i' X^i \in 1 + X\Omega[[X]].$$

By Lemma 8, $f_1(X)$ converges on $D(p^{\lambda_1})$. Let $c = 1/\alpha$, so that: $f(X) = (1 - cX)f_1(X)$. If the Newton polygon of $f_1(X)$ had first slope λ_1' less than λ_1, it would follow by Lemma 7 that $f_1(X)$ has a root with p-adic ordinal $-\lambda_1'$, and then so would $f(X)$, which it is easy to check is impossible. Hence $\lambda_1' \geq \lambda_1$, and we have the conditions of Lemma 6 (with f_1, f, λ_1', and λ_1 playing the roles of f, g, λ_1, and λ, respectively). Lemma 6 then tells us that $f_1(X)$ has the same Newton polygon as $f(X)$, minus the segment from (0, 0) to $(1, \lambda_1)$. In addition, in the case when f (and hence f_1) have last slope λ, because f converges on $D(p^\lambda)$, Lemma 6 further tells us that f_1 must also converge on $D(p^\lambda)$.

Thus, $f_1(X)$ satisfies the conditions of the theorem with N replaced by $N - 1$. By the induction assumption, we can find an $h_1(X) \in 1 + X\Omega[X]$ of degree $N - 1$ and a series $g(X) \in 1 + X\Omega[[X]]$ which converges and is nonzero on $D(p^\lambda)$, such that

$$h_1(X) = f_1(X) \cdot g(X).$$

Then, multiplying both sides by $(1 - cX)$ and setting $h(X) = (1 - cX)h_1(X)$, we have

$$h(X) = f(X) \cdot g(X),$$

with $h(X)$ and $g(X)$ having the required properties.

Finally, suppose that $h_1(X) \in 1 + X\Omega[X]$ is another polynomial of degree N such that $h_1(X) = f(X)g_1(X)$, where $g_1(X)$ converges and is nonzero on $D(p^\lambda)$. Since $h_1(X)g(X) = f(X)g(X)g_1(X) = h(X)g_1(X)$, uniqueness of $h(X)$ follows if we prove the claim: $h_1 g = h g_1$ implies that h_1 and h have the same zeros with the same multiplicities. This can be shown by induction on N. For $N = 1$ it is obvious, because $h_1(x) = 0 \Leftrightarrow h(x) = 0$ for $x \in D(p^\lambda)$. Now suppose $N > 1$. Without loss of generality we may assume that $-\lambda$ is ord_p of a root α of $h(X)$ having minimal ord_p. Since α is a root of both $h(X)$ and $h_1(X)$ of minimal ord_p, we can divide both sides of the equality $h_1(X)g(X) = h(X)g_1(X)$ by $(1 - X/\alpha)$, using Lemma 8, and thereby reduce to the case of our claim with N replaced by $N - 1$. This completes the proof of Theorem 14. □

Corollary. *If a segment of the Newton polygon of $f(X) \in 1 + X\Omega[[X]]$ has finite length N and slope λ, then there are precisely N values of x counting multiplicity for which $f(x) = 0$ and $\text{ord}_p\, x = -\lambda$.*

Another consequence of Theorem 14 is that a power series which converges everywhere factors into the (infinite) product of $(1 - X/r)$ over all of its roots r, and, in particular, if it converges everywhere and has no zeros, it must be a constant. (See Exercise 13 below.) This contrasts with the real or complex case, where we have the function e^x (or, more generally, $e^{h(x)}$, where h is any everywhere convergent power series). In complex analysis, the analogous infinite product expansion of an everywhere convergent power series in terms of its roots is more complicated than in the p-adic case; exponential factors have to be thrown in to obtain the "Weierstrass product" of an "entire" function of a complex variable.

Thus, the simple infinite product expansion that results from Theorem 14 in the p-adic case is possible thanks to the absence of an everywhere convergent exponential function. So in the present context we're lucky that $\exp_p$ has bad convergence. But in other contexts—for example, p-adic differential equations—the absence of a nicely convergent exp makes life very complicated.

Exercises

1. Find the Newton polygon of the following polynomials:
   (i) $1 - X + pX^2$ (ii) $1 - X^3/p^2$ (iii) $1 + X^2 + pX^4 + p^3X^6$
   (iv) $\sum_{i=1}^{p} iX^{i-1}$ (v) $(1 - X)(1 - pX)(1 - p^3X)$ (do this in two ways)
   (vi) $\prod_{i=1}^{p^2} (1 - iX)$.

2. (a) Let $f(X) \in 1 + X\mathbb{Z}_p[X]$ have Newton polygon consisting of one segment joining $(0, 0)$ to the point (n, m). Show that if n and m are relatively prime, then $f(X)$ cannot be factored as a product of two polynomials with coefficients in $\mathbb{Z}_p$.
   (b) Use part (a) to give another proof of the Eisenstein irreducibility criterion (see Exercise 14 of §I.5).
   (c) Is the converse to (a) true or false, i.e., do all irreducible polynomials have Newton polygon of this type (proof or counterexample)?

3. Let $f(X) \in 1 + X\mathbb{Z}_p[X]$ be a polynomial of degree $2n$. Suppose you know that, whenever α is a reciprocal root of $f(X)$, so is p/α (with the same multiplicity). What does this tell you about the shape of the Newton polygon? Draw all possible shapes of Newton polygons of such $f(X)$ when $n = 1, 2, 3, 4$.

4. Find the Newton polygon of the following power series:
   (i) $\sum_{i=0}^{\infty} X^{p^i - 1}/p^i$ (ii) $\sum_{i=0}^{\infty}((pX)^i + X^{p^i})$ (iii) $\sum_{i=0}^{\infty} i!X^i$
   (iv) $\sum_{i=0}^{\infty} X^i/i!$ (v) $(1 - pX^2)/(1 - p^2X^2)$ (vi) $(1 - p^2X)/(1 - pX)$
   (vii) $\prod_{i=0}^{\infty}(1 - p^iX)$ (viii) $\sum_{i=0}^{\infty} p^{[i\sqrt{2}]}X^i$

5. Show that the slopes of the finite segments of the Newton polygon of a power series are rational numbers, but that the slope of the infinite segment (if there is one) need not be (give an example).

6. Show by a counterexample that Lemma 7 is false if we omit the condition that the line through $(0, 0)$ with slope λ_1 pass through a point $(i, \operatorname{ord}_p a_i)$, $i > 0$.

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 (4.5) (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 (4.6), it suffices to verify the condition (4.6) 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 (4.6) 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 [Kat], [MSD74]).

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 [BS85]) $B_{k,f}$ 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 (4.6) and check that for every $f \in \mathrm{Step}(Y, \mathbb{C})$ the right hand side in (4.8) (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 (4.7); 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 (4.9) 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 (4.7) 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

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

of the norm $|\cdot|_{\mathcal{A}}$ (see [Ma73], [Vi76]). In particular if $\mathcal{A} = R = \mathrm{O}_p = \{x \in \mathbb{C}_p \quad | \quad |x|_p \le 1\}$ 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 [Kat]). Let $\{f_i\}$ be a system of continuous functions $f_i \in \mathcal{C}(Y, \mathcal{O}_p)$ in the ring $\mathcal{C}(Y, \mathcal{O}_p)$ of all continuous functions on the compact totally disconnected group Y with values in the ring of integers $\mathcal{O}_p$ 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 $a_i \in \mathcal{O}_p$. Then the existence of an $\mathcal{O}_p$-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

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

Remark

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

Proof of proposition 4.1. The necessity is obvious since

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

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 (4.11) 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 ([Kat]), 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 4.1 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 (4.8), $f \in \mathrm{Step}(Y, \mathbb{Q}_p)$ 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 (4.13) formally implies that

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

and also we see that

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

The last identity can be rewritten symbolically as

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

The equality (4.14) 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 [La76]):

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

where f is a $\mathbb{C}_p$-valued function on $Y = \mathbb{Z}_S$. Indeed, if we replace M in (4.14) by Mp^n with growing n and let D be the common denominator of all coefficients of the polynomial $B^{(M)}_{k,f}(X)$. Then we have from (4.15) that

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

The proof of (4.16) is accomplished by division of (4.17) by Mp^n and by application of the formula (4.14).

Now we can directly show that the distribution E_k^c defined by (4.12) are in fact bounded measures. If we use (4.11) 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 (4.16). 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 (4.12):

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

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 (4.21) 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 (4.17) formally implies 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 (4.21) 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 (4.22):

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

The last congruence is equivalent to saying that the abstract Kummer congruences (4.11) 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 (4.23).

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:

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

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 (4.26) converge absolutely for $\mathrm{Re}(s) > 1 + c$. The identities (4.25) and (4.26) 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 (4.27) 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 $\mathbb{C}_p = \hat{\bar{\mathbb{Q}}}_p$ (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

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

where:

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

and the symbol

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

denotes the functor of all p-adic characters of a topological group G (see [Vi76]).

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:

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

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 [Ma73], [Man76]).

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 [Kob80], [Vi76]). If we apply to these series the Weierstrass preparation theorem (see [Kob80], [Man71]), 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 (4.30). 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 [Ma73], [Man76], [Vi76]).

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

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

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 (4.31), 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 $\mathcal{O}$ be a closed subring in $\mathcal{O}_p = \{z \in \mathbb{C}_p \quad | \quad |z|_p \leq 1\}$,

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

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

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

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

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

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

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

(see the previous section) as follows:

We noticed above that the theorem 4 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 (4.30) 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 $\mathcal{C}(\mathbb{Z}_p, \mathcal{O}_p)$ 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 4.1), which imply that for arbitrary choice of numbers $a_i \in \mathcal{O}_p$ there exists a measure with the property (4.36).

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 (4.36), 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 (4.37) 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 (4.37).

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

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

where $M_0 = \prod_{q \in S} q$. Moreover, the right hand side of (4.38) 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 4.1 the right hand side of (4.38) 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 (4.38) 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 4.1, 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 $(n, m) = 1$,
$|\tau(p)| \le 2p^{11/2}$
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 $Z = \{\left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right) \ |x \in \mathbb{R}^\times\}$ is the center of $G(\mathbb{R})$ and $\mathrm{O}(2)$ is the orthogonal group. The group $\mathrm{GL}_2^+(\mathbb{R})$ of matrices $\gamma = \left(\begin{smallmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{smallmatrix}\right)$ with positive determinant acts on $\mathbb{H}$ by fractional linear transformations; on cosets (4.40) 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 $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ 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 [La76], [Ma-Pa05]

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*

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

(prime denoting $(m_1, m_2) \neq (0, 0)$). For these series the automorphy condition (4.41) can be deduced straight from the definition. One has $G_k(z) \equiv 0$ for odd k and

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

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:

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

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 [Serre70].

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 $E_4 = 1 + 240h_4$ and $E_6 = 1 - 504h_6$.

Computing with PARI-GP see [BBBCO], 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 [Sloane])

```
 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.
```

Let $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}}_p$ denote the completion of an algebraic closure of the field $\mathbb{Q}_p$ of p-adic numbers. Fix a positive integer N, a Dirichlet character $\psi \bmod N$ and consider the commutative profinite group

$$Y = Y_{N,p} = \varprojlim_m (\mathbb{Z}/Np^m\mathbb{Z})^*$$

and its group $X = \mathrm{Hom}_{cont}(Y, \mathbb{C}_p^\times)$ of (continuouos) p-adic characters (this is a $\mathbb{C}_p$-analytic Lie group analogous to $\mathrm{Hom}_{cont}(\mathbb{R}_+^\times, \mathbb{C}^\times) \cong \mathbb{C}$ (by $s \mapsto (y \mapsto y^s)$). The group X is isomorphic to a finite union of discs $U = \{z \in \mathbb{C}_p \mid |z|_p < 1\}$.
The p-adic L-function $L : X \to \mathbb{C}_p$ is a meromorphis function on X coming from a p-adic measure on Y.

1. Traditional method

of constructing these functions is from the special critical values of complex L-functions (which are often algebraic, after a suitable normalisation). Let us fix an embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ in order to consider algebraic numbers as p-adic numbers.

Example 1.1. *The Riemann zeta function.*

$$\zeta(s) = \prod_{l\ primes} (1 - l^{-s})^{-1} \quad = \sum_{n=1}^{\infty} n^{-s} \ (\mathrm{Re}(s) > 1),\ \zeta(1-k) = -\frac{B_k}{k}\ ,$$

where B_k are the Bernoulli numbers given by

$$e^{Bt} = \sum_{n=0}^{\infty} \frac{B_n t^n}{n!} = \frac{t\, e^t}{e^t - 1}\ .$$

Put for $c > 1$ coprime to p

$$\zeta_{(p)}^{(c)}(-k) = (1 - p^k)(1 - c^{k+1})\zeta(-k)$$

Theorem 1.2 (Kummer). *For any polynomial $h(x) = \sum_{i=0}^n \alpha_i\, x^i \in \mathbb{Z}_p[x]$ over $\mathbb{Z}_p$ such that $x \in \mathbb{Z}_p \Longrightarrow h(x) \in p^m\mathbb{Z}_p$ one has*

$$\sum_{i=0}^{n} \alpha_i\, \zeta_{(p)}^{(c)}(-i) \in p^m\mathbb{Z}_p \tag{1.1}$$

This property expresses the fact that the numbers $\zeta_{(p)}^{(c)}(-k)$ depend continuously on k in the p-adic sense:

Corollary 1.3. *Let $k_1, k_2 \in \mathbf{N}^*$, $k_1 \equiv k_2 \ (\mathrm{mod}(p-1)p^{m-1})$, then*

$$\zeta_{(p)}^{(c)}(-k_1) \equiv \zeta_{(p)}^{(c)}(-k_2) \ (\mathrm{mod} p^m)$$

Indeed, it suffices to take $h(x) = x^{k_1} - x^{k_2}$.

Proof of Theorem 1.1 is implied by the well-known formula:

$$S_k(N) = \sum_{n=1}^{N-1} n^k \quad = \quad \frac{1}{k+1}[B_{k+1}(N) - B_{k+1}] \tag{1.2}$$

in which $B_k(x) = (x+B)^k = \sum_{i=0}^{k} \binom{k}{i} B_i x^{k-i}$ is the Bernoulli polynomial.

Definition 1.4. *a) Let A be a normed topological ring containing $\mathbb{Z}_p$ as a closed subring and let h be a positive integer. Consider the A-submodule $\mathcal{C}^h(Y, A)$ of all locally polynomial functions of degre $< h$ on Y (of the variable $y_p : Y \to \mathbb{Z}_p^*$, the canonical projection); in particular, the A-submodule $\mathcal{C}^1(Y, A)$ consists of locally constant functions on Y with values in A. If $A = \mathbb{C}_p$ then*

$$\forall h > 1 \;\; \mathcal{C}^h(Y, A) \subset \mathcal{C}^{\mathrm{loc-an}}(Y, A) = \{\varphi : Y \to A \mid \varphi \text{ locally analytic}\} \subset \mathcal{C}(Y, A),$$

where $\mathcal{C}(Y, A) = \{\varphi : Y \to A \mid \varphi \text{ continuous}\}$.

b) A distribution Φ on Y with values in a normed A-module V is an A-linear map $\Phi : \mathcal{C}^1(Y, A) \to V$, $\varphi \mapsto \int_Y \varphi \, d\mu$.

c) A measure $\Phi : \mathcal{C}^1(Y, A) \to V$ is a bounded distribution: $|\Phi(\varphi)|_p < C|\varphi|_p$ where C does not depend on ϕ.

d) Let $h \in \mathbf{N}^*$. An h-admissible measure on Y with values in V is an A-linear map $\tilde{\Phi} : \mathcal{C}^h(Y, A) \to V$ with the following growth condition: for all $t = 0, 1, \ldots, h-1$,

$$\left| \int_{a+(Np^m)} (y_p - a_p)^t d\tilde{\Phi} \right|_p = o\left(p^{m(h-t)}\right).$$

for $m \to \infty$.

If $A = \mathbb{C}_p$ then according to [AV] and [Vi76], such a map $\tilde{\Phi}$ can be uniquely extended to the A-module $\mathcal{C}^{\mathrm{loc-an}}(Y, A)$ of locally analytic functions on$Y$ of the parameter $y_p : Y \to \mathbb{Z}_p^\times$.

Theorem 1.5 (Mazur). *There exists a unique (bounded) measure $\mu^{(c)}$ on $\mathbb{Z}_p^\times$ with values in $\mathbb{Z}_p$ such that*

$$\int_{\mathbb{Z}_p^\times} x^k d\mu^{(c)} = \zeta_{(p)}^{(c)}(-k), \quad k \geq 0$$

Remark. Theorem 1.2 is equivalent to Theorem 1.5 (by integration of h against $\mu^{(c)}$).

In the present paper we construct p-adic distributions on Y with values in $\mathbb{C}_p$ starting from distributions with values in spaces of modular forms.

The p-adic L-function of Kubota-Leopoldt is the meromorphic function $L_p : X \to \mathbb{C}_p^\times$ given by

$$L_p(x) := \frac{\int_Y x d\mu^{(c)}}{1 - x(c)c}, \quad x \in X \tag{1.3}$$

(with a single simple pole at $x = y_p^{-1}$), and the function (1.3) is independent of a choice of c: for all Dirichlet characters $\chi \bmod p^m$, $\chi : \mathbb{Z}_p^\times \to \overline{\mathbb{Q}}^\times \hookrightarrow \mathbb{C}_p^\times$ one has

$$L_p(\chi y_p^k) = (1 - \chi(p)p^k)L(-k, \chi) \in i_p(\mathbb{Q}^{\mathrm{ab}}).$$

In general every distribution on Y with values in $\mathbb{Z}_p$ defines a p-adic L-function (the non-Archimedian Mellin transform of μ):

$$L_\mu : X \to \mathbb{C}_p, \quad \mu(x) = \int_Y x(y)\, d\mu.$$

If $\mathcal{D}(s, \chi) = \sum_{n\geq 1} \chi(n)c_n n^{-s}$ is an arithmeticaly defined complex L-function twisted with a Dirichlet character χ with the property $\mathcal{D}^*(-k, \chi) \in \overline{\mathbb{Q}}$ for an infinite set of couples k, χ (and with a normalization $\mathcal{D}^*(s, \chi)$ obtained by multiplying $\mathcal{D}(s, \chi)$ with certain elementary factors), one constructs usualy the corresponding p-adic L-function $L = L_{\mu_\mathcal{D}}$ starting from the algebraic special values $\mathcal{D}^*(-k, \chi)$ in such a way that

$$L_{\mu_\mathcal{D}}(\chi y_p^k) = \int_Y \chi y_p^k \, d\mu_\mathcal{D} = i_p(\mathcal{D}^*(-k, \chi)),$$

and the existence of such a measure is equivalent to generalized Kummer congruences for the special values $\mathcal{D}^*(-k, \chi)$. Formulas for these values could be quite complicated and one uses various methods in order to obtain such congruences (like the formulas of type (1.2) in the proof of the Theorem 1). For modular forms one uses geometric tools like modular symbols, continuous fractions, the Rankin-Selberg method etc., (voir [Man73], [Ra52], [Man-Pa], [PLNM]).

We propose a new method which produces a family of p-adic measures starting from a distribution Φ on Y with values in a suitable vector space $\mathcal{M} = \bigcup_{m\geq 0} \mathcal{M}(Np^m)$ of modular forms; this family of p-adic measures $\mu_{\alpha,\Phi,f}$ is parametrized by non-zero eigenvalues $\alpha \in \mathbb{C}_p \neq 0$, of the operator U of Atkin-Lehner on $\mathcal{M}$, and by a primitive cusp eigenform f with an associated eigenvalue $\alpha \neq 0$ (on an easy modification f_0 of f as an eigenfunction). One says that a primitive cusp eigenform $f = \sum_{n\geq 1} a(n, f)e(nz) \in \mathcal{S}_k(\Gamma_0(N), \psi) \subset \mathcal{M}$ (where $(e(nz) = \exp(2\pi i n z)))$ is associated to an eigenvalue α if there exists a cusp form $f_0 = f_{0,\alpha} = \sum_{n\geq 1} a(n, f_0)e(nz)$ such that $f_0 \mid U = \alpha f_0$ and $f_0 \mid T(\ell) = a(\ell) f_0$ for all prime numbers $\ell \nmid Np$)

In the ordinary case $|\alpha|_p = 1$ a construction of such measures could be obtained from Hida's idempotent $e = \lim_{r\to\infty} U(p)^{r!}$ (see Hida [Hi93]) acting on p-adic modular forms; the image of e is contained in a subspace $\mathcal{M}^{\mathrm{ord}} \subset \mathcal{M}$ of finite dimension ("the ordinary part of $\mathcal{M}$") which is known to be generated by certain classical modular forms. One obtains $\mu_{\alpha,\Phi,f} = \ell_f(e\Phi)$ for a suitable linear form $\ell_f \in \mathcal{M}^{\mathrm{ord}\,*}$. In a more general case when $\alpha \neq 0$ one could imitate this method using instead of $\mathcal{M}^{\mathrm{ord}}$ the primary (characteristic) subspace $\mathcal{M}^{\alpha} \subset \mathcal{M}$ of U (which is also of finite dimension).

2. Distributions with values in modular forms

Let A be an algebraic extension K of $\mathbb{Q}_p$ or its ring of integers $\mathcal{O}_K$. Let us fix an embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ and let $\mathcal{M}_k(\Gamma_1(N); A)$, $\mathcal{M}_k(\Gamma_0(N)\psi; A)$ be the submodules of $A[[q]]$ generated by the q-expansions $f = \sum_{n\geq 0} a_n(f)q^n \in \mathcal{M}_k(\Gamma_1(Np^m), \overline{\mathbb{Q}})$ of classical modular forms with algebraic Fourier coefficients $a_n(f) \in \overline{\mathbb{Q}}$ in $i_p^{-1}(A)$. One puts $\mathcal{M} = \cup_{m\geq 0}\mathcal{M}(Np^m)$, where $\mathcal{M}(Np^m) = \mathcal{M}_k(\Gamma_1(Np^m); A)$, and $\mathcal{S} = \cup_{m\geq 0}\mathcal{S}(Np^m)$ the A-submodule of cusp forms.

Examples of distributions with values in $\mathcal{M}$.
Let $\Phi : \mathcal{C}^1(Y, \mathbb{C}_p) \to \mathcal{M}$ be a distribution on Y with values in $\mathcal{M}$.
a) *Eisenstein distributions.* For a complex number $s \in \mathbb{C}$ and $a, b \bmod N$ put (by analytic continuation):

$$E_{\ell,N}(z, s; a, b) = \sum (cz + d)^{-\ell}|cz + d|^{-2s} \quad (0 \neq (c, d) \equiv (a, b) \bmod N)\ .$$

Starting from this series , one obtains the following Eisenstein distributions: put $s = -r$, $0 \leq r \leq \ell - 1$,

$$E_{r,\ell,N}(a, b) := \frac{N^{\ell-2r-1}\Gamma(\ell - r)}{(-2\pi i)^{\ell-2r}(-4\pi y)^r} \sum_{a \bmod N} e(-ax/N)E_{\ell,N}(Nz, -r; x, b)$$
$$= \varepsilon_{r,\ell,N}(a, b) + (4\pi y)^{-r} \sum_{0<dd', d\equiv a, d'\equiv b \bmod N} \operatorname{sgn} d \cdot d^{\ell-2r-1}W(4\pi dd'y, \ell - r, -r)$$
$$\cdot\, e(dd'z) \in \mathcal{M}_{r',\ell}(N), \text{ where } r' = \max(r, \ell - r - 1)\ ,$$

$$W(y, \ell{-}r, -r) = \sum_{j=0}^{r}(-1)^j \binom{r}{j} \frac{\Gamma(\ell - r)}{\Gamma(\ell - r - j)} y^{r-j}\ ,$$

$$\zeta(s; a, N) = \sum_{\substack{n\geq 1\\ n\equiv a (\bmod N)}} n^{-s}\ ,$$

$$\varepsilon_{r,\ell,N}(a, b) = \frac{(-4\pi y)^s\Gamma(\ell + s)}{\Gamma(\ell + 2s)} \delta\Big(\frac{b}{N}\Big)\zeta(1 - \ell - 2s; a, N)\Big|_{s=-r}$$
$$+ \frac{\Gamma(\ell + 2s - 1)}{(4\pi y)^{\ell+s-1}\Gamma(s)} \delta\Big(\frac{a}{N}\Big) \Big[\zeta(\ell + 2s - 1; b, N) + (-1)^{\ell+2s}\zeta(\ell + 2s - 1; -b, N)\Big]\Big|_{s=-r}$$

These series are in general nearly holomorphic modular forms (see Section 7) in spaces $\mathcal{M}_{r',\ell}(N^2)$, where $r' = \max(r, \ell - r - 1)$ but in certain cases they are holomorphic, e.g. $\ell \geq 3$, $r = 0$ or $r = l - 1$) and these series produce distributions on $Y \times Y$ with values in $\mathcal{M}$:

$$E_{r,\ell}((a + (Np^m) \times (b + (Np^m)) := E_{r,\ell,Np^m}(a, b) \in \mathcal{M}_l(N^2p^{2m}).$$

b) *Partial modular forms.* For any $f = \sum_{n \geq 0} a_n(f)q^n \in \mathcal{M}_k(\Gamma_1(Np^m)$ one puts

$$\Phi_f(a + (Np^m)) := \sum_{\substack{n \geq 0 \\ n \equiv a (\bmod p^m)}} a_n(f)q^n \in \mathcal{M}_k(Np^{2m})$$

c) *Partial theta series* (also with a spherical polynomial), see [Hi85].

Remarks. i) For any Dirichlet character χ mod p^m viewed as a function on Y with values in $i_p(\mathbb{Q}^{\text{ab}})$, the integral

$$\int_Y \chi(y)\, d\Phi_f = \Phi_f(\chi) = \sum_{n \geq 0} \chi(n)a_n(f)q^n \in \mathcal{M}_k(N^2p^{2m})$$

coincides then with the twisted modular form f_χ.
ii) The distributions a), b), c) are bounded (after a regularisation of the constant term in a)) with respect to the p-adic norm on $\mathcal{M} = \cup_{p^m}\mathcal{M}_k(\Gamma_1(Np^m), A) \subset A[[q]]$ given by $|g|_p = \sup_n |a(n, g)|_p$ for $g = \sum_{n \geq 0} a(n, g)g^n \in \mathcal{M}_k(\Gamma_1(N), A)$).
iii) Starting from distributions a), b), c) one can construct many other distributions, for example, using the operation of convolution on Y (as in [Hi85], where the case of the convolution of a theta distribution with an Eisenstein distribution was considered).

However we need distributions μ with scalar values (in $\mathbb{Z}_p$ or in $\mathbb{C}_p$) which we construct starting from distributions Φ with values in $\mathcal{M}$. This will be done in two steps:
The first step is the passage from $\mathcal{M}$ to a certain finite-dimensional part $\mathcal{M}^\circ \subset \mathcal{M}$; one uses a suitable projector $\pi : \mathcal{M} \to \mathcal{M}^\circ$ such that one can keep track of denominators when the level of modular forms grows.
The second step is to apply a suitable linear form to the distribution $\pi(\Phi)$ in order to obtain the special values of the L-functions as certain p-adic integrals against the measure $\pi(\Phi)$.

3. First step: projectors on finite dimensional subspaces

The first idea would be to use *the trace operator*

$$Tr_N^{Np^m} f = \sum_{\gamma \in \Gamma_0(Np^m)\backslash\Gamma_0(N)} f \mid_k \gamma.$$

One obtains after a normalisation a projector

$$\pi(f) = [\Gamma_0(N) : \Gamma_0(Np^m)]^{-1} Tr_N^{Np^m} f$$

which is well defined but which introduces inacceptable denominators.

The second idea is to use the operator $U = U_p$ of Atkin-Lehner which acts on $\mathcal{M}$ and on $\mathcal{S}$ by $g \mid U = \sum_{n\geq 0} a(pn, g)q^n$, where $g = \sum_{n\geq 0} a(n, g)q^n \in \mathcal{M} \subset A[[q]]$, $a(n, g) \in A$.

Let $\alpha \in \mathbb{C}_p$ be a non-zero eigenvalue of $U = U_p$ on $\mathcal{M}$, associated to a primitive cusp eigenform $f = \sum_{n\geq 1} a(n, f)e(nz) \in \mathcal{S}_k(\Gamma_0(N), \psi) \subset \mathcal{M}$.

In the ordinary case $|\alpha|_p = 1$ there exists a p-adic construction of a projector π given by Hida's idempotent $e = \lim_{r\to\infty} U(p)^{r!}$ acting on p-adic modular forms, whoses image is in the finite dimensional subspace $\mathcal{M}^{\mathrm{ord}} \subset \mathcal{M}$ ("the ordinary part of $\mathcal{M}$"). Then one gets $\mu_{\alpha,\Phi,f} = \ell_f(e\Phi)$ with a suitable p-adic linear form $\ell_f \in \mathcal{M}^{\mathrm{ord}\,*}$.

4. A new construction

It provides a rather simple method which attaches to a distribution Φ on Y with values in a suitable vector space

$$\mathcal{M} = \bigcup_{m\geq 0} \mathcal{M}(Np^m)$$

of modular forms, a family $\mu_{\alpha,\Phi,f}$ of p-adic measures on Y parametrized by non-zero eigenvalues α associated with primitive cusp eigenforms f. This construction does not use any p-adic limit procedure and in fact it uses only standard linear algebra considerations in the finite dimensional primary (characteristic) subspace of the eigenvalue α.

Definition 4.1. *a) For an $\alpha \in A$ put $\mathcal{M}^{(\alpha)} = \mathrm{Ker}(U - \alpha I)$ the A-submodule of $\mathcal{M}$ of eigenfunctions of the A-linear operator U (of the eigenvalue α).*

b) Put $\mathcal{M}^{\alpha} = \cup_{n\geq 1} \mathrm{Ker}(U - \alpha I)^n$ the α-primary (characteristic) A-submodule of $\mathcal{M}$.

c) Put $\mathcal{M}^{\alpha}(Np^m) = \mathcal{M}^{\alpha} \cap \mathcal{M}(Np^m)$, $\mathcal{M}^{(\alpha)}(Np^m) = \mathcal{M}^{(\alpha)} \cap \mathcal{M}(Np^m)$.

Proposition 4.2. *Let $A = \overline{\mathbb{Q}}_p$. Define $N_0 = Np$, then $U^m(\mathcal{M}(N_0p^m)) \subset \mathcal{M}(N_0)$.*

Proof follows from a known formula [Se73],

$$U^m = p^{m(k/2-1)} W_{N_0p^m} \mathrm{Tr}^{N_0p^m}_{N_0} W_{N_0},$$

where $g|_k W_N(z) = (\sqrt{N}z)^{-k} g(-1/Nz) : \mathcal{M}(N) \to \mathcal{M}(N)$ the main involution of level N (over the complex numbers).

Proposition 4.3. *Let $A = \overline{\mathbb{Q}}_p$ and let α be a non-zero element of A; hence*

a) $(U^{\alpha})^m : \mathcal{M}^{\alpha}(N_0p^m) \xrightarrow{\sim} \mathcal{M}^{\alpha}(N_0p^m)$ is an invertible $\overline{\mathbb{Q}}_p$-linear operator.

b) The $\overline{\mathbb{Q}}_p$-vector subspace $\mathcal{M}^{\alpha}(N_0p^m) = \mathcal{M}^{\alpha}(N_0)$ is independent of m.

c) Let $\pi_{\alpha,m} : \mathcal{M}(N_0p^m) \to \mathcal{M}^\alpha(N_0p^m)$ *the canonical projector onto the* α*-primary subspace of* U *(of the kernel* $\operatorname{Ker}\pi_{\alpha,m} = \bigcap_{n\geq 1} \operatorname{Im}(U - \alpha I)^n = \oplus_{\beta\neq\alpha}\mathcal{M}^\beta(N_0p^m)$*), then the following diagram is commutative*

$$\begin{array}{ccc} \mathcal{M}(N_0p^m) & \xrightarrow{\pi_{\alpha,m}} & \mathcal{M}^\alpha(N_0p^m) \\ {\scriptstyle U^m}\downarrow & & \downarrow{\scriptstyle \wr (U^\alpha)^m} \\ \mathcal{M}(N_0) & \xrightarrow[\pi_{\alpha,0}]{} & \mathcal{M}^\alpha(N_0) \end{array}$$

Proof. Due to the reduction theory of endomorphisms in a finite dimensional subspace over a field K, the projector $\pi_{\alpha,m}$ onto the α-primary subspace $\bigcup_{n\geq 1}\operatorname{Ker}(U - \alpha I)^n$ has the kernel $\bigcap_{n\geq 1}\operatorname{Im}(U - \alpha I)^n$ and it can be expressed as a polynomial of U with coefficients in K, hence $\pi_{\alpha,m}$ commutes with U. On the other hand, the restriction of $\pi_{\alpha,m}$ on $\mathcal{M}(N_0)$ coincides with $\pi_{\alpha,0} : \mathcal{M}(N_0) \to \mathcal{M}^\alpha(N_0)$ because its image is

$$\bigcup_{n\geq 1}\operatorname{Ker}(U - \alpha I)^n \cap \mathcal{M}(N_0) = \bigcup_{n\geq 1}\operatorname{Ker}(U\mid_{\mathcal{M}(N_0)} - \alpha I)^n,$$

and the kernel is

$$\bigcap_{n\geq 1}\operatorname{Im}(U - \alpha I)^n \cap \mathcal{M}(N_0) = \bigcap_{n\geq 1}\operatorname{Im}(U\mid_{\mathcal{M}(N_0)} - \alpha I)^n.$$

5. Distributions with values in p-adic modular forms

Let $g = \sum_{n\geq 0} a(n,g)g^n \in \mathcal{M}_k(\Gamma_1(N), A)$ then $|g|_p = \sup_n |a(n,g)|_p$ is a well-defined p-adic norm on

$$\mathcal{M} = \cup_{m\geq 0}\mathcal{M}_k(\Gamma_1(Np^m), A) \subset A[[q]].$$

Let us denote by $\overline{\mathcal{M}}$ the completion of $\mathcal{M}$ in $A[[q]]$ with respect to this norm. Let V be a normed A-module.

Theorem 5.1. *Let* $\alpha \neq 0$ *be a non-zero eigenvalue of the operator* U *on the* A*-module* $\mathcal{M}$*. The* α*-primary part* Φ^α *of a distribution on* Y *with values in* $\mathcal{M}$ *is given by* $\int_Y \varphi\Phi^\alpha := (U^\alpha)^{-m}\pi_{\alpha,0}\Big(\big(\int_Y \varphi\ d\Phi\big) \mid U^m\Big) \in \mathcal{M}^\alpha$ *for all* $\varphi \in \mathcal{C}^1(Y, A)$ *and for all* p^m *sufficiently large so that* $\int_Y \varphi\ d\Phi$ *is a finite linear combination in* $\mathcal{M}(N_0p^m)$*).*

Put $\Phi(a+(Np^m)) = \int_Y \chi_{a+(Np^m)}d\Phi$ *where* $\chi_{a+(Np^m)}$ *denotes the characteristic function of an open subset* $a+(Np^m) \subset Y$ *; hence there exists* $m' \in \mathbf{N}$ *such that*

$$\Phi(a + (Np^m)) = \Phi(\chi_{(a+(Np^m))}) \in \mathcal{M}(Np^{m'+1}),$$

and the α*-primary part* Φ^α *of* Φ *is defined by*

$$\Phi^\alpha(a + (Np^m)) = (U^\alpha)^{-m'}\left[\pi_{\alpha,0}(\Phi(a + (Np^m)) \mid U^{m'}\right]. \qquad (5.1)$$

6. Main theorems

Let Φ be a bounded distribution with values in $\mathcal{M}$ and α an eigenvalue of U on $\mathcal{M}$.

Theorem 6.1. *If $|\alpha|_p = 1$ then Φ^α is a bounded distribution on Y with values in $\mathcal{M}^\alpha$ (an A-module of finite rank).*

Theorem 6.2. *Suppose that for all $m \in \mathbf{N}^*$ and for $t = 0, 1, \ldots, h\varkappa - 1$*

$$\int_{a+(N_0p^m)} y_p^t \, d\Phi \in \mathcal{M}(N_0 p^{\varkappa m}) \text{ (with } h = [\operatorname{ord}_p \alpha] + 1) \tag{6.1}$$

for a suitable non-negative integer $\varkappa$ (the condition of the modularity of a suitable level). Then there exists an $h\varkappa$-admissible distribution $\tilde{\Phi}^\alpha$ on Y with values in $\mathcal{M}^\alpha$ such that for all m' sufficiently large (with $m' \geq \varkappa m$) and for all $t = 0, 1, \ldots, h\varkappa - 1$ one has

$$\int_{a+(N_0p^m)} y_p^t d\tilde{\Phi}^\alpha = (U^\alpha)^{-m'} \pi_{\alpha,0} \left(\left(\int_{a+(N_0p^m)} y_p^t d\Phi \right) \mid U^{m'} \right).$$

Remark. If $A = \overline{\mathbb{Q}}_p$ then the condition of the theorem 4 is equivalent to $\int_Y \chi y_p^t d\Phi \in \mathcal{M}(N_0 p^{m\varkappa})$ for all Dirichlet characters $\chi \bmod N_0 p^m$ (with values in A) because

$$\int_{a+(N_0p^m)} y^t \, d\Phi = \frac{1}{\varphi(N_0p^m)} \sum_{\chi \bmod N_0p^m} \chi^{-1}(a) \int_Y \chi y_p^t \, d\Phi.$$

Proof of Theorem 6.1. It suffices to show that for a constant $C > 0$ and for all the open subsets of type $a + (Np^m) \subset Y$ one has $|\Phi^\alpha(a + (Np^m))|_p \leq C$. By our assumption there exists $m' \in \mathbf{N}$ such that

$$\Phi(a + (Np^m)) = \Phi(\chi_{(a+(Np^m))}) \in \mathcal{M}(Np^{m'+1}),$$

then the α-primary part Φ^α of Φ is given by (5.1):

$$\Phi^\alpha(a + (Np^m)) = (U^\alpha)^{-m'} \left[\pi_{\alpha,0}(\Phi(a + (Np^m)) \mid U^{m'} \right].$$

On the α-primary subspace $\mathcal{M}^\alpha \subset \mathcal{M}$ one has $U^\alpha = \alpha I + Z$ for a nilpotent p-integral operator Z: for all $g = \sum_{n \geq 0} a(n, g) q^n \in \mathcal{M}$, $g \mid U = \sum_{n \geq 0} a(pn, g) q^n$, $|g \mid U|_p \leq |g|_p$ and $|g \mid Z|_p \leq |g|_p$.

Next all the functions $\Phi^\alpha(a+(Np^m)) = \alpha^{-m}(\alpha(U^\alpha)^{-1})^m \left[\pi_{\alpha,0}(\Phi(a + (Np^m)) \mid U^m\right]$ are bounded because $|\alpha^{-1}|_p = 1$ and

$$(\alpha(U^\alpha)^{-1})^m = (\alpha^{-1}U^\alpha)^{-m} = (I + \alpha^{-1}Z)^{-m} = \sum_{j=0}^{n-1} \binom{-m}{j} \alpha^{-j} Z^j. \tag{6.2}$$

Proof of Theorem 6.2. Let $\mathrm{ord}_p\,\alpha > 0$ and let $h = [\mathrm{ord}_p\,\alpha] + 1$. Hence one has to bound

$$\int_{a+(N_0p^m)} (y_p - a_p)^t \, d\tilde{\Phi}^\alpha = \alpha^{-m\varkappa}(\alpha(U^\alpha)^{-1})^{m\varkappa}\left[\pi_{\alpha,0}\left(\int_{a+(N_0p^m)} (y_p - a_p)^t \, d\Phi\right) \mid U^\alpha\right].$$

The norms of the operators

$$(\alpha(U^\alpha)^{-1})^{\varkappa m} = (\alpha^{-1}U^\alpha)^{-\varkappa m} = \sum_{j=0}^{n-1}\binom{-\varkappa m}{j}\alpha^{-j}Z^j$$

are uniformly bounded by $C_1 > 0$ as $n = \dim \mathcal{M}^\alpha$ does not depend on m. Hence for all $t = 0, 1, \ldots, h\varkappa - 1$ one has

$$\left|\int_{a+(N_0p^m)} (y_p - a_p)^t \, d\tilde{\Phi}^\alpha\right|_p \le C_1 \cdot |\alpha|_p^{-m\varkappa} \cdot \mathrm{Max}_{y\in a+(N_0p^m)}\, |y_p - a_p|^t \cdot |\Phi|_p$$

$$\le C_1 \cdot C_2 |p^m|^{t-\mathrm{ord}_p\,\alpha\cdot\varkappa} = o(p^{m(h\varkappa - t)}),\ \ h > \mathrm{ord}_p\,\alpha$$

as $m \to \infty$ (because $|\Phi|_p \le C_2$ and $|\alpha|_p^{-m} = p^{m\,\mathrm{ord}_p\,\alpha}$).

7. Nearly holomorphic p-adic modular forms of type $r \ge 0$

Let us specialize us now to the case when A is either an algebraic extension K of $\mathbb{Q}_p$ or the ring $\mathcal{O}_K$ of integers of K. Fix an embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \widehat{\overline{\mathbb{Q}}}_p = \mathbb{C}_p$. Let r be a non-negative integer and q, ω two variables (over the complex numbers $q = e(z) = e^{2\pi i z}$, $\omega = 4\pi y = 4\pi\,\mathrm{Im}(z)$, $z \in \mathbb{C}$). In the ring $A[[q]][\omega^{-1}]$ let us consider the $A[[q]]$-submodules $P_r(A) = \left\{g = \sum_{j=0}^r \omega^{-j} g_j \text{ with } g_j = \sum_{n\ge0} a(j,n,g)q^n \in A[[q]]\right\}$. Consider also for any positive integer a the complex vector spaces of nearly holomorphic functions (see [Hi85]) $Q_{r,a} = \left\{\sum_{j=0}^r \mathrm{Im}(4\pi z)^{-j} g_j(z) \text{ with } g_j = \sum_{n\ge0} a(j,n,g)e(nz/a)\right\}$ and put $Q_r = \cup_{a\ge1} Q_{r,a}$.

Theorem 7.1. *a) The A-module $\mathcal{M}_{r,k}(\Gamma_1(N), A) \subset A[[q_1]][\omega^{-1}]$ of modular forms of type $r \ge 0$ and of weight $k \ge 1$ for $\Gamma_1(N)$ is generated by the series $g \in \mathcal{M}_{r,k}$ with algebraic coefficients $a(j,n,g) \in i_p(\overline{\mathbb{Q}})$ such that the correspondent complex series (denoted also g)*

$$g = i_p^{-1}(g) = \sum_{j=0}^r \mathrm{Im}(4\pi z)^{-j} \sum_{n\ge0} i_p^{-1}(a(j,n,g))e(nz) \in Q_{r,1}$$

satisfy to two conditions: $\forall\gamma \in \Gamma_1(N)$, $g|_k\gamma = g$ and $\forall\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $g|_k\gamma \in Q_r$.

b) Put $\mathcal{M}_{r,k} = \mathcal{M}_{r,k}(N,p) = \cup_{m\ge0}\mathcal{M}_{r,k}(Np^m)$, where $\mathcal{M}_{r,k}(Np^m) = \mathcal{M}_{r,k}(\Gamma_1(Np^m), A)$.

8. Example: real analytic Eisenstein series of weight $\ell > 0$

(see [Ka76])| For $s \in \mathbb{C}$ and $a, b \bmod N$ define (as in Section 2) the Eisenstein series:

$E_{\ell,N}(z,s;a,b) = \sum (cz+d)^{-\ell}|cz+d|^{-2s} \quad (0 \neq (c,d) \equiv (a,b) \bmod N)$.

Starting from this series one obtains the following Eisenstein distribution with values in nearly holomorphic forms (for all $s = -r$ with $0 \leq r \leq \ell - 1$):

$$E_{r,\ell,N}(a,b) := \frac{N^{\ell-2r-1}\Gamma(\ell-r)}{(-2\pi i)^{\ell-2r}(-4\pi y)^r} \sum_{a \bmod N} e(-ax/N)E_{\ell,N}(Nz,-r;x,b)$$

$$= \varepsilon_{r,\ell,N}(a,b) + (4\pi y)^{-r} \sum_{\substack{0<dd', d\equiv a \\ d'\equiv b \bmod N}} \operatorname{sgn} d\cdot d^{\ell-2r-1} W(4\pi dd'y, \ell-r, -r)$$

(8.1)

$$\cdot e(dd'z) \in \mathcal{M}_{r',\ell}(N^2),$$

where $r' = \max(r, \ell - r - 1)$,

$$W(y,\ell-r,-r) = \sum_{j=0}^{r} (-1)^j \binom{r}{j} \frac{\Gamma(\ell-r)}{\Gamma(\ell-r-j)} y^{r-j} \ , \ \zeta(s;a,N) = \sum_{\substack{n\geq 1 \\ n\equiv a (\bmod N)}} n^{-s} \ ,$$

$$\varepsilon_{r,\ell,N}(a,b) = \frac{(-4\pi y)^s\Gamma(\ell+s)}{\Gamma(\ell+2s)} \delta\Big(\frac{b}{N}\Big)\zeta(1-\ell-2s;a,N)\Big|_{s=-r}$$
$$+ \frac{\Gamma(\ell+2s-1)}{(4\pi y)^{\ell+s-1}\Gamma(s)} \delta\Big(\frac{a}{N}\Big)\Big[\zeta(\ell+2s-1;b,N) + (-1)^{\ell+2s}\zeta(\ell+2s-1;-b,N)\Big]\Big|_{s=}$$

9. Distributions with values in nearly holomorphic p-adic modular forms of type $r \geq 0$

Let $g = \sum_{j=0}^{r} \omega^{-j} \sum_{n\geq 0} a(j,n,g)q^n \in \mathcal{M}_{r,k} \subset A[[q]][\omega^{-1}]$. Put $|g|_p = \sup_{n,j} |a(j,n,g)|_p$. One has a p-adic norm on $\mathcal{M}_{r,k}$.

Let α be an eigenvalue of U on $\mathcal{M}_{r,k}$, $g|U^m = p^{m(k/2-1)} \sum_{u \bmod p^m} g|\left(\begin{smallmatrix}1 & u\\ 0 & p^m\end{smallmatrix}\right) = p^{-m}\sum_{u \bmod p^m} g\Big(\frac{z+u}{p^m}\Big)$,

$$\operatorname{Im}\Big(\frac{z+u}{p^m}\Big) = \frac{\operatorname{Im} z}{p^m} \Longrightarrow g|U^m = \sum_{j=0}^{k} \omega^{-j} p^{mj} \sum_{n\geq 0} a(j,p^m n,g)q^n$$

(an integral operator on $\overline{\mathcal{M}}_{r,k}$).

Definition 9.1. *a)* $\mathcal{M}_{r,k}^{(\alpha)} = \operatorname{Ker}(U - \alpha I)$,

b) $\mathcal{M}_{r,k}^{\alpha} = \bigcup_{n\geq 1} \operatorname{Ker}(U-\alpha I)^n$,

c) $\mathcal{M}_{r,k}^{\alpha}(Np^m) = \mathcal{M}_{r,k}(Np^m) \cap \mathcal{M}_{r,k}^{\alpha}$.

THEOREM 9.2. *a) For all $m \geq 1$ the A-module $\mathcal{M}^{\alpha}_{r,k}(N_0p^m) = \mathcal{M}^{\alpha}_{r,k}(N_0)$ is of finite rank and it does not depend on m.*

b) The following diagram is commutative (for $A = \overline{\mathbb{Q}}_p$)

$$\begin{array}{ccc} \mathcal{M}_{r,k}(N_0p^m) & \xrightarrow{\pi_{\alpha,m}} & \mathcal{M}^{\alpha}_{r,k}(N_0p^m) \\ \big\downarrow{\scriptstyle U^m} & & \big\downarrow{\scriptstyle \wr (U^{\alpha})^m} \\ \mathcal{M}(N_0) & \xrightarrow[\pi_{\alpha,0}]{} & \mathcal{M}^{\alpha}_{r,k}(N_0) \end{array}$$

($\pi_{\alpha,m}$ is the projector onto the α-primary subspace with the kernel $\bigcap_{n\geq 1} \mathrm{Im}(U-\alpha I)^n \cap \mathcal{M}_{r,k}(N_0)$ (equal to the direct sum of all the other primary subspaces; $\pi_{\alpha,m} = R_{\alpha,m}(U)$ with a suitable polynomial $R_{\alpha,m} \in A[x]$ see Proposition 4.3).

Definition 9.3. *Let $\alpha \in A$ be a non-zero eigenvalue of the operator U on $\mathcal{M}_{r,k}$ and $\Phi : \mathcal{C}^1(Y, A) \to \mathcal{M}_{r,k}$ a distribution. The α-primary part $\Phi^{\alpha} : \mathcal{C}^1(Y, A) \to \mathcal{M}^{\alpha}_{r,k}$ of Φ is given by*

$$\Phi^{\alpha}(\varphi) = U^{-m}\big[\pi_{\alpha,0}U^m(\Phi(\varphi)\big] \in \mathcal{M}^{\alpha}_{r,k}$$

for all m sufficiently large (avec $\Phi(\varphi) \in \mathcal{M}_{r,k}(N_0p^m)$).

The definition is independent of the choice of m (assumed sufficiently large) by Prop. 9.2, b).

THEOREM 9.4. *Let $|\alpha|_p = 1$ and Φ a bounded distribution with values in the A-module $\mathcal{M}_{r,k}$ of p-adic nearly holomorphic modular forms. Then the distribution Φ^{α} defined in 9.3 is also bounded.*

Proof. It is identical to that of Theorem 6.1 (in which the holomorphic case was treated).

10. h-ADMISSIBLE DISTRIBUTIONS.

Let $\Phi_j : \mathcal{C}^1(Y, A) \to \mathcal{M}_{r,k}$ be a family of distributions (non necessarily bounded, $j = 0, 1, \ldots, r^*$, $r^* \geq 1$). For any open subset $a + (Np^m) \subset Y$ put $\Phi_j(a + (Np^m)) = \Phi_j(\chi_{a+(Np^m)})$.

THEOREM 10.1. *Let $0 < |\alpha|_p < 1$ and $h = [\mathrm{ord}_p\,\alpha] + 1$. Suppose that there exists $\varkappa \in \mathbf{N}^*$ such that for all $j = 0, 1, \ldots, h\varkappa - 1$ and for all $m \geq 1$ one has $\Phi_j(a + (N_0p^m)) \in \mathcal{M}_{r,k}(N_0p^{m\varkappa})$ (the level condition). Suppose next that for $t = 0, 1, \ldots, h\varkappa - 1$ and for all $a + (Np^m) \subset Y$ one has*

$$|U^{\varkappa m} \sum_{j=0}^{t} \binom{t}{j} (-a_p)^{t-j} \Phi_j(a + (Np^m))|_p \leq C|p^m|_p^t = Cp^{-mt} \tag{10.1}$$

with a suitable constant $C > 0$ (the divisibility condition). Then there exists an $h\varkappa$-admissible measure $\tilde{\Phi}^{\alpha} : \mathcal{C}^{h\varkappa}(Y, A) \to \mathcal{M}^{\alpha}_{r,k} \subset \mathcal{M}_{r,k}$ such that $\int_{a+(N_0p^m)} y_p^j d\tilde{\Phi}^{\alpha} = \Phi^{\alpha}_j(a + (N_0p^m))$ (for $j = 0, 1, \ldots, h\varkappa - 1$).

Proof. It suffices to verify the condition of growth (1.1 d)) for $\Phi_j^\alpha(a + (N_0p^m)) \in \mathcal{M}_{r,k}(N_0p^{m\varkappa})$. One has $U = \alpha I + Z$, $Z^n = 0$ on $\mathcal{M}_{r,k}^\alpha(N_0)$, $n = rk_A\mathcal{M}_{r,k}^\alpha(N_0p^m; A)$.

On the other hand by the conditions of the theorem we have

$$\int_{a+(N_0p^m)} (y_p - a_p)^t d\tilde{\Phi}^\alpha = \sum_{j=0}^{t} \binom{t}{j} (-a_p)^{t-j} \Phi_j^\alpha(a + (N_0p^m))$$
$$= \alpha^{-m\varkappa}\alpha^{m\varkappa}(U^\alpha)^{-m\varkappa}\left[\pi_{\alpha,0}U^{m\varkappa}\left(\sum_{j=0}^{t}\binom{t}{j}(-a_p)^{t-j}\Phi_j(a + (N_0p^m))\right)\right].$$

The operators $\alpha^{-1}(U^\alpha)^{-m\varkappa} = \sum_{i=0}^{n-1}\binom{-m\varkappa}{i}(\alpha^{-1}Z)^i$ are uniformly bounded by a constant $C_1 > 0$ hence the condition (10.1) implies

$$\left|\int_{a+(N_0p^m)} (y_p - a_p)^t d\tilde{\Phi}^\alpha\right|_p \le C\cdot C_1|\alpha|_p^{-m\varkappa}|p^m|_p^t = o(p^{m(h\varkappa - t)})$$

when $m \to \infty$ because $|\alpha|_p = |p|^{\mathrm{ord}_p\alpha}$, $\mathrm{ord}_p\alpha < h$, $|p^m|_p^{-\varkappa\mathrm{ord}_p\alpha} = o(p^{m\varkappa h})$.

11. The second step: application of a suitable linear form

Let $\alpha \in \overline{\mathbb{Q}} \subset \mathbb{C}$ be a non-zero eigenvalue of U on $\mathcal{M}_{r,k}(\mathbb{C})$ associated with a primitive cusp eigenform $f \in \mathcal{S}_k(\Gamma_0(N), \psi)$ and let $f_0 = f_{0,\alpha}$ be a corresponding eigenfunction ($f_0|U = \alpha f_0$), let us define $f^0 = f_0^\rho|W_{N_0}$, $f_0^\rho = \sum_{n\ge1}\overline{a_n(f_0)}q^n$, $W_{N_0} = \begin{pmatrix}0 & -1\\ N_0 & 0\end{pmatrix}$.

Proposition 11.1. *a)* $U^* = W_{N_0}^{-1}UW_{N_0}$ *in the hermitian vector space* $\mathcal{S}_{r,k}(\Gamma_1(N_0), \mathbb{C})$*, the adjoint operator with respect to the Petersson scalar product.*

b) One has $f^0|U^* = \bar{\alpha}f^0$*, and for all "good" prime numbers* $l \nmid Np$ *one has* $T_lf^0 = a_l(f)f^0$.

c) The linear form $\ell_{f,\alpha} : g \mapsto \langle f^0, g\rangle$ *on* $\mathcal{M}_{r,k}(\Gamma_1(N_0), \mathbb{C})$ *vanishes on* $\mathrm{Ker}\,\pi_{\alpha,0}$*, where* $\pi_{\alpha,0} : \mathcal{M}_{r,k}(\Gamma_1(N_0), \mathbb{C}) \to \mathcal{M}_{r,k}^\alpha(\Gamma_1(N_0), \mathbb{C})$ *(the projector onto the* α*-primary subspace with the kernel* $\mathrm{Ker}\,\pi_{\alpha,0} = \mathrm{Im}(U - \alpha I)^n$*) hence*

$$\langle f^0, g\rangle = \langle f^0, \pi_{\alpha,0}(g)\rangle.$$

d) If $g \in \mathcal{M}(Np^{m+1}, \overline{\mathbb{Q}}) = \mathcal{M}(N_0p^m, \overline{\mathbb{Q}})$ *et* $\alpha \ne 0$*, one has*

$$\langle f^0, g^\alpha\rangle = \alpha^{-m}\langle f^0, g \mid U^m\rangle$$

where

$$g^\alpha = (U^\alpha)^{-m}\pi_{\alpha,0}(g \mid U^m) \in \mathcal{M}^\alpha(Np)$$

is the α*-primary part of* g.

e) One puts

$$\mathcal{L}_{f,\alpha}(g) = \frac{\langle f^0, \alpha^{-m} g|U^m\rangle_{N_0}}{\langle f^0, f_0\rangle_{N_0}},$$

hence $\mathcal{L}_{f,\alpha} : \mathcal{M}(Np^{m+1}; \overline{\mathbb{Q}}) \to \overline{\mathbb{Q}}$ *(the linear form* $\mathcal{L}_{f,\alpha}$ *sur* $\mathcal{M}_{r,k}(\Gamma_1(Np), \mathbb{C})$ *is defined over* $\overline{\mathbb{Q}}$*) and there exists a unique* A*-linear form* $\ell_{f,\alpha} \in \mathcal{M}^{\alpha}_{r,k}(N_0)^*$ *such that*

$$i_p^{-1}(\ell_{f,\alpha}(g^\alpha)) = \frac{\langle f^0, \alpha^{-m} U^m(g)\rangle_{N_0}}{\langle f^0, f_0\rangle_{N_0}}$$

($\forall g$ *with coefficients in* $i_p^{-1}(A)$*).*

Proof of Proposition 11.1 a) See [Miy], Th. 4.5.5.

b) By definition, $f^0|U^* = f_0^\rho \mid W_{Np} W_{Np}^{-1} U W_{Np} = \bar{\alpha} f_0^\rho \mid W_{Np} = \bar{\alpha} f^0$.

c) For any function

$$g_1 = (U - \alpha I)^n g \in \operatorname{Ker} \pi_{\alpha,0} = \operatorname{Im}(U - \alpha I)^n$$

one has

$$\langle f^0, g_1\rangle = \langle f^0, (U - \alpha I)^n g\rangle = \langle (U^* - \bar{\alpha} I) f^0, (U - \alpha I)^{n-1} g\rangle = 0$$

hence for $g_1 = g - \pi_{\alpha,0}(g)$ we get

$$\langle f^0, g\rangle = \langle f^0, \pi_{\alpha,0}(g) + (g - g^\alpha)\rangle = \langle f^0, \pi_{\alpha,0}(g)\rangle + \langle f^0, g_1\rangle = \langle f^0, \pi_{\alpha,0}(g)\rangle$$

d) Let us use directly the equality $(U^*)^m f^0 = \bar{\alpha}^m f^0$ of b):

$$\alpha^m \cdot \langle f^0, g^\alpha\rangle = \langle (U^*)^m f^0, U^{-m} \pi_{\alpha,0}(g \mid U^m)\rangle =$$
$$\langle f^0, \pi_{\alpha,0}(g \mid U^m)\rangle = \langle f^0, g \mid U^m\rangle$$

by c) because $g|U^m \in \mathcal{M}(Np)$.

e) Note that $\mathcal{L}_{f,\alpha}(f_0) = 1$, $f_0 \in \mathcal{M}(Np; \overline{\mathbb{Q}})$; consider the complex vector space

$$\operatorname{Ker} \mathcal{L}_{f,\alpha} = \langle f^0\rangle^\perp = \{g \in \mathcal{M}(Np; \mathbb{C}) \mid \langle f^0, g\rangle = 0\}$$

which admits a $\overline{\mathbb{Q}}$-rational basis because it is stable by the action of all "good" Hecke operators T_l ($l \nmid Np$):

$$\langle f^0, g\rangle = 0 \Longrightarrow \langle f^0, T_l g\rangle = \langle T_l^* f^0, g\rangle = 0$$

and one obtains such a basis by the diagonalisation of the action of all the T_l (a commutative family of normal operators) and e) follows.

12. Relations to the L-functions: convolutions of the Eisenstein distributions

Let $\xi \bmod N$ be an auxiliary Dirichlet character $\xi : Y \to A^*$,

$$Y \stackrel{y_p}{\to} \mathbb{Z}_p^*, \quad Y = \varprojlim Y_{Np^m},$$

$Y_{Np^m} = (\mathbb{Z}/Np^m\mathbb{Z})^*$. Consider two Eisenstein distributions

$$E_{0,\ell,Np^m}(\xi,b)=\textstyle\sum_{a\in Y_{Np^m}}\xi(a)E_{0,\ell}(a,b;Np^m)\in\begin{cases}\mathcal{M}_{0,\ell} & \text{if } \ell\ge 3 \text{ or } \xi\ne 1\\ \mathcal{M}_{1,\ell} & \text{if } \xi=1,\ell=1,2,\end{cases}$$
$$E_{r,\ell,Np^m}(a)=\textstyle\sum_{b\in Y_{Np^m}}E_{r,\ell,Np^m}(a,b)\in\mathcal{M}_{r',\ell},\qquad r'=\max(r,\ell-r-1).$$

Proposition 12.1. *Let $\chi,\psi:Y\to A^\times$ be two Dirichlet characters $\bmod Np^m$,*

a) Let $f\in\mathcal{S}_k(N,\psi)$, $k\ge 2$, define

$$\Phi_j(a)_{Np^m}=\sum_{y\in Y_{Np^m}}\psi\bar\xi(y)E_{0,k-1-j}(\xi,ya)E_{j,1+j}(y)$$

(a twisted convolution, $j=0,\dots,k-2$). Hence for any Dirichlet character $\chi \bmod Np^m$ one has

$$\Phi_j(\chi)=E_{0,k-1-j}(\xi,\chi)E_{j,1+j}(\psi\overline{\xi\chi});$$

b) the special values of the function $L_f(s,\chi)=\sum_{n\ge1}\chi(n)a_n(f)n^{-s}$ with a primitive Dirichlet character $\chi \bmod Np^m$ ($m\ge 1$) admit the following integral representation

$$\langle f^0,\Phi_j(\chi)\rangle_{Np}=\frac{G(\chi)\Gamma(j+1)L_f(k-1,\bar\xi)L_f(j+1,\overline{\chi})}{(-2\pi i)^{j+k}}\cdot t,$$

(where $G(\chi)$ is the Gauss sum of χ, $t\in\overline{\mathbb{Q}}^*$ is an explicitly given elementary constant independent of j and χ);

c) the distributions Φ_j satisfy the conditions of Theorem 6 and they produce an h-admissible measure (compare with [Vi76]) which interpolates the normalised critical values

$$\frac{\alpha^{-m}G(\chi)\Gamma(j+1)L_f(j+1,\overline{\chi})L_f(k-1,\bar\xi)}{(-2\pi i)^{j+k}\langle f,f\rangle}$$

where $\langle f,f\rangle$ denotes the normalized Petersson product.

Proof of Proposition 12.1 a) This is a general property of multiplicative convolutions.

b) Implied from the Rankin-Selberg method for the convolution

$$D(s,f,g)=L_N(2s+2-l,\psi\overline{\xi\chi})\sum_{n=1}^{\infty}a_nb_nn^{-s},$$

where ξ is an auxiliary non-trivial Dirichlet character ξ and the numbers

$$b_n=\sigma_{l-1,\bar\chi,\bar\xi}(n)=\sum_{d|n,d>0}\bar\chi(d)\bar\xi(n/d)d^{l-1}$$

are Fourier coefficients of a certain Eisenstein series $g=\sum_{n=0}^{\infty}b_n\exp(2\pi inz)$ of weight l (and of Dirichlet character $\bar\chi\bar\xi$) if $\chi\xi(-1)=(-1)^l$ so that

$$L_g(s)=\sum_{n=1}^{\infty}b_nn^{-s}=L(s-l+1,\bar\chi)L(s,\bar\xi)$$

and we know by Rankin's lemma (see [Ra52], or a general lemma of Shimura [Shi76], Lemma 1 (generalized Rankin's lemma), see also [Shi77], [Hi85], [Man-Pa]) that $D(s, f, g)$ can be expressed through $L_f(s - l + 1, \bar{\chi}) L_f(s, \bar{\xi})$. In order to get the integral representation of b), we evaluate then the function $L_f(s - l + 1, \bar{\chi}) L_f(s, \bar{\xi})$ at points $s = k - 1$, and put $l = k - j - 1$, where $1 \le l \le k - 1$).

c) One checks coefficient-by-coefficient that the distributions Φ_j satisfy the level condition and the divisibility condition of Theorem 6 with $\varkappa = 2$. Then one directly applies Theorem 6 and proposition 11.1 c), d) in order to obtain the desired h-admissible measure $\mu_{f,\alpha}$ in the form $\mu_{f,\alpha} = \ell_{f,\alpha}(\tilde{\Phi}^\alpha)$.

13. Application to triple products

Consider the vector space

$$\mathcal{M} := \bigcup_{m \ge 0} \mathcal{M}_k(\Gamma_1(Np^m))^{\otimes 3}$$

and let $L(f \otimes g \otimes h, s)$ be the triple L-function attached to $f \otimes g \otimes h \in \mathcal{S}_k(\Gamma_1(N))^{\otimes 3}$ associated with an *ordinary* eigenvalue $\alpha\beta\gamma$, hence

$$f_0 \otimes g_0 \otimes h_0 \in \mathcal{S}_k(\Gamma_1(Np))^{\otimes 3}$$

is an eigenfunction of $U^{\otimes 3}$ on $\mathcal{S}_k(\Gamma_1(Np))^{\otimes 3}$, and $f^0 \otimes g^0 \otimes h^0$ is an eigenfunction of $(U^*)^{\otimes 3}$. Let us use the restriction to the diagonal $\Phi = E_k^3(z_1, z_2, z_3) \in \mathcal{M}_k(\Gamma_1(Np))^{\otimes 3}$ of the Siegel-Eisenstein distribution (see [PIsr]) viewed as a formal Fourier series. One obtains a distribution on Y^3 with values in $\mathcal{M}$.

Put

$$l_{f \otimes g \otimes h, \alpha\beta\gamma}(\Phi) := i_p \left(\frac{\langle f^0 \otimes g^0 \otimes h^0, \Phi^{\alpha\beta\gamma} \rangle}{\langle f^0, f_0 \rangle \langle g^0, g_0 \rangle \langle h^0, h_0 \rangle} \right)$$

THEOREM 13.1. *(a work in progress with Siegfried Böcherer)] The distribution $l_{f \otimes g \otimes h, \alpha\beta\gamma}(\Phi)$ on Y^3 with values in $\mathcal{M}$ is bounded and the integrals $l_{f \otimes g \otimes h, \alpha\beta\gamma}(\Phi)(\chi_1 \otimes \chi_2 \otimes \chi_3)$ on the characters $\chi_1 \otimes \chi_2 \otimes \chi_3$ coincide with the special values $L^*(f_{\chi_1} \otimes g_{\chi_2} \otimes h_{\chi_3}, s_0)$, where the normalisation of L^* involves Gauss sums, Petersson scalar products , powers of π, $\alpha\beta\gamma$.*

Proof. The existence of $l_{f \otimes g \otimes h, \alpha\beta\gamma}(\Phi)$ follows from the existence of Φ using Theorem 3, and the equality is implied by the integral formula of Garrett-Harris [GaHa], see also [LBP], [PTr].

References

[Am-Ve] Y. AMICE, J. VÉLU, *Distributions p-Adiques associées aux Séries de Hecke*, Journées Arithmétiques de Bordeaux (Conf. Univ. Bordeaux (1974)), Astérisque N° 24/25, Soc. Math. France, Paris (1975), p 119-131.

[And74] A.N. ANDRIANOV, *Euler products attached to Siegel Modular Forms of Degree 2*, Uspekhi Mat. Nauk 29 (1974), p 44-109 (in Russian).

[And76] A.N. ANDRIANOV, *Symmetric Squares of Zeta Functions of Siegel Modular Forms of degree 2*, Trudy Steklov Math. Institut USSR. 142 (1976), p 22-45 (in Russian).

[And77] A.N. ANDRIANOV, *Euler Expansions of the Theta Transformations of Siegel Modular Forms of Degree n*, Mat. Sbornik 104 (1977), p 390-427.

[And78] A.N. ANDRIANOV, *On the Decomposition of Hecke Polynomials for the Symplectic Group of Degree n*, Mat. Sbornic 104 (1978), p. 291-341 (in Russian).

[And79] A.N. ANDRIANOV, *Multiplicative Arithmetic of Siegel Modular Forms*, Uspekhi Mat. Nauk 34 (1979), p 67-135 (in Russian).

[An-Ka] A.N. ANDRIANOV, V.L. KALININ, *On Analytic Properties of Standard Zeta Functions of Siegel Modular Forms*, Mat. Sbornik 106 (1978), p 323-339 (in Russian).

[An-Pa] A.N. ANDRIANOV, A.A.PANCHISHKIN, *Singular Frobenius operators on Siegel modular forms with characters and zeta functions*, St.-Petersbourg Math.J., vol. 12, no. 2 (2001), pp.233-257.

[Bö85] S. BÖCHERER, *Über die Funktionalgleichung Automorpher L-Funktionnen zur Siegelschen Modulgruppe*, J. reine angew. Math. 362 (1985), p 146-168.

[BöSch] S. BÖCHERER, C.-G. SCHMIDT, *p-adic measures attached to Siegel modular forms*, Ann. Inst. Fourier 50 (2000), no. 5, 1375–1443.

[Ch-Eh] YOUNGJU CHOIE, W. EHOLZER, *Rankin-Cohen operators for Jacobi and Siegel forms*, J. Number Theory 68 (1998), no. 2, 160–177.

[Co-PeRi] J. COATES, B. PERRIN-RIOU, *On p-adic L-functions attached to Motives over $\mathbb{Q}$*, Advanced Studies in Pure Math. 17 (1989), 23-54

[Co] H. COHEN, *Sums Involving the Values at Negative Integers of L- Functions of Quadratic Characters*, Math. Ann. 217 (1975), p. 271-285.

[CoPB] R. COLEMAN, *p-adic Banach spaces and families of modular forms.* Invent. Math. 127, No.3, 417-479 (1997)

[Co-Ma] R. COLEMAN, B. MAZUR, *The eigencurve. Galois representations in arithmetic algebraic geometry* (Durham, 1996), 1–113, London Math. Soc. Lecture Note Ser., 254,

[CST98] 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).

[Colm98] P. COLMEZ, *Fonctions L p-adiques*, Séminaire Bourbaki, 51 ème année, 1998–99, n° 851. Novembre 1998. Cambridge Univ. Press, Cambridge, 1998.

[Colm03] P.COLMEZ, La conjecture de Birch et Swinnerton-Dyer p-adique. Séminaire Bourbaki. [Exposé No.919] (Juin 2003)

[Cour] M. COURTIEU, *Familles d'opérateurs sur les formes modulaires de Siegel et fonctions L p-adiques*, http://www-fourier.ujf-grenoble.fr/THESE/ps /t101.ps.gz, Thèse de Doctorat, Institut Fourier, 2000, 1–122.

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

[Eh-Ib] W. EHOLZER, T. IBUKIYAMA *Rankin-Cohen type differential operators for Siegel modular forms.* , Internat. J. Math , 9 (1998) no. 4, 443–463.

[Da-De] A.DABROWSKI, D.DELBOURGO, S-adic L-functions attached to the symmetric square of a Newform Proc. London Math. Soc. (3) 74 (1997) pp. 559-611

[Eh-Ib98] E. EHOLZER, T. IBUKIYAMA, *Rankin-Cohen type differential operators for Siegel modular forms.* Internat. J. Math , 9 (1998) no. 4, 443–463.

[Fa-Ch90] 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).

[Ga-Ha] P.B.GARRETT, M.HARRIS, *Special values of triple product L–functions*, Amer. J. Math 115 (1993) 159–238.

[Go02] Bertrand GORSSE, Carrés symétriques de formes modulaires et intégration p-adique. Mémoire de DEA de l'Institut Fourier, juin 2002

[Gou-Ma] 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).

[Gue] P.GUERZHOY, *Jacobi-Eisenstein series and p-adic interpolation of symmetric squares of cusp forms*, Annales de l'Institut Fourier, 45, N3, 605-624 (1995).

[Ha1] M. HARRIS, *The Rationality of Holomorphic Eisenstein Series*, Invent. Math. 63, 305-310 (1981).

[Ha2] M. HARRIS, *Special Values of Zeta-Functions attached to Siegel Modular Forms*, Ann. Sci. Ec. Norm. Sup. 14, 77-120 (1981).

[Ha3] M. HARRIS, *Eisenstein Series on Shimura Varieties*, Ann. of Math. 119 (1984), p. 59-94.

[Hi1] 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.

[Hi2] H. HIDA, *Galois representations into $GL_2(\mathbb{Z}_p[\![X]\!])$ attached to ordinary cusp forms*, Invent. Math. 85 (1986) 545–613.

[Hi5] H. HIDA, *Elementary theory of L-functions and Eisenstein series*, London Mathematical Society Student Texts. 26 Cambridge University Press

[Hi6] H. HIDA, *p-adic ordinary Hecke algebras for* GL(2), Ann. Inst. Fourier (Grenoble) 44 (1994), no. 5, 1289–1322.

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

[JoH98] Fabienne JORY–HUGUE, *Familles de symboles modulaires et fonctions L p-adiques*, Thèse de Doctorat, Institut Fourier (Grenoble), 18 décembre 1998

[JoH04] Fabienne JORY–HUGUE, *Unicité des h–mesures admissibles p-adiques données par des valeurs de fonctions L sur les caractères*, (in preparation), Institut Fourier (Grenoble), 2005

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

[KMS2000] D. KAZHDAN, B. MAZUR, C.-G. SCHMIDT, *Relative modular symbols and Rankin-Selberg convolutions.* J. Reine Angew. Math. 519, 97-141 (2000).

[Kl67] H. KLINGEN, *Zum Darstellungssatz für Siegelsche Modulformen*, Math. Z. 102 (1967) 30–43

[Ku-Le] T. KUBOTA, H.W. LEOPOLDT, *Eine p-Adische Theorie der Zetawerte*, J. Reine Angew. Math. 214/215 (1964), p 328-339.

[LBP] Y.-H. LE BRAS, A.A. PANCHISHKIN, *Sur les produits triples Λ-adiques*, Communications in Algebra, 29 (2001) No. 9, 3727-3740.

[Maa] H. MAASS, *Siegel's Modular Forms and Dirichlet Series*, Springer-Verlag, Lect. Notes in Math. N° 216 (1971).

[Ma73] Yu.I. MANIN, *Periods of cusp forms and p-adic Hecke series*, Mat. Sbornik,
92 , 1973, pp. 378-401

[Man3] Y.I. MANIN, *Non-Archimedean Integration and p-Adic L-Functions of Jacquet-Langlands*, Uspekhi Mat. Nauk 31 (1976), p 5-54 (in Russian).

[Ma-Vi] Yu.I. MANIN, M. M.VISHIK, *p-adic Hecke series of imaginary quadratic fields*, (Russian) Mat. Sb. (N.S.) 95(137) (1974), 357-383.

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

[MTT] B. MAZUR; J. TATE; J. TEITELBAUM: On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. Invent. Math. 84, 1-48 (1986).

[Nag1] S. NAGAOKA, *A remark on Serre's example of p-adic Eisenstein series*, Math. Z. 235 (2000) 227-250.

[Nag2] S. NAGAOKA, *Note on* $\bmod p$ *Siegel modular forms*, Math. Z. 235 (2000) 405-420.

[PTr] A.A. PANCHISHKIN, *Produits triples des formes modulaires et leur interpolation p–adique par la méthode d'Amice–Vélu*, Manuscrit de l'exposé au Colloque à la mémoire d'Yvette Amice, mars, 1994, pp.1-27

[Pa94] 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.

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

[PaIAS] 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).

[PaMMJ] 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

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

[PaAD] A.A. PANCHISHKIN, *Arithmetical differential operators on nearly holomorphic Siegel modular forms*, MPIM, April 2002, MPI 2002 - 41, MPI-2002-41.dvi - MPI-2002-41.ps, 1-49.

[PaJTNB] A.A. PANCHISHKIN, *Sur une condition suffisante pour l'existence des mesures p-adiques admissibles*, Journal de Théorie des Nombres de Bordeaux, v. 15 (2003), pp. 1-24

[Puy] J. PUYDT, *Valeurs spéciales de fonctions L de formes modulaires adéliques*, Thèse de Doctorat, Institut Fourier (Grenoble), 19 décembre 2003

[Se2] 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.

[Sh71] G. SHIMURA, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press. (1971).

[Sh75] G. SHIMURA, *On the Holomorphy of certain Dirichlet Series*, Proc. Lond. Math. Soc. 31 (1975), p 79-98.

[Sh77] G. Shimura, *On the Periods of Modular Forms*, Math. Annalen 229 (1977), p 211-221.

[Sh78] G. Shimura, *The Special Values of Zeta Functions associated with Hilbert Modular Forms* Duke Math. J. 48 (1978), p 637-679.

[Sh81] G. Shimura, *Arithmetic of Differential Operators on Symetric Domains*, Duke Math. J. 48 (1981), p 813-843.

[Sh82] G. Shimura, *Confluent Hypergeometric Functions on Tube Domains*, Math. Ann. 260 (1982), p. 269-302.

[Sh83] G. Shimura, *On Eisentsein Series*, Duke Math. J; 50 (1983), p. 417-476.

[Sh2000] G. Shimura, *Arithmeticity in the theory of automorphic forms*, Mathematical surveys and monographs, **82** AMS, Providence, RI 2000, 302 p.

[Sie39] C.L. Siegel, *Einührung in die Theorie des Modulfunktionnen n-ten Grades*, Math. Ann. **116**, 617-657 (1939).

[St1] J. Sturm, *Special Values of Zeta Functions and Eisenstein Series of half integral weight*, Amer. J. Math. **102**, 219-240 (1980).

[St2] J. Sturm, *The Critical Values of Zeta-Functions associated to the Symplectic group*, Duke Math. J. **48**, 327-350 (1981).

[Ti-U] J. Tilouine, E. Urban, *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.

[Vi1] M.M. Višik, *Non-Archimedean Measures associated with Dirichlet series*, Mat. Sbornik 99 (1976), p 248-260.

[We56] 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.

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

[Za77] 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.

Institut Fourier, Université de Grenoble I
E-mail address: panchish@ujf-grenoble.fr

A motivation: why study L-values attached to modular forms?

A popular proceedure in number theory is the following:

Construct a generating function $f = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{C}[[q]]$ of an arithmetical function $n \mapsto a_n$, for example $a_n = p(n)$	$\rightsquigarrow$	Compute f via modular forms, for example $\sum_{n=0}^{\infty} p(n) q^n = (\Delta/q)^{-1/24}$	$\rightsquigarrow$	A number (solution)
		$\uparrow$		$\uparrow$
Example 1 [Chand70]: (Hardy-Ramanujan) $p(n) = \frac{e^{\pi\sqrt{2/3(n-1/24)}}}{4\sqrt{3}\lambda_n^2} + O(e^{\pi\sqrt{2/3(n-1/24)}}/\lambda_n^3)$, $\lambda_n = \sqrt{n-1/24}$,		Good bases, finite dimensions, many relations and identities		Values of L-functions, periods, congruences, ...

Other examples: Birch and Swinnerton-Dyer conjecture, ... L-values attached to modular forms

Statement of the problem of Coleman-Mazur

This talk is about the paper [PaTV] by A.P., *Two variable p-adic L functions attached to eigenfamilies of positive slope*, Invent. Math. v. 154, N3 (2003), pp. 551 - 615, and about some further developments.

The Tate field $\mathbb{C}_p$

Fix a prime p, and let $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}}_p$ be the Tate field (the completion of the field of p-adic numbers)

We fix an embedding $i_p : \overline{\mathbb{Q}} \to \mathbb{C}_p$, and view algebraic numbers as p-adic numbers via i_p.

A primitive cusp eigenform f

$f = f_k = \sum_{n\geq 1} a_n q^n \in \mathcal{S}_k(\Gamma_0(N), \psi)$, (where $q = e(z) = \exp(2\pi i z)$, $\mathrm{Im}\,(z) > 0$)

a primitive cusp eigenform $f = f_k$ of weight $k \geq 2$ for $\Gamma_0(N)$ with a Dirichlet character $\psi \pmod N$.

The special values of the L-function attached to f at $s = 1, \cdots, k-1$:

$$L_f(s,\chi) = \sum_{n\geq 1} \chi(n) a_n n^{-s},$$

(χ are Dirichlet characters)

where $1 - a_p X + \psi(p) p^{k-1} X^2$
$= (1 - \alpha_p X)(1 - \alpha'_p X)$
is the Hecke polynomial
α_p and α'_p are called
the Satake parameters of f

Periods of f Following a known theorem of Shimura [Sh59] and Manin [Ma73], there exist two non-zero complex constants $c^+(f), c^-(f) \in \mathbb{C}^\times$ (the *periods* of f) such that for all $s = 1, \cdots, k-1$ and for all Dirichlet characters χ of fixed parity, $(-1)^{k-s}\chi(-1) = \pm 1$, the normalized special values are *algebraic numbers*:

$$L^*(f,s,\chi) = \frac{(2i\pi)^{-s}\Gamma(s) L_f(s,\chi)}{c^\pm(f)} \in \overline{\mathbb{Q}}. \tag{2.1}$$

A family of slope $\sigma > 0$ of cusp eigenforms f_k of weight $k \geq 2$ containing f

$$k \mapsto f_k = \sum_{n=1}^{\infty} a_n(k) q^n \in \overline{\mathbb{Q}}[\![q]\!] \subset \mathbb{C}_p[\![q]\!]$$

1) the Fourier coefficients $a_n(k)$ of f_k and the Satake p-parameter $\alpha_p(k)$ are given by certain p-adic analytic functions $k \mapsto a_n(k)$ for $(n, p) = 1$
2) the slope is constant and positive: $\mathrm{ord}(\alpha_p(k)) = \sigma > 0$

A model example of a p-adic family (not cusp and $\sigma = 0$): Eisenstein series

$$a_n = \sum_{d|n} d^{k-1}, f_k = E_k$$

the Fourier coefficients $a_n(k)$ and one of the Satake p-parameters $\alpha_p(k) = 1$ are p-adic analytic functions, and $\mathrm{ord}_p(\alpha_p(k)) = \mathrm{ord}_p(1) = 0$

The existence of families of slope $\sigma > 0$: R.Coleman, [CoPB]

He gave an example with $p = 7$, $f = \Delta$, $k = 12$ $a_7 = \tau(7) = -7 \cdot 2392, \sigma = 1$, and a program in PARI for computing such families is contained in [CST98] (see also the Web-page of W.Stein, `http://modular.fas.harvard.edu/`)

The Problem, *see [Co-Ma] R. Coleman, B. Mazur, The eigencurve. Galois representations in arithmetic algebraic geometry, (Durham, 1996), London Math. Soc. Lecture Note Ser., 254, at p.6*

Given a p-adic analytic family $k \mapsto f_k = \sum_{n=1}^{\infty} a_n(k)q^n \in \overline{\mathbb{Q}}[\![q]\!]$ *of positive slope* $\sigma > 0$, *to construct a two-variable p-adic L-function interpolating* $L^*(f_k, s, \chi)$ *on* (s, k).

Known cases:

- One-variable case ($k = k$ is fixed, $\sigma > 0$), treated in [Am-Ve] by Y. Amice, J. Vélu, in [Vi76] by M.M. Višik, and in [MTT] by B. Mazur; J. Tate; J. Teitelbaum

- $\sigma = 0$ (H.Hida) ("ordinary families") (see in [Hi93])

- Special values of L-functions attached to families f_k of Yu.I. Manin and M. M.Vishik, [Ma-Vi] : $f_k = \sum_{\mathfrak{a} \subset \mathcal{O}_K} \lambda^{k-1}(\mathfrak{a}) q^{N\mathfrak{a}}$ and of N.M.Katz, [Kat]), which are are certain ordinary families they correspond to powers of a grössen-character λ of an imaginary quadratic field K at a *splitting prime p*, (resp. to grössencharacters of type A_0 of the idèle class group $\mathbb{A}_K^*/K^*$ (in the sense of Weil [We56],) of a CM-field K.

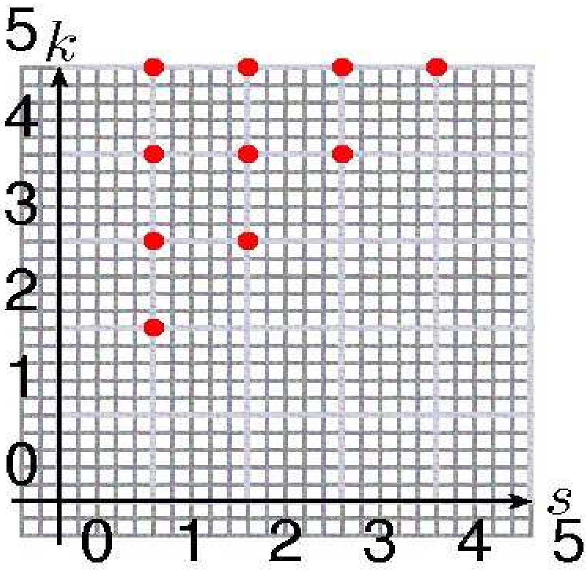
Motivation comes from the conjecture of Birch and Swinnerton-Dyer, see in [Colm03]

For a cusp eigenform $f = f_2$, corresponding to an elliptic curve E by Wiles [Wi], we consider a family containing f.

One can try to approach $k = 2, s = 1$ from the other direction, taking $k \to 2$ instead of $s \to 1$, this leads to a formul linking the derivative over s at $s = 1$ of the p-adic L-function with the derivative over k at $k = 2$ of the p-adic analytic function $\alpha_p(k)$, see in [CST98]:

$$\boxed{L'_{p,f}(1) = \mathcal{L}_p(f) L_{p,f}(1)}$$

with $\mathcal{L}_p(f) = -2 \frac{d\alpha_p(k)}{dk}\Big|_{k=2}$



The validity of this formula needs the existence of our two variable L-function!

Our method

is a combination of the Rankin-Selberg method, the theory of p-adic integration with values in p-adic Banach algebras $\mathcal{A}$ and the spectral theory of Atkin's U-operator: $U = U_p : \mathcal{A}[\![q]\!] \to \mathcal{A}[\![q]\!]$ defined by:

$$U\left(\sum_{n\geq 1} a_n q^n\right) = \sum_{n\geq 1} a_{pn} q^n \in \mathcal{A}[\![q]\!].$$

Here $\mathcal{A} = \mathcal{A}(\mathcal{B})$ is a certain p-adic Banach algebra of functions on an open analytic subspace $\mathcal{B} \subset X$ of the weight space $X = \mathrm{Hom}_{cont}(Y, \mathbb{C}_p^*)$. This is an analytic space over $\mathbb{C}_p$, which consists of all continuous characters of the profinite group $Y \cong (\mathbb{Z}/N\mathbb{Z})^* \times \mathbb{Z}_p^*$.
The classical analogue of the weight space is the whole complex plane

$$\mathbb{C} = \mathrm{Hom}_{cont}(\mathbb{R}_+^*, \mathbb{C}^*), s \mapsto (y \mapsto y^s).$$

The weights k correspond to certain points in $\mathcal{B} \subset X$. Any series $f = \sum_{n\geq 1} a_n q^n \in \mathcal{A}[q]$ produces a family of q-expansions $\{f_k = ev_k(f) = \sum_{n\geq 1} ev_k(a_n) q^n \in \mathbb{C}_p[\![q]\!]\}$, which can be classical modular forms in $\overline{\mathbb{Q}}[\![q]\!]$.

1) We construct first an analytic function $\mathcal{L}_\mu : X \to \mathcal{A} = \mathcal{A}(\mathcal{B})$ as the Mellin transform

$$\mathcal{L}_\mu(x) = \int_Y x(y)\, d\mu(y) \quad (\text{where } x \in X = \mathrm{Hom}_{cont}(Y, \mathbb{C}_p^*), x = x(y)),$$

μ is a certain measure with values in $\mathcal{A}$, on the profinite group Y.

2) For each $s \in \mathcal{B} \subset X$, there is the evaluation homomorphism $ev_s : \mathcal{A}(\mathcal{B}) \to \mathbb{C}_p$; we obtain $\mathcal{L}_\mu(x, s)$ by evaluation of an $\mathcal{A}$-valued integral:

$$\mathcal{L}_\mu(x, s) = ev_s(\mathcal{L}_\mu(x)) = ev_s\left(\int_Y x d\mu\right) \quad (x \in X, \quad \mathcal{L}_\mu(x) \in \mathcal{A}).$$

This gives a p-adic analytic L-function in two variables $(x, s) \in X \times \mathcal{B} \subset X \times X$:

$$(x, s) \longmapsto \mathcal{L}_\mu(x, s).$$

3) We check an equality relating the algebraic numbers $L^*_{f_k}(s, \chi)$ $(s = 1, \cdots, k-1)$ with the values $\mathcal{L}_\mu(x, k)$ at certain points $x \in X$ (more precisely, at $x = \chi \cdot y_p^k$).

p-adic integration and the p-adic weight space

Consider the group
$Y = \varprojlim_v (\mathbb{Z}/Np^v\mathbb{Z})^\times \cong (\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}_p^\times$ (a profinite group with a projection $y_p : Y \to \mathbb{Z}_p^\times$)

and the group of p-adic characters
$X = X_N = \mathrm{Hom}_{\mathrm{cont}}(Y, \mathbb{C}_p^\times) \ni \chi, y_p^n,$ (the p-adic weight space, which is a $\mathbb{C}_p$-analytic group)

where
$\chi \bmod Np^v\mathbb{Z} : (\mathbb{Z}/Np^v\mathbb{Z})^\times \to \mathbb{C}_p^\times$ (a Dirichlet character)
$y_p : Y \to \mathbb{Z}_p^\times$ (the canonical projection, a p-adic character of Y)

The analytic structure on $X = X_N = \mathrm{Hom}_{\mathrm{cont}}(Y, \mathbb{C}_p^\times)$ over $\mathbb{C}_p$ is given by the decomposition:

$$X \xrightarrow{\sim} \mathrm{Hom}((\mathbb{Z}/Np\mathbb{Z})^\times, \mathbb{C}_p^\times) \times \mathrm{Hom}_{\mathrm{cont}}(\Gamma, \mathbb{C}_p^\times)$$

where $Y \cong (\mathbb{Z}/Np\mathbb{Z})^\times \times \Gamma$, $\Gamma = (1 + p\mathbb{Z}_p)^\times$, is a procyclic group of generator $\gamma = 1 + p$, and we see that X is a finite cover of the p-adic unit disc:

$$X \twoheadrightarrow \mathrm{Hom}_{\mathrm{cont}}(\Gamma, \mathbb{C}_p^\times) \xrightarrow{\sim} \mathfrak{U} = \{t \in \mathbb{C}_p \mid |t-1|_p < 1\} \cong \{\chi_t : \gamma \mapsto t \mid t \in \mathfrak{U}\}.$$

Distributions with values in Banach modules: notation

$(k,\psi) = y_p^k\psi \in X$	is a point in the weight space $X = \mathrm{Hom}_{\mathrm{cont}}(Y, \mathbb{C}_p^\times)$ (we write simply k for (k,ψ))
$\mathcal{A}$	(a p-adic Banach algebra)
V	(an $\mathcal{A}$-module)
$\mathcal{C}(Y,\mathcal{A})$	(the $\mathcal{A}$-Banach algebra
$\cup$	of continuous functions on Y)
$\mathcal{C}^{loc-const}(Y,\mathcal{A})$	(the $\mathcal{A}$-algebra
	of locally constant functions on Y)

Definition

a) A distribution $\mathcal{D}$ on Y with values in V is an $\mathcal{A}$-linear form

$$\mathcal{D} : \mathcal{C}^{loc-const}(Y,\mathcal{A}) \to V, \quad \varphi \mapsto \mathcal{D}(\varphi) = \int_Y \varphi d\mathcal{D}.$$

b) A measure μ on Y with values in V is a continuous $\mathcal{A}$-linear form

$$\mu : \mathcal{C}(Y,\mathcal{A}) \to V, \quad \varphi \mapsto \int_Y \varphi d\mu.$$

The integral $\int_Y \varphi d\mu$ can be defined for any continuous function φ, and any bounded distribution μ, using the Riemann sums.

Admissible measures of Amice-Vélu

A more delicate notion of an h-admissible measure was introduced in [Am-Ve] by Y. Amice, J. Vélu (see also [MTT], [Vi76]):

Definition

a) For $h \in \mathbb{N}, h \geq 1$ let $\mathcal{P}^h(Y, \mathcal{A})$ denote the $\mathcal{A}$-module of locally polynomial functions *of degree $< h$ of the variable $y_p : Y \to \mathbb{Z}_p^\times \hookrightarrow \mathcal{A}^\times$; in particular,*

$$\mathcal{P}^1(Y, \mathcal{A}) = \mathcal{C}^{loc-const}(Y, \mathcal{A})$$

(the $\mathcal{A}$-submodule of locally constant functions*). Let also denote $\mathcal{C}^{loc-an}(Y, \mathcal{A})$ the $\mathcal{A}$-module of* locally analytic functions*, so that*

$$\mathcal{P}^1(Y, \mathcal{A}) \subset \mathcal{P}^h(Y, \mathcal{A}) \subset \mathcal{C}^{loc-an}(Y, \mathcal{A}) \subset \mathcal{C}(Y, \mathcal{A}).$$

Admissible measures of Amice-Vélu (continued)

b) Let V be a normed $\mathcal{A}$-module with the norm $|\cdot|_{p,V}$. For a given positive integer h an h-admissible measure on Y with values in V is an $\mathcal{A}$-module homomorphism

$$\tilde{\Phi} : \mathcal{P}^h(Y, \mathcal{A}) \to V$$

such that for fixed $a \in Y$ and for $v \to \infty$ the following growth condition is satisfied:

$$\left| \int_{a+(Np^v)} (y_p - a_p)^{h'} d\tilde{\Phi} \right|_{p,V} = o(p^{-v(h'-h)}) \qquad (3.2)$$
$$\text{for all} \quad h' = 0, 1, \ldots, h-1, a_p := y_p(a)$$

The condition (3.2) allows to integrate only the locally-analytic functions: there exists a unique extension of $\tilde{\Phi}$ to $\mathcal{C}^{loc-an}(Y, \mathcal{A}) \to V$ (via the embedding $\mathcal{P}^h(Y, \mathcal{A}) \subset \mathcal{C}^{loc-an}(Y, \mathcal{A})$). The integral is defined using generalized Riemann sums: take the beginning of the Taylor expansion of a locally-analytic function $\phi \in \mathcal{C}^{loc-an}(Y, \mathcal{A})$ (of order $h-1$) instead of just values of a function ϕ.

The p-adic Mellin transform and two variable p-adic analytic functions

Any h-admissible measure $\tilde{\mu}$ on Y with values in a p-adic Banach algebra $\mathcal{A}$ can be caracterized by the logarithmic growth $o(\log^h(\cdot))$ of its *Mellin transform* $\mathcal{L}_{\tilde{\mu}}(x)$ (see [Am-Ve], [Vi76], [HaH]):

$$\mathcal{L}_{\tilde{\mu}} : X \to \mathcal{A}, \text{ defined by } \mathcal{L}_{\tilde{\mu}}(x) = \int_Y x(y) d\tilde{\mu}(y),$$

where $x \in X, \ \mathcal{L}_{\tilde{\mu}}(x) \in \mathcal{A}, \ X \subset \mathcal{C}^{loc-an}(Y, \mathcal{A})^{\times}$

Key property of h-admissible measures $\tilde{\mu}$: its Mellin transform $\mathcal{L}_{\tilde{\mu}}$ is analytic with values in $\mathcal{A}$.

Then we obtain the function $\mathcal{L}_{\mu}(x, s)$ by evaluation at (s, ψ): this is a p-adic analytic function in two variables $(x, s) \in X \times \mathcal{B} \subset X \times X$:

$$\mathcal{L}_{\tilde{\mu}}(x, s) = ev_s(\mathcal{L}_{\tilde{\mu}}) \quad (x \in X, \ \ \mathcal{L}_{\tilde{\mu}}(x) \in \mathcal{A}).$$

Example ([Am-Ve], [MTT], [Vi76])

For a primitive cusp eigenform $f = f_k = \sum_{n\geq 1} a_n q^n \in \mathcal{S}_k(\Gamma_0(N), \psi)$ *of weight* $k \geq 2$ *for* $\Gamma_0(N)$ *with a Dirichlet character* ψ *and positive slope* $\sigma = \mathrm{ord}_p(\alpha)$ *define the integer* $h = [\sigma] + 1$ *(where* $\sigma < k-1$*, and* $1 - a_p X + \psi(p)p^{k-1}X^2 = (1-\alpha_p X)(1-\alpha'_p X)$ *as above).*
Then there exists an h*-admissible* $\mathbb{C}_p$*-valued measure* $\tilde{\mu} = \tilde{\mu}_{\alpha,f}(y)$ *on* Y *such that for all couples* (j, χ) *with* $0 \leq j \leq k-2$*, and for any nontrivial primitive Dirichlet character* $\chi \bmod p^v$ *satisfying* $\chi\xi(-1) = (-1)^{k-1-j}$*, there is the following equality (in* $\mathbb{C}_p$*):*

$$\int_Y \chi(y)\, y_p^j \, d\tilde{\mu} = i_p\left(\frac{p^{vj} G(\chi)}{\alpha^v} L_f^*(1+j, \bar{\chi})\right) \quad \left(= \mathcal{L}_{\tilde{\mu}}(\chi\, y_p^j)\right), \qquad (3.3)$$

where $G(\chi)$ *is the Gauss sum of the character* $\chi \bmod p^v$*, and* $L_f^*(1+j, \bar{\chi})$ *is given by a choice of periods (2.1).* In other words, the complex L-values (3.3) attached to f coincide with the values $\mathcal{L}_{\tilde{\mu}}(\chi\, y_p^j)$ of the p-adic Mellin transform of $\tilde{\mu}$.

Coleman's families: notation

The proof of the existence of families of slope $\sigma > 0$ by R.Coleman, [CoPB], uses the following ideas: let us consider

$[K : \mathbb{Q}_p] < \infty$	– a finite extension of $\mathbb{Q}_p$ contaning all the Fourier coefficients $i_p(a_n)$ of f
$\mathcal{A} = \mathcal{A}_K(\mathcal{B})$	– the K-Banach algebra of rigid-analytic functions
$ev_k : \mathcal{A} \to K$	– the evaluation map defined for all $(k, \psi) \in \mathcal{B}$ (a neigbourhood around $(k, \psi) \in X$).
$\mathcal{M}(N; \mathcal{A})^\dagger = \bigcup_{v \geq 1} \mathcal{M}(Np^v, \psi; \mathcal{A})^\dagger \subset \mathcal{A}[\![q]\!]$	– a Banach $\mathcal{A}$-module of overconvergent families of modular forms: this module is generated by some $g = \sum_{n=0}^{\infty} b_n q^n \in \mathcal{A}[\![q]\!]$ such that $ev_k(g) \in K[\![q]\!]$ are classical cusp eigenforms for all k with (k, ψ) in a neighbourhood $\mathcal{B}$ of $(k, \psi) \in X$.

Coleman proved:

• The operator U acts as a completely continuous operator on each $\mathcal{A}$-submodule $\mathcal{M}(Np^v;\mathcal{A})^\dagger \subset \mathcal{A}[\![q]\!]$ (i.e. U is a limit of finite-dimensional operators)

$\implies$ there exists the Fredholm determinant $P_U(T) = \det(Id - T\cdot U) \in \mathcal{A}[\![T]\!]$

• there is a version of the Riesz theory: for any inverse root $\alpha \in \mathcal{A}^*$ of $P_U(T)$ there exists an eigenfunction g, $Ug = \alpha g$

such that $ev_k(g) \in K[\![q]\!]$ are classical cusp eigenforms for all k such that (k,ψ) is in a neigbourhood $\mathcal{B}$ around $(k,\psi) \in X$ (see in [CoPB])

Definition

a) *A function* $g \in \mathcal{M}(Np^v; \mathcal{A})^\dagger \subset \mathcal{A}[\![q]\!]$ *is called Coleman's family if* $Ug = \alpha g$*, and the functions* $ev_k(g) \in K[\![q]\!]$ *are cusp eigenforms for all* k *such that* (k, ψ) *is in a neigbourhood* $\mathcal{B}$ *around* (k, ψ) *in the p-adic weight space* X*, and* $\mathrm{ord}_p(\alpha(k)) = \sigma > 0$ *is constant and positive, where* $\alpha(k) = ev_k(\alpha) \in K \cap i_p(\overline{\mathbb{Q}})$
b) *Let* $f_k \in \overline{\mathbb{Q}}[\![q]\!]$ *denote the primitive cusp eigenform attached to* $ev_k(g) \in K[\![q]\!]$*. Then the family* $\{f_k\}$ *of classical primitive cusp forms is also called Coleman's family.*

Remark

Hida's families correspond to $\sigma = 0$*, they were constructed in [Hi86] (see also [Hi93]).*
There exist analogues of Hida's families in the Siegel modular case.

Recall that by [Ra52], [Za77] and [Sh77], the numbers

$$\frac{L_f(1+j,\bar{\chi})L_f(k-1,\bar{\xi})}{\pi^{k+r}\langle f_k, f_k\rangle_{Np}} \text{ are algebraic for all } j \in \mathbb{Z} \text{ with } 0 \le j \le k-2,$$

$\chi\xi(-1) = (-1)^{k-1-j}$ (here $\langle f_k, f_k\rangle_{Np}$ denotes the Petersson scalar product.

Main Theorem

Consider a nonzero analytic function $\alpha = \alpha(s) \in \mathcal{A}^\times$ defined in a neigbourhood $\mathcal{B}$ of $(k,\psi) \in X$, and consider Coleman's family

$$f = \left\{ f_k = \sum_{n=1}^{\infty} a_n(k)q^n \right\} \in \mathcal{A}[\![q]\!]$$

with coefficients in the algebra $\mathcal{A} = \mathcal{A}(\mathcal{B})$, where $\alpha \in \mathcal{A}^\times$ is the corresponding eigenvalue of U. Suppose that the slope $\mathrm{ord}_p(\alpha) = \sigma > 0$ is fixed for all $\alpha = \alpha(k)$ with (k,ψ) in $\mathcal{B}$, and define the integer $h = [\sigma] + 1$.
Then there exists an h-admissible measure $\tilde{\mu} = \mu_{\alpha,f}$ with values in $\mathcal{A}$ on the group Y, determind by the following property:

Main theorem (continued)

for all couples (j, χ) with $0 \leq j \leq k-2$, $k > 2\sigma + 2$, any primitive Dirichlet character χ mod p^v satisfying $\chi\xi(-1) = (-1)^{k-1-j}$, the following equality holds:

$$ev_k \left(\int_Y \chi(y)\, y_p^j \, d\tilde{\mu} \right) = i_p \left(R_k \cdot \frac{p^{vj} G(\chi)}{\alpha_p(k)^v} L^*_{f_k}(1+j, \bar{\chi}), \right) \quad (5.4)$$

where $G(\chi)$ is the Gauss sums of χ mod p^v, and $R_k \in \mathbb{Q}^\times$ is an elementary factor coming from an explicit choice of periods $c^\pm(f_k)$. The choice of periods: fix two Dirichlet characters ξ mod p of different parity then

$$c^\pm(f_k) = \frac{(-2i\pi)^{k-1} \langle f_k, f_k \rangle_{Np}}{\Gamma(k-1) L_{f_k}(k-1, \bar{\xi})}, \text{ where } \xi(-1) = \pm(-1)^{k-1}. \quad (5.5)$$

A key ingredient in our construction

is the use of a linear form

$$\ell_{\alpha(k)} : \mathcal{M}_k(Np, \psi, \overline{\mathbb{Q}}) \to \overline{\mathbb{Q}},$$

such that $\alpha(k) \in \mathbb{Q}^\times$, $\ell_{\alpha(k)}(U_p h) = \alpha \ell_{\alpha(k)}(h)$ for all $h \in \mathcal{M}_k(Np, \psi, \overline{\mathbb{Q}})$, and $1 - a_p X + \psi(p) p^{k-1} X^2 = (1 - \alpha(k)X)(1 - \alpha(k)' X)$ for a primitive cusp eigenform $f = \sum_{n=1}^{\infty} a_n q^n \in \mathcal{S}_k(\Gamma_0(N), \psi, \overline{\mathbb{Q}})$ of weight $k \geq 2$ for $\Gamma_0(N)$ with a Dirichlet character $\psi \pmod N$. One can define such linear form by

$\ell_\alpha : h \longmapsto \dfrac{\langle f^0, h \rangle}{\langle f^0, f_0 \rangle}$, where

f_0 is an eigenfunction of U_p: $f_0 | U_p = \alpha(k) f_0$, and

f^0 is the corresponding eigenfunction of U_p^*: $f^0 | U_p^* = \overline{\alpha(k)} f^0$,

Functions f_0 and f^0

Recall that for any primitive cusp eigenform $f = \sum_{n=1}^{\infty} a_n(f)q^n$, there is an eigenfunction of $U = U_p$ with the eigenvalue $\alpha = \alpha_p^{(1)} \in \overline{\mathbb{Q}}$ $(U(f_0) = \alpha f_0)$ given by

$$f_0 = \sum_{n\geq 1} a_n q^n - \alpha' \sum_{n\geq 1} a_n q^{pn} = \sum_{n\geq 1} a(f_0, n) q^n \in \mathcal{S}_k(\Gamma_0(Np), \psi, \overline{\mathbb{Q}}), \text{ and}$$

$$f^0 = f_0^\rho \Big|_k \begin{pmatrix} 0 & -1 \\ Np & 0 \end{pmatrix}, \quad f_0^\rho = \sum_{n\geq 1} \overline{a}(f_0, n) q^n \in \mathcal{S}_k(\Gamma_0(Np), \overline{\psi}, \overline{\mathbb{Q}})$$

is an eigenfunction of the adjoint operator U_p^*, is explicitely computed in [Go-Ro].

The answer to the question of Coleman–Mazur

is given by the function (5.6) of the following theorem:

Theorem

Under the assumptions and notations of Theorem 5.2 there exists a unique p-adic analytic function on $X \times \mathcal{B}$ (of two variables x, s),

$$\mathcal{L}_{\alpha,f}(\cdot_1, \cdot_2, \xi, f) : X \times \mathcal{B} \to \mathbb{C}_p \qquad (5.6)$$

such that
i) for any fixed $(s, \psi) \in \mathcal{B}$, the function $\mathcal{L}_{\alpha,f}(x, s; \xi, f)$ of the variable x is $\mathbb{C}_p$-analytic and has the logarithmic growth $o(\log^h(x))$,
ii) for each couple (χ, j) with $0 \le j \le k-2$, $k > 2\sigma + 2$ and any primitive Dirichlet character $\chi \bmod p^v \in X^{\mathrm{tors}}$ with values in $K^\times$ satisfying $v \ge 2$, $\chi\xi(-1) = (-1)^{k-1-j}$, the special value $\mathcal{L}(\chi y_p^j, k; \xi, f_k)$ is given by the image under i_p of the algebraic number $R_k \cdot \dfrac{p^{vj} G(\chi)}{\alpha_p(k)^v} L^*_{f_k}(1+j, \bar{\chi})$, where $G(\chi)$ is the Gauss sums of $\chi \bmod p^v$, and $R_k \in \mathbb{Q}^\times$ is an elementary factor given by the explicit choice of periods $c^\pm(f_k)$, as in (5.5).

Construction of the admissible measure $\tilde{\mu}$

Recall the Definition 3.2: an *h-admissible measure* on a profinite group Y with values in an $\mathcal{A}$-module V is an $\mathcal{A}$-module homomorphism

$$\tilde{\mu} : \mathcal{P}^h(Y, \mathcal{A}) \to V,$$

satisfying a certain growth condition (3.2).
This means that $\tilde{\mu}$ is given by a sequence $\{\mu_j\}$ of certain distributions on Y, in such a way that for $j = 0, 1, \cdots, h-1$ and for all compact open subsets $U \subset Y$ one has

$$\int_U y_p^j d\tilde{\mu} = \mu_j(U). \qquad (6.7)$$

Recall: the growth condition (3.2)

is needed in order to define an h-admissible measure $\tilde{\mu}$ out of a sequence $\{\mu_j\}$ of distributions on Y, in such a way that

$$\int_U y_p^j d\tilde{\mu} = \mu_j(U)$$

for $j = 0, 1, \cdots, h-1$ and for all compact open subsets $U \subset Y$. This condition has the form: for $t = 0, 1, \cdots, h-1$

$$\left| \int_{a+(Np^v)} (y_p - a_p)^t d\tilde{\mu} \right|_p \tag{6.8}$$

$$= \left| \sum_{j=0}^{t} \binom{t}{j} (-a_p)^{t-j} \mu_j(a + (Np^v)) \right|_p = o(p^{v(h-t)}) \text{ for } v \to \infty.$$

In this condition the elements $\mu_j(a + (Np^v))$ belong to a p-adic Banach algebra $\mathcal{A}$.

We construct the sequence μ_j out of products of Eisenstein series:

$$\mu_j = \ell_\alpha(\pi_\alpha(\Phi_j)), \quad (j = 0, 1, \cdots, h-1), h = [\sigma] + 1.$$

- Φ_j is a sequence of modular distributions on Y with values in a certain $\mathcal{A}$-module $\mathcal{M} = \mathcal{M}_N(\psi; \mathcal{A})$ of modular forms with coefficients in $\mathcal{A}$ (it has infinite rank):

$$\mathcal{M}_N(\psi; \mathcal{A}) := \bigcup_{v \geq 0} \mathcal{M}(Np^v, \psi; \mathcal{A}),$$

  (our modular forms $\Phi_j(\chi)$ are products of certain families of classical Eisenstein series in $\mathcal{A}[\![q]\!]$)
- π_α is the canonical projector onto the characteristic $\mathcal{A}$-submodule $\mathcal{M}^\alpha = \mathcal{M}^\alpha(\mathcal{A})$ of Atkin's operator $U\left(\sum_{n\geq 0} b_n q^n\right) = \sum_{n \geq 0} b_{pn} q^n$
  (Key point: the $\mathcal{A}$-module $\mathcal{M}^\alpha(\mathcal{A})$ is locally free of finite rank)
- $\ell_\alpha \in \mathrm{Hom}_{\mathcal{A}}(\mathcal{M}^\alpha, \mathcal{A})$ is a $\mathcal{A}$-linear form (given by the Petersson scalar product with $h \in \mathcal{M}^\alpha$, as in Section 3: $h \longmapsto \dfrac{\langle f^0, h\rangle}{\langle f^0, f_0\rangle}$, normalized by the equality $\ell_\alpha(g) = 1$ for Coleman's eigenfunction $g = f_0 \in \mathcal{M}^\alpha$.

Main congruence: criterion of admissibility

Theorem

Let $0 < |\alpha|_p < 1$ and suppose that the following conditions are satisfied: for all $r = 0, 1, \cdots, h-1$ with $h = [\mathrm{ord}_p \alpha] + 1$, and $v \geq 1$,

$$\Phi_r(a + (Np^v)) \in \mathcal{M}(Np^v)^\dagger \qquad \text{(the level condition)} \tag{6.9}$$

and the following p-adic congruence holds: for all $t = 0, 1, \cdots, h-1$

$$U^v \sum_{r=0}^{t} \binom{t}{r} (-a_p)^{t-r} \Phi_r(a + (Np^v)) \equiv 0 \bmod p^{vt} \tag{6.10}$$

(the divisibility condition)

Consider the linear form $\tilde{\Phi}^\alpha(\delta_{a+(Np^v)} y_p^r) := \pi_\alpha(\Phi_r(a + (Np^v))$ (defined on local monomials of degree $r = 0, 1, \cdots, h-1$).
Then $\tilde{\Phi}^\alpha$ is an h-admissible measure: $\tilde{\Phi}^\alpha : \mathcal{P}^h(Y, \overline{\mathbb{Q}}) \to \mathcal{M}^\alpha \subset \mathcal{M}$

Proof uses the commutative diagram:

$$\begin{array}{ccccc}
\mathcal{M}(Np^{v+1},\psi;\mathcal{A})^{\dagger} & \xrightarrow{\pi_{\alpha,v}} & \mathcal{M}^{\alpha}(Np^{v+1},\psi;\mathcal{A})^{\dagger} & & \\
U^{v}\downarrow & & \downarrow\wr\, U^{v} & & \\
\mathcal{M}(Np,\psi;\mathcal{A})^{\dagger} & \xrightarrow[\pi_{\alpha,0}]{} & \mathcal{M}^{\alpha}(Np,\psi;\mathcal{A})^{\dagger} & = & \mathcal{M}^{\alpha}(Np^{v+1},\psi;\mathcal{A})^{\dagger}.
\end{array}$$

The existence of the projectors $\pi_{\alpha,v}$ comes from Coleman's Theorem A.4.3 [CoPB].
On the right: $\mathcal{M}^{\alpha}(Np^{v+1},\psi;\mathcal{A})^{\dagger}$ does not depend on v (a version of Hida's Control Theorem), and U acts on the locally free $\mathcal{A}$-module $\mathcal{M}^{\alpha}(Np^{v+1},\mathcal{A})^{\dagger}$ via the matrix:

$$\begin{pmatrix} \alpha & \cdots & \cdots & * \\ 0 & \alpha & \cdots & * \\ 0 & 0 & \ddots & \cdots \\ 0 & 0 & \cdots & \alpha \end{pmatrix} \text{ where } \alpha \in \mathcal{A}^{\times}$$

$\Longrightarrow U^{v}$ is an isomorphism over $\mathrm{Frac}(\mathcal{A})$,

One controls the denominators

of the modular forms of all levels v by the relation:

$$\pi_{\alpha,v}(h) = U^{-v}\pi_{\alpha,0}(U^v h) =: \pi_\alpha(h) \quad (6.11)$$

The equality (6.11) can be used as the definition of π_α. The growth condition (3.2) for $\pi_\alpha(\Phi_r)$ is deduced from the congruences (6.10) between modular forms, using the relation (6.11).

Recall: then we obtain the function $\mathcal{L}_\mu(x,s)$ by evaluation at (s,ψ): this is a p-adic analytic function in two variables $(x,s) \in X \times \mathcal{B} \subset X \times X$:

$$\boxed{\mathcal{L}_{\tilde{\mu}}(x,s) = ev_s(\mathcal{L}_{\tilde{\mu}}) \quad (x \in X, \quad \mathcal{L}_{\tilde{\mu}}(x) \in \mathcal{A}).}$$

Modular Eisenstein distributions Φ_j

Consider again two auxiliary Dirichlet characters $\xi \mod p$, $\xi(-1) = \pm 1$, and use the method of Rankin-Selberg for the convolution

$$D(s, f, g) = L_N(2s + 2 - k - l, \psi\overline{\xi\chi}) \sum_{n=1}^{\infty} a_n b_n n^{-s}, \text{ where} \quad (7.12)$$

$$b_n = \sigma_{l-1,\bar{\chi},\bar{\xi}}(n) = \sum_{d|n, d>0} \bar{\chi}(d)\bar{\xi}(n/d)d^{l-1},$$

are the Fourier coefficients of an Eisenstein series $g = \sum_{n=0}^{\infty} b_n q^n$ of weight l (and of Dirichlet character $\bar{\chi}\bar{\xi}$) if $\chi\xi(-1) = (-1)^l$, so that

$$L_g(s) = \sum_{n=1}^{\infty} b_n n^{-s} = L(s - l + 1, \bar{\chi})L(s, \bar{\xi}).$$

Rankin's lemma (cf. [Ra52]) gives

$$D(s,f,g) = L_N(2s+2-k-l, \psi\overline{\xi\chi}) \sum_{n=1}^{\infty} a_n b_n n^{-s} \quad (7.13)$$

$$= L_f(s-l+1,\bar{\chi}) L_f(s,\bar{\xi}),$$

and evaluation at $s = k-1$ is expressed through the Rankin-Selberg integral of f with the product of two Eisenstein series of weights $k-1-j$ and $1+j$:

$$\langle f, E_{k-1-j}(\xi,\chi) E_{1+j}(\psi\overline{\xi\chi}) \rangle_{Np^v}.$$

One defines the modular distributions Φ_j on the group $Y = \varprojlim_v (\mathbb{Z}/Np^v\mathbb{Z})^\times$ in such a way that the modular form $\Phi_j(\chi) \in \mathcal{A}[\![q]\!]$ is the product of these Eisenstein series with variable coefficients in $\mathcal{A}$:

$$ev_k(\Phi_j(\chi)) := (-1)^j E_{k-1-j}(\xi,\chi) E_{1+j}(\psi\overline{\xi\chi}) =: \Phi_{j,k}(\chi).$$

Main congruence

Explicitely, the Fourier coefficients of Φ_j (for $j = 0, \ldots, k-2$) are given by

$$\Phi_j(a + (Np^v)) \tag{7.14}$$
$$= \sum_{b \bmod Np^v} \psi\bar{\xi}(b) \sum_{n \geq 0}^{\infty} \sum_{n_1+n_2=n} A_j(n_1, ab)B_j(n_2, b)q^n \in \mathcal{A}[\![q]\!], \text{ where}$$

$$A_j(n_1, ab)(k) = \sum_{\substack{d_1 | n_1 \\ (n_1/d_1) \equiv ab \bmod Np^v}} \xi(d_1) \operatorname{sgn}(d_1) d_1^{k-2-j} \tag{7.15}$$

$$B_j(n_2, b)(k) = \sum_{\substack{d_2 | n_2 \\ d_2 \equiv b \bmod Np^v}} \operatorname{sgn}(d_2)(n_2/d_2)^j \text{ for } n_2 > 0.$$

(Note that the last series has constant coefficients). One verifies coefficient-by-coefficient that the consructed modular distributions Φ_j satisfy the level condition and the divisibility condition (6.9), (6.10):

Main congruence (continued)

$$U^v \sum_{j=0}^{t} \binom{t}{j} (-a_p)^{t-j} \Phi_j(a + (Np^v)) \tag{7.16}$$

$$= \sum_{j=0}^{t} \binom{t}{j} (-a_p)^{t-j} \sum_{n\geq 0}^{\infty} \sum_{n_1+n_2=p^v n} (-1)^j A_j(n_1, ab) B_j(n_2, b) q^n$$

$$\stackrel{?}{\equiv} 0 (\bmod p^{tv}).$$

Let us fix n_1 et n_2 with $n_1 + n_2 = p^v n$, $d_1 | n_1$ and $d_2 | n_2$ with $(n_1/d_1) \equiv ab \bmod Np^v$ et $d_2 \equiv b \bmod Np^v$, and write only the terms which depend on j:

$$\sum_{j=0}^{t} \binom{t}{j} (-a)^{t-j} (-1)^j d_1^{k-2-j} \left(\frac{n_2}{d_2}\right)^j = d_1^{k-2} \left(-a - \left(\frac{n_2}{d_1 d_2}\right)\right)^t \tag{7.17}$$

$$\equiv d_1^{k-2} d_2^{-t} \left(-a d_2 + \left(\frac{n_1}{d_1}\right)\right)^t \equiv 0 \bmod p^{vt}.$$

The congruence (7.17) is then satisfied because $p \nmid d_2$ and

$$-a - \left(\frac{n_2}{d_1 d_2}\right) \equiv \bmod p^v.$$

Algebraic $\mathcal{A}$-linear form $\ell_\alpha : \mathcal{M}^\alpha(\mathcal{A})^\dagger \to \mathcal{A}$

Let us describe a linear form ℓ_α on the locally free module $\mathcal{M}_N(\psi;\mathcal{A})^\alpha = \pi_\alpha(\mathcal{M}_N(\psi;\mathcal{A}))$ of finite rank.

Let use a basis $\{g^i\}$ of $\mathcal{M}^\alpha(\mathcal{A})^\dagger$ over the field of fractions Frac($\mathcal{A}$), such that $g^1 = g$ is fixed Coleman's eigenvector as above, and g^i are eigenfunctions of all Hecke operators T_l, $(l \nmid Np)$.
Define $\ell_\alpha(h) = x_1,$ where $h = \sum_i x_i g^i, x \in \mathcal{A}$
(the first coordinate of $h \in \mathcal{M}^\alpha(\mathcal{A})^\dagger$. An explicit evaluation in terms of the Peterson product shows:

$$ev_k(\ell_\alpha(h)) = \ell_{\alpha(k)}(h_k), \text{ where } h_k = ev_k(h) \in \mathcal{M}_k(N,\psi).$$

The R.H.S. can be computed for classical modular forms h_k through the (normalized) Petersson scalar product, moreover, $\ell_\alpha(g) = 1$.

Proof of Main Theorem

Take the admissible measure $\tilde{\mu}_\alpha := \ell_{\alpha,f}(\tilde{\Phi}^\alpha)$, with $\tilde{\Phi}^\alpha$ constructed by the admissibility criterium of Theorem 6.1 out of products of Eisenstein series Φ_j and the linear form $\ell_{\alpha,f}$ (the Petersson product over $\mathcal{A}$). Let us compute the integrals

$$ev_k\left(\int_Y \chi y_p^j \, d\tilde{\mu}_{\alpha,f}\right) = ev_k(\ell_\alpha(\pi_\alpha(\Phi_j(\chi))) = \quad (9.18)$$
$$ev_k(\ell_\alpha(U^{-v}\pi_{\alpha,0}U^v\Phi_j(\chi)))$$
$$= \ell_{\alpha(k)}(\pi_{\alpha(k)}\Phi_{j,k}(\chi)) = \alpha(k)^{-v}\frac{\langle f_k^0, U^v\Phi_{j,k}(\chi)\rangle}{\langle f_k^0, (f_k)_0\rangle}$$

for primitive Dirichlet characters χ mod p^v, using the relation (6.11): $\pi_\alpha(h) = U^{-v}\pi_{\alpha,0}(U^v h)$, where $\Phi_{j,k} = ev_k(\Phi_j) = (-1)^j E_{k-1-j}(\xi,\chi)E_{1+j}(\psi\overline{\xi\chi})$.

Proof of Main Theorem (continued)

The value of the p-adic integral (9.18) can be computed using the Rankin–Selberg convolution:

$$L_{f_k}(s-l+1,\bar{\chi})L_{f_k}(s,\bar{\xi}) = L_N(2s+2-k-l,\psi\overline{\xi\chi})\sum_{n=1}^{\infty} a_n(k)b_n n^{-s}, \tag{9.19}$$

where $b_n = \sigma_{l-1,\bar{\chi},\bar{\xi}}(n) = \sum_{d|n,d>0} \bar{\chi}(d)\bar{\xi}(n/d)d^{l-1}$, are the Fourier coefficients of an Eisenstein series $g = \sum_{n=0}^{\infty} b_n q^n$ of weight l with character $\bar{\chi}\bar{\xi}$) (if $\chi\xi(-1) = (-1)^l$).
Put $s = k-1$, $l = k-1-j$, $j = 0, \cdots k-2$ with $k > 2+j$, into (9.19):

$$L_{f_k}(1+j,\bar{\chi})L_{f_k}(k-1,\bar{\xi}) = L_N(1+j,\psi\overline{\xi\chi})\sum_{n=1}^{\infty} a_n(k)b_n n^{-k+1}.$$

Proof of Main Theorem (continued)

Using this equality, the R.H.S. of (9.18): is then computed using the Rankin–Selberg integral in the form:

$$ev_k(\ell_\alpha(\pi_\alpha(\Phi_j(\chi))) = t_k \cdot \frac{p^{\nu j} G(\chi)}{\alpha(k)^\nu} L^*_{f_k}(1+j, \bar{\chi}),$$

$$\text{where } c^\pm(f_k) = \frac{(-2i\pi)^{k-1}\langle f_k, f_k\rangle}{\Gamma(k-1)L_{f_k}(k-1, \bar{\xi})},$$

$G(\chi)$ denotes the Gauss sum of the character χ mod p^v, and $t_k \in \mathbb{Q}^\times$ is an explicit elementary constant. Then one applies directly theorem 6.1 (the admissibility criterion) with $\varkappa = 1$, and the congruences (7.16) in order to obtain the required h-admissibles measures $\tilde{\mu} = \mu_{f,\alpha}$ in the form $\mu_{f,\alpha} = \ell_{f,\alpha}(\tilde{\Phi}^\alpha)$ (given by the sequence of the distributions $\Phi^\alpha_j = \pi_\alpha(\Phi_j))$.

Conclusion

After having an admissible measure $\tilde{\Phi}^\alpha$ with values in modular forms over the algebra $\mathcal{A}$, we then construct the required h-admissibles measures $\tilde{\mu} = \tilde{\mu}_{f,\alpha}$ in the form $\tilde{\mu}_{f,\alpha} = \ell_\alpha(\tilde{\Phi}^\alpha)$, as explained above.

Indeed, we obtain the function in question $\mathcal{L}_\mu(x, \mathbf{s})$ by evaluation at $\mathbf{s} = (s, \psi) \in \mathcal{B}$: this is a p-adic analytic function in two variables $(x, \mathbf{s}) \in X \times \mathcal{B} \subset X \times X$:

$$\mathcal{L}_{\tilde{\mu}}(x, \mathbf{s}) := ev_{\mathbf{s}}(\mathcal{L}_{\tilde{\mu}})(x) \quad (x \in X,\ \mathbf{s} \in \mathcal{B},\ \mathcal{L}_{\tilde{\mu}}(x) \in \mathcal{A}).$$

Here $\mathcal{A} = \mathcal{A}(\mathcal{B})$ denote again the Banach algebra $\mathcal{A}$ and $\mathcal{B}$ is an affinoid neighbourhood around $\mathbf{s} = (s, \psi) \in \mathcal{B}$ (with a given Dirichlet character ψ mod N).

A further development: Garrett's triple products

Our data: three primitive cusp eigenforms

$$f_j(z) = \sum_{n=1}^{\infty} a_{n,j} q^n \in \mathcal{S}_{k_j}(N_j, \psi_j), \ (j = 1, 2, 3) \tag{10.20}$$

of weights k_1, k_2, k_3, of conductors N_1, N_2, N_3, and of nebentypus characters ψ_j mod N_j, $N := \mathrm{LCM}(N_1, N_2, N_3)$.

Let p be a prime, $p \nmid N$. We view $f_j \in \overline{\mathbb{Q}}[\![q]\!] \overset{i_p}{\hookrightarrow} \mathbb{C}_p[\![q]\!]$ via a fixed embedding $\overline{\mathbb{Q}} \overset{i_p}{\hookrightarrow} \mathbb{C}_p$, $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}}_p$ is Tate's field.
Let χ denote a variable Dirichlet character mod $Np^v, v \geq 0$.
We view k_j as a variable weight in the weight space
$X = X_{Np^v} = \mathrm{Hom}_{cont}(Y, \mathbb{C}_p^*),\ Y = (\mathbb{Z}/N\mathbb{Z})^* \times \mathbb{Z}_p^* \ni (y_0, y_p)$.
The space X is a p-adic analytic space first used in Serre's [Se2] *Formes modulaires et fonctions zêta p-adiques.* Denote by $(k, \chi) \in X$ the homomorphism $(y_0, y_p) \mapsto \chi(y_0)\chi(y_p \bmod p^v)y_p^k$. We write simply k_j for the couple $(k_j, \psi_j) \in X$.

A four variable p-adic L function

attached to Garrett's triple product of three Coleman's families

$$k_j \mapsto \left\{ f_{j,k_j} = \sum_{n=1}^{\infty} a_{n,j}(k_j) q^n \right\}$$

of cusp eigenforms of three constant slopes $\sigma_j = \mathrm{ord}_p(\alpha^{(1)}_{p,j}(k_j)) \geq 0$ where $\alpha^{(1)}_{p,j}(k_j)$, $\alpha^{(2)}_{p,j}(k_j)$ are the Satake parameters given as inverse roots of the Hecke p–polynomial
$1 - a_{p,j}X - \psi_j(p)p^{k_j-1}X^2 = (1 - \alpha^{(1)}_{p,j}(p)X)(1 - \alpha^{(2)}_{p,j}(p)X)$.
We assume that $\mathrm{ord}_p(\alpha^{(1)}_{p,j}(k_j)) \leq \mathrm{ord}_p(\alpha^{(2)}_{p,j}(k_j))$.
This extends a previous result: (see [PaTV], where a two variable p-adic L-function was constructed interpolating on all k a function $(k, s) \mapsto L^*(f_k, s, \chi)$ $(s = 1, \cdots, k-1)$ for such a family.
We use the theory of p-adic integration with values in spaces of nearly holomorphic modular forms (in the sense of Shimura, see [Sh2000]).

Generalities on triple products

The triple product with a Dirichlet character χ is defined as the following complex L-function (an Euler product of degree eight):

$$L(f_1 \otimes f_2 \otimes f_3, s, \chi) = \prod_{p \nmid N} L((f_1 \otimes f_2 \otimes f_3)_p, \chi(p)p^{-s}), \qquad (10.21)$$

where $L((f_1 \otimes f_2 \otimes f_3)_p, X)^{-1} =$ (10.22)

$$\det\left(1_8 - X \begin{pmatrix} \alpha_{p,1}^{(1)} & 0 \\ 0 & \alpha_{p,1}^{(2)} \end{pmatrix} \otimes \begin{pmatrix} \alpha_{p,2}^{(1)} & 0 \\ 0 & \alpha_{p,2}^{(2)} \end{pmatrix} \otimes \begin{pmatrix} \alpha_{p,3}^{(1)} & 0 \\ 0 & \alpha_{p,3}^{(2)} \end{pmatrix}\right)$$

$$= \prod_{\eta} (1 - \alpha_{p,1}^{(\eta(1))} \alpha_{p,2}^{(\eta(2))} \alpha_{p,3}^{(\eta(3))} X)$$

$$= (1 - \alpha_{p,1}^{(1)} \alpha_{p,2}^{(1)} \alpha_{p,3}^{(1)} X)(1 - \alpha_{p,1}^{(1)} \alpha_{p,2}^{(1)} \alpha_{p,3}^{(2)} X) \cdot \ldots \cdot (1 - \alpha_{p,1}^{(2)} \alpha_{p,2}^{(2)} \alpha_{p,3}^{(2)} X),$$

product taken over all 8 maps $\eta : \{1, 2, 3\} \to \{1, 2\}$.

Critical values and functional equation

We use the corresponding normalized L function (see [De79], [Co], [Co-PeRi]), which has the form:

$$\Lambda(f_1 \otimes f_2 \otimes f_3, s, \chi) = \tag{10.23}$$
$$\Gamma_{\mathbb{C}}(s)\Gamma_{\mathbb{C}}(s-k_3+1)\Gamma_{\mathbb{C}}(s-k_2+1)\Gamma_{\mathbb{C}}(s-k_1+1)L(f_1 \otimes f_2 \otimes f_3, s, \chi),$$

where $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$.
The Gamma-factor determines the critical values $s = k_1, \cdots, k_2+k_3-2$ of $\Lambda(s)$, which we explicitely evaluate (like in the classical formula $\zeta(2) = \frac{\pi^2}{6}$). A functional equation of $\Lambda(s)$ has the form:

$$s \mapsto k_1 + k_2 + k_3 - 2 - s.$$

Statement of the problem

Given three p-adic analytic families $\mathbf{f}_j$ of slope $\sigma_j \geq 0$, to construct a four-variable p-adic L-function attached to Garrett's triple product of these families

We show that this function interpolates the special values

$$(s, k_1, k_2, k_2) \longmapsto \Lambda(f_{1,k_1} \otimes f_{2,k_2} \otimes f_{3,k_3}, s, \chi)$$

at critical points $s = k_1, \cdots, k_2 + k_3 - 2$ for balanced weights $k_1 \leq k_2 + k_3 - 2$; we prove that these values are algebraic numbers afters dividing by certain "periods".

However, our construction uses directly modular forms, and not the L-values in question.
A comparison of special values of two functions is done after the construction.

References

Y. Amice, J. Velu, *Distributions p-Adiques associées aux Séries de Hecke*, Journées Arithmétiques de Bordeaux (Conf. Univ. Bordeaux (1974)), Astérisque N° 24/25, Soc. Math. France, Paris (1975), p 119-131.

A.N. Andrianov, *Euler products attached to Siegel Modular Forms of Degree 2*, Uspekhi Mat. Nauk 29 (1974), p 44-109 (in Russian).

A.N. Andrianov, A.A.Panchishkin, *Singular Frobenius operators on Siegel modular forms with characters and zeta functions*, St.-Petersbourg Math.J., vol. 12, no. 2 (2001), pp.233-257.

S. Böcherer, *Über die Funktionalgleichung Automorpher L-Funktionnen zur Siegelschen Modulgruppe*, J. reine angew. Math. 362 (1985), p 146-168.

- S. Böcherer, C.-G. Schmidt, *p-adic measures attached to Siegel modular forms*, Ann. Inst. Fourier 50 (2000), no. 5, 1375–1443.
- K. Buecker, *Congruences between Siegel modular forms on the level of group cohomology.* Ann. Inst. Fourier (Grenoble) 46 (1996), no. 4, 877–897.
- Chandrasekharan, K. Arithmetical functions. Berlin–Heidelberg–New York, Springer–Verlag (1970).
- YoungJu Choie, W. Eholzer, *Rankin-Cohen operators for Jacobi and Siegel forms*, J. Number Theory 68 (1998), no. 2, 160–177.
- J. Coates, B. Perrin-Riou, *On p-adic L-functions attached to Motives over* $\mathbb{Q}$, Advanced Studies in Pure Math. 17 (1989), 23-54
- Coates, J. *On p–adic L–functions.* Sem. Bourbaki, 40eme annee, 1987-88, n° 701, Asterisque (1989) 177–178.

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.

- P.Colmez, La conjecture de Birch et Swinnerton-Dyer p-adique. Séminaire Bourbaki. [Exposé N°919] (Juin 2003)
- M. Courtieu, *Familles d'opérateurs sur les formes modulaires de Siegel et fonctions L p-adiques*, `http://www-fourier.ujf-grenoble.fr/THESE/ps/t101.ps.gz`, Thèse de Doctorat, Institut Fourier, 2000, 1–122.
- M. Courtieu, A.A.Panchishkin, *Non-Archimedean L-Functions and Arithmetical Siegel Modular Forms*, Lecture Notes in Mathematics 1471, Springer-Verlag, 2004 (2nd augmented ed.)
- A.Dabrowski, D.Delbourgo, *S*-adic *L*-functions attached to the symmetric square of a Newform Proc. London Math. Soc. (3) 74 (1997) pp. 559-611
- Deligne P., *Valeurs de fonctions L et périodes d'intégrales*, Proc. Symp. Pure Math AMS 33 (part 2) (1979) 313–342.

- E. Eholzer, T. Ibukiyama, *Rankin-Cohen type differential operators for Siegel modular forms.* Internat. J. Math , 9 (1998) no. 4, 443–463.
- 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).
- P.B.Garrett, M.Harris, *Special values of triple product L–functions*, Amer. J. Math 115 (1993) 159–238.
- Bertrand Gorsse, Carrés symétriques de formes modulaires et intégration p-adique. Mémoire de DEA de l'Institut Fourier, juin 2002
- Bertrand Gorsse, Gilles Robert, Computing the Petersson product $\langle f^0, f_0\rangle$. Prépublication de l'Institut Fourier, N654, (2004).

- 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).
- P.Guerzhoy, *Jacobi-Eisenstein series and p-adic interpolation of symmetric squares of cusp forms*, Annales de l'Institut Fourier, 45, N3, 605-624 (1995).
- 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.

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 ordinary Hecke algebras for* $\mathrm{GL}(2)$, Ann. Inst. Fourier (Grenoble) 44 (1994), no. 5, 1289–1322.
- H. Hida, *p-adic automorphic forms on Shimura varieties.* Springer Monographs in Mathematics. Springer-Verlag, New York, 2004. xii+390 pp.
- K. Iwasawa, *Lectures on p-Adic L-Functions*, Ann. of Math. Studies, N° 74. Princeton Univ. Press (1972).

Fabienne Jory–Hugue, *Familles de symboles modulaires et fonctions L p-adiques*, Thèse de Doctorat, Institut Fourier (Grenoble), 18 décembre 1998

Fabienne Jory–Hugue, *Unicité des h–mesures admissibles p-adiques données par des valeurs de fonctions L sur les caractères*, (in preparation), Institut Fourier (Grenoble), 2004 `http://www-fourier.ujf-grenoble.fr/THESE/ps/t92.ps.gz`

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).

W. Kim, Ramification points on the Eigencurve. Manuscript, 2004, pp.1-21

H. Klingen, *Über Poincarésche Reihen vom Exponentialtyp*, Math. Ann. 234 (1978), p. 145-170.

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

Y.-H. Le Bras, A.A. Panchishkin, *Sur les produits triples Λ-adiques*, Communications in Algebra, 29 (2001) No. 9, 3727-3740.

H. Maass, *Siegel's Modular Forms and Dirichlet Series*, Springer-Verlag, Lect. Notes in Math. N° 216 (1971).

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.

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

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

S. Mizumoto, *Fourier Coefficients of Generalized Eisenstein Series of Degree two*, Proc. Jap. Acad. A59 (1983), p. 231-264.

S. Mizumoto, *Fourier Coefficients of Generalized Eisenstein Series of Degree two*, Kodai Math. J. 7 (1984), p. 86-110.

S. Nagaoka, *A remark on Serre's example of p-adic Eisenstein series*, Math. Z. 235 (2000) 227-250.

S. Nagaoka, *Note on* mod *p Siegel modular forms*, Math. Z. 235 (2000) 405-420.

A.A. Panchishkin, *Produits triples des formes modulaires et leur interpolation p–adique par la méthode d'Amice–Vélu*, Manuscrit de l'exposé au Colloque à la mémoire d'Yvette Amice, mars, 1994, pp.1-27

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, Admissible measures for standard L-functions and nearly holomorphic Siegel modular forms. MPI 2002 - 42 (MPI-2002-42.dvi - MPI-2002-42.ps)

A.A. Panchishkin, Arithmetical differential operators on nearly holomorphic Siegel modular forms. MPI 2002 - 41, MPI-2002-41.dvi - MPI-2002-41.ps

A.A. Panchishkin, *Sur une condition suffisante pour l'existence des mesures p-adiques admissibles*, Journal de Théorie des Nombres de Bordeaux, v. 15 (2003), pp. 1-24

Julien Puydt, *Valeurs spéciales de fonctions L de formes modulaires adéliques*, Thèse de Doctorat, Institut Fourier (Grenoble), 19 décembre 2003

R.A.Rankin, The scalar product of modular forms. Proc. London math. Soc. 2 (3) (1952) 198-217

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.

G. Shimura, Sur les intégrales attachées aux formes automorphes, J.Math. Soc Japan, 11, 291-311 (1959)

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

G. Shimura, *On the Holomorphy of certain Dirichlet Series*, Proc. Lond. Math. Soc. 31 (1975), p 79-98.

G. Shimura, *On the Periods of Modular Forms*, Math. Annalen 229 (1977), p 211-221.

G. Shimura, *The Special Values of Zeta Functions associated with Hilbert Modular Forms* Duke Math. J. 48 (1978), p 637-679.

G. Shimura, *Arithmetic of Differential Operators on Symetric Domains*, Duke Math. J. 48 (1981), p 813-843.

G. Shimura, *On Eisentsein Series*, Duke Math. J; 50 (1983), p. 417-476.

G. Shimura, *Arithmeticity in the theory of automorphic forms.* Mathematical Surveys and Monographs, **82**. American Mathematical Society, Providence, RI, 2000. x+302 pp.

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).

J. Tilouine, E. Urban, *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.

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

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.