ANNALES

DE

L'INSTITUT FOURIER

Kenichi BANNAI & Shinichi KOBAYASHI

Integral structures on p-adic Fourier theory

Tome 66, nº 2 (2016), p. 521-550.

<http://aif.cedram.org/item?id=AIF_2016__66_2_521_0>

Ann. Inst. Fourier, Grenoble
66, 2 (2016) 521-550

INTEGRAL STRUCTURES ON p-ADIC FOURIER THEORY

by Kenichi BANNAI & Shinichi KOBAYASHI (*)

Abstract. — In this article, we give an explicit construction of the p-adic Fourier transform by Schneider and Teitelbaum, which allows for the investigation of the integral property. As an application, we give a certain integral basis of the space of K-locally analytic functions on the ring of integers $\mathcal{O}_K$ for any finite extension K of $\mathbb{Q}_p$, generalizing the basis constructed by Amice for locally analytic functions on $\mathbb{Z}_p$. We also use our result to prove congruences of Bernoulli-Hurwitz numbers at non-ordinary (i.e. supersingular) primes originally investigated by Katz and Chellali.

Résumé. — Dans cet article, nous donnons une construction explicite de la transformation de Fourier p-adique de Schneider et Teitelbaum, qui nous permet d'étudier son integralité. Comme application, pour toute extension finie K de $\mathbb{Q}_p$ nous donnons une certaine base entière de l'espace de K-fonctions localement analytiques sur l'anneau des entiers $\mathcal{O}_K$, en généralisant la base construite par Amice pour les fonctions localement analytiques sur $\mathbb{Z}_p$. Nous utilisons également notre résultat pour démontrer certaines relations de congruence étudiées initialement par Katz et Chellali entre nombres de Bernoulli-Hurwitz aux places non-ordinaires (c'est-à-dire supersingulières).

1. Introduction

One important method in studying the congruences and p-adic properties of important invariants in number theory is the use of p-adic measures interpolating such values. Such theory was applied to obtain the Kummer congruence between special values of Riemann zeta function as well as the

Keywords: p-adic distribution, p-adic Fourier theory, Amice transform, integrality, congruence, Lubin-Tate group, Bernoulli-Hurwitz number, p-adic periods.
Math. classification: 11S40.
(*) The first and second authors were supported by the JSPS Postdoctoral Fellowships for Research Abroad 2005-2007/2004-2006. This work was also supported in part by KAKENHI (21674001, 25707001, 26247004).

construction of the p-adic L-functions for elliptic curves with ordinary reduction at p. When dealing with the non-ordinary case, it is necessary to use the theory of p-adic analytic distributions, which is a generalization of the theory of p-adic measures. For such p-adic distributions on $\mathbb{Z}_p$, the Amice transform gives a one-to-one correspondence between $\mathbb{C}_p$-valued distributions on $\mathbb{Z}_p$ and rigid analytic functions on the open unit disc. The general idea is to study the congruences and p-adic properties of the interpolated invariants through the p-adic property of the rigid analytic function corresponding to the p-adic distribution. However, contrary to the case of p-adic measures, the Amice transform is not well-behaved integrally for general p-adic distributions, hence it is necessary to investigate in detail the precise integral structure of this transform. Amice [1, §10] investigated the precise integral structure of the Amice transform.

Let $\mathcal{O}_K$ be the ring of integers of a finite extension K of $\mathbb{Q}_p$. In [8, §4], Schneider and Teitelbaum constructed the p-adic Fourier transform, which is a one-to-one correspondence between $\mathbb{C}_p$-valued distributions on $\mathcal{O}_K$ and rigid analytic functions on an open unit disc. The purpose of this article is to give an explicit and elementary construction of the p-adic Fourier transform of Schneider-Teitelbaum, which allows investigation of the precise integral structure of this correspondence. We then determine an integral structure on the ring of locally analytic functions on $\mathcal{O}_K$. The integrality of the p-adic Fourier transform for general K is even less well behaved than for the case of $\mathbb{Q}_p$; even if the rigid analytic function corresponding to a p-adic distribution has bounded coefficients, the p-adic distribution may not necessarily be a p-adic measure. As an application of our result, we obtain the congruences originally proved by Katz [7, Theorem 3.11] and Chellali [4, Théorème 1.1] of Bernoulli-Hurwitz numbers, which are essentially special values of p-adic L-functions of CM elliptic curves at non-ordinary primes.

We now give the exact statements of our theorems. Let p be a rational prime and let $|\cdot|$ be the absolute value of $\mathbb{C}_p$ such that $|p| = p^{-1}$. Let π be an uniformizer of $\mathcal{O}_K$, and let $\mathbb{F}_q$ be the residue field of $\mathcal{O}_K$. We define $LA_N(\mathcal{O}_K, \mathbb{C}_p)$ to be the space of locally analytic functions on $\mathcal{O}_K$ of order N which take values in $\mathbb{C}_p$. That is, $f(x) \in LA_N(\mathcal{O}_K, \mathbb{C}_p)$ if and only if $f(x)$ is defined as a convergent power series $\sum_{n=0}^{\infty} a_n(x-a)^n$ on $a+\pi^N\mathcal{O}_K$ for any $a \in \mathcal{O}_K$. We let $\|f\|_{a,N} := \max_n\{|a_n\pi^{nN}|\}$. The space $LA_N(\mathcal{O}_K, \mathbb{C}_p)$ is a p-adic Banach space induced by the norm $\max_{a\in\mathcal{O}_K}\{\|f\|_{a,N}\}$ and we denote by $LA_N(\mathcal{O}_K, \mathbb{C}_p)_0$ the submodule of elements whose absolute values are less than or equal to 1. We let $\mathcal{G}$ be a Lubin-Tate group of K corresponding to

π, and let $\varpi_p \in \mathbb{C}_p$ be a p-adic period of $\mathcal{G}$. We let

$$\overline{\rho}(k) = \max_{k \leqslant m}\{|m!/\varpi_p^m|\}, \quad \underline{\rho}(k) = \min_{0 \leqslant m \leqslant k}\{|m!/\varpi_p^m|\}.$$

See Proposition 3.1 for the properties of these numbers.

Let $\varphi(t)$ be a rigid analytic function on the open unit disc. In other words, $\varphi(t)$ is a power series of the form $\varphi(t) = \sum_{n=0}^{\infty} c_n t^n$ such that $|c_n| r_0^n \to 0$ for any $0 < r_0 < 1$. Let μ_φ be the distribution on $\mathcal{O}_K$ corresponding to $\varphi(t)$ given by Schneider-Teitelbaum's p-adic Fourier theory [8, Theorem 2.3]. Then we have the following:

Theorem 1.1. — *Let $f \in LA_N(\mathcal{O}_K, \mathbb{C}_p)$. Then we have*

$$\left| \int_{a+\pi^N \mathcal{O}_K} f(x)\, d\mu_\varphi \right| \leqslant \overline{\rho}(0) \left| \frac{\pi}{q} \right|^N \|f\|_{a,N} \|\varphi\|_N \tag{1.1}$$

where

$$\|\varphi\|_N := \max_k \left\{ |c_k| \overline{\rho}\left(\left[\frac{k}{q^N} \right] \right) \right\} \tag{1.2}$$

and $[x]$ is the integral part of x.

The crucial difference from the case when $K = \mathbb{Q}_p$ is the fact that $|\pi/q| > 1$ when $K \neq \mathbb{Q}_p$. A finer version of the above is given as Theorem 4.3. Since $\overline{\rho}\left(\left[\frac{k}{q^N}\right]\right) \sim p^{-kr}$ where $r = 1/eq^N(q-1)$, the value $\|\varphi\|_N$ is approximated by

$$\|\varphi\|_{\overline{\mathbf{B}}(p^{-r})} = \max_{x \in \overline{\mathbf{B}}(p^{-r})} \{ |\varphi(x)| \},$$

where $\overline{\mathbf{B}}(p^{-r}) \subset \mathbb{C}_p$ is the closed disc of radius p^{-r} centered at the origin.

As an application of our main theorem, we obtain an estimate of the Fourier coefficients of Mahler like expansion of functions in $LA_N(\mathcal{O}_K, \mathbb{C}_p)$. Let $\lambda(t)$ be the formal logarithm of $\mathcal{G}$, and following [8], we define the polynomial $P_n(x)$ by

$$\exp(x\lambda(t)) = \sum_{n=0}^{\infty} P_n(x) t^n.$$

Note that when $\mathcal{G}$ is the multiplicative formal group $\mathcal{G} = \widehat{\mathbb{G}}_m$, then $\lambda(t) = \log(1+t)$ and the above expansion is simply

$$(1+t)^x = \sum_{n=0}^{\infty} \binom{x}{n} t^n.$$

Hence the polynomial $P_n(x)$ is a generalization of the binomial polynomial

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

Then we have the following.

Theorem 1.2 (Theorem 4.7). — *The series* $\sum_{n=0}^{\infty} a_n P_n(x\varpi_p)$ *converges to an element of* $LA_N(\mathcal{O}_K, \mathbb{C}_p)_0$ *for* a_n *satisfying*

$$|a_n| \leqslant \underline{\rho}\left(\left[\frac{n}{q^N}\right]\right), \qquad \lim_{n\to 0}|a_n|/\underline{\rho}\left(\left[\frac{n}{q^N}\right]\right) = 0.$$

Conversely, if $f(x) \in LA_N(\mathcal{O}_K, \mathbb{C}_p)_0$, *then it has an expansion*

$$f(x) = \sum_{n=0}^{\infty} a_n P_n(x\varpi_p)$$

of the form

$$|a_n| \leqslant c\left|\frac{\pi}{q}\right|^N \overline{\rho}\left(\left[\frac{n}{q^N}\right]\right), \qquad \lim_{n\to 0}|a_n|/\overline{\rho}\left(\left[\frac{n}{q^N}\right]\right) = 0,$$

where $c = 1$ *if* $e \leqslant p-1$, *and* $c = \overline{\rho}(0)$ *otherwise.*

Corollary 1.3 (Corollary 4.8). — *Suppose*

$$e_{N,n} := \underline{\gamma}\left(\left[\frac{n}{q^N}\right]\right) P_n(x\varpi_p), \qquad (n = 0, 1, \cdots),$$

where $\underline{\gamma}(u)$ *is an element in* $\mathbb{C}_p$ *such that* $\underline{\rho}(u) = |\underline{\gamma}(u)|$. *If we denote by* L_N *the* $\mathcal{O}_{\mathbb{C}_p}$*-module topologically generated by* $e_{N,n}$, *then*

$$\overline{\rho}(0)^{-2}\left|\frac{q}{\pi}\right|^N LA_N(\mathcal{O}_K, \mathbb{C}_p)_0 \subset L_N \subset LA_N(\mathcal{O}_K, \mathbb{C}_p)_0.$$

In particular, $L_N \otimes \mathbb{Q}_p = LA_N(\mathcal{O}_K, \mathbb{C}_p)$. *In other words, the functions* $e_{N,n}$ *form a* p*-adic Banach basis of* $LA_N(\mathcal{O}_K, \mathbb{C}_p)$. *Moreover, if* $e \leqslant p-1$, *then*

$$\left|\frac{q}{\pi}\right|^{N+1} LA_N(\mathcal{O}_K, \mathbb{C}_p)_0 \subset L_N \subset LA_N(\mathcal{O}_K, \mathbb{C}_p)_0.$$

This result for the case $\mathcal{O}_K = \mathbb{Z}_p$ *gives the result of Amice* [1, Théorème 3], *namely that the functions*

$$\left[\frac{n}{p^N}\right]!\binom{x}{n} \qquad (n = 0, 1, \cdots)$$

form a topological basis of $LA_N(\mathbb{Z}_p, \mathbb{C}_p)_0$ *(actually, we can show that it is a basis of* $LA_N(\mathbb{Z}_p, \mathbb{Q}_p)_0$*).*

As another application, in Theorem 5.8, we derive from our estimate of the integral the congruence of Bernoulli-Hurwitz numbers $BH(n)$ at supersingular primes established by Katz [7, Theorem 3.11] and Chellali [4, Théorème 1.1].

Acknowledgment. — Part of this research was conducted while the first author was visiting the Ecole Normale Supérieure in Paris, and the second author Institut de Mathématiques de Jussieu. The authors would like to thank their hosts Yves André and Pierre Colmez for hospitality. The authors would also like to thank Seidai Yasuda for reading an earlier version of the manuscript and pointing out mistakes.

2. Schneider-Teitelbaum's p-adic Fourier theory.

Let K be a finite extension of $\mathbb{Q}_p$ and $k = \mathbb{F}_q$ the residue field. Let e be the absolute ramification index of K. We fix a uniformizer π of K and let $\mathcal{G}$ be a Lubin-Tate formal group of K associated to π. For a natural number N and an element a of $\mathcal{O}_K$, we define the space $A(a+\pi^N\mathcal{O}_K, \mathbb{C}_p)$ of K-analytic functions on $a+\pi^N\mathcal{O}_K$ by

$$\begin{aligned}&A(a+\pi^N\mathcal{O}_K,\mathbb{C}_p)\\ &:=\left\{f : a+\pi^N\mathcal{O}_K \to \mathbb{C}_p \mid f(x) = \sum_{n=0}^{\infty} a_n(x-a)^n,\ a_n \in \mathbb{C}_p,\ \pi^{nN}a_n \to 0\right\}.\end{aligned}$$

We equip the space $A(a+\pi^N\mathcal{O}_K,\mathbb{C}_p)$ with the norm

$$\|f\|_{a,N} := \max_n \{|\pi^{nN}a_n|\} = \max_{x\in a+\pi^N\mathcal{O}_{\mathbb{C}_p}} \{|f(x)|\}.$$

We also define the space $LA_N(\mathcal{O}_K,\mathbb{C}_p)$ of locally K-analytic functions on $\mathcal{O}_K$ of order N by

$$\begin{aligned}&LA_N(\mathcal{O}_K,\mathbb{C}_p)\\ &:=\left\{f : \mathcal{O}_K \to \mathbb{C}_p \mid f|_{a+\pi^N\mathcal{O}_K} \in A(a+\pi^N\mathcal{O}_K,\mathbb{C}_p) \quad \text{for any } a \in \mathcal{O}_K\right\},\end{aligned}$$

which is a p-adic Banach space by the norm $\max_a \{\|f\|_{a,N}\}$. We denote by $LA_N(\mathcal{O}_K,\mathbb{C}_p)_0$ the submodule of elements whose absolute values are less than or equal to 1. We put

$$LA(\mathcal{O}_K,\mathbb{C}_p) = \bigcup_N LA_N(\mathcal{O}_K,\mathbb{C}_p)$$

and equip it with the inductive limit topology. A continuous $\mathbb{C}_p$-linear function $LA(\mathcal{O}_K,\mathbb{C}_p) \to \mathbb{C}_p$ is called a $\mathbb{C}_p$-valued distribution on $\mathcal{O}_K$. We denote the space of $\mathbb{C}_p$-valued distributions on $\mathcal{O}_K$ by $D(\mathcal{O}_K,\mathbb{C}_p)$, i.e.

$$D(\mathcal{O}_K,\mathbb{C}_p) = \varprojlim_N \mathrm{Hom}^{\mathrm{cont}}_{\mathbb{C}_p}(LA_N(\mathcal{O}_K,\mathbb{C}_p),\mathbb{C}_p).$$

We write an element of $D(\mathcal{O}_K, \mathbb{C}_p)$ symbolically as

$$\int d\mu : LA(\mathcal{O}_K, \mathbb{C}_p) \to \mathbb{C}_p, \quad f \mapsto \int f d\mu = \int_{\mathcal{O}_K} f(x)\, d\mu(x).$$

The space $D(\mathcal{O}_K, \mathbb{C}_p)$ has a product structure given by the convolution product. For a compact open set U of $\mathcal{O}_K$, we let

$$\int_U f(x) d\mu(x) := \int_{\mathcal{O}_K} f(x) \cdot 1_U(x)\, d\mu(x),$$

where 1_U is the characteristic function of U.

The structure of $D(\mathcal{O}_K, \mathbb{C}_p)$ is well-known for the case $K = \mathbb{Q}_p$ and described through the so-called Amice transform. We denote by R^{rig} the ring of rigid analytic functions on the open disc of radius 1, that is, the ring of power series of the form $\varphi(T) = \sum_{n=0}^{\infty} c_n T^n$ such that $|c_n| r_0^n \to 0$ for any $0 < r_0 < 1$. Then there exists an isomorphism of topological $\mathbb{C}_p$-algebras

$$D(\mathbb{Z}_p, \mathbb{C}_p) \cong R^{\mathrm{rig}}, \qquad \mu \mapsto \varphi \tag{2.1}$$

that is characterized by the equation

$$c_n = \int_{\mathbb{Z}_p} \binom{x}{n} d\mu(x)$$

or equivalently

$$\varphi(T) = \int_{\mathbb{Z}_p} (1+T)^x\, d\mu(x).$$

For the Mahler expansion

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

of $f \in LA(\mathbb{Z}_p, \mathbb{C}_p)$, Amice showed that $|a_n| r^n \to 0$ for some $r > 1$ and hence we can compute the integral as

$$\int_{\mathbb{Z}_p} f(x)\, d\mu = \sum_{n=0}^{\infty} a_n c_n. \tag{2.2}$$

Schneider-Teitelbaum [8, Theorem 2.3] constructed an isomorphism analogous to (2.1) for a general local field K.

Let ϖ_p be a p-adic period of $\mathcal{G}$. By Tate's theory of p-divisible groups and Lubin-Tate theory, we have

$$\mathrm{Hom}_{\mathcal{O}_{\mathbb{C}_p}}(\mathcal{G}, \widehat{\mathbb{G}}_m) \cong \mathrm{Hom}_{\mathbb{Z}_p}(T_p\mathcal{G}, T_p\widehat{\mathbb{G}}_m) \cong \mathcal{O}_K.$$

(The last isomorphism is non-canonical.) Hence there exists a generator of the $\mathcal{O}_K$-module $\mathrm{Hom}_{\mathcal{O}_{\mathbb{C}_p}}(\mathcal{G}, \widehat{\mathbb{G}}_m)$, which is written in the form of the integral power series $\exp(\varpi_p \lambda(t)) \in \mathcal{O}_{\mathbb{C}_p}[[t]]$ where $\lambda(t)$ is the logarithm of

$\mathcal{G}$. The element $\varpi_p \in \mathcal{O}_{\mathbb{C}_p}$ is determined uniquely up to an element of $\mathcal{O}_K^\times$. We fix such a ϖ_p and call it the p-adic period of $\mathcal{G}$ (if the height of $\mathcal{G}$ is equal to 1, then the *inverse* of ϖ_p is often called a p-adic period of $\mathcal{G}$. For example, see [9]). It is known that $|\varpi_p| = p^{-s}$, where $s = \frac{1}{p-1} - \frac{1}{e(q-1)}$ (see Appendix of [8] or an elementary proof in [3] when $K/\mathbb{Q}_p$ is unramified). We define the polynomials $P_n(X) \in K[X]$ by the formal expansion

$$\exp(X\lambda(t)) = \sum_{n=0}^{\infty} P_n(X)\, t^n.$$

Note that in the case $\mathcal{G} = \widehat{\mathbb{G}}_m$, $\pi = p$ and $\lambda(t) = \log(1+t)$, the polynomial $P_n(X)$ is simply the binomial polynomial $\binom{X}{n}$. By construction, $P_n(x\varpi_p)$ is in $\mathcal{O}_{\mathbb{C}_p}$ if $x \in \mathcal{O}_K$.

Theorem 2.1 (Schneider-Teitelbaum [8, §4]).

i) The series

$$\sum_{n=0}^{\infty} a_n P_n(x\varpi_p)$$

converges to an element of $LA(\mathcal{O}_K, \mathbb{C}_p)$ *if* $\overline{\lim}_n |a_n|^{\frac{1}{n}} < 1$. *Conversely, any locally K-analytic function $f(x)$ on $\mathcal{O}_K$ has a unique expansion*

$$f(x) = \sum_{n=0}^{\infty} a_n P_n(x\varpi_p)$$

for some sequence $(a_n)_n$ in $\mathbb{C}_p$ such that $\overline{\lim}_n |a_n|^{\frac{1}{n}} < 1$.

ii) There exists an isomorphism of topological $\mathbb{C}_p$-algebras

$$D(\mathcal{O}_K, \mathbb{C}_p) \cong R^{\mathrm{rig}}. \tag{2.3}$$

having the following characterization property: if $\varphi(T) = \sum_{n=0}^{\infty} c_n T^n$ *corresponds to a distribution μ, then*

$$c_n = \int_{\mathcal{O}_K} P_n(x\varpi_p)\, d\mu(x)$$

or equivalently

$$\varphi(t) = \int_{\mathcal{O}_K} \exp(x\varpi_p\lambda(t))\, d\mu(x).$$

Schneider and Teitelbaum called the power series $\varphi(t)$ corresponding to μ the Fourier transform of μ and denoted it by $F_\mu(t)$.

3. Power sums

In this section, we give an estimate of the absolute value of the power sum

$$S_{N,n,k} := \partial_{\mathcal{G}}^n \sum_{t_N \in \mathcal{G}[\pi^N]} (t \oplus t_N)^k|_{t=0},$$

where $x \oplus y = \mathcal{G}(x,y)$, $\partial_{\mathcal{G}}$ is the differential operator $\lambda'(t)^{-1}(d/dt)$, and $\mathcal{G}[\pi^N]$ is the kernel of the multiplication $[\pi^N]$ of $\mathcal{G}$. This estimate is crucial for everything in this paper. We use Newton's method to compute this value.

We define $\overline{\rho}[l,n]$ and $\underline{\rho}[l,n]$ by

$$\overline{\rho}[l,n] = \max_{l \leqslant m \leqslant n} \{|m!/\varpi_p^m|\}, \qquad \underline{\rho}[l,n] = \min_{l \leqslant m \leqslant n} \{|m!/\varpi_p^m|\}$$

for $l \leqslant n$. For $l > n$, we put $\overline{\rho}[l,n] = 0$ and $\underline{\rho}[l,n] = \infty$. Then $\overline{\rho}(k) = \overline{\rho}[k,\infty]$ and $\underline{\rho}(k) = \underline{\rho}[0,k]$ are the constants appearing in the introduction.

Proposition 3.1.

i) *The values $\overline{\rho}(k)$ and $\underline{\rho}(k)$ are decreasing with k.*

ii) *We have*

$$\underline{\rho}(k) \leqslant \overline{\rho}(k), \qquad \overline{\rho}(k) \leqslant \overline{\rho}(0)\underline{\rho}(k).$$

iii) *We have*

$$\underline{\rho}(k_1 + \cdots + k_n) \leqslant \underline{\rho}(k_1) \cdots \underline{\rho}(k_n).$$

iv) *We have*

$$p^{\frac{1}{p-1} - \frac{k}{e(q-1)}} \;\leqslant\; \underline{\rho}(k) \leqslant 1.$$

Proof. — i) is clear. For ii), first we have $\overline{\rho}(k) \geqslant |k!/\varpi_p^k| \geqslant \underline{\rho}(k)$. Suppose $\overline{\rho}(k) = |k_1!/\varpi_p^{k_1}|$ and $\underline{\rho}(k) = |k_2!/\varpi_p^{k_2}|$. Then $k_1 \geqslant k \geqslant k_2$ and

$$\left| \frac{k_1!}{\varpi_p^{k_1}} \Big/ \frac{k_2!}{\varpi_p^{k_2}} \right| = \left| \binom{k_1}{k_2} \frac{(k_1-k_2)!}{\varpi_p^{k_1-k_2}} \right| \leqslant \overline{\rho}(0).$$

For iii), suppose that $\underline{\rho}(k_i) = |l_i!/\varpi_p^{l_i}|$ for $l_i \leqslant k_i$. Then the assertion for $\underline{\rho}$ follows from

$$\underline{\rho}(k_1 + \cdots + k_n) \leqslant \left| \frac{(l_1 + \cdots + l_n)!}{\varpi_p^{l_1 + \cdots + l_n}} \right| \leqslant \left| \frac{(l_1 + \cdots + l_n)!}{l_1! \cdots l_n!} \right| \left| \frac{l_1!}{\varpi_p^{l_1}} \right| \cdots \left| \frac{l_n!}{\varpi_p^{l_n}} \right|.$$

For iv), suppose that $\underline{\rho}(k) = |l!/\varpi_p^l|$ for $l \leqslant k$. Then

$$p^{\frac{1}{p-1} - \frac{k}{e(q-1)}} \;\leqslant\; p^{\frac{1}{p-1} - \frac{l}{e(q-1)}} \;\leqslant\; \left| \frac{l!}{\varpi_p^l} \right| = \underline{\rho}(k).$$

□

If $e \leqslant p-1$, then we can determine $\overline{\rho}(k)$ and $\underline{\rho}(k)$ explicitly.

Lemma 3.2. — *Let k be a non-negative integer and let q be a power of p.*

i) For any integer $0 \leqslant r < q$, we have $\binom{kq+r}{r} \equiv 1 \mod p$.
ii) We have $\binom{k}{q} \in [k/q]\mathbb{Z}_p$.

Proof. — i) is clear. For ii), we write $k = aq + r$ with $0 \leqslant r < q$. We put $(1+x)^q = 1 + x^q + pf(x)$ for some integral polynomial $f(x)$. Then

$$(1+x)^k = (1 + x^q + pf(x))^a(1+x)^r \equiv (1+x^q)^a(1+x)^r \mod ap\mathbb{Z}_p[x].$$

Hence the coefficient of x^q in the above is in $a\mathbb{Z}_p$. □

Proposition 3.3. — *Let i, e and h be natural numbers. We put $q = p^h$. Then we have*

$$v_p(i!) \geqslant \frac{i}{p-1} - \frac{i}{e(q-1)} - h + \frac{1}{e} + \left[\frac{i}{q}\right]\left(\frac{1}{e} - \frac{1}{p-1} + \frac{1}{e(q-1)}\right) + v_p\left(\left[\frac{i}{q}\right]!\right).$$

In the above, equality holds if and only if $i \equiv -1 \mod q$. In particular, if $e \leqslant p-1$ or $i < q$, then we have

$$v_p(i!) \geqslant \frac{i}{p-1} - \frac{i}{e(q-1)} - h + \frac{1}{e}$$

and equality holds if and only if $i = q-1$. In this case, we have $\overline{\rho}(0) = |\pi/q|$.

Proof. — First, we assume that $i < q$. We prove the inequality by induction on h. If $h = 1$, then $i < p$. Hence the left-hand side $v_p(i!)$ is equal to zero, and the right-hand side takes the maximum value when $i = p-1$, which is also equal to zero. We assume that the inequality holds for natural numbers less than h. Since the right-hand side is strictly increasing for i, and $v_p(i!)$ strictly increases only when p divides i, we may assume that i is of the form $i = kp - 1$ for some natural number $k \leqslant p^{h-1}$. We have

$$v_p(i!) = v_p((kp)!) - v_p(kp) = k - 1 + v_p((k-1)!).$$

On the other hand, we have

$$\begin{aligned}
&\frac{i}{p-1} - \frac{i}{e(q-1)} - h + \frac{1}{e} \\
&\quad = (k-1) + \frac{k-1}{p-1} - \frac{k-1}{e(p^{h-1}-1)} - (h-1) + \frac{1}{e} + \frac{k-1}{e(p^{h-1}-1)} - \frac{kp-1}{e(q-1)} \\
&\quad \leqslant k - 1 + v_p((k-1)!).
\end{aligned}$$

In the last inequality, we used the inductive hypothesis and $k \leqslant p^{h-1}$. Hence we have the desired inequality, and equality holds only when $k = p^{h-1}$, i.e. when $i = q-1$. For $i \geqslant q$, by Lemma 3.2 ii) and by induction, we have

$$\begin{aligned} v_p(i!) \geqslant v_p((i-q)!) + v_p(q!) + v_p\left(\left[\frac{i}{q}\right]\right) \\ \geqslant \frac{i}{p-1} - \frac{i}{e(q-1)} - h + \frac{1}{e} \\ + \left[\frac{i}{q}\right]\left(\frac{1}{e} - \frac{1}{p-1} + \frac{1}{e(q-1)}\right) + v_p\left(\left[\frac{i}{q}\right]!\right). \end{aligned}$$

From the above argument and by induction, to have the equality, i must be congruent to -1 modulo q. On the other hand, if $i \equiv -1 \mod q$, then direct calculations give the equality. □

Proposition 3.4. — *Suppose that $e \leqslant p-1$, and that $e > 1$ or $h > 1$.*

i) We have $|n!/\varpi_p^n| > 1$ for $0 < n < q$.

ii) For any non-negative integer n, $\underline{\rho}(n) = |n_0!/\varpi_p^{n_0}|$ where $n_0 = [n/q]q$.

iii) For $n \equiv -1 \mod q$ and a natural number $i \neq q$, we have

$$\left|\frac{n!}{\varpi_p^n}\right| > \left|\frac{(n+q)!}{\varpi_p^{n+q}}\right| > \left|\frac{(n+i)!}{\varpi_p^{n+i}}\right|$$

In particular, for any non-negative integer n, we have $\overline{\rho}(n) = |n_1!/\varpi_p^{n_1}|$ where $n_1 = [n/q]q + q - 1$.

Proof. — We prove i) by induction on h of $q = p^h$. If $h = 1$, then $n!$ is a p-adic unit and the assertion is clear. Assume that $h > 1$. We write as $n = kp + r$ with $0 \leqslant r < p$. Then

$$\frac{n!}{\varpi_p^n} = \binom{n}{r}\frac{(kp)!}{\varpi_p^{kp}}\frac{r!}{\varpi_p^r}.$$

Hence by Lemma 3.2 i) and the induction on n, we may assume that $r = 0$ and $k \geqslant 1$. Then

$$v_p\left(\frac{(kp)!}{\varpi_p^{kp}}\right) = v_p((kp)!) - \frac{kp}{p-1} + \frac{kp}{e(q-1)} < v_p(k!) - \frac{k}{p-1} + \frac{k}{e(p^{h-1}-1)}.$$

By the inductive hypothesis for h, the right-hand side is negative or 0.

Next we prove ii). Suppose that $m < n_0$. Then

$$\left|\frac{n_0!}{\varpi^{n_0}}/\frac{m!}{\varpi_p^m}\right| = \left|\frac{n_0}{\varpi_p}\binom{n_0-1}{m}\frac{(n_0-m-1)!}{\varpi_p^{n_0-m-1}}\right| \leqslant \left|\frac{n_0}{\varpi_p}\right|\overline{\rho}(0) = \left|\frac{n_0\pi}{q\varpi_p}\right| < 1.$$

Suppose that $n \geqslant m > n_0$. We write as $m = [n/q]q + r$ with $0 < r < q$. Then i) and Lemma 3.2 i) show that

$$\left|\frac{n_0!}{\varpi_p^{n_0}} \Big/ \frac{m!}{\varpi_p^m}\right| = \left|\binom{m}{r}^{-1} \frac{\varpi_p^r}{r!}\right| < 1.$$

Finally, we show iii). Let n be such that $n \equiv -1 \mod q$. We have

$$\frac{(n+i)!}{\varpi_p^{n+i}} \Big/ \frac{(n+q)!}{\varpi_p^{n+q}} = \frac{(n+i)!}{(n+q)!}\varpi_p^{q-i} = u\frac{q}{\pi}\frac{(i-1)!}{\varpi_p^{i-1}}\frac{\pi\varpi_p^{q-1}}{q!},$$

where $u = \binom{n+q}{q-1}^{-1}\binom{n+i}{i-1}$ is a p-adic integer by Lemma 3.2 i). By Proposition 3.3, the p-adic (additive) valuation of the right-hand side is positive. Since $v_p(\pi/\varpi_p) > 0$, the p-adic (additive) valuation of

$$\frac{(n+q)!}{\varpi_p^{n+q}} \Big/ \frac{n!}{\varpi_p^n} = \binom{n+q}{q}\frac{q!}{\pi\varpi_p^{q-1}}\frac{\pi}{\varpi_p}$$

is positive. □

Next we investigate the absolute values of the coefficients of a power of the logarithm and the exponential map of the Lubin-Tate group. The case $k = 1$ in the proposition below is obtained in [10].

Proposition 3.5. — *We put $\partial = d/dt$. Then we have*

$$\left|\frac{\varpi_p^k \partial^n \lambda(t)^k}{k!n!}|_{t=0}\right| \leqslant \underline{\rho}[k,n]^{-1}, \qquad \left|\partial^n \exp_{\mathcal{G}}^k(t)|_{t=0}\right| \leqslant |\varpi_p^n|\overline{\rho}[k,n].$$

Proof. — The case for $n < k$ or $k = 0$ is trivial. Suppose that $n \geqslant k \geqslant 1$. We first assume that the formal logarithm of $\mathcal{G}$ is given by

$$\lambda(t) = \sum_{m=0}^{\infty} \frac{t^{q^m}}{\pi^m}.$$

Then it suffices to show inequalities

$$\left|\partial^n \lambda(t)^k|_{t=0}\right| \leqslant |k!\varpi_p^{n-k}|, \qquad \left|\partial^n \exp_{\mathcal{G}}^k(t)|_{t=0}\right| \leqslant |k!\varpi_p^{n-k}|.$$

When $k = 1$, the inequality for $\lambda(t)$ is proven by direct calculations. We prove the general case by induction on k. We have

$$\begin{aligned}
\partial^n \lambda(t)^k|_{t=0} &= k\partial^{n-1}(\lambda(t)^{k-1}\lambda'(t))|_{t=0} \\
&= k\partial^{n-1}\sum_{m=0}^{\infty} \lambda(t)^{k-1}\frac{q^m t^{q^m-1}}{\pi^m}|_{t=0} \\
&= \sum_{m=0}^{\infty} \binom{n-1}{q^m-1}\frac{q^m!k}{\pi^m}\partial^{n-q^m}\lambda(t)^{k-1}|_{t=0}.
\end{aligned}$$

Hence we have $|\partial^n \lambda(t)^k|_{t=0}| \leqslant |k!\varpi_p^{n-k}|$.

We put $\exp_{\mathcal{G}}^k(t) = \sum_{n=k}^{\infty} a_n t^n$. We prove that $|n! a_n| \leqslant |k!\varpi_p^{n-k}|$ by induction on n. If $n = k$, then the assertion is true since $a_k = 1$. We assume that the assertion is true for integers less than n. Since $\exp_{\mathcal{G}}^k(\lambda(t)) = t^k$, we have

$$t^k = a_k \lambda(t)^k + a_{k+1}\lambda(t)^{k+1} + \cdots + a_n \lambda(t)^n + \cdots .$$

By i) and the inductive hypothesis, we have

$$|a_m \partial^n \lambda(t)^m|_{t=0}| \leqslant |k!\varpi_p^{n-k}|$$

for $m < n$. Since $\partial^n \lambda(t)^n|_{t=0} = n!$ and $\partial^n \lambda(t)^m|_{t=0} = 0$ for $n < m$, the assertion is also true for n.

Now we consider a general parameter s. Then the logarithm and the exponential for $\mathcal{G}$ with parameter s are of the form $\lambda(\phi(s))$ and $\psi(\exp_{\mathcal{G}}(s))$ for some $\phi(s), \psi(s) \in s\mathcal{O}_K[[s]]^\times$. We put $\lambda(t)^k = \sum_{n=k}^{\infty} c_n^{(k)} t^n$ and $\lambda(\phi(s))^k = \sum d_n^{(k)} s^n$. Then we have shown that $|c_n^{(k)}| \leqslant |k!\varpi_p^{n-k}/n!|$. Since $d_n^{(k)}$ is a linear sum of $c_l^{(k)}$ $(k \leqslant l \leqslant n)$ with integral coefficients, we have

$$\left|\frac{\varpi_p^k d_n^{(k)}}{k!}\right| \leqslant \max_{k \leqslant l \leqslant n} \left\{ \left| c_l^{(k)} \frac{\varpi_p^k}{k!} \right| \right\} \leqslant \max_{k \leqslant l \leqslant n} \left\{ \left| \frac{\varpi_p^l}{l!} \right| \right\} = \underline{\rho}[k,n]^{-1}.$$

Hence we have the inequality for the logarithm. The inequality for the exponential is straightforward. □

Lemma 3.6.

i) *Suppose that $f(t) \in \mathcal{O}_K[[t]]$ satisfies $f(t \oplus t_N) = f(t)$ for all $t_N \in \mathcal{G}[\pi^N]$. Then there exists a power series $g(t) \in \mathcal{O}_K[[t]]$ such that $f(t) = g([\pi^N]t)$.*

ii) *There exists an integral power series $g_k(t) \in \mathcal{O}_K[[t]]$ such that*

$$\pi^{-N} \sum_{t_N \in \mathcal{G}[\pi^N]} (t \oplus t_N)^k = g_k([\pi^N]t).$$

Proof. — See [5], Chapter III. □

We put

$$F(t,X) = \prod_{t_N \in \mathcal{G}[\pi^N]} (1 - (t \oplus t_N)X) = 1 + \alpha_1(t)X + \cdots + \alpha_{q^N}(t)X^{q^N}.$$

For $\partial_X = \partial/\partial X$, we consider the power series

$$\text{(3.1)} \qquad \frac{\pi^{-N}\partial_X F(t,X)}{F(t,X)} = -\sum_{k=0}^{\infty} \left(\pi^{-N} \sum_{t_N \in \mathcal{G}[\pi^N]} (t \oplus t_N)^{k+1} \right) X^k.$$

By Lemma 3.6 and the above formula, $\pi^{-N}\partial_X F(t,X) \in \mathcal{O}_K[[t]][X]$.

Proposition 3.7. — *Let k, n be non-negative integers and N a natural number. Then we have*

$$\left|\pi^{-N}\sum_{t_N\in\mathcal{G}[\pi^N]}\partial_{\mathcal{G}}^n(t\oplus t_N)^k|_{t=0}\right| \leqslant \left|\pi^{Nn+k_0(1-\frac{1}{q-1})}\varpi_p^n\right|\overline{\rho}\left(\left[\frac{k}{q^N}\right]\right)\overline{\rho}(0), \tag{3.2}$$

where $k_0=\max\{[k/q^N]-n,0\}$. We also have

$$\left|\pi^{-N}\sum_{t_N\in\mathcal{G}[\pi^N]}\partial_{\mathcal{G}}^n(t\oplus t_N)^k|_{t=0}\right| \leqslant \left|\pi^{Nn}\varpi_p^n\right|\overline{\rho}\,[0,n]\,. \tag{3.3}$$

Moreover, if $e\leqslant p-1$, we have

$$\left|\pi^{-N}\sum_{t_N\in\mathcal{G}[\pi^N]}\partial_{\mathcal{G}}^n(t\oplus t_N)^k|_{t=0}\right| \leqslant \left|\pi^{Nn}\varpi_p^n\right|\overline{\rho}\left(\left[\frac{k}{q^N}\right]\right). \tag{3.4}$$

Proof. — We put $G(t,X)=F(0,X)-F(t,X)$, then $G(0,X)=G(t,0)=0$. We have

$$\frac{1}{F(t,X)}=\frac{1}{F(0,X)-G(t,X)}=\sum_{l=0}^{\infty}\frac{G(t,X)^l}{F(0,X)^{l+1}}\quad\in\mathcal{O}_K[[t,X]].$$

Since $G(0,X)=0$ and $G(t,X)$ is invariant for the translation $t\mapsto t_N$, it is of the form

$$G(t,X)=([\pi^N]t)H([\pi^N]t,X) \tag{3.5}$$

for some element H in $\mathcal{O}_K[[t]][X]$. Since $F(0,X)\equiv 1 \mod \pi$, the power series $F(0,X)^{-l-1}$ is equal to

$$\sum_{m=0}^{\infty}\binom{-l-1}{m}(F(0,X)-1)^m=\sum_{m=0}^{\infty}\binom{l+m}{m}\pi^m\left(\frac{1-F(0,X)}{\pi}\right)^m.$$

Hence we have

$$\begin{aligned}\frac{\pi^{-N}\partial_X F(t,X)}{F(t,X)}&=\sum_{l=0}^{\infty}\pi^{-N}\partial_X F(t,X)\cdot G(t,X)^l\cdot F(0,X)^{-l-1}\\&=\sum_{l=0}^{\infty}\sum_{m=0}^{\infty}\binom{l+m}{m}\pi^m(\pi^{-N}\partial_X F(t,X))G(t,X)^l\left(\frac{1-F(0,X)}{\pi}\right)^m.\end{aligned} \tag{3.6}$$

To show the assertion for $k+1$, we look the coefficient of X^k in the last term of (3.6). We consider the coefficients of the terms X^a, X^b and X^c with $a+b+c=k$ of $\pi^{-N}\partial_X F(t,X)$, $G(t,X)^l$ and $(1-F(0,X))^m\pi^{-m}$ respectively. Since $\deg\partial_X F(t,X)=q^N-1$, $\deg G(t,X)=q^N$ and $\deg(1-$

$F(0,X)) = q^N - 1$ as polynomials for X, we have $a \leqslant q^N - 1, b \leqslant lq^N$ and $c \leqslant m(q^N - 1)$. Then by (3.5), the product of these coefficients is an integral linear combination of the terms of the form

$$\binom{l+m}{m}\pi^m G_l([\pi^N]t)$$

where $G_l(t)$ is a power series in $t^l\mathcal{O}_K[[t]]$ and l, m satisfies

$$a + lq^N + m(q^N-1) \geqslant a+b+c = k. \tag{3.7}$$

We estimate the absolute value of

$$\binom{l+m}{m}\pi^m \partial_{\mathcal{G}}^n\, G_l([\pi^N]t)\mid_{t=0}. \tag{3.8}$$

By Proposition 3.5, we have

$$\left|\partial_{\mathcal{G}}^n([\pi^N]t)^d|_{t=0}\right| = \left|\pi^{Nn}\frac{d^n}{dz^n}\exp_{\mathcal{G}}^d(z)|_{z=0}\right| \leqslant \left|\pi^{Nn}\varpi_p^n\right|\overline{\rho}[d,n].$$

Therefore, we have

$$\left|\partial_{\mathcal{G}}^n G_l([\pi^N]t)|_{t=0}\right| \leqslant \left|\pi^{Nn}\varpi_p^n\right|\overline{\rho}[l,n].$$

Hence we have (3.3). If $n < l$, then (3.8) is zero and there is nothing to prove. We assume that $n \geqslant l$. We let $l' \geqslant l$ be such that $\overline{\rho}(l) = |l'!/\varpi_p^{l'}|$. Then

$$\left|\binom{l+m}{m}\pi^m\partial_{\mathcal{G}}^n G_l([\pi]^N t)|_{t=0}\right| \leqslant \left|\binom{l+m}{m}\pi^{m+Nn}\varpi_p^n\right|\overline{\rho}[l,n] \tag{3.9}$$

$$\leqslant \left|\pi^{Nn}\varpi_p^n\frac{(l+m)!}{\varpi_p^{l+m}}\frac{(l'-l)!}{\varpi_p^{l'-l}}\binom{l'}{l}\frac{\varpi_p^m\pi^m}{m!}\right|. \tag{3.10}$$

First we consider the case $a \leqslant q^N - 2$ or $m \neq 0$. Then by (3.7) we have

$$l+m \geqslant \left[\frac{k+1}{q^N}\right].$$

In particular, $m \geqslant [(k+1)/q^N] - n$ and the value (3.10) is less than or equal to

$$|\pi^{Nn+k_0(1-\frac{1}{q-1})}\varpi_p^n|\overline{\rho}\left(\left[\frac{k+1}{q^N}\right]\right)\overline{\rho}(0)$$

where $k_0 = \max\{[(k+1)/q^N] - n, 0\}$. Hence in this case we have (3.2). Suppose that $e \leqslant p-1$. If $l' < l+m$, then $\left|\varpi_p^m\right| < \left|\varpi_p^{l'-l}\right|$ and hence the value (3.10) is less than $|\pi^{Nn}\varpi_p^n|\overline{\rho}\left(\left[\frac{k+1}{q^N}\right]\right)$. If $l' \geqslant l+m$, then

$$\overline{\rho}(l) = \left|\frac{l'!}{\varpi_p^{l'}}\right| \leqslant \overline{\rho}(l+m) \leqslant \overline{\rho}\left(\left[\frac{k+1}{q^N}\right]\right).$$

Hence the value (3.9) is also less than or equal to $|\pi^{m+Nn}\varpi_p^n|\overline{\rho}\left(\left[\frac{k+1}{q^N}\right]\right)$. Hence in this case we have (3.4).

Finally we consider the case when $a = q^N - 1$ and $m = 0$. Then the coefficient of $\pi^{-N}\partial_X F(t,X)$ of degree a is $(q/\pi)^N \alpha_{q^N}(t)$, which is divisible by $[\pi^N]t$. Hence in this case the product of the coefficient of X^a in $\pi^{-N}\partial_X F(t,X)$, the coefficient of X^b in $G(t,X)^l$ and the coefficient of X^c in $(1-F(0,X))^m\pi^{-m}$ is an integral linear combination of terms in the form $G_{l+1}([\pi^N]t)$ for some $G_{l+1}(t) \in t^{l+1}\mathcal{O}_K[[t]]$. In this case l satisfies $l+1 \geqslant \left[(k+1)/q^N\right]$. Therefore

$$\left|\partial_{\mathcal{G}}^n G_{l+1}([\pi]^N t)|_{t=0}\right| \leqslant \left|\pi^{Nn}\varpi_p^n\right|\overline{\rho}[l+1,n] \leqslant \left|\pi^{Nn}\varpi_p^n\right|\overline{\rho}\left(\left[\frac{k+1}{q^N}\right]\right).$$

If $n < l+1$, then (3.8) is zero and there is nothing to prove. We assume that $n \geqslant l+1$. In particular, by (3.7) we have $n \geqslant [(k+1)/q^N]$, and hence $k_0 = \max\{[(k+1)/q^N] - n, 0\} = 0$. Therefore we have (3.2) and (3.4). □

4. Integral structures on p-adic Fourier theory

In this section, we give an explicit construction of Schneider-Teitelbaum's p-adic distribution associated to a rigid analytic function on the open unit disc.

Let $\varphi(t)$ be a rigid analytic function on the open unit disc. We will construct a distribution μ_φ on $\mathcal{O}_K$ such that

$$\int_{\mathcal{O}_K} \exp(x\varpi_p\lambda(t))d\mu_\varphi = \varphi(t).$$

If we were able to first prove a Mahler like expansion for K-analytic functions as in the case of $K = \mathbb{Q}_p$, then it would be possible to define the integral by (2.2). However, as in [8], we will first define the integral then use this integral to prove the existence of the Mahler like expansion for K-analytic functions. Our construction of the integral is different from that of [8] in that we investigate directly the explicit power series corresponding to the moments of the integral, instead of formally reducing to the case of $\mathbb{Z}_p$.

We fix a Lubin-Tate formal group $\mathcal{G}$ associated to π, and denote its addition by $\oplus$. For $a \in \mathcal{O}_K$ and a natural number N, we let

$$\int_{a+\pi^N\mathcal{O}_K} (x-a)^n \, d\mu_\varphi := \frac{1}{q^N\varpi_p^n}\left(\partial_{\mathcal{G}}^n \sum_{t_N\in\mathcal{G}[\pi^N]} \varphi_a(t\oplus t_N)\right)\Bigg|_{t=0}$$

where

$$\varphi_a(t) := \exp(-a\varpi_p\lambda(t))\varphi(t).$$

We put $\varphi(t) = \sum_{k=0}^{\infty} c_k t^k$ and $\varphi_a(t) = \sum_{k=0}^{\infty} c_k^{(a)} t^k$. Then by Proposition 3.7, we have

$$\left|\int_{a+\pi^N\mathcal{O}_K} (x-a)^n \, d\mu_\varphi\right| \leqslant \overline{\rho}(0)\left|\frac{\pi}{q}\right|^N |\pi|^{Nn} \sup_k\{\, |c_k^{(a)}|\overline{\rho}\left(\left[\frac{k}{q^N}\right]\right)\} \tag{4.1}$$
$$\leqslant \overline{\rho}(0)\left|\frac{\pi}{q}\right|^N |\pi|^{Nn} \sup_k\{\, |c_k|\overline{\rho}\left(\left[\frac{k}{q^N}\right]\right)\}.$$

Here for the last estimate, we used the facts that $c_k^{(a)}$ is an integral linear combination of $c_0, \dots, c_k$ and the function $\overline{\rho}(m)$ for m is decreasing.

We define the distribution μ_φ on $LA_N(\mathcal{O}_K, \mathbb{C}_p)$ as follows. For an element f of $LA_N(\mathcal{O}_K, \mathbb{C}_p)$, suppose f is of the form $\sum_{n=0}^{\infty} a_n(x-a)^n$ such that $a_n\pi^{nN} \to 0$ if $n \to \infty$ on $a + \pi^N\mathcal{O}_K$. Then we define the integral of f on $a + \pi^N\mathcal{O}_K$ by

$$\int_{a+\pi^N\mathcal{O}_K} f(x)\, d\mu_\varphi := \sum_{n=0}^{\infty} a_n \int_{a+\pi^N\mathcal{O}_K} (x-a)^n \, d\mu_\varphi. \tag{4.2}$$

We define

$$\int_{\mathcal{O}_K} f(x)\, d\mu_\varphi = \sum_{a \bmod \pi^N} \int_{a+\pi^N\mathcal{O}_K} f(x)\, d\mu_\varphi. \tag{4.3}$$

We have to show the well-definedness of the integral.

Proposition 4.1.

i) *The integral* (4.2) *converges and does not depend on the choice of the representative of* $a \bmod \pi^N$. *The integral* (4.3) *does not depend on the choice of* N. *Hence* μ_φ *gives a well-defined element of* $D(\mathcal{O}_K, \mathbb{C}_p)$.

ii) *For a polynomial* $f(x)$, *we have*

$$\int_{\mathcal{O}_K} f(x)\, d\mu_\varphi = f(\varpi_p^{-1}\partial_{\mathcal{G}})\varphi(t)|_{t=0}.$$

Proof. — Since $\overline{\rho}([k/q^N]) \leqslant Ckp^{-\frac{k}{eqN(q-1)}}$ for some constant C which depends only on e, q and N, the value $\sup_k\{\, |c_k|\overline{\rho}\left(\left[\frac{k}{q^N}\right]\right)\}$ is finite. Hence the convergence follows from (4.1). We show that the integral (4.2) depends only on the class of a modulo π^N. Since the integral is convergent, we may assume that f is a monomial $(x-a)^n$. For a' such that $a' \equiv a \mod \pi^N$, we put $b = a' - a$. Since

$$(x-a)^n|_{a'+\pi^N\mathcal{O}_K} = \sum_{l=0}^{n} \binom{n}{l} b^{n-l}(x-a')^l|_{a'+\pi^N\mathcal{O}_K},$$

it suffices to show that

$$\int_{a+\pi^N\mathcal{O}_K} (x-a)^n \, d\mu_\varphi = \sum_{l=0}^{n} \binom{n}{l} b^{n-l} \int_{a'+\pi^N\mathcal{O}_K} (x-a')^l \, d\mu_\varphi.$$

This follows from

$$\begin{aligned}\varpi_p^{-n}\partial_{\mathcal{G}}^n\varphi_a(t\oplus t_m) &= \varpi_p^{-n}\partial_{\mathcal{G}}^n\left(\exp(b\varpi_p\lambda(t))\varphi_{a'}(t\oplus t_N)\right)\\ &= \exp(b\varpi_p\lambda(t))\sum_{l=0}^{n}\binom{n}{l}b^{n-l}\varpi_p^{-l}\partial_{\mathcal{G}}^l\left(\varphi_{a'}(t\oplus t_m)\right).\end{aligned}$$

Now we show that the integral (4.3) does not depend on N. It is sufficient to show the distribution relation

$$\int_{a+\pi^N\mathcal{O}_K} f(x)\, d\mu_\varphi = \sum_{b\equiv a \bmod \pi^N} \int_{b+\pi^{N+1}\mathcal{O}_K} f(x)\, d\mu_\varphi \tag{4.4}$$

where the sum runs over a representative b of $\mathcal{O}_K/\pi^{N+1}$ such that $b \equiv a$ mod π^N. To show this, replacing φ by φ_a, we may assume that $a = 0$ and $f(x) = x^n$. Then

$$\begin{aligned}&q^{N+1}\varpi_p^n \sum_{b\equiv 0 \mod \pi^N} \int_{b+\pi^{N+1}\mathcal{O}_K} x^n \, d\mu_\varphi\\ &= \sum_{b\equiv 0 \mod \pi^N} \sum_{i=0}^{k}\binom{n}{k} b^{n-k}\left(\varpi_p^{n-k}\partial_{\mathcal{G}}^k \sum_{t_{N+1}\in\mathcal{G}[\pi^{N+1}]} \varphi_b(t\oplus t_{N+1})\right)\Bigg|_{t=0}\\ &= \sum_{b\equiv 0 \mod \pi^N}\left(\partial_{\mathcal{G}}^n \sum_{t_{N+1}\in\mathcal{G}[\pi^{N+1}]} \exp(b\varpi_p\lambda(t))\varphi_b(t\oplus t_{N+1})\right)\Bigg|_{t=0}\\ &= \sum_{t_{N+1}\in\mathcal{G}[\pi^{N+1}]}\left(\sum_{b\equiv 0 \mod \pi^N} \exp(-b\varpi_p\lambda(t))|_{t=t_{N+1}}\right)\partial_{\mathcal{G}}^n\varphi(t\oplus t_{N+1})\Bigg|_{t=0}\\ &= q\left(\partial_{\mathcal{G}}^n \sum_{t_N\in\mathcal{G}[\pi^N]}\varphi(t\oplus t_N)\right)|_{t=0} = q^{N+1}\varpi_p^n\int_{\pi^N\mathcal{O}_K} x^n\, d\mu_\varphi.\end{aligned}$$

The above calculation is also true when $a = N = 0$, and hence we have

$$\varpi_p^n \sum_{b\in\mathcal{O}_K/\pi} \int_{b+\pi\mathcal{O}_K} x^n \, d\mu_\varphi = \partial_{\mathcal{G}}^n\varphi(t)|_{t=0}.$$

Assertion ii) follows from this equality. □

For $\varphi(t) = \sum_{k=0}^{\infty} c_k t^k \in R^{\mathrm{rig}}$, we define $\|\varphi\|_N$ by

$$\|\varphi\|_N := \max_k \left\{ |c_k| \overline{\rho}\left(\left[\frac{k}{q^N}\right]\right) \right\}. \tag{4.5}$$

Since $\overline{\rho}\left(\left[\frac{k}{q^N}\right]\right) \sim p^{-kr}$ where $r = 1/eq^N(q-1)$, the value $\|\varphi\|_N$ is approximately,

$$\|\varphi\|_{\overline{\mathbf{B}}(p^{-r})} = \max_{x \in \overline{\mathbf{B}}(p^{-r})} \{ |\varphi(x)| \}$$

where $\overline{\mathbf{B}}(p^{-r}) \subset \mathbb{C}_p$ is the closed disc with radius p^{-r} at origin.

Lemma 4.2. — *For an element $a \in \mathcal{O}_K$, let $\varphi_a(t) = \exp(-a\varpi_p \lambda(t))\varphi(t)$ as before. Then $\|\varphi_a\|_N = \|\varphi\|_N$.*

Proof. — It suffices to show that $\|\varphi_a\|_N \leqslant \|\varphi\|_N$. This follows from the same argument showing (4.1). □

Then Proposition 3.7 may rewritten as follows, which is a precise version of Theorem 1.1 of the introduction.

Theorem 4.3.

i) Suppose that the function $f \in LA_N(\mathcal{O}_K, \mathbb{C}_p)$ is given by a polynomial of degree d on $a + \pi^N\mathcal{O}_K$ for $a \in \mathcal{O}_K$. For $\varphi_k(t) = t^k$, we have

$$\left| \int_{a+\pi^N\mathcal{O}_K} f(x)\, d\mu_{\varphi_k} \right| \leqslant \overline{\rho}[0,d] \left| \frac{\pi}{q} \right|^N \|f\|_{a,N}. \tag{4.6}$$

We also have

$$\left| \int_{a+\pi^N\mathcal{O}_K} f(x)\, d\mu_{\varphi_k} \right| \leqslant \overline{\rho}(0) \left| \frac{\pi^{k_0(1-\frac{1}{q-1})+N}}{q^N} \right| \|f\|_{a,N} \overline{\rho}\left(\left[\frac{k}{q^N}\right]\right) \tag{4.7}$$

where $k_0 = \max\{[k/q^N] - d, 0\}$. Moreover, if $e \leqslant p-1$, then we have

$$\left| \int_{a+\pi^N\mathcal{O}_K} f(x)\, d\mu_{\varphi_k} \right| \leqslant \left| \frac{\pi}{q} \right|^N \|f\|_{a,N} \overline{\rho}\left(\left[\frac{k}{q^N}\right]\right). \tag{4.8}$$

ii) We have

$$\left| \int_{a+\pi^N\mathcal{O}_K} f(x)\, d\mu_{\varphi} \right| \leqslant \overline{\rho}(0) \left| \frac{\pi}{q} \right|^N \|f\|_{a,N} \|\varphi\|_N.$$

Moreover, if $e \leqslant p-1$, then

$$\left| \int_{a+\pi^N\mathcal{O}_K} f(x)\, d\mu_{\varphi} \right| \leqslant \left| \frac{\pi}{q} \right|^N \|f\|_{a,N} \|\varphi\|_N.$$

Corollary 4.4. — *We have*

$$\left|\int_{a+\pi^N\mathcal{O}_K} f(x)\, d\mu_\varphi\right| \leqslant p^{\frac{p}{p-1}+\frac{1}{e(q-1)}}\overline{\rho}(0)|\pi|^N \,\|f\|_{a,N}\|\varphi\|_{\mathbf{B}'(p^{-r})} \tag{4.9}$$

where $r = 1/eq^N(q-1)$ *and*

$$\|\varphi\|_{\mathbf{B}'(p^{-r})} := \max_k \left\{\, |c_k|kp^{-kr} \,\right\}.$$

Moreover, if $e \leqslant p-1$*, then*

$$\left|\int_{a+\pi^N\mathcal{O}_K} f(x)\, d\mu_\varphi\right| \leqslant p^{\frac{p}{p-1}+\frac{1}{e(q-1)}}|\pi|^N \,\|f\|_{a,N}\|\varphi\|_{\mathbf{B}'(p^{-r})}. \tag{4.10}$$

Proof. — The formula follows from

$$\overline{\rho}\left(\left[\frac{k}{q^N}\right]\right) \leqslant kq^{-N}p^{\frac{p}{p-1}+\frac{1}{e(q-1)}-\frac{k}{eq^N(q-1)}}.$$

□

As before, we define polynomials P_n by

$$\exp(x\lambda(T)) = \sum_{n=0}^{\infty} P_n(x)T^n.$$

Then by formal computation, we have

$$P_k(\partial_{\mathcal{G}})\varphi(t)|_{t=0} = \frac{1}{k!}\partial^k\varphi(t)|_{t=0}$$

where $\partial = d/dt$ (for example, formula 6 of Lemma 4.2 of [8]). We let $\varphi_n(t) = t^n$ and μ_{φ_n} the distribution associated to $\varphi_n(t)$. Then by Proposition 4.1 ii) we have

$$\int_{\mathcal{O}_K} P_k(x\varpi_p)\, d\mu_{\varphi_n} = \sum_{n=0}^{\infty} P_k(\partial_{\mathcal{G}})\varphi_n(t)|_{t=0} = \begin{cases} 1 & (k=n) \\ 0 & (k \neq n). \end{cases}$$

Hence if $\varphi(t) = \sum_{k=0}^{\infty} c_k t^k$, then

$$\int_{\mathcal{O}_K} P_k(x\varpi_p)\, d\mu_\varphi = c_k.$$

Equivalently,

$$\varphi(t) = \int_{\mathcal{O}_K} \exp(x\varpi_p\lambda(t))d\mu_\varphi.$$

Proposition 4.5. — *For* $N \geqslant 1$*, we have*

$$\left|\frac{q}{\pi}\right|^N \overline{\rho}\left(\left[\frac{n}{q^N}\right]\right)^{-1} c^{-1} \leqslant ||P_n(x\varpi_p)||_N \leqslant \underline{\rho}\left(\left[\frac{n}{q^N}\right]\right)^{-1}$$

where $c = 1$ *if* $e \leqslant p-1$ *and* $c = \overline{\rho}(0)$*, otherwise.*

Proof. — We have

$$1 = \left|\int_{\mathcal{O}_K} P_n(x\varpi_p)\, d\mu_{\varphi_n}\right| \leqslant \max_a\{\left|\int_{a+\pi^N\mathcal{O}_K} P_n(x\varpi_p)\, d\mu_{\varphi_n}\right|\}$$
$$\leqslant \left|\frac{\pi}{q}\right|^N ||P_n(x\varpi_p)\|_N\ \overline{\rho}\left(\left[\frac{n}{q^N}\right]\right)\overline{\rho}(0).$$

Similarly, if $e \leqslant p-1$, then by using (4.8), we obtain the lower estimate.

For the upper estimate, we put $P_n(x\pi^N\varpi_p) = \sum_{k=1}^n a_k^{(n)} x^k$ for $n \geqslant 1$. By the definition of P_n, the value $a_k^{(n)}$ is the coefficient of t^n of $\varpi_p^k\lambda([\pi^N]t)^k/k!$. Since $\underline{\rho}(k)$ is decreasing with k, we may assume that $\lambda(t) = \sum_{l=0}^\infty t^{q^l}/\pi^l$. Since $[\pi^N]t \equiv t^{q^N} \mod \pi$, we have

$$\lambda([\pi^N]t) \equiv \lambda(t^{q^N}) + \pi t f(t)$$

for some $f(t) \in \mathcal{O}_{\mathbb{C}_p}[[t]]$. (cf. [6, Lemma 4].) Hence we have

$$\frac{\varpi_p^k\lambda([\pi^N]t)^k}{k!} = \sum_{i=0}^k t^i f(t)^i \frac{\varpi_p^i\pi^i}{i!}\frac{\varpi_p^{k-i}\lambda(t^{q^N})^{k-i}}{(k-i)!}.$$

Therefore by Proposition 3.5 we have

$$|a_k^{(n)}| \leqslant \underline{\rho}\left(\left[\frac{n}{q^N}\right]\right)^{-1}.$$

Hence we have $||P_n(x\varpi_p)||_{0,N} \leqslant \underline{\rho}\left(\left[\frac{n}{q^N}\right]\right)^{-1}$. Then by the formula before Lemma 4.4 of [8], for $a \in \mathcal{O}_K$, we have

$$||P_n(x\varpi_p)||_{a,N} \leqslant \max_{0\leqslant i\leqslant n} ||P_i(x\varpi_p)||_{0,N} \leqslant \underline{\rho}\left(\left[\frac{n}{q^N}\right]\right)^{-1}.$$

□

Now we prove that our definition of the distribution coincides with that of Schneider-Teitelbaum. Namely, we will prove that the distribution has the characterization property (2.3).

THEOREM 4.6. — *Let μ_φ be the distribution associated to a rigid analytic function $\varphi(t)$ on the open unit disc. Then*

$$\varphi(t) = \int_{\mathcal{O}_K} \exp(x\varpi_p\lambda(t))d\mu_\varphi.$$

Conversely, for every distribution μ, there exists a unique rigid analytic function φ such that $\mu = \mu_\varphi$. Then φ is the Fourier transform of μ, and we have $F_{\mu_\varphi} = \varphi$. In particular, we have an isomorphism of algebras,

$$D(\mathcal{O}_K, \mathbb{C}_p) \cong R^{\mathrm{rig}}.$$

Proof. — We have already shown the first assertion. For a given μ, we put

$$c_k := \int_{\mathcal{O}_K} P_k(x\varpi_p)\, d\mu.$$

Since the distribution is a continuous linear operator on the p-adic Banach space $LA_N(\mathcal{O}_K, \mathbb{C}_p)$ for every natural number N, there exists a positive constant C depending only on μ and N such that

$$|c_k| = \left| \int_{\mathcal{O}_K} P_k(x\varpi_p)\, d\mu \right| \leqslant C\|P_k(x\varpi_p)\|_N \leqslant Cp^{-\frac{1}{p-1}+\frac{k}{eq^N(q-1)}}$$

where for the last inequality, we used Proposition 3.1 and Proposition 4.5. Hence for any $0 \leqslant r < 1$, if we choose sufficiently large N, we have $|c_k|r^k \to 0$ when $k \to \infty$. Hence $\varphi(t) = \sum_{k=0}^{\infty} c_k t^k$ is a rigid analytic function on the open unit disc. Then by construction

$$\varphi(t) = \int_{\mathcal{O}_K} \exp(x\varpi_p\lambda(t))d\mu.$$

Since the function $(x-a)|_{a+\pi^N\mathcal{O}_K}$ is given by

$$\frac{1}{q^N\varpi_p^n}\partial_{\mathcal{G}}^n \left(\sum_{t_N\in\mathcal{G}[\pi^N]} \exp((x-a)\varpi_p\lambda(t))|_{t=t\oplus t_N} \right) |_{t=0},$$

we have

$$\begin{aligned}\int_{a+\pi^N\mathcal{O}_K} (x-a)^n d\mu &= \frac{1}{q^N\varpi_p^n}\partial_{\mathcal{G}}^n \sum_{t_N\in\mathcal{G}[\pi^N]} \varphi_a(t\oplus t_N)|_{t=0} \\ &= \int_{a+\pi^N\mathcal{O}_K} (x-a)^n d\mu_\varphi.\end{aligned}$$

Since $\pi^{-nN}(x-a)^n|_{a+\pi^N\mathcal{O}_K}$ for $a \in \mathcal{O}_K$ and $n = 0, 1, \cdots$ are topological generators of $LA_n(\mathcal{O}_K, \mathbb{C}_p)$, we have

$$\int_{\mathcal{O}_K} f(x)d\mu = \int_{\mathcal{O}_K} f(x)d\mu_\varphi$$

for all $f \in LA_N(\mathcal{O}_K, \mathbb{C}_p)$. Hence $\mu = \mu_\varphi$. □

Now we prove Theorem 4.7.

THEOREM 4.7.

i) The series $\sum_{n=0}^{\infty} a_n P_n(x\varpi_p)$ converges to an element of $LA_N(\mathcal{O}_K, \mathbb{C}_p)_0$ for a_n satisfying

$$|a_n| \leqslant \underline{\rho}\left(\left[\frac{n}{q^N}\right]\right), \qquad \lim_{n\to 0}|a_n|/\underline{\rho}\left(\left[\frac{n}{q^N}\right]\right) = 0.$$

ii) If $f(x) \in LA_N(\mathcal{O}_K, \mathbb{C}_p)_0$, then it has an expansion

$$f(x) = \sum_{n=0}^{\infty} a_n P_n(x\varpi_p)$$

of the form

$$|a_n| \leqslant c \left|\frac{\pi}{q}\right|^N \overline{\rho}\left(\left[\frac{n}{q^N}\right]\right), \qquad \lim_{n\to 0} |a_n|/\overline{\rho}\left(\left[\frac{n}{q^N}\right]\right) = 0,$$

where $c = 1$ if $e \leqslant p-1$, and $c = \overline{\rho}(0)$, otherwise.

Proof. — i) follows from Proposition 4.5. For ii), we proceed as in the proof of Theorem 4.7 of [8] except the estimate of the Mahler coefficients. We put

$$a_n := \int_{\mathcal{O}_K} f(x)\, d\mu_{\varphi_n}.$$

Then by Theorem 4.3, we have

$$|a_n| = \left|\int_{\mathcal{O}_K} f(x)\, d\mu_{\varphi_n}\right| \leqslant c \left|\frac{\pi}{q}\right|^N \overline{\rho}\left(\left[\frac{n}{q^N}\right]\right).$$

We next prove the limit in ii). We may assume that $f(x) = \sum_{i=0}^{\infty} c_i (x-a)^i$ on $a + \pi^N \mathcal{O}_K$ and $f(x) = 0$ outside of $a + \pi^N \mathcal{O}_K$. For a given $\epsilon > 0$, we can take N_0 so that

$$\|\sum_{i=N_0}^{\infty} c_i (x-a)^i\|_{a,N} < \epsilon.$$

Hence by (4.7), we have

$$\left|\int_{a+\pi^N\mathcal{O}_K} \sum_{i=N_0}^{\infty} c_i (x-a)^i\, d\mu_{\varphi_n}\right| \leqslant \epsilon\, C_1 \overline{\rho}\left(\left[\frac{n}{q^N}\right]\right)$$

where C_1 is a positive constant independent of n. On the other hand, also by 4.7, we have

$$\left|\int_{a+\pi^N\mathcal{O}_K} \sum_{i=0}^{N_0} c_i (x-a)^i\, d\mu_{\varphi_n}\right| \leqslant C_2 p^{-\frac{n_0}{e}\left(1-\frac{1}{q-1}\right)} \overline{\rho}\left(\left[\frac{n}{q^N}\right]\right)$$

where $n_0 = \max\{[n/q^N] - N_0, 0\}$ and C_2 is a positive constant independent of n. Hence we have

$$\left|\int_{a+\pi^N\mathcal{O}_K} f(x)\, d\mu_{\varphi_n}\right| \leqslant \epsilon\, C_1 \overline{\rho}\left(\left[\frac{n}{q^N}\right]\right)$$

for sufficiently large n. Hence we have $|a_n|/\overline{\rho}\left(\left[\frac{n}{q^N}\right]\right) \to 0$ when $n \to \infty$. Then by i), the series $\sum_{k=0}^{\infty} a_n P_n(x\varpi_p)$ converges to a function in $LA_N(\mathcal{O}_K, \mathbb{C}_p)$. We put

$$g(x) = f(x) - \sum_{k=0}^{\infty} a_n P_n(x\varpi_p).$$

Then we have $\int_{\mathcal{O}_K} g(x)d\mu_{\varphi_n} = 0$ for all n, and hence $\int_{\mathcal{O}_K} g(x)d\mu = 0$ for all distribution μ. Considering the Dirac distribution $\delta_a : h \mapsto h(a)$, we have $g(a) = 0$ for any a. Hence $f(x) = \sum_{n=0}^{\infty} a_n P_n(x\varpi_p)$. □

Corollary 4.8. — *Suppose*

$$e_{N,n} = \underline{\gamma}\left(\left[\frac{n}{q^N}\right]\right) P_n(x\varpi_p), \qquad (n = 0, 1, \cdots),$$

where $\underline{\gamma}(u)$ is an element in $\mathbb{C}_p$ satisfying $\underline{\rho}(u) = |\underline{\gamma}(u)|$. If L_N is the $\mathcal{O}_{\mathbb{C}_p}$-module topologically generated by $e_{N,n}$, then

$$\overline{\rho}(0)^{-2}\left|\frac{q}{\pi}\right|^N LA_N(\mathcal{O}_K, \mathbb{C}_p)_0 \subset L_N \subset LA_N(\mathcal{O}_K, \mathbb{C}_p)_0.$$

In particular, the functions e_n form a topological basis of the p-adic Banach space $LA_N(\mathcal{O}_K, \mathbb{C}_p)$. Moreover, if $e \leqslant p-1$, then

$$\left|\frac{q}{\pi}\right|^{N+1} LA_N(\mathcal{O}_K, \mathbb{C}_p)_0 \subset L_N \subset LA_N(\mathcal{O}_K, \mathbb{C}_p)_0.$$

In addition, if $\mathcal{O}_K = \mathbb{Z}_p$, we recover Amice's result, namely that

$$\left[\frac{n}{p^N}\right]!\binom{x}{n}$$

for $n = 0, 1, \cdots$ form a topological basis of $LA_N(\mathbb{Z}_p, \mathbb{C}_p)_0$.

5. Relations to Katz's and Chellali's results.

As an application, we reprove Katz's and Chellali's results ([4], [7]) by using our results.

First we recall results of Katz [7] and Chellali [4]. Let E be an elliptic curve with complex multiplication by the ring of integer $\mathcal{O}_{\mathcal{K}}$ of an imaginary quadratic field $\mathcal{K}$. For simplicity, we assume that E is defined over $\mathcal{K}$, and fix a Weierstrass model

$$y^2 = 4x^3 - g_2x - g_3, \qquad g_2, g_3 \in \mathcal{O}_{\mathcal{K}}$$

of $E/\mathcal{K}$. Let p be an odd prime. We assume that p is inert in $\mathcal{K}$ and does not divide the discriminant of the above Weierstrass model, or equivalently, E

has good *supersingular* reduction at p. Then the Bernoulli-Hurwitz number $BH(n)$ is defined by

$$\wp(z) = \frac{1}{z^2} + \sum_{n \geqslant 2} \frac{BH(n+2)}{n+2} \frac{z^n}{n!},$$

where $\wp(z)$ is the Weierstrass $\wp$-function for the model. Let ϵ be a root of unity in $\mathcal{O}_\mathcal{K}$ such that the multiplication by $-\epsilon p$ gives the Frobenius $(x, y) \mapsto (x^{p^2}, y^{p^2})$ of $E \mod p$. Let γ be a unit in the Witt ring $W(\overline{\mathbb{F}}_p)$ such that

$$\gamma^{p^2-1} = -\epsilon^{-1} \frac{p^2!}{p^{p+1}(p^2-1)}.$$

For a fixed $b \in \mathcal{O}_K$ prime to p, we put

$$L(n) = \frac{(1-b^{n+2})(1-p^n)}{\gamma^n p^{[np/(p^2-1)]}} \frac{BH(n+2)}{n+2}.$$

Theorem 5.1 (Katz [7]). — *The number $L(n)$ is integral. Let l and n be non-negative integers. Then*

$$L(n + p^l(p^2-1)) \equiv L(n) \qquad \mod p^l.$$

Later, Chellali [4] refined the congruences as follows.

Theorem 5.2 (Chellali [4]). — *Let l and n be non-negative integers. If $n \not\equiv 0 \mod p^2 - 1$, we have*

$$L(n + p^l(p^2-1)) \equiv L(n) \qquad \mod p^{l+1}.$$

If $n \equiv 0 \mod p^2 - 1$ and $n \neq 0$, put $L'(n) = L(n)/n$, then

$$L'(n + p^l(p^2-1)) \equiv L'(n) \qquad \mod p^{l+1}.$$

In the following, let K be the unramified quadratic extension of $\mathbb{Q}_p$ and let $\mathcal{G}$ be the Lubin-Tate group of height $h = 2$ associated to the uniformizer $\pi = -\epsilon p$. We assume that $[\pi]T = \pi T + T^q$ for $q = p^2$ is an endomorphism of $\mathcal{G}$. It is known that the formal group of E at p is isomorphic to $\mathcal{G}$.

Proposition 5.3. — *Let φ be an integral power series and let μ_φ be the corresponding distribution associated to φ.*

i) We have

$$\left| \int_{\mathcal{O}_K^\times} x^n \, d\mu_\varphi \right| \leqslant p.$$

ii) If $m \equiv n \mod p^l(q-1)$, then

$$\left| \int_{\mathcal{O}_K^\times} (x^m - x^n) \, d\mu_\varphi \right| \leqslant p^{-l+\frac{p}{q-1}}.$$

iii) If $(q-1)|n$ *and* $m \equiv n \mod p^l(q-1)$*, then*

$$\left|\int_{\mathcal{O}_K^\times} \left(\frac{x^m-1}{m} - \frac{x^n-1}{n}\right) d\mu_\varphi\right| \leqslant p^{-l-1+\frac{2p}{q-1}}.$$

Proof. — We have

$$\int_{a+\pi\mathcal{O}_K} x^n \, d\mu_\varphi = a^n \int_{a+\pi\mathcal{O}_K} d\mu_\varphi + \sum_{k=1}^{n} \int_{a+\pi\mathcal{O}_K} \binom{n}{k}(x-a)^k a^{n-k} \, d\mu_\varphi.$$

Then by the estimate (4.6) the absolute value of the first integral is less than or equal to p. By the estimate (4.8), the absolute value of the second integral is also less than or equal to p since $||(x-a)||_{a,1}\overline{\rho}(0) = 1$. We put $m-n = k(q-1)$. Then

$$\begin{aligned} x^m - x^n &= x^n \sum_{i=1}^{k} \binom{k}{i} (x^{q-1}-1)^i \\ &= kx^n(x^{q-1}-1) + x^n \sum_{i=2}^{k} k \binom{k-1}{i-1} \frac{(x^{q-1}-1)^i}{i} \\ &= k\left(c_0 + c_1(x-a) + c_2\frac{(x-a)^2}{2} + c_3\frac{(x-a)^3}{3} + \cdots\right) \end{aligned}$$

where c_i are integers satisfying $p|c_0$. Since $\|(x-a)^i/i\|_{a,1} \leqslant p^{-2}$ for $i \geqslant 2$, the assertion ii) follows from the estimates (4.6).

For an integer s, we have

$$\begin{aligned} \frac{(x^{q-1})^s - 1}{s} &= \sum_{i=1}^{\infty} \frac{(\log_p x^{q-1})^i}{i!} s^{i-1} \\ &= \sum_{i=1}^{\infty} \sum_{n=i}^{\infty} c_{i,n} \frac{(x^{q-1}-1)^n}{n!} \\ &= \sum_{i=1}^{\infty} \sum_{j+k\geqslant i}^{\infty} c_{i,j,k} \frac{\pi^k}{k!} \frac{(x-a)^j}{j!} s^{i-1} \end{aligned}$$

for some integers $c_{i,n}$ and $c_{i,j,k}$. If we write $m = s_1(q-1)$ and $n = s_2(q-1)$, then

$$\frac{(x^{q-1})^{s_1}-1}{s_1} - \frac{(x^{q-1})^{s_2}-1}{s_2} = \sum_{i\geqslant 2, j+k\geqslant i}^{\infty} c_{i,j,k} \frac{\pi^k}{k!} \frac{(x-a)^j}{j!} (s_1^{i-1} - s_2^{i-1})$$

By the estimate (4.6), the integral of $\frac{\pi^k}{k!}\frac{(x-a)^j}{j!}$ is divisible by $p^{1-\frac{2p}{q-1}}$. The assertion iii) follows from this fact. □

For $b \in \mathcal{O}_K$ prime to p, we put

$$\wp_b(z) = (1 - b^2[b]^*)\wp(z)$$

and $\phi(t) = \wp_b(z)|_{z=\lambda(t)}$. Then $\wp_b(z)$ has no pole at $z = 0$ and

$$\wp_b(z) = \sum_{n \geqslant 2} (1 - b^{n+2}) \frac{BH(n+2)}{n+2} \frac{z^n}{n!}.$$

It is known that $\phi(t)$ is an integral power series. Similarly, for $c \in \mathcal{O}_K$ prime to p, we put

$$\zeta_c(z) = (c - [c]^*)\zeta(z), \qquad \zeta_{b,c}(z) = (1 - b[b]^*)\zeta_c(z),$$

where $\zeta(z)$ is the Weierstrass zeta function and $\psi(t) = \zeta_{b,c}(z)|_{z=\lambda(t)}$. Note that $\zeta_c(z)$ is double periodic and $\zeta_{b,c}(z)$ has no pole at $z = 0$. Then

$$\zeta_{b,c}(z) = \sum_{n \geqslant 3} (c - c^n)(1 - b^{n+1}) \frac{BH(n+1)}{n+1} \frac{z^n}{n!}$$

and $\psi(t)$ is an integral power series.

Lemma 5.4.

$$\sum_{z_0 \in \frac{1}{p}\Gamma/\Gamma} \wp_b(z + z_0) = p^2 \wp_b(pz), \sum_{z_0 \in \frac{1}{p}\Gamma/\Gamma} \zeta_c(z + z_0) = p\zeta_c(pz).$$

Proof. — It is known that

$$\sum_{z_0 \in \frac{1}{p}\Gamma/\Gamma} \wp(z + z_0) = p^2 \wp(pz).$$

The first formula follows from this. The above formula also shows that for a set S of representatives of $\frac{1}{p}\Gamma/\Gamma$, there exists a constant $A(S)$ such that

$$\sum_{z_0 \in S} \zeta(z + z_0) = p\zeta(pz) + A(S).$$

We take S so that $S = -S$. Then since $\zeta(z)$ is an odd function, $A(S)$ should be zero. Therefore,

$$\sum_{z_0 \in S} \zeta_c(z + z_0) = p\zeta_c(pz).$$

Since $\zeta_c(z)$ is an elliptic function, the left-hand side does not depend on the choice of S. □

Proposition 5.5. — *We put* $B(n) = BH(n+2)/(n+2)$ *if* $n \geqslant 2$ *and* 0 *if* $n = -1, 0, 1$. *For* $n \geqslant 0$, *we have*

$$\varpi_p^n \int_{\mathcal{O}_K^\times} x^n d\mu_\phi = (1 - p^n)(1 - b^{n+2})B(n),$$

$$\varpi_p^n \int_{\mathcal{O}_K^\times} x^n d\mu_\psi = (1-p^{n-1})(c-c^n)(1-b^{n+1})B(n-1).$$

Proof. — Since $\wp_b(z)$ and $\zeta_{b,c}(z)$ are double periodic, for $t_0 \in \mathcal{G}[p]$ we have $\psi(t\oplus t_0) = \zeta_{b,c}(z+z_0)|_{z=\lambda(t)}$ and $\phi(t\oplus t_0) = \wp_b(z+z_0)|_{z=\lambda(t)}$ where z_0 is an image of t_0 by $\mathcal{G}[p] \to E[p] \to \frac{1}{p}\Gamma/\Gamma$ (see for example, [2], Lemma 2.18). From this fact and the previous lemma, we have

$$\phi(t) - \frac{1}{q}\sum_{t_0\in\mathcal{G}[p]} \phi(t\oplus t_0) = (\wp_b(z) - \wp_b(pz))\,|_{z=\lambda(t)},$$

$$\psi(t) - \frac{1}{q}\sum_{t_0\in\mathcal{G}[p]} \psi(t\oplus t_0) = (\zeta_{b,c}(z) - p^{-1}\zeta_{b,c}(pz))\,|_{z=\lambda(t)}.$$

Hence

$$\begin{aligned}\varpi_p^n \int_{\mathcal{O}_K^\times} x^n d\mu_\phi &= \partial_{\mathcal{G}}^n \left(\phi(t) - \frac{1}{q}\sum_{t_0\in\mathcal{G}[p]} \phi(t\oplus t_0)\right)\Bigg|_{t=0} \\ &= \partial_z(\wp_b(z) - \wp_b(pz))|_{z=0} = (1-p^n)(1-b^{n+2})B(n).\end{aligned}$$

The other equality is also shown similarly. □

We put

$$c(n) = (1-p^n)(1-b^{n+2})\frac{BH(n+2)}{n+2}.$$

Corollary 5.6.

i) We have

$$\left|\frac{c(n)}{\varpi_p^n}\right| \leqslant p.$$

Furthermore, if $n \equiv 0 \mod q-1$, *then*

$$\left|\frac{c(n)}{\varpi_p^n}\right| \leqslant p^{\frac{p}{q-1}}.$$

ii) Suppose that $m \equiv n \mod p^l(q-1)$. *Then*

$$\frac{c(m)}{\varpi_p^m} \equiv \frac{c(n)}{\varpi_p^n} \qquad \mod p^{l-\frac{p}{q-1}}\mathcal{O}_{\mathbb{C}_p}.$$

Furthermore, if $n \not\equiv 0 \mod q-1$, *then*

$$\frac{c(m)}{\varpi_p^m} \equiv \frac{c(n)}{\varpi_p^n} \qquad \mod p^l\mathcal{O}_{\mathbb{C}_p}.$$

If $n \equiv 0 \mod q-1$, *then*

$$\frac{c(m)}{m\varpi_p^m} \equiv \frac{c(n)}{n\varpi_p^n} \qquad \mod p^{l+1-\frac{2p}{q-1}}.$$

Proof. — For i), the first inequality follows from Proposition 5.3 i) for μ_ϕ. The second inequality follows from Proposition 5.3 ii) for $l = 0$. Note that $\int_{\mathcal{O}_K^\times} d\mu_\phi = 0$. For ii), the first and third congruences follow from Proposition 5.3 for ϕ, and the second inequality for ψ. □

Next, we compare $c(n)$ with $L(n)$.

Lemma 5.7. — *We choose $u \in \mathbb{C}_p$ so that $\varpi_p^{q-1} = p^p u^{q-1}$. Then u is a unit of $\mathcal{O}_{\mathbb{C}_p}$ and*

$$\left(\frac{u}{\gamma}\right)^{q-1} \equiv 1 \qquad \mathrm{mod}\ p.$$

Proof. — Simple calculation shows the valuation of u is zero. We have $\lambda(t) = t + \theta t^q + \cdots$ with $\theta = 1/\epsilon(p^q - p)$. The q-th coefficient of the integral power series $\exp(\varpi_p \lambda(t))$ is

$$\frac{\varpi_p^q}{q!} + \varpi_p\theta = \varpi_p\theta\left(\frac{\varpi_p^{q-1}}{\theta q!} + 1\right).$$

Since $\varpi_p\theta$ is not integral, the valuation $v_p((\varpi_p^{q-1}/\theta q!) + 1) \geqslant 1$. Thus

$$\frac{\varpi_p^{q-1}}{\theta q!} + 1 \equiv \left(\frac{u}{\gamma}\right)^{q-1} \frac{(1-p^{q-1})}{(q-1)} + 1 \equiv -\left(\frac{u}{\gamma}\right)^{q-1} + 1 \qquad \mathrm{mod}\ p.$$

must be congruent to zero. □

Let $n = n'(q-1) + r$ with $0 \leqslant r < q-1$ and put $c_r = u^{-r} p^{-[pr/(q-1)]} \varpi_p^r$. Then

$$\varpi_p^n = c_r p^{[pn/(q-1)]} u^n.$$

Hence we have

$$L(n) = c_r \left(\frac{u}{\gamma}\right)^n \frac{c(n)}{\varpi_p^n}.$$

Therefore by Corollary 5.6 i), we have $|L(n)| < p$ (note that if $n \not\equiv 0 \mod q-1$, then $|c_r| < 1$). Since $L(n)$ is contained in the unramified field K, we have $L(n) \in \mathcal{O}_K$. Similary, for $m \equiv n \mod p^l(q-1)$, the fact $L(n) \in \mathcal{O}_K$, Lemma 5.7 and Corollary 5.6 ii) imply the congruence

$$L(m) \equiv L(n)\left(\frac{u}{\gamma}\right)^{m-n} \equiv L(n) \qquad \mathrm{mod}\ p^{l-\frac{p}{q-1}}.$$

Since this is a congruence between elements of $\mathcal{O}_K$, we have

$$L(m) \equiv L(n) \qquad \mathrm{mod}\ p^l.$$

Similarly, from Corollary 5.6, we obtain the congruences originally proved by Katz [7, Theorem 3.1] and Chellali [4, Théorème 1.1].

Theorem 5.8.

i) We have $L(n) \in \mathcal{O}_K$.

ii) Suppose that $m \equiv n \mod p^l(q-1)$. *Then*

$$L(m) \equiv L(n) \qquad \mod p^l.$$

Furthermore, if $n \not\equiv 0 \mod q-1$, *then*

$$L(m) \equiv L(n) \qquad \mod p^{l+1}.$$

If $n \equiv 0 \mod q-1$, *then*

$$L'(m) \equiv L'(n) \qquad \mod p^{l+1}.$$

BIBLIOGRAPHY

[1] Y. Amice, "Interpolation p-adique", *Bull. Soc. Math. France* **92** (1964), p. 117-180.

[2] K. Bannai & S. Kobayashi, "Algebraic theta functions and the p-adic interpolation of Eisenstein-Kronecker numbers", *Duke Math. J.* **153** (2010), no. 2, p. 229-295.

[3] J. L. Boxall, "p-adic interpolation of logarithmic derivatives associated to certain Lubin-Tate formal groups", *Ann. Inst. Fourier (Grenoble)* **36** (1986), no. 3, p. 1-27.

[4] M. Chellali, "Congruences entre nombres de Bernoulli-Hurwitz dans le cas supersingulier", *J. Number Theory* **35** (1990), no. 2, p. 157-179.

[5] R. F. Coleman, "Division values in local fields", *Invent. Math.* **53** (1979), no. 2, p. 91-116.

[6] T. Honda, "Formal groups and zeta-functions", *Osaka J. Math.* **5** (1968), p. 199-213.

[7] N. M. Katz, "Divisibilities, congruences, and Cartier duality", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28** (1981), no. 3, p. 667-678 (1982).

[8] P. Schneider & J. Teitelbaum, "p-adic Fourier theory", *Doc. Math.* **6** (2001), p. 447-481 (electronic).

[9] E. de Shalit, *Iwasawa theory of elliptic curves with complex multiplication*, Perspectives in Mathematics, vol. 3, Academic Press, Inc., Boston, MA, 1987, p-adic L functions, x+154 pages.

[10] K. Shiratani & T. Imada, "The exponential series of the Lubin-Tate groups and p-adic interpolation", *Mem. Fac. Sci. Kyushu Univ. Ser. A* **46** (1992), no. 2, p. 351-365.

Manuscrit reçu le 27 mars 2015,
accepté le 11 juin 2015.

Kenichi BANNAI
Department of Mathematics,
Keio University,
3-14-1 Hiyoshi,
Kouhoku-ku, Yokohama
223-8522 (Japan)
bannai@math.keio.ac.jp

Shinichi KOBAYASHI
Mathematical Institute,
Tohoku University,
6-3 Aramaki-aza-Aoba,
Aoba-ku, Sendai
980-8578 (Japan)
shinichi@math.tohoku.ac.jp