Annales mathématiques Blaise Pascal

Lucien van Hamme

The p-adic Z-transform

Annales mathématiques Blaise Pascal, tome 2, nº 1 (1995), p. 131-146
<http://www.numdam.org/item?id=AMBP_1995__2_1_131_0>

Ann. Math. Blaise Pascal, Vol. 2, N° 1, 1995, pp.131-146

THE P-ADIC Z-TRANSFORM

Lucien van Hamme

Abstract. Let $a+p^n\mathbb{Z}_p$ be a ball in $\mathbb{Z}_p$ and assume that a is the smallest natural number contained in the ball. We define a measure μ_z on $\mathbb{Z}_p$ by putting $\mu_z(a+p^n\mathbb{Z}_p) = \frac{z^a}{1-z^{p^n}}$ where $z \in \mathbb{C}_p, |z-1|_p \geq 1$. Let f be a continuous function defined on $\mathbb{Z}_p$. The mapping $f \to \int_{\mathbb{Z}_p} f(x)\mu_z(x)$ is similar to the classical Z-transform. We use this transform to give new proofs of several known results : the Mahler expansion with remainder for a continuous function, the Van der Put expansion, the expansion of a function in a series of Sheffer polynomials. We also prove some new results.

1991 Mathematics subject classification : 46S10

1. Introduction

Let $\mathbb{Z}_p$ be the ring of p-adic integers, where p is a prime.
$\mathbb{Q}_p$ and $\mathbb{C}_p$ denote, as usual, the field of the p-adic numbers and the completion of the algebraic closure of $\mathbb{Q}_p$. $|.|$ denotes the normalized p-adic valuation on $\mathbb{C}_p$.
We start by defining a measure on $\mathbb{Z}_p$.
Let $a+p^n\mathbb{Z}_p$ be a ball in $\mathbb{Z}_p$. We may assume that a is the smallest natural number contained in the ball. Our measure will depend on a parameter $z \in \mathbb{C}_p$.
Put $\mu_z(a+p^n\mathbb{Z}_p) = \frac{z^a}{1-z^{p^n}}$.
It is well-known that this defines a distribution on $\mathbb{Z}_p$.
Let D denote the set $\{z \in \mathbb{C}_p \mid |z-1| \geq 1\}$.
An easy calculation shows that if $z \in D$ then $\left|\frac{z^a}{1-z^{p^n}}\right| \leq 1$.
Throughout this paper we will assume that $z \in D$. Hence μ_z is a measure.
Now let $f : \mathbb{Z}_p \to \mathbb{C}_p$ be a continuous function.

If we associate with f the integral $F(z) = \int_{\mathbf{Z}_p} f(x)\mu_z(x)$ we get a transformation that we call the p-adic Z-transform since it is similar to the classical Z-transform used by engineers. The aim of this paper is to show how this transform can be used to obtain a number of results in p-adic analysis. In section 2 we start by studying the integral $F(z)$. In sections 3 and 4 we use the p-adic Z-transform to give new proofs of several known results : the Mahler expansion with remainder for a continuous function, the Van der Put expansion, the expansion of a function in a series of Sheffer polynomials. In section 5 we use the results of section 2 to find approximations to the p-adic logarithm of 2. We prove e.g. that the following congruence is valid in $\mathbf{Z}_p$

$$2\left(1-\frac{1}{p}\right)\lg 2 \equiv \sum_{\substack{k=1\\(k,p)=1}}^{p^n} \frac{(-1)^{k+1}}{k} \equiv 4(-1)^{n.\frac{p-1}{2}} \sum_{\substack{k=0\\(2k+1,p)=1}}^{\frac{p^n-3}{2}} \frac{(-1)^k}{2k+1} \qquad (\mathrm{mod}\ p^{2n}\mathbf{Z}_p)$$

2. The integral $\int_{\mathbf{Z}_p} f(x)\mu_z(x)$

This integral has already been studied and used by Y. Amice and others in [1] and [4].
A fundamental property of this integral is
Proposition : $F(z)$ is an analytic element in D (in the sense of Krasner).
This means that $F(z)$ is the uniform limit of a sequence of rational functions with poles outside D. But, by definition

$$F(z) = \int_{\mathbf{Z}_p} f(x)\mu_z(x) = \lim_{n\to\infty} \frac{\sum_{k=0}^{p^n-1} f(k)z^k}{1-z^{p^n}} \tag{1}$$

It is not difficult to show that the sequence in (1) is uniformly convergent. Since the zeroes of $1-z^{p^n}$ are outside D, $F(z)$ is an analytic element in D.
Corollary : F satisfies the "principle of analytic continuation" i.e. if $F(z)$ is zero on a ball in D it is zero in the whole of D.

The fact that $F(z)$ is an analytic element in D is very useful in proving properties of the integral (1). As an example we prove that

$$\int_{\mathbf{Z}_p} f(x)\mu_z(x) = f(0) + z\int_{\mathbf{Z}_p} f(x+1)\mu_z(x) \quad \text{in } D \tag{2}$$

Proof : For $|z| < 1$ formula (1) reduces to

$$\int_{\mathbf{Z}_p} f(x)\mu_z(x) = \sum_{k=0}^{\infty} f(k)z^k \tag{3}$$

The trivial identity

$$\sum_{k=0}^{\infty} f(k)z^k = f(0) + z\sum_{k=0}^{\infty} f(k+1)z^k \qquad (|z|<1)$$

can be written as

$$\int_{\mathbf{Z}_p} f(x)\mu_z(x) = f(0) + z\int_{\mathbf{Z}_p} f(x+1)\mu_z(x)$$

This is a priori valid for $|z| < 1$. By analytic continuation it is valid in D.

We now list some properties of the integral $\int_{\mathbf{Z}_p} f(x)\mu_z(x)$. We only give a few indications about the proofs.

P1 $$\int_{\mathbf{Z}_p} f(x)\mu_z(x) = \sum_{k=0}^{n-1} f(k)z^k + z^n\int_{\mathbf{Z}_p} f(x+n)\mu_z(x) \quad \text{in } D \tag{4}$$

Proof : This follows by iterating (2)

P2 $$\begin{aligned}\int_{\mathbf{Z}_p} f(x)\mu_z(x) &= -\sum_{k=1}^{n} \frac{f(-k)}{z^k} + \frac{1}{z^n}\int_{\mathbf{Z}_p} f(x-n)\mu_z(x) \quad \text{in } D \\ &= -\sum_{k=1}^{\infty} \frac{f(-k)}{z^k} \quad \text{if } |z|>1\end{aligned} \tag{5}$$

Proof : Replace $f(x)$ by $f(x-1)$ in (2) to get

$$\int_{\mathbf{Z}_p} f(x)\mu_z(x) = -\frac{f(-1)}{z} + \frac{1}{z}\int_{\mathbf{Z}_p} f(x-1)\mu_z(x)$$

Iteration of this formula yields (5).

P3 $$\begin{aligned}\int_{\mathbf{Z}_p} f(x)\mu_z(x) &= \sum_{k=0}^{n-1} (\Delta^k f)(0)\frac{z^k}{(1-z)^{k+1}} + \frac{z^n}{(1-z)^n}\int_{\mathbf{Z}_p} (\Delta^n f)(x)\mu_z(x) \\ &= \sum_{k=0}^{\infty} (\Delta^k f)(0)\frac{z^k}{(1-z)^{k+1}} \quad \text{in } D\end{aligned} \tag{6}$$

Here Δ is the difference operator defined by $(\Delta f)(x) = f(x+1) - f(x)$.

Proof : Write (2) in the form

$$\int_{\mathbf{Z}_p} f(x)\mu_z(x) = \frac{f(0)}{1-z} + \frac{z}{1-z}\int_{\mathbf{Z}_p} (\Delta f)(x)\mu_z(x)$$

then iterate.

Let E be the translation operator defined by $(Ef)(x) = f(x+1)$ and put $Q = \Delta E^{-1}$ then

P4 $$\int_{\mathbf{Z}_p} f(x)\mu_z(x) = \sum_{k=0}^{n-1} \frac{(Q^k f)(-1)}{(1-z)^{k+1}} + \frac{1}{(1-z)^n}\int_{\mathbf{Z}_p} (Q^n f)(x)\mu_z(x) \qquad (7)$$

Proof : This follows from the obvious

$$\int_{\mathbf{Z}_p} f(x)\mu_z(x) = \frac{f(-1)}{1-z} + \frac{1}{1-z}\int_{\mathbf{Z}_p} (Qf)(x)\mu_z(x)$$

P5 $$\int_{\mathbf{Z}_p} f(x)\mu_z(x) + \int_{\mathbf{Z}_p} f(-x)\mu_{1/z}(x) = f(0) \text{ in } D \qquad (8)$$

Proof : Suppose first that $|z| > 1$ and use (5) for the first integral and (3) for the second integral. The formula then reduces to the obvious identity.

$$-\sum_{k=1}^{\infty} \frac{f(-k)}{z^k} + \sum_{k=0}^{\infty} \frac{f(-k)}{z^k} = f(0)$$

The formula is valid in D by analytic continuation.

P6 If f is an even function then $\int_{\mathbf{Z}_p} f(x)\mu_{-1}(x) = \frac{f(0)}{2}$ (9)

Proof : Put $z = -1$ in (8).

P7 If $F(z) = \int_{\mathbf{Z}_p} f(x)\mu_z(x), G(z) = \int_{\mathbf{Z}_p} g(x)\mu_z(x)$

then $F(z)G(z) = \int_{\mathbf{Z}_p} (f * g)(x)\mu_z(x)$ in D (10)

where $f * g$ the convolution of f and g.

$f*g$ is by definition the continuous function with value equal to $(f * g)(n) = \sum_{k=0}^{n} f(k)g(n-k)$ if n is a natural number.

Proof : For $|z| \leq 1$ the equality $F(z)G(z) = \int_{\mathbb{Z}_p} (f * g)(x)\mu_z(x)$ is simply

$$\left(\sum_{k=0}^{\infty} f(k)z^k\right)\left(\sum_{k=0}^{\infty} g(k)z^k\right) = \sum_{k=0}^{\infty}(f * g)(k)z^k$$

which is obvious. The formula is valid in D by analytic continuation.

P8 $$\left|\int_{\mathbb{Z}_p} f(x)\mu_z(x)\right| \leq ||f|| \tag{11}$$

where $||f||$ denotes the sup-norm.

Remark : It follows from (5) that $\lim_{z\to\infty} zF(z)G(z) = -(f * g)(-1)$.

But $\lim_{z\to\infty} zF(z)G(z) = -f(-1) \lim_{z\to\infty} G(z) = 0$.
Hence we deduce the (known) fact that $(f * g)(-1) = 0$, i.e. the convolution of the two continuous functions is 0 at the point -1.

3. The p-adic Z-transform

Let $C(\mathbb{Z}_p)$ denote the Banach space of the all continuous functions from $\mathbb{Z}_p$ to $\mathbb{C}_p$, equipped with the sup-norm.
Let (a_n) be a sequence in $\mathbb{C}_p$. A series of the form

$$\sum_{k=0}^{\infty} a_k \frac{z^k}{(1-z)^{k+1}} \qquad \text{with} \qquad \lim_{k\to\infty} a_k = 0 \tag{12}$$

is convergent in D.
Let B be the set of all functions $F : D \to \mathbb{C}_p$ that are the sum of a series of the form (12) with $\lim_{k\to\infty} a_k = 0$.
If we define $||F|| = \sup_{z\in D} |F(z)|$ then B is a Banach space.
Formula (6) shows that $F(z) = \int_{\mathbb{Z}_p} f(x)\mu_z(x))$ belongs to B if $f \in C(\mathbb{Z}_p)$.
Hence it makes sense to consider the mapping

$$T : C(\mathbb{Z}_p) \to B : f \to F(z) = \int_{\mathbb{Z}_p} f(x)\mu_z(x)$$

We will call $F(z)$ the p-adic z-transform of f for the following reason. If $|z| < 1$ then

$F(z) = \sum_{k=0}^{\infty} f(k)z^k$. In applied mathematics it is customary to call the "generating function" $F(z)$ the z-transform of f.

We now examine the properties of the z-transform.
It is easily verified that T is linear and continuous.
If $F(z)$ is identical 0 then $\sum_{k=0}^{\infty} f(k)z^k = 0$ for $|z| < 1$. Hence $f(x) \equiv 0$.
This proves that T is injective.
T is also surjective. To see this we start from a given $F(z) = \sum_{k=0}^{\infty} a_k \frac{z^k}{(1-z)^{k+1}}$ with $\lim_{k\to\infty} a_k = 0$. It follows from (6) that the z-transform of the function $f(x) = \sum_{k=0}^{\infty} a_k \binom{x}{k}$ is equal to the given $F(z)$ since $(\Delta^k f)(0) = a_k$.

Although we do not need it in the sequel we will also prove that T is an isometry. For this we need a lemma.

Lemma 1
If $a = (a_k)$ is a sequence in $\mathbb{C}_p$, with $\lim_{k\to\infty} a_k = 0$, then
$\sup |a_k| = \sup\{|a_0|, |a_0 + a_1|, |a_1 + a_2|, ..., |a_k + a_{k+1}|, ...\}$.

Proof : Put $||a|| = \sup |a_k|, |||a||| = \sup\{|a_0|, ..., |a_k + a_{k+1}|, ...\}$.
Since $|a_k + a_{k+1}| \leq \max\{|a_k|, |a_{k+1}|\} \leq ||a||$ we see that $|||a||| \leq ||a||$.
Put $b_0 = a_0, b_1 = a_0 + a_1, ..., b_k = a_{k-1} + a_k, ...$.
Then $a_k = b_k - b_{k-1} + b_{k-2} - ... \pm b_0$.
Hence $|a_k| \leq \max\{|b_0|, |b_1|, ..., |b_k|\} \leq |||a|||$
thus $||a|| \leq |||a|||$ and the lemma is proved.

Proposition : T is an isometry.

Proof : Let $F(z) = \sum_{k=0}^{\infty} a_k \frac{z^k}{(1-z)^{k+1}}$ be the z-transform of $f(x) = \sum_{k=0}^{\infty} (\Delta^k f)(0) \binom{x}{k}$.

$$||f|| = \sup_k |(\Delta^k f)(0)| \text{ since the polynomials } \binom{x}{k} \text{ form an orthogonal base for } C(\mathbb{Z}_p)$$
$$= \sup |a_k|$$
$$= \sup\{|a_0|, |a_0 + a_1|, ..., |a_k + a_{k+1}|, ...\} \text{ by lemma 1}$$

Writing $u = \frac{z}{1-z}$ we observe that $z \in D$ if and only if $|u + 1| \leq 1$.
Now

$$
\begin{aligned}
||f|| &= \sup\{|a_0|, |a_0 + a_1|, \dots, |a_k + a_{k+1}|, \dots\} \\
&= \sup_{|u|\leq 1} \{a_0 + (a_0 + a_1)u + \dots + (a_{k-1} + a_k)u^k + \dots\} \\
&= \sup_{|u+1|\leq 1} \{a_0 + (a_0 + a_1)u + \dots + (a_{k-1} + a_k)u^k + \dots\} \\
&= \sup_{z\in D} |F(z)| = ||F||
\end{aligned}
$$

We now show how the z-transform can be used in p-adic analysis.

Application 1 Mahler's expansion with remainder
We start from formula (6)

$$F(z) = \sum_{k=0}^{n-1} (\Delta^k f)(0) \frac{z^k}{(1-z)^{k+1}} + \frac{z^n}{(1-z)^n} \int_{\mathbf{Z}_p} (\Delta^n f)(x) \mu_z(x) \tag{6}$$

If $f(x) = \binom{x}{n-1}$ all terms on the R.H.S. vanish except the term $\frac{z^{n-1}}{(1-z)^n}$. This means that the z-transform of $\binom{x}{n-1}$ is $\frac{z^{n-1}}{(1-z)^n}$.
Hence every term of (3) is the transform of a function in $C(\mathbf{Z}_p)$. Taking the inverse transform we get something of the form

$$f(x) = \sum_{k=0}^{n-1} (\Delta^k f)(0) \binom{x}{k} + r_n(x)$$

where $r_n(x)$ is the inverse transform of

$$z.\frac{z^{n-1}}{(1-z)^n}. \int_{\mathbf{Z}_p} (\Delta^n f)(x) \mu_z(x) \tag{13}$$

Using (10) we see that $r_n(x) = \left\{ \binom{x}{n-1} * \Delta^n f \right\} (x-1)$.
The presence of the first factor z in the product (13) makes it necessary to evaluate the convolution of $\binom{x}{n-1}$ and $\Delta^n f$ at the point $x-1$ instead of x.
This gives Mahler's expansion with an expression for the remainder

$$f(x) = \sum_{k=0}^{n-1} (\Delta^k f)(0) \binom{x}{k} + \left\{ \binom{x}{n-1} * \Delta^n f \right\} (x-1)$$

This was obtained in [5] by a different method.

Remark : Until now we have assumed that the functions of $C(\mathbb{Z}_p)$ take their values in $\mathbb{C}_p$. If we replace $\mathbb{C}_p$ by a field that is complete for a non archimedean valuation containing $\mathbb{Q}_p$, the method still works. The only restriction is that we can no longer use any property whose proof uses analytic continuation.

Application 2 Van der Put's expansion

Notation : If $n = a_0 + a_1 p + ... + a_s p^s$ with $a_s \neq 0$ then we put $m(n) = s$ and $n_- = a_0 + a_1 p + ... + a_{s-1} p^{s-1}$.

Take $f \in C(\mathbb{Z}_p)$ and let f_r denote the locally constant function defined by

$$f_r(k) = f(k) \qquad \text{for } k = 0, 1, ..., p^r - 1$$
$$f_r(x) = f_r(x + p^r)$$

By induction on r we can verify that

$$\sum_{0 \leq n < p^r} (f(n) - f(n_-)) \frac{z^n}{1 - z^{m(n)}} = \frac{\sum_{n=0}^{p^r - 1} f(n) z^n}{1 - z^{p^r}} \tag{14}$$

Using the definition (1) we see that the R.H.S. of (14) is the z-transform of f_r. In the same way we can verify that $\frac{z^n}{1 - z^{m(n)}}$ is the z-transform of the function

$$e_n(x) = 1 \qquad \text{if } |x - n| < \frac{1}{n}$$
$$e_n(x) = 0 \qquad \text{if } |x - n| \geq \frac{1}{n}$$

The inverse transform of (8) gives the identity

$$\sum_{0 \leq n < p^r} [f(n) - f(n_-)] e_n(x) = f_r(x)$$

If $r \to \infty$ we recover the Van der Put expansion of $f(x)$.

Application 3

If we put $f(x) = \binom{x+n}{n}$ in (7) we see that z-transform of $\binom{x+n}{n}$ is $\frac{1}{(1-z)^{n+1}}$. The inverse of (7) yields

$$f(x) = \sum_{k=0}^{n} (Q^k f)(-1) \binom{x+k}{k} + \left\{ \binom{x+n}{n} * Q^{n+1} f \right\}(x) \qquad Q = \Delta E^{-1}$$

4. The expansion of a continuous function in a series of Sheffer polynomials

In this section we will use the p-adic z-transform to generalize the main theorem of [6]. We first recall a few elements of the p-adic umbral calculus developed in [6].

Let R be a linear continuous operator on $C(\mathbb{Z}_p, K)$, where K is a field containing $\mathbb{Q}_p$ that is complete for a non archimedean valution. If R commutes with E it can be written in the form $R = \sum_{i=0}^{\infty} b_i \Delta^i$ where (b_i) is a bounded sequence in K. The result that we want to generalize is the following.

Proposition [6]
If $Q = \sum_{i=0}^{\infty} b_i \Delta^i$ is a linear continous operator on $C(\mathbb{Z}_p, K)$ such that $b_0 = 0, |b_1| = 1, |b_i| \le 1$ for $i \ge 2$ then

a) there exists a unique sequence of polynomials $p_n(x)$ such that

$$Qp_n = p_{n-1},\ \deg p_n = n,\ p_n(0) = 0 \text{ for } n \ge 1 \text{ and } p_0 = 1$$

b) every continuous function $f : \mathbb{Z}_p \to K$ has a uniformly convergent expansion of the form

$$f(x) = \sum_{n=0}^{\infty} (Q^n f)(0) p_n(x) \tag{15}$$

With an operator $R = \sum_{i=0}^{\infty} b_i \Delta^i$ we can associate a measure on $\mathbb{Z}_p$ by means of the functional sending a $f \in C(\mathbb{Z}_p, K)$ to $(Rf)(0)$.

Example : Take $R = \frac{1}{1-Ez}$ with $z \in D$. Then

$$R = \frac{1}{1 - z + \Delta z} = \sum_{k=0}^{\infty} \Delta^k \frac{z^k}{(1-z)^{k+1}}$$

Formula (6) shows that the measure obtained in this way is the measure introduced in section 1.

Now let $Q = \sum_{i=0}^{\infty} b_i \Delta^i$ and $S = \sum_{i=0}^{\infty} s_i \Delta^i$ be two operators commuting with E where S is invertible.

If $b_0 = 0$, any operator R, commuting with E, can be written in the form

$$R = \sum_{n=0}^{\infty} r_n Q^n, \qquad r_n \in K$$

We can see this as an equality between operators or as an identity between formal power series in Δ. If we take $R = \frac{S}{1-Ez}$ the coefficients r_n will depend on z. Let us write it in the form

$$\frac{S}{1-Ez} = \sum_{n=0}^{\infty} \frac{T_n(z)}{(1-z)^{n+1}} Q^n \tag{16}$$

Writing out everything as a powerseries in Δ and comparing the coefficient of Δ^n we see that $T_n(z)$ is a polynomial of degree n in z. If, moreover, $|b_1| = 1$ the sequence $\frac{T_n(z)}{(1-z)^{n+1}}$ is bounded.
Multiplying (16) with S^{-1} and applying the operators on both sides to a function $f \in C(\mathbb{Z}_p, K)$ we get the series

$$F(z) = \sum_{n=0}^{\infty} (S^{-1}Q^n f)(0) \frac{T_n(z)}{(1-z)^{n+1}} \tag{17}$$

This series is uniformly convergent since $\lim_{n\to\infty} (S^{-1}Q^n f)(0) = 0$.
The idea is now to take the inverse z-transform of (17).
Now the z-transform of $\binom{x}{n}$ is $\frac{z^n}{(1-z)^{n+1}}$. Hence the z-transform of a polynomial of degree n is of the form $\frac{P_n(z)}{(1-z)^{n+1}}$ where $P_n(z)$ is also a polynomial of degree n.
Taking the inverse transform of (17) we get

$$f(x) = \sum_{n=0}^{\infty} (S^{-1}Q^n f)(0) t_n(x) \tag{18}$$

where $t_n(x)$ is a polynomial of degree n.
This is the expansion we wanted to obtain.
To see that (18) is a generalization of (15) take S equal to the identity operator and take f equal to the polynomial p_n in (15). (18) then reduces to $p_n(x) = t_n(x)$.
In the general case the polynomials $t_n(x)$ are called "Sheffer polynomials" in umbral calculus.

Remark

It is possible to work in an even more general situation. Let $Q_1, Q_2, \ldots, Q_n, \ldots$ be a sequence operators satisfying the same conditions as the operator Q above. There exists a sequence of polynomials $T_n(z), \deg T_n = n$, such that

$$\frac{S}{1-Ez} = \sum_{n=0}^{\infty} \frac{T_n(z)}{(1-z)^{n+1}} Q_1 Q_2 \ldots Q^n$$

5. A formula for $\lg 2$

The formula

$$2(1-\frac{1}{p})\lg 2 = \lim_{n\to\infty} \sum_{\substack{k=1\\(k,p)=1}}^{p^n} \frac{(-1)^{k+1}}{k}, \qquad p \neq 2$$

is proved in [2] p. 180 and [3] p. 38. Here $\lg 2$ is the p-adic logarithm.

In this section we show that it is possible to refine this result using the properties of the integral studied in section 2.

$$\text{Let } f(x) = 0 \quad \text{for } |x| < 1$$
$$= \frac{1}{x} \quad \text{for } |x| = 1$$

In [1] (lemma 6.4, chapter 12) it is proved that, for $z \in D$,

$$\int_{\mathbf{Z}_p} f(x)\mu_z(x) = \frac{1}{p}\lg\frac{1-z^p}{(1-z)^p} \tag{19}$$

If $U_p = \mathbf{Z}_p \setminus p\mathbf{Z}_p$ denotes the group of units of $\mathbf{Z}_p$ the integral can be written as

$$\int_{U_p} \frac{\mu_z(x)}{x} = \frac{1}{p}\lg\frac{1-z^p}{(1-z)^p}$$

Putting $z = -1$ we get

$$\int_{U_p} \frac{\mu_{-1}(x)}{x} = -(1-\frac{1}{p})\lg 2 \tag{20}$$

The idea is to construct approximations for the integral on the LHS of (20). This will yield the following theorem.

Theorem : If $p \neq 2$ then

a) $$2(1-\frac{1}{p})\lg 2 \equiv \sum_{k=1,(k,p)=1}^{p^n} \frac{(-1)^{k+1}}{k} \pmod{p^{2n}}$$

b) $$2(1-\frac{1}{p})\lg 2 \equiv 4\varepsilon_n \sum_{\substack{k=0\\(2k+1,p)=1}}^{\frac{p^n-3}{2}} \frac{(-1)^{k+1}}{2k+1} \pmod{p^{2n}}$$

where $\varepsilon_n = (-1)^{n\cdot\frac{p-1}{2}}$

c) $$-2(1-\frac{1}{p})\lg 2 \equiv \sum_{\substack{k=1\\(k,p)=1}}^{p^n} \frac{(-1)^{k+1}}{k} - 8\varepsilon_n \sum_{k=0}^{\frac{p^n-3}{2}} \frac{(-1)^{k+1}}{2k+1} \pmod{p^{4n}}$$

For the proof we need the value of a few integrals. We collect these results in the following lemma. i denotes a squareroot of -1.

Lemma 2

(1) $$\int_{U_p} \frac{\mu_{-1}(x)}{x^2} = \int_{U_p} \frac{\mu_{-1}(x)}{x^4} = 0$$

(2) $$\int_{U_p} \frac{\mu_i(x)}{x^2} + \int_{U_p} \frac{\mu_{-i}(x)}{x^2} = 0$$

$$\int_{U_p} \frac{\mu_i(x)}{x^4} + \int_{U_p} \frac{\mu_{-i}(x)}{x^4} = 0$$

(3) $$\int_{U_p} \frac{\mu_i(x)}{x} = \int_{U_p} \frac{\mu_{-i}(x)}{x} = -\frac{1}{2}(1-\frac{1}{p})\lg 2 \quad \text{for } p \neq 2$$

(4) $$\int_{U_p} \frac{\mu_i(x)}{x^3} = \int_{U_p} \frac{\mu_{-i}(x)}{x^3} = \frac{1}{8}\int_{U_p} \frac{\mu_{-1}(x)}{x^3}$$

Proof of the lemma

(1) These are special cases of formula (9).
(2) These are special cases of (8) with $z = i$.

(3) Suppose first that $p \equiv 1 \pmod 4$. Then $i^p = i$, hence

$$\int_{U_p} \frac{\mu_i(x)}{x} = \frac{1}{p} \lg \frac{1-i}{(1-i)^p} = -(1-\frac{1}{p}) \lg(1-i)$$

Since $(1-i)^2 = -2i$ and $\lg i = 0$ we see that $\lg(1-i) = \frac{1}{2}\lg 2$ and the assertion is proved.
If $p \equiv 3 \pmod 4$ we have $i^p = -i$ and we get

$$\int_{U_p} \frac{\mu_i(x)}{x} = \frac{1}{p} \lg \frac{1+i}{(1-i)^p}$$

Since $\frac{1+i}{1-i} = i$ and $\lg i = 0$ we conclude that

$$\frac{1}{p} \lg \frac{1+i}{(1-i)^p} = -(1-\frac{1}{p}) \lg(1-i) = -\frac{1}{2}(1-\frac{1}{p}) \lg 2$$

The integral $\displaystyle\int_{U_p} \frac{\mu_{-i}(x)}{x}$ is calculated in the same way.

(4) Let k be a natural number and let $\zeta(s)$ be the Riemann zeta function. It is well-known that the numbers $\zeta(-k)$ are rational and that the sequence $k \to (1-p^k)\zeta(-k)$ can be interpolated p-adically. This can be deduced from the following formula (see [1] p. 295).

$$(1-p^k)\zeta(-k) = \frac{1}{q^{k+1}-1} \sum \int_{U_p} x^k \mu_\theta(x) \tag{21}$$

The sum is extended over all primitive q-th roots of unity θ with $\theta \neq 1$. q is an integer prime to p.
In [1] the author supposes that q is a prime but this restriction is not necessary.
Clearly the LHS of (21) is independant of q. Taking respectively $q = 2$ and $q = 4$ we get

$$\frac{1}{2^{k+1}-1} \int_{U_p} x^k \mu_{-1}(x) = \frac{1}{4^{k+1}-1} \left\{ \int_{U_p} x^k \mu_{-1}(x) + \int_{U_p} x^k \mu_i(x) + \int_{U_p} x^k \mu_{-i}(x) \right\}$$

or

$$2^{k+1} \int_{U_p} x^k \mu_{-1}(x) = \int_{U_p} x^k \mu_i(x) + \int_{U_p} x^k \mu_{-i}(x) \tag{22}$$

If k remains in a fixed residue class mod $(p-1)$ the LHS of (21) is a continuous function of k. Hence (21) and (22) remain valid for negative integers (except possibly for $k=-1$). Taking $k=-3$ we get

$$4\int_{U_p}\frac{\mu_{-1}(x)}{x^3}=\int_{U_p}\frac{\mu_i(x)}{x^3}+\int_{U_p}\frac{\mu_{-i}(x)}{x^3}$$

Since (8) implies that $\int_{U_p}\frac{\mu_i(x)}{x^3}=\int_{U_p}\frac{\mu_{-i}(x)}{x^3}$ the last assertion of lemma 2 is proved.

Proof of the theorem

Starting from (1) we have

$$\int_{U_p}\frac{\mu_z(x)}{x}=\sum_{\substack{k=1\\(k,p)=1}}^{p^n}\frac{z^k}{k}+z^{p^n}\int_{U_p}\frac{\mu_z(x)}{x+p^n}$$

Now $$\frac{1}{x+p^n}=\frac{1}{x}-\frac{p^n}{x^2}+\frac{p^{2n}}{x^3}-\frac{p^{3n}}{x^4}+\frac{p^{4n}}{x^4(x+p)}$$

Integrating this over U_p and observing that (11) implies

$$\left|\int_{U_p}\frac{\mu_z(x)}{x^4(x+p^n)}\right|\leq 1$$

we see that the (p-adic) value of

$$(1-z^{p^n})\int_{U_p}\frac{\mu_z(x)}{x}-\sum_{\substack{k=1\\(k,p)=1}}^{p^n}k+z^{p^n}\left[p^n\int_{U_p}\frac{\mu_z(x)}{x^2}-p^{2n}\int_{U_p}\frac{\mu_z(x)}{x^3}+p^{3n}\int_{U_p}\frac{\mu_z(x)}{x^4}\right]\quad(23)$$

is $\leq\frac{1}{p^4}$.

For $z=-1$ the first assertion of lemma 2 implies that two of these integrals are zero. Since the other integrals clearly lie in $\mathbb{Z}_p$ we obtain the following congruence in $\mathbb{Z}_p$

$$2\int_{U_p}\frac{\mu_{-1}(x)}{x}\equiv\sum_{\substack{k=1\\(k,p)=1}}^{p^n}\frac{(-1)^k}{k}-p^{2n}\int_{U_p}\frac{\mu_{-1}(x)}{x^3}\qquad(\bmod p^{4n})\qquad(24)$$

If we compare this with (20) we see that point (a) of the theorem is proved.
In order to prove (b) note that $i^p = (-1)^{\frac{p-1}{2}}$ and hence $i^{p^n} = \varepsilon_n i$.

Now put $z = i$ in (23). This gives

$$\left|(1-\varepsilon_n i)\int_{U_p}\frac{\mu_i(x)}{x} - \sum_{\substack{k=1\\(k,p)=1}}^{p^n}\frac{i^k}{k} + p^n\varepsilon_n i\int_{U_p}\frac{\mu_i(x)}{x^2} - p^{2n}\varepsilon_n i\int_{U_p}\frac{\mu_z(x)}{x^3} + p^{3n}\varepsilon_n i\int_{U_p}\frac{\mu_z(x)}{x^4}\right|$$
$$\leq \frac{1}{p^4}$$

Replace i by $-i$ and subtract. When the integrals are replaced by their values given in lemma 2 we obtain the congruence

$$\varepsilon_n i(1-\frac{1}{p})\lg 2 \equiv 2i \sum_{\substack{k=0\\(2k+1,p)=1}}^{\frac{p^n}{2}} \frac{(-1)^k}{2k+1} + \frac{\varepsilon_n i p^{2n}}{4}\int_{U_p}\frac{\mu_{-1}(x)}{x^3} \qquad (\text{mod } p^{4n}) \qquad (25)$$

Neglecting the last term we see that (b) is proved.
To obtain (c) it is sufficient to take a linear combination of (24) and (25) such that the integral $\int_{U_p}\frac{\mu_{-1}(x)}{x^3}$ disappears.

We can deduce the following purely arithmetical result from the theorem.

Corollary

For $p \neq 2$

$$2.\frac{2^{(p-1)}-1}{p^2} \equiv 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots - \frac{1}{p-1} \qquad (\text{mod } p^2)$$
$$\equiv 4(-1)^{\frac{p-1}{2}}(1 - \frac{1}{3} + \frac{1}{5} - \ldots \pm \frac{1}{p-2}) \qquad (\text{mod } p^2)$$

Proof : Since $2^{(p-1)p} \equiv 1 \pmod{p^2}$ we have

$$p(p-1)\lg 2 = \lg(2^{(p-1)p} - 1 + 1) \equiv 2^{(p-1)p} - 1 \qquad (\text{mod } p^4)$$

and hence

$$(1-\frac{1}{p})\lg 2 \equiv \frac{2^{(p-1)p}-1}{p^2} \qquad (\mathrm{mod}\ p^4)$$

Combining this with the congruences (a) and (b) of the theorem (for $n = 1$) we see that the required congruences are established.

REFERENCES

[1] J.W.S. CASSELS : Local Fields.
Cambridge University Press, 1986.

[2] W. SCHIKHOF : Ultrametric Calculus.
Cambridge University Press, 1984.

[3] N. KOBLITZ : p-Adic Analysis : A Short Course on Recent Work.
Cambridge University Press, 1980.

[4] Y. AMICE - J. FRESNEL : Fonctions zêta p-adiques des corps de nombres abéliens réels.
Acta Arithmetica, vol 20 (1972) p. 355-385.

[5] L. VAN HAMME : Three generalizations of Mahler's expansion for continuous functions on $\mathbb{Z}_p$.
in "p-adic analysis" - Lecture Notes on Mathematics vol 1454 (1990) p. 356-361, Springer Verlag.

[6] L. VAN HAMME : Continuous operators which commute with translations on the space of continuous functions on $\mathbb{Z}_p$.
in "p-adic Functional Analysis" J. Bayod, N. De Grande-De Kimpe, J. Martinez - Maurica (editors) p. 75-88, Marcel Dekker, New York (1992).

Vrije Universiteit Brussel

Faculty of Applied Sciences

Pleinlaan 2

B - 1050 Brussels

Belgium