PACIFIC JOURNAL OF MATHEMATICS
Vol. 120, No. 1, 1985

p-ADIC INTEGRAL TRANSFORMS ON COMPACT SUBGROUPS OF $\mathbf{C}_p$

NEAL KOBLITZ

Let p be a fixed prime, and let $\mathbf{C}_p$ denote the p-adic completion of the algebraic closure of $\mathbf{Q}_p$. For d a fixed positive integer prime to p, set $X = X_d = \lim_{\leftarrow N-} \mathbf{Z}/dp^N\mathbf{Z}$. For example, $X_1 = \mathbf{Z}_p$. We shall first discuss the "inverse Mellin" integral transform $f_\mu(\rho) = \int_X \rho(x)\,d\mu(x)$ for ρ a $\mathbf{C}_p$-valued bounded measure on X. We then discuss a second type of p-adic integral transform, which to a continuous function $f(x)$ on X associates the analytic function whose Taylor expansion coefficients are $f(n)$. Thirdly, for σ a compact subset of $\mathbf{C}_p$ the p-adic Stieltjes transform $\varphi(z) = \int_\sigma (z-x)^{-1}\,d\mu(x)$ was shown by Barsky and Vishik to give a correspondence between measures μ on σ and a certain class of analytic functions φ on the complement of σ. We shall show that when σ is a compact subgroup of $\mathbf{C}_p$, the Stieltjes transform is closely related to the first two transforms. Some examples and arithmetic applications will also be discussed.

1. Let p, $\mathbf{C}_p$ and $X = X_d$ be as above. The p-adic absolute value in $\mathbf{C}_p$ is normalized so that $|p|_p = 1/p$. For $u \in \mathbf{C}_p$ with $|u|_p = 1$, let $\bar{u}$ denote its residue in $F_p^{\text{alg cl}}$, and let $\omega(u)$ be the Teichmüller representative of u, i.e., the unique root of unity of order prime to p with the same residue in $F_p^{\text{alg cl}}$. Set $\langle u\rangle = u/\omega(u)$. The ring X is isomorphic to the product of rings $\mathbf{Z}/d\mathbf{Z}$ and $\mathbf{Z}_p$ under the two projections π_1 and π_2, where for $x \in X$ we set $\pi_1(x) =$ *the image of x modulo d* and $\pi_2(x) =$ *the limit of the image of x modulo p^N* ("forget mod d information"). Let $a + dp^N\mathbf{Z}_p$ denote the set of $x \in X$ for which $x \equiv a \bmod dp^N$. Let $X^m = X_d \times \mathbf{Z}_p^{m-1}$ denote the product of X with $m-1$ copies of $\mathbf{Z}_p$.

A function $f(n)$ mapping the nonnegative integers to $\mathbf{C}_p$ extends to a continuous function on X if and only if for every $\varepsilon > 0$ we have $|f(n_1) - f(n_2)|_p < \varepsilon$ whenever $n_1 \equiv n_2 \bmod dp^N$ for N sufficiently large. In particular, for $u \in \mathbf{C}_p$ the function $f(n) = u^n$ extends to X if and only if $|u^d - 1|_p < 1$. In that case $u^x = \omega(u)^{\pi_1(x)}\langle u\rangle^{\pi_2(x)}$.

Let $U_1 \subset \mathbf{C}_p$ denote the open unit disc about 1, and let $U_d = \{u \in \mathbf{C}_p \mid |u^d - 1|_p < 1\}$ denote the union of the open unit discs around the dth roots of unity. Let $U^m = U_d \times U_1^{m-1}$. We say that a set $\{u_1, u_2, \ldots, u_m\} \in U^m$ is (*multiplicatively*) *X^m-independent* if the relation $u_1^{x_1}u_2^{x_2}\cdots u_m^{x_m} = 1$ for $x = (x_1, \ldots, x_m) \in X^m$ implies $x = 0$. By replacing u_j by $u_j^{dp^N}$ for some large N, one sees that a set is multiplicatively X^m-independent if and only if its p-adic logarithms are $\mathbf{Q}_p$-linearly independent.

Let σ be a compact subset of $\mathbf{C}_p^* = \mathbf{C}_p - \{0\}$. Suppose that σ is a sub*group* of $\mathbf{C}_p^*$. Then clearly $\sigma \subset U_d$ for some d. Choose d to be minimal with $\sigma \subset U_d$. It is not hard to see that there exists a finite X^m-independent set $u = \{u_1, u_2, \ldots, u_m\}$ such that $\sigma = \sigma_{\text{tors}, p}\, u^{X^m}$, where

$$u^{X^m} =_{\text{def}} \{u_1^{x_1} \cdots u_m^{x_m} | x_1 \in X, x_j \in \mathbf{Z}_p\,(j > 1)\}$$

and $\sigma_{\text{tors}, p} \subset \sigma$ is the (finite) subgroup of pth power roots of unity. For some finite N_0 any $u \in \sigma$ can be written uniquely in the form $u = \zeta u_1^{x_1} \cdots u_m^{x_m}$ with $x \in X^m$ and $\zeta^{p^{N_0}} = 1$. We say that σ has no p-torsion if $\sigma_{\text{tors}, p} = \{1\}$.

Let ρ denote a (continuous) one-dimensional representation of X^m in $\mathbf{C}_p$. The image $\rho(X^m) \subset \mathbf{C}_p^*$ is a compact subgroup; it has no p-torsion if ρ is faithful.

Let $\delta_j \in X^m$ be the m-tuple with 1 in the jth place and 0 everywhere else. Then the map $\rho \mapsto (\rho(\delta_1), \ldots, \rho(\delta_m))$ gives a one-to-one correspondence between one-dimensional representations of X^m and U^m. For $u = (u_1, \ldots, u_m) \in U^m$, we sometimes let ρ_u denote the representation such that $\rho_u(\delta_j) = u_j$. Note that ρ_u is faithful if and only if u is X^m-independent.

Let μ be a measure on X^m, i.e., a bounded finitely additive map $U \mapsto \mu(U)$ from compact-open subsets $U \subset x^m$ to $\mathbf{C}_p$.

DEFINITION. If μ denotes a measure on X^m and ρ denotes a representation of X^m in a finite dimensional $\mathbf{C}_p$-vector space, then the map

$$(1.1) \qquad (\mu, \rho) \mapsto f_\mu(\rho) = \int_{X^m} \rho(x)\, d\mu(x)$$

is called the *p-adic inverse Mellin transform of* μ.

REMARKS. 1. The terminology comes by analogy with the transform $g_f(x) = \int x^s f(s)\, ds$ which is inverse to the Mellin transform $f(s) = \int x^s g(x)\, dx/x$. Here the characters of $\mathbf{R}$ are parametrized by x. In addition, this definition generalizes the construction used by Hà Huy Khoái [5] to invert the p-adic Mellin-Mazur transform.

2. If $m = 1$ and ρ is a faithful one-dimensional representation of X_d, then this integral can be viewed as a Mellin-Mazur transform by a change of variables. Namely, we fix the image σ of ρ_1, and we let ρ vary over representations with image contained in σ. If we set $u_1 = \rho_1(1)$, so that

$\sigma = u_1^{X_d}$, then such ρ are parametrized by $y \in X_d$, that is, $\rho_y = \rho_1^y$: $x \mapsto u_1^{xy}$. Finally, let ν be the measure on σ obtained by pulling back μ: $d\nu(u_1^x) = d\mu(x)$. In this situation

$$(1.2) \qquad f_\mu(\rho_1^y) = \int_{X^m} u_1^{xy}\, d\mu(x) = \int_\sigma x^y\, d\nu(x) = L_\nu(y),$$

which is the p-adic L-function corresponding to the measure ν on σ.

THEOREM 1. *The inverse Mellin transform $f_\mu(\rho_u)$ of a measure μ on X^m is a bounded analytic function of $u \in U^m$, and any bounded analytic function on U^m is the inverse Mellin transform of some measure.*

Proof. Clearly the map

$$u = (u_1, \ldots, u_m) \mapsto f_\mu(\rho_u) = \int_{X^m} u_1^{x_1} \cdots u_m^{x_m}\, d\mu(x_1, \ldots, x_m)$$

is bounded and analytic. To go the other way, given f we define

$$(1.3) \qquad \mu_f(a + dp^N X^m) = \frac{1}{dp^N} \sum_\xi \xi^{-a} f(\xi),$$

where $a + dp^N X^m$ denotes the compact-open subset

$$a_1 + dp^{N_1}\mathbf{Z}_p \times a_2 + p^{N_2}\mathbf{Z}_p \times \cdots \times a_m + p^{N_m}\mathbf{Z}_p \subset X^m;$$

in the notation p^N on the right N denotes $N_1 + \cdots + N_m$; the sum on the right is over all $\xi = (\xi_1, \ldots, \xi_m) \in U^m$ for which $\xi_1^{dp^{N_1}} = \xi_2^{p^{N_2}} = \cdots = \xi_m^{p^{N_m}} = 1$; and ξ^{-a} denotes $\prod \xi_j^{-a_j}$. Clearly the mapping μ_f defined by (1.3) on the usual basis of compact-open subsets of X^m extends to an additive function of compact-open subsets; it is not hard to show that μ_f is bounded, using the analyticity and boundedness of f. We claim that $f(u) = \int u^x\, d\mu(x)$ for any $u \in U^m$. Since $f(u)$ can be approximated by a finite linear combination of monomials in $(\langle u_1 \rangle, u_2, \ldots, u_m) \in U_1^m$ multiplied by the characteristic function with respect to u_1 of one of the d unit discs in U_d, it suffices to check the claim in the case when $f(u)$ is such a function. But in this case the desired equality is proved in a standard way, essentially by orthogonality of characters on $\mathbf{Z}/dp^{N_1}\mathbf{Z} \times \mathbf{Z}/p^{N_2}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{N_m}\mathbf{Z}$. □

REMARKS. 1. In the case $m = 1$, Hà Huy Khoái proves a more general theorem, namely that the so-called h-admissible distributions μ correspond to all functions on U_d which grow more slowly than $(\log_p u)^h$ as u approaches the boundary of U_d. In particular, for $h = 1$ the same construction (1.3) of the measure applies. The point is that, like a bounded analytic function, an analytic function which grows more slowly than $\log_p$ is determined by its values at the roots of unity ξ.

2. A conjecture of R. Greenberg asserts that for any X^m-independent set $u \in U^m$, a bounded analytic function on U^m (with coefficients in $\mathbf{Z}_p$) is determined by its values on u^y as y varies over X_d, where u^y denotes $(u_1^y, u_2^{\pi_2(y)}, \ldots, u_m^{\pi_2(y)})$. Equivalently, the conjecture is that, if ρ is a faithful one-dimensional representation of X^m and if $\int_{X^m} \rho(xy)\, d\mu(x) = 0$ for $y \in X_d$, then $\mu \equiv 0$.

2. We now let $m = 1$, and consider higher dimensional continuous representations of $X = X_d = \lim_{\leftarrow N-} \mathbf{Z}/dp^N\mathbf{Z}$. If ρ_1 is an irreducible representation of X in an n-dimensional $\mathbf{C}_p$-vector space, then $\rho_1(1)$ has a single eigenvalue v_1, and $\rho_1(x)$ has eigenvalue v_1^x. Note that $v_1 \in U_d$. For μ a measure on X, let $f_\mu(\rho_1)$ be defined by (1.1), and let ν be the measure on $\sigma = v_1^X$ defined by $d\nu(v_1^x) = d\mu(x)$. Now define $L_\nu(y)$ by the Mellin-Mazur transform: $L_\nu(y) = \int_\sigma x^y\, d\nu(x)$.

THEOREM 2. *With these assumptions and notation, when* $f_\mu(\rho_1) \neq 0$ *the order of zero of* $L_\nu(y)$ *at* $y = 1$ *is equal to the co-rank of* $f_\mu(\rho_1)$.

Proof. Let $V_1 = \rho_1(1)$, and let $V = CV_1C^{-1}$ be the Jordan normal form. Since ρ_1 is irreducible, it follows that V is a single $n \times n$ Jordan block. Thus, $V = v_1 + \varepsilon$, where $v_1 = v_1 J$ is a scalar matrix and ε denotes the matrix with ones just above the main diagonal and zeros elsewhere. Then

$$f_\mu(\rho_1) = \int_X V_1^x\, d\mu(x) = C^{-1}\int_X (v_1 + \varepsilon)^x\, d\mu(x) C.$$

Thus, the co-rank of $f_\mu(\rho_1)$ is the same as that of

$$\sum_{j=0}^{n-1} \varepsilon^j \int_X \binom{x}{j} v_1^{x-j}\, d\mu(x) = \sum_{j=0}^{n-1} \frac{1}{j!} \varepsilon^j \left(\frac{d}{dv}\right)^j \int_X v^x d\mu(x)\Big|_{v=v_1}$$
$$= \sum_{j=0}^{n-1} \frac{g^{(j)}(v_1)}{j!} \varepsilon^j,$$

where $g(v) = \int_X v^x\, d\mu(x)$. Making the change of variables $v = v_1^y$, we have

$$g(v_1^y) = \int_X v_1^{yx}\, d\mu(x) = \int_\sigma x^y\, d\nu(x) = L_\nu(y).$$

Let r be the order of zero of $L_\nu(y)$ at $y = 1$. Then $L_\nu(1) = L_\nu'(1) = \cdots = L_\nu^{(r-1)}(1) = 0$, $L_\nu^{(r)}(1) \neq 0$, and so $g(v_1) = g'(v_1) = \cdots = g^{(r-1)}(v_1) = 0$,

$g^{(r)}(v_1) \neq 0$. Then $f_\mu(\rho_1)$ has the same co-rank as $\Sigma_{j=r}^{n-1} g^{(j)}(v_1)/j!\,\varepsilon^j$, where $r < n$, because $f_\mu(\rho_1) \neq 0$. But the latter co-rank is obviously r. □

3. Let $\overline{U}_d = \{u \in \mathbf{C}_p \mid |u^d - 1|_p \geq 1\}$ denote the complement of U_d, and set $\overline{U}^m = \overline{U}_d \times \overline{U}_1^{m-1}$. For any $z = (z_1,\ldots,z_m) \in \overline{U}^m$, let μ_z denote the bounded measure on X^m which is defined on the standard basis of compact-open sets by

$$\mu_z(a + dp^N X^m) = \frac{z^a}{\left(1 - z_1^{dp^{N_1}}\right)\left(1 - z_2^{p^{N_2}}\right)\cdots\left(1 - z_m^{p^{N_m}}\right)},$$

where the notation $a + dp^N X^m$ has the same meaning as in (1.3), except that we agree to take the representatives a_j in the range $0 \leq a_1 < dp^{N_1}$, $0 \leq a_j < p^{N_j}$ ($j > 1$), and z^a denotes $\prod z_j^{a_j}$. (It is easy to check that this μ_z actually extends to a bounded measure on X^m.)

THEOREM 3. *For any continuous function* $f\colon X^m \to \mathbf{C}_p$, *the transform*

$$g(z) = \int_{X^m} f(x)\, d\mu_z(x), \qquad z \in \overline{U}^m, \tag{3.1}$$

has the properties

(1) $g(z)$ *is bounded and Krasner analytic in each* z_j *on* $\overline{U}^m$;

(2) $g(z) \to 0$ *as* $|z_j|_p \to \infty$ *for each variable* z_j *with any fixed values of the remaining variables*;

(3) *in the open unit polydisc* $|z_j|_p < 1$, $g(z)$ *has the expansion* $\Sigma f(n) z^n$, *where* $n = (n_1,\ldots,n_m)$ *runs through all m-tuples of nonnegative integers*;

(4) *for* $|z_j|_p > 1$, $j = 1,\ldots,m$, $g(z)$ *has the expansion* $-\Sigma f(-n) z^{-n}$, *where n runs through all m-tuples of positive integers.*

Conversely, if g is any function satisfying (1) *and* (2), *and if* $g(z) = \Sigma a_n z^n$ *is its expansion in the open unit polydisc, then the sequence* $f(n) = a_n$ *extends to a continuous function on* X^m, *and we have* (3.1) *and also property* (4).

Proof. This is essentially a theorem of Amice and Vélu [**1**] when $m = 1$ (see the Appendix to [**8**] for a treatment using the measure μ_z), and the general case is handled in the same way. □

EXAMPLES. 1. For fixed $u \in U^m$, the transform of the representation ρ_u (in the notation of §1) is simply $g(z) = \int_{X^m} u^x\, d\mu_z(x) = \prod_j (1 - u_j z_j)^{-1}$.

2. Let $m = 1$. According to results of Katz [4], a p-adic modular form F of weight zero (and level 1) can be written as a function of the j-invariant which is Krasner analytic outside of small discs around the

supersingular points. Let $\{\bar{s}_i\} \subset F_p^{\text{alg cl}}$ be the residues of all supersingular values of j. It is known that in fact $\{\bar{s}_i\} \subset F_{p^2}$ (for a table of $\bar{s}_i$ for $p \leq 307$, see [10]). Suppose that $j = 0$ is *not* supersingular, i.e., $p \equiv 1 \bmod 6$. Let F_∞ be the value at the cusp. Then $F - F_\infty = g(j)$ satisfies properties (1) and (2) of Theorem 3, with j playing the role of the variable z. Here d is some divisor of $p^2 - 1$, since $\bar{s}_i^{p^2-1} = 1$ for each i. Thus, if $F(j) = F_\infty + \sum_{n=0}^{\infty} a_n j^n$ for $|j|_p < 1$, the coefficients $f(n) = a_n$ extend to a continuous function on X_d, and

$$F(j) = F_\infty + \int_{X_d} f(x)\, d\mu_j(x), \qquad j \in \overline{U}_d.$$

In addition,

$$F(j) = F_\infty - \sum_{n=1}^{\infty} f(-n) j^{-n} \quad \text{for } |j|_p > 1.$$

Hence, we have congruences for the j- and $1/j$-expansion coefficients which generalize those in Ashworth [2] and Koblitz [6].

4. We now discuss a third type of integral transform. Let $\rho\colon X^m \to U_d$ be a one-dimensional continuous representation, as in §1, and let ρ_j denote the jth component, i.e., $\rho_j(x_1,\ldots,x_m) = \rho(0,\ldots,0, x_j, 0,\ldots,0)$. Let μ be a bounded measure on X^m. For $z \in \mathbf{C}_p^m$ with z_j in the complement of the image of ρ_j, in particular for $z \in \overline{U}^m$, we define the Stieltjes transform of ρ and μ as follows:

$$\psi_{\rho,\mu}(z) = \int_{X^m} \frac{d\mu(x)}{\prod_{j=1}^{m}\left(1 - z_j\rho_j(x)\right)}. \tag{4.1}$$

The next theorem gives a relation between the three transforms in §§1, 3 and 4.

THEOREM 4. *Let μ be a measure on X^m, and let ρ be a one-dimensional representation of X^m in $\mathbf{C}_p^*$. Let $f_\mu(\rho)$ be the inverse Mellin transform defined by* (1.1). *For $y \in X_d$, let ρ^y denote the representation $\rho^y(x) = \rho(xy) = \rho(x_1 y, x_2\pi_2(y),\ldots,x_m\pi_2(y))$. If the transform* (3.1) *associated to the measure μ_z for $z \in \overline{U}^m$ is applied to the function $y \mapsto f_\mu(\rho^y)$, then the result is the Stieltjes transform $\psi_{\rho,\mu}(z)$.*

Proof.

$$\int_{X^m} f_\mu(\rho^y)\, d\mu_z(y) = \int_{X^m}\int_{X^m} \rho^y(x)\, d\mu(x)\, d\mu_z(y)$$

$$= \int_{X^m}\int_{X^m} \rho^y(x)\, d\mu_z(y)\, d\mu(x).$$

But

$$\int_{X^m} \rho(xy)\, d\mu_z(y) = \prod_j \int \rho_j(x)^y\, d\mu_{z_j}(y) = \prod_j (1 - z_j\rho_j(z))^{-1},$$

and so

$$\int_{X^m} f_\mu(\rho^y)\, d\mu_z(y) = \int_{X^m} \frac{d\mu(x)}{\prod_j (1 - z_j\rho_j(x))},$$

as claimed. □

REMARKS. 1. When $m = 1$, our ψ in (4.1) is essentially the transform $\varphi_\nu(z) = \int_\sigma (z - x)^{-1} d\nu(x)$, $z \in \bar{\sigma}$, that is studied in [3], [12] (see also the Appendix to [8]). Namely, $\psi_{\rho_u,\mu}(z) = z^{-1}\varphi_\nu(z^{-1})$, where $\nu(u^x) = d\mu(x)$. Barsky and Vishik have shown that any Krasner analytic function on $\bar{\sigma}$ which vanishes at infinity and which grows more slowly than $1/\text{dist}(z, \sigma)$ as $z \to \sigma$ is of the form $\varphi(z)$. On the other hand, if $\sigma \subset U_d$ and $z \in \overline{U}_d$, then such a function of z can also be written in the form $\int_{X_d} f(x)\, d\mu_z(x)$, with f the continuous function which interpolates the Taylor expansion coefficients. Theorem 4 says that, because our function of z is actually analytic on $\bar{\sigma}$ (not only on $\overline{U}_d$) and σ is a compact sub*group* of $\mathbf{C}_p^*$, it follows that f extends to an analytic function on $U_d \supset \sigma = u^{X_d}$ (not just a continuous function on σ) and so is given by the inverse Mellin transform of a measure.

2. Theorem 4 is the p-adic analog of the fact that the classical Stieltjes transform is the square of the Laplace transform $L(f) = \int_0^\infty e^{-xy} f(x)\, dx$. Compare the proof of Theorem 4 with the relation (in which we think of $e^{-zy}dy$ as $d\mu_z(y)$):

$$L(L(f))(z) = \int_0^\infty \int_0^\infty e^{-xy} f(x)\, dx\, (e^{-zy}\, dy) = \int_0^\infty (z + x)^{-1} f(x)\, dx.$$

REFERENCES

[1] Y. Amice and J. Vélu, *Distributions p-adiques associées aux séries de Hecke*, Journées Arith., 1974.

[2] M. H. Ashworth, *Congruence properties of coefficients of modular forms using sigma functions*, Ph.D. thesis (Oxford University, 1966).

[3] D. Barsky, *Transformation de Cauchy p-adique et algébre d'Iwasawa*, Math. Ann., **232** (1978), 255–266.

[4] N. M. Katz, *p-adic Properties of Modular Schemes and Modular Forms*, Proc. 1972 Antwerp Summer School, Springer Lectures Notes in Math., **350** (1973), 70–189.

[5] Hà Huy Khoái, *Inverse formula for the Mellin-Mazur transform and some applications*, to appear.

[6] N. Koblitz, 2*-adic and* 3*-adic ordinals of* $(1/j)$*-expansion coefficients for the weight* 2 *Eisenstein series*, Bull. London Math. Soc., **9** (1977), 188–192.

[7] ______, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, 1977.

[8] ______, *p-adic Analysis: a Short Course on Recent Work*, Cambridge Univ. Press, 1980.

[9] B. Mazur, *Analyse p-adique*, Bourbaki report (unpublished), 1972.

[10] B. Mazur and H. P. F. Swinnerton-Dyer, *Arithmetic of Weil curves*, Inventiones Math., **25** (1974), 1–61.

[11] *Modular Functions in One Variable IV*, Springer Lecture Notes in Math., **476**, Springer-Verlag, 1975.

[12] M. M. Vishik, *On applications of the Shnirelman integral in non-archimedean analysis*, Uspekhi Mat. Nauk, **34** (1979), 223–224.

Received February 23, 1984.

UNIVERSITY OF WASHINGTON
SEATTLE, WA 98195