Sci. Rep. Kanazawa Univ.
Vol. 30 No. 2 pp. 33—38
December 1986

The λ-invariants of p-adic measures on Z_p and $1+qZ_p$

Yûji KIDA

Department of Mathematics, Faculty of Science, Kanazawa University

(Received October 31, 1985)

Abstract. We show the λ-invariant of the p-adic measure on $1+qZ_p$ is q times that of the p-adic measure on Z_p if those measures are related by the natural isomorphism between $1+qZ_p$ and Z_p.

§1 Introduction

In a recent paper [3], W. Sinnott studied the μ-invariant of the Γ-transform of a p-adic measure and as an application of the result he gave a new proof for the theorem of Ferrero and Washington. His method also suggests the importance of his rational function. Since the λ-invariant of his function is a multiple of q, one may think that the λ-invariant of the Γ-transform is also a multiple of q.

In this paper, we will show one may not necessarily think so. In fact, we will prove that the λ-invariant is devided by q in the final step of the Γ-transform. Let α be a p-adic measure on Z_p taking values in the integer ring O of some finite extension of Q_p. Let φ be the isomorphism from the additive group Z_p to the multiplicative group $1+qZ_p$ sending 1 to $\exp(q)$, where $q=4$ if $p=2$, $q=p$ otherwise. Then we can define the new measure β by $\beta(A) = \alpha(\varphi^{-1}(A \cap 1+qZ_p))$ for each compact open subset A of Z_p. With these notation, our result can be stated simply as follows.

THEOREM

$$\lambda(\beta) = q\lambda(\alpha)$$

§2 Proof of THEOREM

The proof will be carried out by elementary calculation. We use the following two

This research is supported by Grant-in-Aid for Scientific Research (No. 60540095), Ministry of Education.

elementary lemmas without proof.

LEMMA 1 *Let* $m=\sum_{i=0}^{r} m_i p^i$ and $n=\sum_{i=0}^{r} n_i p^i$, $0 \leqq m_i, n_i < p$ *be the standard* p-*adic expansions of nonnegative integers* m *and* n. *Then*

$$\binom{m}{n} \equiv \binom{m_0}{n_0} \cdots \binom{m_r}{n_r} \pmod{p}$$

where ( ) *is the binomial coefficient as usual.*

LEMMA 2 *Let* $m=\sum_{i=0}^{r} m_i p^i$ *be as in Lemma* 1. *Then we have*

$$m\,!\,(-p)^{-e} \equiv m_0\,! \cdots m_r\,! \pmod{p},$$

where p^e *is the highest power of* p *dividing* $m\,!$.

Let α and β be p-*adic* measures defined above and let $f(X)=\sum_{i=0}^{\infty} a_i X^i$ and $g(X)=\sum_{i=0}^{\infty} b_i X^i$ be the power series associated to α and β, respectively. Let $S(n, i)$ be the rational integer defined by:

(1) $\quad \psi_n(X)=X(X-1)\cdots(X-n+1)=\sum_{i=1}^{n} S(n, i)\, X^i.$

$(-1)^{n-i}S(n, i)$ is called the Stirling number of the lst kind ([1], p65).

PROPOSITION 3 *We have* $b_0=a_0$ *and for each* $n>1$

(2) $\quad b_n=\sum_{i=0}^{\infty} a_i \sum_{j=1}^{n} \{S(n, j)/n\,!\}\,(u^i-1)^j.$

In particular if $n \equiv 0 \pmod{q}$ *then* $b_n \equiv b_{n+1} \pmod{p}$ *otherwise if* $n \not\equiv 0, 1 \pmod{q}$ *then* $b_n \equiv 0 \pmod{p}$.

Proof A fundamental relation of measures and power series ([2], p. 97, Theorem 1.1) shows $b_0=\beta(1+qZ_p)=\alpha(Z_p)=a_0$ and for $n>1$

$$b_n=\int_{1+qZ_p} \binom{x}{n}\, d\beta(x)$$

$$=\sum_{j=1}^{n} \{S(n, j)/n\,!\} \int_{1+qZ_p} x^j\, d\beta(x)$$

$$=\sum_{j=1}^{n} \{S(n, j)/n\,!\} \int_{1+qZ_p} x^j\, d\beta(x).$$

From the definition of β,

$$\int_{1+qZ_p} x^j\, d\beta(x)=\int_{Z_p} \exp(qy)^j\, d\alpha(y)$$

$$=\int_{Z_p} u^{jy}\, d\alpha(y)\,; \text{ where } u=\exp(q).$$

Then again a fundamental relation ([2], p. 98, Theorem 1. 2) shows the right hand side equals to $f(u^i-1)$.

Therefore we have:

$$b_n=\sum_{i=1}^{n} \{S(n, i)/n!\} f(u^i-1)$$

$$=\sum_{j=0}^{\infty} a_j \sum_i \{S(n, i)/n!\} (u^i-1)^j.$$

This is the former half. To prove the latter half, first we study for $n=0$. That is clear because x is congruent to 1 modulo q on $1+qZ_p$. For other n, we must continue the modification.

$$b_n=\sum_j a_j \sum_i \{S(n, i)/n!\} \sum_{k=0}^{j} \binom{j}{k} u^{ik}(-1)^{j-k}$$

$$=\sum_j a_j \sum_k \binom{j}{k} (-1)^{j-k} \sum_i \{S(n, i)/n!\} u^{ik}$$

$$=\sum_j a_j \sum_k \binom{j}{k} (-1)^{j-k} \binom{u^k}{n}.$$

If $n\equiv 0 \pmod q$ then by Lemma 1, we have

$$\binom{u^k}{n} \equiv \binom{1}{0} \binom{[u^k/p]}{[n/p]} \pmod p$$

$$\binom{u^k}{n+1} \equiv \binom{1}{1} \binom{[u^k/p]}{[n/p]} \pmod p,$$

where $[x]$ denotes the biggest integer not greater than x. Thus we have $b_n\equiv b_{n+1} \pmod p$.

If $n\not\equiv 0, 1 \pmod q$ then also by Lemma 1, we have for odd p

$$\binom{u^k}{n} \equiv \binom{1}{n_0} \binom{[u^k/p]}{[n/p]} \equiv 0 \pmod p,$$

and for $p=2$

$$\binom{u^k}{n} \equiv \binom{1}{n_0} \binom{1}{0} \binom{[u^k/p]}{[n/p]} \equiv 0 \pmod p.$$

Therefore $b_n\equiv 0 \pmod p$. This completes the proof.

Clearly the μ-inveriants of α and β coincide, we may be well to assume they are both 0 by dividing by a suitable power of a prime element π of O. Thus the Theorem is equivalent to

(*) $b_n \equiv 0 \pmod{\pi}$ for all $n < q\lambda(\alpha)$, and $b_{q\lambda(\alpha)} \not\equiv 0 \pmod{\pi}$.

By the latter half of Proposition 3, it suffices to study only when n is a multiple of q. In fact we prove

(3) If $a_j \equiv 0 \pmod{\pi}$ for all $j < n$ then $b_{qn} \equiv a_n \pmod{\pi}$.

Since we have already proven for $n=0$, we assume in the rest that $n>1$ to avoid the ambiguity of the binomial coefficients.

Put

$$(4) \qquad A_{qn,j} = \sum_{i=1}^{qn} \{S(qn,i)/(qn)!\} (u^i-1)^j.$$

Then the proof of Proposition 3 shows

$$A_{qn,j} = \sum_{k=0}^{j} \binom{j}{k} (-1)^{j-k} \binom{u^k}{qn}.$$

Therefore $A_{qn,j}$ is an element of Z_p.

Since $b_{qn} = \sum_j a_j A_{qn,j}$, we can deduce the claim (3) from the following two congruences:

$$(5) \qquad A_{qn,n} \equiv 1 \pmod{p}.$$

$$(5') \qquad A_{qn,j} \equiv 0 \pmod{p} \text{ if } j > n.$$

From the formal series identity:

$$\{\exp(Z)-1\}^j = j! \sum_{k=0}^{\infty} T(k, j) Z^k/k!$$

we have the equality in Z_p:

$$(u^i-1)^j = j! \sum_k T(k, j) (qi)^k/k!$$

because $T(k, j)$ is an integer. $T(k, j)$ is called the Starling number of the 2nd kind ([1], p. 65, 90). Thus we have

$$A_{qn,j} = \sum_{i=1}^{qn} \{S(qn,i)/(qn)!\} j! \sum_k T(k, j) (qi)^k/k!$$

$$= \{j!q^n/(qn)!\} \sum_{i=1}^{qn} S(qn, i) \sum_k T(k, j) q^{k-n} i^k/k!.$$

In the rest of this paper, we study only for $p=2$, because for odd p, we can study in a similar but rather easy way. So let $p=2$ and $q=4$. But for the proof for odd p, we still use p and q instead of 2 and 4 and treat the signs carefully.

We modify $A_{qn,j}$ a little more for $p=2$:

$$(6) \qquad A_{qn,j} = \{j!2^{3n}/(qn)!\} \sum_i S(qn,i) \sum_k T(k, j) 2^{2k-3j} i^k/k!.$$

LEMMA 4 *If $j \geqq n$, $j!\, 2^{3n}/(qn)!$ is a 2-adic integer and in particular,*

$$n!\, 2^{3n}/(qn)! \equiv (-1)^n \pmod{2}.$$

Proof It suffices to show for $j=n$. Let $p^e$and $p^{e'}$ be the highest power of p dividing $n!$ and $(qn)!$, respectively. Then by Lemma2,

$$n!(-p)^{-e}\equiv n_0!\cdots n_r!\equiv (qn)!\ (-p)^{-e'}\ (mod\ p).$$

Since $e'=e+3n$, the lemma follows.

Let

(7) $B_{qn,j}=\sum_{i=1}^{qn}S(qn,\ j)\ \sum_{k=0}^{\infty}T(k,\ j)p^{2k-3n}i^k/k!,$

then the congruences (5) and (5′) are reduced to the following new congruences:

(8) $B_{qn,n}\equiv(-1)^n(mod\ p)$

(8′) $B_{qn,j}\equiv 0\ (mod\ p)$ for $j>n$.

Let h_i be the rational number defined by the formal series identity:

$$\psi_n(\exp(Z))=\sum_{i=1}^{\infty}h_iZ^i.$$

By the k-times differentiation with respect to Z of the identity:

$$\sum_{i=1}^{qn}S(qn,\ i)\exp(Z)^i=\sum_{i=1}^{\infty}h_iZ^i,$$

we have the equality of rational numbers:

$$\sum_{i=1}^{qn}S(qn,\ i)i^k=k!h_k.$$

Therefore we have

(9) $B_{qn,j}=\sum_k T(k,\ j)\ p^{2k-3n}h_k.$

Now from the congruence: $\exp(qZ)\equiv 1+qZ$ (mod $pqZ_p[[Z]]$), we have

$$\exp(qZ)-k\equiv 1-k\ (\text{mod}\ qZ_p[[Z]]),$$

$$\{\exp(qZ)-1-pm\}/p\equiv -m\ (mod\ pZ_p[[Z]]),$$

$$\{\exp(qZ)-1-qm\}/q\equiv -m+Z\ (mod\ pZ_p[[Z]]).$$

Using these congruences, we have

$$p^{-n}q^{-n}\psi_n(\exp(qZ))\equiv\prod_1(1-k)\prod_2(-m)\prod_3(-m+Z)\ (mod\ pZ_p[[Z]]\ ),$$

where $\prod_1$ is taken over all k such that $0\leqq k<qn$ and $k\equiv 1\ (mod\ p)$, $\prod_2$ over all m such that $0\leqq m<pn$ *and* $m\equiv 0\ (mod\ p)$ and $\prod_3$ over all $m$such that $0\leqq m<n$.

Thus we have the congruence of formal series:

$$p^{-n}q^{-n}\sum_{i=0}^{\infty}h_i\ (qZ)^i\equiv(-1)^n\prod_{m=0}^{n-1}(-m+Z)\ (mod\ pZ_p[[Z]]\ ).$$

By comparing the coefficients in both sides, we have

$p^{2i-3n}h_i \in Z_p$ for any i,

$p^{-n}h_n \equiv (-1)^n \pmod{p}$,

$p^{2i-3n}h_i \equiv 0 \pmod{p}$ for $i > n$.

Putting these into (9), we get the desired congruences (8) and (8′).

References

[1] D. E. Knuth *The Art of Computer Programing. Vol. 1/Fundamental Argorithms.* Reading, Addison-Wesley, 1973

[2] S. Lang *Cyclotomic Fields. Graduate Texts in Math. 59.* New York-Heidelberg-Berlin, Springer-Verlag 1978

[3] W. Sinnott On the μ-invariant of the Γ-transform of a. rational function. Invent. math. 75 (1984), 273-282