BOREL'S CONJECTURE AND THE TRANSCENDENCE OF THE IWASAWA POWER SERIES

HAE-SANG SUN

Abstract. We deduce the transcendence of the Iwasawa power series from Borel's conjecture, namely the normality of the irrational algebraic p-adic integers.

1. Introduction

Let p be a prime number. For an even Dirichlet character χ there exists a p-adic analytic function $L_p(s,\chi)$ on $\mathbb{Z}_p$, called the Kubota-Leopoldt p-adic L-function such that

$$L_p(1-k,\chi) = -(1-\chi\omega^{-k}(p)p^{k-1})L(1-k,\chi\omega^{-k}) \text{ for the integers } k \geq 1$$

where $L(z,\chi)$ is the Dirichlet L-function associated to χ and ω is the Teichmüller character. Let $v=1$ if $p \geq 3$ and $v=2$ if $p=2$. Let θ be the first factor of χ in Iwasawa's sense. The *Iwasawa power series* $f(T;\theta)$ ([Iw]) is the unique power series in $\mathbb{Z}_p[\theta][[T-1]]$ such that

$$2f(\chi(1+vp)(1+vp)^{-s};\theta) = L_p(s,\chi).$$

Let π be a uniformizer of $\mathbb{Z}_p[\theta]$. Several properties of $f(T;\theta)\,(\bmod\ \pi)$ have been studied such as non-triviality ([FW]), irrationality ([Si2]), pseudo-irrationality ([A2]), and so on ([A, Su]). In [A2], after studying pseudo-irrationality Anglès raises the question about the transcendence of $f(T;\theta)\,(\bmod\ \pi)$ over $\overline{\mathbb{F}}_p(T)$.

Let Q be a p-power, say $Q=p^m$ and for $\alpha \in \mathbb{Z}_p$ let $s_m(\alpha)$ be the $(m-1)$-th partial sum of p-adic expansion of α. Set $\frac{\alpha}{Q}\,(\bmod\ 1) := \frac{s_m(\alpha)}{Q}$. In the paper, we are going to omit the modulus 1 for convenience of calculations unless it causes any confusion. One of main ingredients in [FW] is the following joint normality: p-Adic integers $\alpha_1, \cdots, \alpha_r$ are called *jointly normal* to a base Q if the sequence $(\frac{\alpha_1}{Q^n}, \cdots, \frac{\alpha_r}{Q^n})_{n\geq 1}$ is equi-distributed on the cube $[0,1)^r$ or equivalently if it satisfies Weyl's criterion: For each $(n_1,\cdots,n_r) \in \mathbb{Z}^r \setminus \{(0,\cdots,0)\}$, one has

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} e^{\frac{2\pi i(\alpha_1 n_1+\cdots+\alpha_r n_r)}{Q^n}} = 0.$$

When $r=1$, we simply call it *normal* to the base Q.

There is a famous conjecture suggested by Émile Borel ([B]), which has been unsolved for more than a half of a century. It concerns about the normality of the real irrational algebraic numbers. We state the p-adic version of the conjecture:

Date: September 15, 2009.

The manuscript was prepared while the author was visiting Mathematics department, Université de Caen. He thanks for support and hospitality provided by the department.

Conjecture 1.1 (Borel)**.** *If $\alpha \in \mathbb{Z}_p$ is irrational algebraic and Q a p-power, then α is normal to the base Q.*

The main purpose of present paper is to show that

Theorem 1.2. *Borel's conjecture implies the transcendence of the Iwasawa power series over $\overline{\mathbb{F}}_p(T)$.*

The proof of Theorem 1.2 goes in a similar way as [FW] or [Su]. In order to prove the non-triviality of $f(T,\theta) \pmod{\pi}$, that is, the vanishing of the μ-invariant of $f(T,\theta)$, Ferrero and Washington utilized Proposition 4 in [FW] which comes from the following proposition:

Proposition 1.3 ([FW])**.** *Let $\alpha_1, \cdots, \alpha_r \in \mathbb{Z}_p$ are linearly independent over $\mathbb{Q}$. Then for almost all $\alpha \in \mathbb{Z}_p$ i.e. for all α outside a measure zero subset of $\mathbb{Z}_p$, $\alpha\alpha_1, \cdots, \alpha\alpha_r$ are jointly normal to the base Q.*

In order to obtain Lemma 3.3 which plays a similar role as Proposition 4 in [FW], we make use of Proposition 4.1 instead of Proposition 1.3.

2. The Iwasawa power series

In this section, we represent the Iwasawa power series as the Γ-transform of a suitable p-adic measure on $\mathbb{Z}_p^\times$ in the sense of Sinnott ([Si]).

Let $\mathfrak{o}$ be the integer ring of a finite extension of $\mathbb{Q}_p$ with a fixed uniformizer π. To a periodic function $\Psi : \mathbb{Z} \to \mathfrak{o}$ of a period M, we associate a rational function $R_\Psi(T)$ defined by

$$R_\Psi(T) := \frac{\sum_{r=1}^{M} \Psi(r) T^r}{1 - T^M}.$$

Observe that if $\sum_{r=1}^{M} \Psi(r) = 0$, then we know that $R_\Psi(T) \in \mathfrak{o}[[T-1]]$ since $\frac{1-T^M}{1-T} \in \mathfrak{o}[[T-1]]^\times$. Furthermore, assuming $\Psi(0) = 0$ we obtain that

$$R_\Psi(T^{-1}) = -R_{\Psi \circ -1}(T). \tag{2.1}$$

The poles of $R_\Psi(e^{2\pi i z})$ are $\frac{r}{M}$, $r \in \mathbb{Z}$ and the residues are

$$\mathrm{Res}_{z=\frac{r}{M}} R_\Psi(e^{2\pi i z}) = -\frac{\widehat{\Psi}(r)}{2\pi i M},$$

where the Fourier transform $\widehat{\Psi}$ of Ψ defined as follows:

$$\widehat{\Psi}(r) =: \sum_{s=0}^{M-1} \Psi(s) \zeta_M^{rs}$$

where $\zeta_M = e^{\frac{2\pi i}{M}}$. Observe that we have $\widehat{\widehat{\Psi}}(r) = M\Psi(-r)$.

Assuming that $\Psi(0) = \widehat{\Psi}(0) = 0$, we have

$$R_\Psi(T) = \begin{cases} O(\frac{1}{T}) \text{ if } T \to \infty \\ O(T) \text{ if } T \to 0 \end{cases}. \tag{2.2}$$

Furthermore we assume that $\widehat{\Psi}(p^m) \neq 0$ for all $m \geq 1$. Then we define a function σ_Ψ on the basic open subsets of $\mathbb{Z}_p$ such that for $a \in \mathbb{Z}_p$ and $m \geq 1$

$$\sigma_\Psi(a + p^m\mathbb{Z}_p) := \frac{1}{\widehat{\Psi}(p^m)} \int_{\frac{a}{p^m} - i\infty}^{\frac{a}{p^m} + i\infty} R_{\widehat{\Psi}}(e^{2\pi i z}) dz,$$

which is well-defined because of (2.2). For an integer $\alpha > 0$ relatively prime to p, we also set

$$\sigma_{\Psi,\alpha} := \sigma_\Psi - \alpha^{-1}\sigma_\Psi \circ \alpha.$$

The followings are reformulation of results in [H].

Proposition 2.1. *Assume that $p \nmid M$ and $\widehat{\Psi}(p^m)\widehat{\Psi}(pr) = \widehat{\Psi}(p^{m+1})\widehat{\Psi}(r)$ for all $m, r \geq 1$. Then σ_Ψ is a p-adic measure on $\mathbb{Z}_p$ and, hence so is $\sigma_{\Psi,\alpha}$.*

Proof. We need to show that σ_Ψ is a p-adically bounded distribution on $\mathbb{Z}_p$. First of all, we have $\int_{x-i\infty}^{x+i\infty} R_{\widehat{\Psi}}(e^{2\pi iz})dz = \int_{y-i\infty}^{y+i\infty} R_{\widehat{\Psi}}(e^{2\pi iz})dz$ if $\frac{r}{M} < x, y < \frac{r+1}{M}$ for some $r = 0, \cdots, M-1$ because of (2.2). Therefore the integration $\int_{x-i\infty}^{x+i\infty} R_{\widehat{\Psi}}(e^{2\pi iz})dz$ depends only on $\lfloor xM \rfloor \pmod M$ and the number of possible values of σ_Ψ is finite. Hence σ_Ψ is p-adically bounded.

Secondly, we consider the expression

$$\sum_{r=0}^{p-1} \sigma_\Psi(a + p^m r + p^{m+1}\mathbb{Z}_p) \tag{2.3}$$

By definition, (2.3) is equal to

$$\frac{1}{\widehat{\Psi}(p^{m+1})} \sum_{r=0}^{p-1} \int_{\frac{a}{p^{m+1}}+\frac{r}{p}-i\infty}^{\frac{a}{p^{m+1}}+\frac{r}{p}+i\infty} R_{\widehat{\Psi}}(e^{2\pi iz})dz = \frac{p^{-1}}{\widehat{\Psi}(p^{m+1})} \int_{\frac{a}{p^m}-i\infty}^{\frac{a}{p^m}+i\infty} \sum_{r=0}^{p-1} R_{\widehat{\Psi}}(e^{\frac{2\pi iz}{p}}\zeta_p^r)dz.$$

Observe that

$$p^{-1}\sum_{r=0}^{p-1} R_{\widehat{\Psi}}(\zeta_p^r T^{\frac{1}{p}}) = p^{-1}\sum_{n=0}^{\infty} \widehat{\Psi}(n) \sum_r \zeta_p^{rn} T^{\frac{n}{p}} = \frac{\sum_{r=1}^{M-1} \widehat{\Psi}(pr)T^r}{1 - T^M}.$$

From this calculation and the hypothesis on Ψ we deduce that the sum (2.3) is equal to $\sigma_\Psi(a + p^m\mathbb{Z}_p)$. □

Let λ be a Dirichlet character of conductor N with $p \nmid N$, $N > 1$ and λ_0 be a periodic function with a period α defined by

$$\lambda_0(r) = \begin{cases} 1 & \text{if } \alpha \nmid r \\ 1-\alpha & \text{if } \alpha \mid r \end{cases}.$$

Observe that

$$\widehat{\lambda_0}(r) = \begin{cases} -\alpha & \text{if } \alpha \nmid r \\ 0 & \text{if } \alpha \mid r \end{cases}.$$

Corollary 2.2. *σ_{λ_0}, σ_λ, and $\sigma_{\lambda,\alpha}$ are p-adic measures on $\mathbb{Z}_p$. Furthermore, $\sigma_{\lambda,\alpha} = \sigma_{\lambda_\alpha}$ for a periodic function λ_α with period αN defined by*

$$\widehat{\lambda_\alpha}(r) = \begin{cases} \widehat{\lambda}(r) & \text{if } \alpha \nmid r \\ \widehat{\lambda}(r) - \widehat{\lambda}(r/\alpha) & \text{if } \alpha \mid r \end{cases}. \tag{2.4}$$

Proof. The first statement is an immediate consequence of Proposition 2.1. For the second one, observe that

$$\sigma_{\lambda,\alpha}(a + p^m\mathbb{Z}_p) = \frac{1}{\widehat{\lambda}(p^m)} \int_{\frac{a}{p^m}-i\infty}^{\frac{a}{p^m}+i\infty} R_{\widehat{\lambda}}(e^{2\pi iz}) - R_{\widehat{\lambda}}(e^{2\pi i\alpha z})dz$$

From the following calculation

$$\begin{aligned} R_{\widehat{\lambda}}(q) - R_{\widehat{\lambda}}(q^{\alpha}) &= \frac{\sum_{r=1}^{N}\widehat{\lambda}(r)q^{r}}{1-q^{N}} - \frac{\sum_{r=1}^{N}\widehat{\lambda}(r)q^{\alpha r}}{1-q^{\alpha N}} \\ &= \frac{\sum_{r=1}^{\alpha N}\widehat{\lambda}(r)q^{r}}{1-q^{\alpha N}} - \frac{\sum_{r=1}^{N}\widehat{\lambda}(r)q^{\alpha r}}{1-q^{\alpha N}} = \frac{\sum_{r=1}^{\alpha N}\widehat{\lambda_{\alpha}}(r)q^{r}}{1-q^{\alpha N}} \\ &= R_{\widehat{\lambda_{\alpha}}}(q) \end{aligned}$$

and the observation that $\widehat{\lambda_{\alpha}}(p^m) = \widehat{\lambda}(p^m)$, we finish the proof. □

Let χ be a Dirichlet character with the decomposition $\chi = \chi_p \chi^{(p)}$, where χ_p is of p-power conductor and $\chi^{(p)}$ is of conductor N with $p \nmid N$. We set $\sigma = \sigma_{\chi^{(p)},\alpha}$ if $N > 1$ and set $\sigma = \sigma_{\lambda_0}$ if $N = 1$. Then we have

Proposition 2.3. *Let χ be an even Dirichlet character. We have*

$$L_p(s,\chi) = \frac{1}{1-\alpha^{-1}\chi\omega^{-1}(\alpha)\langle\alpha\rangle^{-s}} \int_{\mathbb{Z}_p^{\times}} \chi\omega^{-1}(x)\langle x\rangle^{-s} d\sigma(N^{-1}x), \tag{2.5}$$

Proof. Refer to [Su, Section 4] or [H, Chapter 4]. □

Let W be the set of the $v(p-1)$-th roots of unity. Observe that we have the decomposition

$$\mathbb{Z}_p^{\times} = W \times (1 + vp\mathbb{Z}_p). \tag{2.6}$$

Recall that θ is the first factor of χ, i.e. $\theta = \chi|_{W\times(\mathbb{Z}/N\mathbb{Z})^{\times}}$. Define a measure τ_θ as

$$d\tau_\theta(x) := \chi\omega^{-1}(x)d\sigma(N^{-1}x).$$

Let us choose a topological generator $\gamma \in \mathbb{Z}_p^{\times}$ of $1 + vp\mathbb{Z}_p$ so that we have an isomorphism $\gamma^x : \mathbb{Z}_p \xrightarrow{\sim} 1 + vp\mathbb{Z}_p$. Let V be a set of the coset representatives of $W/\{\pm 1\}$. We define a power series $G_{\tau_\theta,\gamma}(T)$ such that

$$G_{\tau_\theta,\gamma}(T) = \int_{\mathbb{Z}_p} T^x d\overline{\tau}_\theta(\gamma^x) := \sum_{n=0}^{\infty} \int_{\mathbb{Z}_p} \binom{x}{n} d\overline{\tau}_\theta(\gamma^x)(T-1)^n$$

where

$$\overline{\tau}_\theta = \sum_{\eta \in V} \tau_\theta \circ \eta$$

and

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

The power series $G_{\tau_\theta,\gamma}(T)$ is called the Γ-*transform* of the p-adic measure τ_θ, which is essentially the Iwasawa power series $f(T;\theta)$:

Proposition 2.4. *Let $h > 0$ be an integer with $p \nmid h$. Setting $\gamma = (1+vp)^{\frac{1}{h}}$ and $\alpha = 1 + vp$, we obtain that*

$$(1 - \alpha^{-1}T^h)f(T^h;\theta) = -G_{\tau_\theta,\gamma}(T).$$

Proof. From (2.1), we are able to conclude that

$$\tau_\theta \circ -1 = \tau_\theta. \tag{2.7}$$

Using the decomposition (2.6) and (2.7), we have

$$\begin{aligned}
&\int_{\mathbb{Z}_p^\times} \chi\omega^{-1}(y)\langle y\rangle^{-s} d\sigma(N^{-1}y) \\
&= \sum_{\eta\in W} \theta\omega^{-1}(\eta) \int_{\mathbb{Z}_p} \chi(\gamma^x)\gamma^{-xs} d\sigma(N^{-1}\gamma^x\eta) \\
&= \sum_{\eta\in W} \int_{\mathbb{Z}_p} \chi(\gamma^x)\gamma^{-xs} d\tau_\theta(\eta x) \\
&= 2G_{\tau_\theta,\gamma}(\chi(\gamma)\gamma^{-s}).
\end{aligned}$$

From (2.5) and the last calculation, we obtain that

$$\frac{-2G_{\tau_\theta,\gamma}(\chi(\gamma)\gamma^{-s})}{1-\alpha^{-1}\chi(\gamma)^h\gamma^{-hs}} = L_p(s,\chi) \text{ for all } s\in\mathbb{Z}_p.$$

and therefore deduce the proposition. □

3. Proof of the main theorem

The coefficients of $G_{\tau_\theta,\gamma}(T)$. The coefficient of a power series in $\overline{\mathbb{F}}_p[[T-1]]$ that is algebraic over $\overline{\mathbb{F}}_p(T)$ is completely characterized in terms of a special class of sequences, called the automatic sequences. A sequence $(a_n)_{n\geq 1}\subseteq \overline{\mathbb{F}}_p$ is called *p-automatic* if the collection of the subsequences

$$\{(a_{p^\ell n+r})_{n\geq 1} | \ell\geq 0,\, 0\leq r<p^\ell\}$$

is a finite set. The following theorem is due to G. Christol.

Theorem 3.1. *(1)(Christol) Let $\mathbb{F}_q$ be the finite field with q elements for a p-power q. A power series $F(T)=\sum_{n=0}^\infty a_n(T-1)^n\in\mathbb{F}_q[[T-1]]$ is algebraic over $\mathbb{F}_q(T)$ if and only if the sequence (a_n) is p-automatic. (2) If (a_n) is p-automatic, then $(a_{p^n-1})_{n\geq 1}$ is eventually periodic.*

Proof. Refer to [AS, Theorem 12.2.5, Corollary 5.5.3]. □

For a power series $P(T):=\sum_{n=0}^\infty c_n(T-1)^n\in\mathfrak{o}[[T-1]]$, set $c(P,n):=c_n$. Theorem 3.1 suggests that in order to obtain the transcendence of $G_{\tau_\theta,\gamma}(T) \pmod{\pi}$ we need to show that $c(G_{\tau_\theta,\gamma},p^n-1)$ is not eventually periodic. We collect another property for the coefficients of the Γ-transform of τ_θ.

Proposition 3.2. $c(G_{\tau_\theta,\gamma}(T),p^n-1)\equiv\overline{\tau}_\theta(\gamma^{-1}+vp^{n+1}\mathbb{Z}_p) \pmod{\pi}$.

Proof. Lucas' theorem asserts that if $a=pa'+r_1$ and $b=pb'+r_2$ with $0\leq r_1,r_2<p$, then we have

$$\binom{a}{b}\equiv\binom{a'}{b'}\binom{r_1}{r_2} \pmod{p}.$$

From this we deduce that $x\mapsto\binom{x}{p^n-1} \pmod{p}$ is periodic with a period p^n. Therefore we have

$$c(G_{\tau_\theta,\gamma}(T),p^n-1)=\int_{\mathbb{Z}_p}\binom{x}{p^n-1}d\overline{\tau}_\theta(\gamma^x)\equiv\sum_{x=0}^{p^n-1}\binom{x}{p^n-1}\overline{\tau}_\theta(\gamma^{x+p^n\mathbb{Z}_p}) \pmod{\pi}$$

Since $\binom{x}{p^n-1}=0$ for $x<p^n-1$, we conclude the proof. □

Proof of Theorem 1.2. In order to deduce contradiction in the end, we begin with the assumption that $f(T;\theta) \pmod{\pi}$ is algebraic over $\overline{\mathbb{F}}_p(T)$. By Proposition 2.4, $G_{\tau_\theta,\gamma}(T) \pmod{\pi}$ is also algebraic over $\mathbb{F}_q(T)$ for a p-power q. By Theorem 3.1, $c(G_{\tau_\theta,\gamma}(T), p^n-1) \pmod{\pi}$ is eventually periodic. Let M be the period with $p^M \equiv 1 \pmod{\alpha N}$. Therefore there exists $N_0 > 0$ such that for all $m, n \geq N_0$, we have

$$c(G_{\tau_\theta,\gamma}(T), \frac{p^{Mn}}{v} - 1) \equiv c(G_{\tau_\theta,\gamma}(T), \frac{p^{Mm}}{v} - 1) \pmod{\pi}.$$

By Proposition 3.2, for all $m, n \geq N_0$ we have

$$\overline{\tau}_\theta(\gamma^{-1} + p^{Mn}\mathbb{Z}_p) \equiv \overline{\tau}_\theta(\gamma^{-1} + p^{Mm}\mathbb{Z}_p) \pmod{\pi}. \tag{3.1}$$

First consider the case of $N = 1$. Note that $\widehat{\lambda_0}(p^{Mn}) = \widehat{\lambda_0}(1) \not\equiv 0 \pmod{\pi}$ for all $n \geq 1$. From the definition of $\overline{\tau}_\theta$ and the congruence (3.1) we have for all $m, n \geq N_0$

$$\sum_{i=1}^{\frac{p-1}{2}} \theta(\gamma^{-1}\eta_i)\omega(\eta_i) \left(\int_{\frac{\gamma^{-1}\eta_i}{p^{Mn}} - i\infty}^{\frac{\gamma^{-1}\eta_i}{p^{Mn}} + i\infty} - \int_{\frac{\gamma^{-1}\eta_i}{p^{Mm}} - i\infty}^{\frac{\gamma^{-1}\eta_i}{p^{Mm}} + i\infty} \right) R_{\widehat{\lambda_0}}(e^{2\pi i z})dz \equiv 0 \pmod{\pi}. \tag{3.2}$$

We now state a lemma to control the above integrals, the proof of which is presented in the next section.

Lemma 3.3. *Assume Borel's conjecture and choose a positive integer h so that $p \nmid h$ and $\gamma = (1 + vp)^{\frac{1}{h}} \notin \mathbb{Q}(W)$. Then for all $K > 0$, there exist n, $m \geq K$ such that*

$$0 < \frac{\gamma^{-1}\eta_1}{Q^n} < \frac{1}{N} < \frac{\gamma^{-1}\eta_1}{Q^m} < \frac{2}{N}$$

and

$$\frac{s_i}{N} < \frac{\gamma^{-1}\eta_i}{Q^n}, \frac{\gamma^{-1}\eta_i}{Q^m} < \frac{s_i + 1}{N}$$

for some $0 \leq s_i < N$ and each $i = 2, \cdots, \frac{p-1}{2}$.

Now we choose m, n which satisfy the condition in Lemma 3.3 with $N = \alpha$ and $Q = p^M$. Then we have

$$\left(\int_{\frac{\gamma^{-1}\eta_1}{p^{Mn}} - i\infty}^{\frac{\gamma^{-1}\eta_1}{p^{Mn}} + i\infty} - \int_{\frac{\gamma^{-1}\eta_1}{p^{Mm}} - i\infty}^{\frac{\gamma^{-1}\eta_1}{p^{Mm}} + i\infty} \right) R_{\widehat{\lambda_0}}(e^{2\pi i z})dz = -2\pi i \mathrm{Res}_{z=\frac{1}{\alpha}} R_{\widehat{\lambda_0}}(e^{2\pi i z}) = \frac{\alpha\lambda_0(-1)}{\alpha}.$$

For $i = 2, \cdots, \frac{p-1}{2}$ we also obtain that

$$\left(\int_{\frac{\gamma^{-1}\eta_i}{p^{Mn}} - i\infty}^{\frac{\gamma^{-1}\eta_i}{p^{Mn}} + i\infty} - \int_{\frac{\gamma^{-1}\eta_i}{p^{Mm}} - i\infty}^{\frac{\gamma^{-1}\eta_i}{p^{Mm}} + i\infty} \right) R_{\widehat{\lambda_0}}(e^{2\pi i z})dz = 0$$

In total, the congruence (3.2) becomes

$$\theta(\gamma^{-1}\eta_1)\omega(\eta_1)\lambda_0(-1) \equiv 0 \pmod{\pi}.$$

This is contradiction.

For $N > 1$ case, we do a similar calculation as above. The similar congruence as (3.2) with $R_{\widehat{\lambda_\alpha}}(q)$ instead of $R_{\widehat{\lambda_0}}(q)$ enables us to deduce

$$-2\pi i \mathrm{Res}_{z=\frac{1}{\alpha N}} R_{\widehat{\lambda_\alpha}}(q) = \frac{\widehat{\widehat{\lambda_\alpha}}(1)}{\alpha N} \equiv 0 \pmod{\pi}.$$

In fact from (2.4) we have

$$\widehat{\lambda_\alpha}(1) = \sum_{s=1}^{\alpha N} \widehat{\lambda}(s)\zeta_{\alpha N}^s - \sum_{s=1}^{N} \widehat{\lambda}(\alpha s)\zeta_N^s = -N\lambda(-\overline{\alpha}).$$

From the absurd congruence $N\lambda(-\overline{\alpha}) \equiv 0 \pmod{\pi}$, we finish the proof of Theorem 1.2. □

4. Proof of Lemma 3.3

Proposition 4.1. *Let $\alpha_1, \cdots, \alpha_r$ be algebraic p-adic integers such that $1, \alpha_1, \cdots, \alpha_r$ are linearly independent over $\mathbb{Q}$. Then Borel's conjecture implies that $\alpha_1, \cdots, \alpha_r$ are jointly normal to the base Q.*

Proof. We show that the sequence $\{(\frac{\alpha_1}{Q^n}, \cdots, \frac{\alpha_r}{Q^n}) | n \geq 1\}$ is equi-distributed on $[0,1)^r$. Let $n_1, \cdots, n_r$ be integers which are not all zero. By Weyl's criterion for the multi-dimensional case, we need to show that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{\frac{2\pi i(\alpha_1 n_1 + \cdots + \alpha_r n_r)}{Q^n}} = 0$$

Observe that $\alpha_1 n_1 + \cdots + \alpha_r n_r$ is non-zero and irrational algebraic by the hypothesis. Therefore by Borel's conjecture and Weyl's criterion again for $r = 1$ case, we obtain the above limit. □

The following is immediate from the definition of equi-distribution (see [KN]).

Corollary 4.2. *Let $(x_i)_{i=1}^r \in [0,1)^r$ and $\epsilon > 0$. For any $K > 0$, we can choose $n \geq K$ so that*

$$\left| \left(\frac{\alpha_i}{Q^n} \right)_{i=1}^r - (x_i) \right| < \epsilon.$$

Let $U = \{\eta_1, \eta_2, \cdots, \eta_t\}$ be a maximal $\mathbb{Q}$-linearly independent subset of V. Set $V = \{\eta_1, \cdots, \eta_t, \tau_1, \cdots, \tau_s\}$. We have an integral $t \times s$ matrix A such that

$$(\tau_1, \cdots, \tau_s) = (\eta_1, \cdots, \eta_t)A.$$

Let $\alpha_1, \cdots, \alpha_t$ be any real numbers and set

$$P(\alpha_1, \cdots, \alpha_t) := (\alpha_1, \cdots, \alpha_t)\,(I|A)$$

for a $t \times t$ identity matrix I and a $t \times \frac{p-1}{2}$ block matrix $(I|A)$. For each integer i with $1 \leq i \leq \frac{p-1}{2}$ we set $P(\alpha_1, \cdots, \alpha_t)_{(i)}$ be the i-th coordinate of $P(\alpha_1, \cdots, \alpha_t)$. We extract the following lemma from the proof of [Su, Proposition 4].

Lemma 4.3. *There exist numbers α_1', α_1'', α_2°, $\cdots$, α_t° such that*

(1) $P(\alpha_1', \alpha_2^\circ, \cdots, \alpha_t^\circ)_{(1)} = \alpha_1' \in (0, \frac{1}{N})$,
(2) $P(\alpha_1'', \alpha_2^\circ, \cdots, \alpha_t^\circ)_{(1)} = \alpha_1'' \in (\frac{1}{N}, \frac{2}{N})$
(3) *For each $i = 2, \cdots, \frac{p-1}{2}$, there is an integer $0 \leq s_i < N$ such that*

$$\frac{s_i}{N} < P(\alpha_1', \alpha_2^\circ, \cdots, \alpha_t^\circ)_{(i)}, P(\alpha_1'', \alpha_2^\circ, \cdots, \alpha_t^\circ)_{(i)} < \frac{s_i + 1}{N}.$$

Proof. Consider a function $P(\frac{1}{N}, \alpha_2, \cdots, \alpha_t)$ of real variables $\alpha_2, \cdots, \alpha_t$. Since A is an integral matrix, we have

$$P\Big(\frac{1}{N}, 0, \cdots, 0\Big)_{(i)} \in \frac{1}{N}\mathbb{Z} \text{ for each } i.$$

Since there is no pair $\eta \neq \eta'$ in V such that $\eta/\eta' \in \mathbb{Q}$, $P(\alpha_1, \cdots, \alpha_t)_{(i)}$ is not a $\mathbb{Z}$-multiple of α_1 for $i = 2, \cdots, \frac{p-1}{2}$. Hence the function $P(\frac{1}{N}, \alpha_2, \cdots, \alpha_t)_{(i)}$ is not constant for each $i = 2, \cdots, \frac{p-1}{2}$ and we can find $(\alpha_2^\circ, \cdots, \alpha_t^\circ)$ around $(0, \cdots, 0)$ such that

$$P\Big(\frac{1}{N}, \alpha_2^\circ, \cdots, \alpha_t^\circ\Big)_{(i)} \notin \frac{1}{N}\mathbb{Z}$$

for $i = 2, \cdots, \frac{p-1}{2}$. Note that $P(\frac{1}{N}, \alpha_2^\circ, \cdots, \alpha_t^\circ)_{(1)} = \frac{1}{N}$. Since $P(\alpha_1, \alpha_2^\circ, \cdots, \alpha_t^\circ)$ is continuous in the variable α_1, we can find two numbers α_1', α_1'' near $\frac{1}{N}$ such that the vectors $P(\alpha_1', \alpha_2^\circ, \cdots, \alpha_t^\circ)$ and $P(\alpha_1'', \alpha_2^\circ, \cdots, \alpha_t^\circ)$ satisfy (1), (2), and (3). □

Proof of Lemma 3.3. The condition on γ implies that $1, \gamma^{-1}\eta_1, \cdots, \gamma^{-1}\eta_t$ are linearly independent over $\mathbb{Q}$. By Corollary 4.2, we can find vectors $(\frac{\gamma^{-1}\eta_1}{Q^n}, \cdots, \frac{\gamma^{-1}\eta_t}{Q^n})$, $(\frac{\gamma^{-1}\eta_1}{Q^m}, \cdots, \frac{\gamma^{-1}\eta_t}{Q^m})$ for some $m, n \geq K$, which are close enough to the vectors $(\alpha_1', \alpha_2^\circ, \cdots, \alpha_t^\circ)$, $(\alpha_1'', \alpha_2^\circ, \cdots, \alpha_t^\circ)$ in Lemma 4.3 respectively. Therefore the two vectors $P((\frac{\gamma^{-1}\eta_1}{Q^n}, \cdots, \frac{\gamma^{-1}\eta_t}{Q^n}))$, $P((\frac{\gamma^{-1}\eta_1}{Q^m}, \cdots, \frac{\gamma^{-1}\eta_t}{Q^m}))$ satisfy the above conditions (1), (2), and (3) in Lemma 4.3. □

References

[AS] J.-P. Allouche and J. Shallit, Automatic sequences, Cambridge Univ. press, Cambridge, 2003.

[A] B. Anglès, On some p-adic power series attached to the arithmetic of $\mathbb{Q}(\zeta_p)$, J. Number Theory 122 (2007), no. 1, 221–246.

[A2] B. Anglès, On the p-adic Leopoldt transform of a power series, Acta Arith. 134. 4 (2008)

[B] É. Borel, Sur les chiffres décimaux de $\sqrt{2}$ et divers problèmes de probabilités en chaîne. C. R. Acad. Sci. Paris 230, (1950). 591–593.

[FW] B. Ferrero and L. C. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math. (2) 109 (1979), no. 2, 377–395.

[H] H. Hida, Elementary Theory of L-Functions and Eisenstein Series, LMSST 26, Cambridge Univ. Press, Cambridge, England, 1993.

[Iw] K. Iwasawa, Lectures on p-adic L-functions, Ann. of Math. Studies 74. Princeton Univ. Press 1972.

[KN] L. Kuipers and H. Niederreiter, Uniform distribution of sequences. Pure and Applied Mathematics. John Wiley & Sons, New York-London-Sydney 1974.

[Si] W. Sinnott, On the μ-invarian of the Γ-transform of a rational function, Invent. Math. 75, 273-282(1984).

[Si2] W. Sinnott, On the power series attached to p-adic L-functions, J. reine angew. Math. 382, 22–34 (1987).

[Su] H.-S. Sun, Derivative of power series attached to Γ-transform of p-adic measures, to appear in J. Number Theory (available at `http://newton.kias.re.kr/~haesang`).

Korea Institute for Advanced Study Hoegiro 87, Dongdaemun-gu, Seoul 130-722, Korea

E-mail address: `haesang@kias.re.kr`