



**HAL**  
open science

## Set Equidistribution of subsets of $(\mathbb{Z}/n\mathbb{Z})$ \*

Jaitra Chattopadhyay, Veekesh Kumar, R Thangadurai

► **To cite this version:**

Jaitra Chattopadhyay, Veekesh Kumar, R Thangadurai. Set Equidistribution of subsets of  $(\mathbb{Z}/n\mathbb{Z})$  \*. Hardy-Ramanujan Journal, 2019, Atelier Digit\_Hum, pp.118 - 126. 10.46298/hrj.2019.5113 . hal-01986709

**HAL Id: hal-01986709**

**<https://hal.science/hal-01986709v1>**

Submitted on 19 Jan 2019

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Set Equidistribution of subsets of $(\mathbb{Z}/n\mathbb{Z})^*$

Jaitra Chattopadhyay, Veekesh Kumar and R. Thangadurai

*To the memory of S. Srinivasan*

**Abstract.** In 2010, Murty and Thangadurai [MuTh10] provided a criterion for the set equidistribution of residue classes of subgroups in  $(\mathbb{Z}/n\mathbb{Z})^*$ . In this article, using similar methods, we study set equidistribution for some class of subsets of  $(\mathbb{Z}/n\mathbb{Z})^*$ . In particular, we study the set equidistribution modulo 1 of cosets, complement of subgroups of the cyclic group  $(\mathbb{Z}/n\mathbb{Z})^*$  and the subset of elements of fixed order, whenever the size of the subset is sufficiently large.

**Keywords.** Set equi-distribution, residue classes mod  $n$

**2010 Mathematics Subject Classification.** 11K45.

## 1. Introduction

We say (as defined in [MuSi09]) that a sequence of finite multisets  $A_n$  with  $A_n \subseteq [0, 1]$  and  $|A_n| \rightarrow \infty$  is *set equidistributed mod 1* with respect to a probability measure  $\mu$ , if for every continuous function  $f$  on  $[0, 1]$ , we have

$$\lim_{n \rightarrow \infty} \frac{1}{|A_n|} \sum_{t \in A_n} f(t) = \int_0^1 f(x) d\mu. \quad (1.1)$$

In order to verify this condition, it suffices to check that this limit exists on a dense family of functions  $f$  in  $C[0, 1]$ . Here, we shall make use of the family of Bernoulli polynomials.

Murty and Thangadurai [MuTh10] proved that the elements of the subgroup  $H_n$  of  $(\mathbb{Z}/n\mathbb{Z})^*$ , are set equidistributed modulo 1, whenever  $|H_n|/\sqrt{n} \rightarrow \infty$  as  $n \rightarrow \infty$ .

Motivated from this, one may ask the following natural question: If  $S_n$  is a subset of  $(\mathbb{Z}/n\mathbb{Z})^*$  such that  $|S_n| > n^{\frac{1}{2}+\epsilon}$ , are the elements of the subset  $S_n$  of  $(\mathbb{Z}/n\mathbb{Z})^*$  set equidistributed modulo 1, as  $n \rightarrow \infty$ ? In other words, does the result of [MuTh10] apply for subsets and not just subgroups?

In general, the answer is not affirmative. For instance, if  $S'_n = \{a_1, a_2, \dots, a_m\} \subset (\mathbb{Z}/n\mathbb{Z})^*$  where  $m = [n^{\frac{1}{2}+\epsilon}] + 1$  and  $a_i$ 's are the first  $m$  integers  $\leq n$  with  $(a_i, n) = 1$ , then the elements of  $S_n := S'_n/n$  are close to 0 in  $[0, 1]$  for all integers  $n \rightarrow \infty$  and hence these sets are not set equidistributed mod 1. However, for many arithmetical subsets like the set of all quadratic non-residues modulo  $p$  (which is not a subgroup of  $(\mathbb{Z}/p\mathbb{Z})^*$ ), and the set of all generators of  $(\mathbb{Z}/n\mathbb{Z})^*$ , whenever it is cyclic, the above question makes sense.

In this article, we give a partial answer to the above question. More precisely, we prove the following theorems:

**Theorem 1.1.** *Let  $\epsilon$  be a given number with  $0 < \epsilon < 1/12$ . Consider an integer  $n = p^k$  or  $2p^k$  for some odd prime  $p$ , some integer  $k \geq 1$  and a positive divisor  $f$  of  $n$  satisfying  $\phi(n)/f \geq n^{1/2+3\epsilon}$ . Let  $S_{n,f}$  be a subset of  $(\mathbb{Z}/n\mathbb{Z})^*$  which consists precisely of those elements whose index is  $f$  in  $(\mathbb{Z}/n\mathbb{Z})^*$  and take the representatives  $\mathcal{S}_{f,n}$  as integers, say,  $s_n$  with  $1 < s_n \leq n-1$  and  $(s_n, n) = 1$ . Let  $S'_{f,n} = \{s/(n-1) : s \in \mathcal{S}_{f,n}\} \subset [0, 1]$ . Then the sets  $S'_{f,n}$ 's are set equidistributed in  $[0, 1]$  with respect to the Lebesgue measure.*

In Theorem 1.1, when we take  $f = 1$ , then trivially the hypothesis is true. Hence, when  $n$  runs through numbers of the form  $n = p^k$  or  $2p^k$  for an odd prime  $p$  and for some integer  $k \geq 1$ , we find that the sets of generators of  $(\mathbb{Z}/n\mathbb{Z})^*$  are set equidistributed modulo 1.

**Theorem 1.2.** *For an integer  $n = p^k$  or  $2p^k$  for some odd prime  $p$  and for some integer  $k \geq 1$ , let  $S_n$  be a subset of  $(\mathbb{Z}/n\mathbb{Z})^*$  such that its complement is a subgroup of  $(\mathbb{Z}/n\mathbb{Z})^*$  and we take the representatives  $S_n$  as integers, say,  $s_n$  with  $1 < s_n \leq n - 1$  and  $(s_n, n) = 1$ . Let  $S'_n = \{s/(n - 1) : s \in S_n\} \subset [0, 1]$ . For a given  $\epsilon > 0$ , if  $|S_n|/n^{\frac{1}{2}+2\epsilon} \rightarrow \infty$  as  $n \rightarrow \infty$ , then the  $S'_n$ s are set equidistributed in  $[0, 1]$  with respect to the Lebesgue measure.*

As an application of Theorem 1.2, we have the following corollary.

**Corollary 1.3.** *Let  $r \geq 2$  be an integer. For any prime number  $p$  such that  $p \equiv 1 \pmod{r}$ , let  $H_p = \{a \in (\mathbb{Z}/p\mathbb{Z})^* : a^{\frac{p-1}{r}} \equiv 1 \pmod{p}\} \subset (\mathbb{Z}/p\mathbb{Z})^*$  and let the representatives of  $H_p$  be  $\{h_1, \dots, h_{(p-1)/r}\}$  as a subset of  $\{1, 2, \dots, p - 1\}$ . Let*

$$S_p = \{a/p : a \in \{1, 2, \dots, p - 1\} \text{ and } a \neq h_i \text{ for any } i\}.$$

*Then, as  $p \rightarrow \infty$  such that  $p \equiv 1 \pmod{r}$ , the sets  $S_p$ 's are set equidistributed in  $[0, 1]$  with respect to Lebesgue measure. In particular, when  $r = 2$ , we get the set of all quadratic non-residues modulo  $p$ , are set equidistributed in  $[0, 1]$ .*

**Theorem 1.4.** *For any integer  $n \geq 2$ , let  $H'_n$  be a subgroup of  $(\mathbb{Z}/n\mathbb{Z})^*$  and take the representatives of  $H'_n$  as integers, say,  $h$  such that  $1 \leq h < n$  and  $(n, h) = 1$ . Let  $H_n = \{h/n : h \in H'_n\}$  be a finite subset of  $[0, 1]$ . If  $|H_n|/\sqrt{n} \rightarrow \infty$  as  $n \rightarrow \infty$ , then for any given  $g_n \in (\mathbb{Z}/n\mathbb{Z})^*$ , the cosets  $g_n H_n$ 's are set equidistributed in  $[0, 1]$  with respect to the Lebesgue measure in  $[0, 1]$ .*

## 2. Preliminaries

In order to prove the sets  $S_n$  are set equidistributed, it suffices to determine the behaviour of sums of the form

$$\sum_{k=1}^{|S_n|} f_m(g_k),$$

for any suitable family of polynomials  $f_m$  of degree  $m$  for each integer  $m \geq 1$ , with  $g_k \in S_n$ . It is convenient to take the Bernoulli polynomials which are defined as

$$B_m(X) = \sum_{k=0}^m \binom{m}{k} B_k X^{m-k},$$

for each integer  $m \geq 1$  where  $B_k$  denotes the  $k$ th-Bernoulli number, because the set of all finite  $\mathbb{Q}$ -linear combinations of  $\{B_m(X)\}$  is a dense subset of  $C[0, 1]$  (see [Apo76]). Therefore, we consider the sum

$$\sum_{k=1}^{|S_n|} B_m\left(\frac{g_k}{n}\right)$$

and we would like to prove that

$$\lim_{n \rightarrow \infty} \frac{1}{|S_n|} \sum_{k=1}^{|S_n|} B_m\left(\frac{g_k}{n}\right) = \int_0^1 B_m(t) dt.$$

A well-known result states that (for instance, see [Mu08], page 19)

**Lemma 2.1.** *For any integer  $m \geq 1$ , we have*

$$\int_0^1 B_m(t) dt = 0.$$

Thus, by Lemma 2.1, in order to prove that the sequence of sets  $\{S_n\}$  are set equidistributed mod 1, it is enough to prove that

$$\lim_{n \rightarrow \infty} \frac{1}{|S_n|} \sum_{k=1}^{|S_n|} B_m\left(\frac{g_k}{n}\right) = 0.$$

The way to understand this sum,  $\sum_{k=1}^{|S_n|} B_m\left(\frac{g_k}{n}\right)$ , is through the generalized Bernoulli numbers (see for instance [Wa97]) which are defined as follows. For any Dirichlet character  $\chi : (\mathbb{Z}/n\mathbb{Z})^* \rightarrow \mathbb{C}^*$  and for any integer  $m \geq 1$ , we define the  $m$ -th generalized Bernoulli number  $B_{m,\chi}$  as

$$B_{m,\chi} = n^{m-1} \sum_{a=1}^n \chi(a) B_m\left(\frac{a}{n}\right).$$

Then we get the connection between  $B_{m,\chi}$  and the Dirichlet  $L$ -function with character  $\chi$  at  $s = m$  and use the estimates of the special values of  $L$ -functions. For more information, we refer to Murty [Mu08]. Indeed, we need the following Lemma which can be found in [Mu08], pp 122.

**Lemma 2.2.** *We have the following;*

1. *For any character  $\chi$  on  $(\mathbb{Z}/n\mathbb{Z})^*$  and for any integer  $m \geq 1$ , we have*

$$L(1 - m, \chi) = -\frac{B_{m,\chi}}{m}.$$

2. *If  $\chi$  is any character on  $(\mathbb{Z}/n\mathbb{Z})^*$ , then, there exists a positive constant  $C(m)$ , depending only on  $m$  such that*

$$|L(1 - m, \chi)| \leq C(m) n^{m-\frac{1}{2}}$$

*for all integers  $m \geq 1$  and for all  $n > e^{17}$ . (Proof of this fact can be seen in the proof of Theorem 2 in [MuTh10]).*

The following lemma is standard and we shall state as follows.

**Lemma 2.3.** *Let  $\sigma_0(n)$  denote the number of positive divisors  $n$ . Then, we have*

$$\sigma_0(n) \leq n^\epsilon \text{ for all large enough integers } n,$$

*for any given  $\epsilon > 0$ . Also, we know that*

$$\phi(n) \gg n^{1-\epsilon}$$

*for any given  $\epsilon > 0$ , where  $\phi$  stands for the Euler's totient function.*

We need the following two crucial lemmas for the proof of Theorems 1.1 and 1.2 (see Lemma 3 in [Jo73]).

**Lemma 2.4.** *Let  $R$  be a finite ring such that  $R^*$  is the cyclic group of order  $n$  for some integer  $n \geq 2$  and let  $f$  be a positive divisor of  $n$ . For any  $a \in R$ , we define*

$$I_f(a) = \begin{cases} 1 & \text{if } a \in R^* \text{ and } a \text{ is of index } f \text{ in } R^*; \\ 0 & \text{otherwise,} \end{cases}$$

where the index of an element  $a \in R^*$  means the index of the subgroup generated by  $a$  in  $R^*$ . Then, for any  $a \in R^*$ , we have,

$$I_f(a) = \frac{1}{f} \sum_{d|(n/f)} \frac{\mu(d)}{d} \sum_{\chi^{fd} = \chi_0} \chi(a),$$

where  $\mu$  is the Möbius function and the inner summation runs over all the multiplicative characters  $\chi$  of  $R$  of order at most  $fd$ .

The following lemma computes the characteristic function for a given subset  $\mathcal{S}$  of a cyclic group  $G$  such that its complement is a subgroup.

**Lemma 2.5.** *Let  $G$  be a cyclic group of order  $n$  for some integer  $n \geq 2$ . Let  $\mathcal{S}$  be a finite subset of  $G$  such that  $G \setminus \mathcal{S}$  is a subgroup of  $G$ . Let*

$$R = \{r \in \mathbb{N} : r \text{ is the index of } a \in \mathcal{S} \text{ for some } a\} = \{r_1, \dots, r_\ell\}$$

be the finite subset of  $\mathbb{N}$ . Then

$$\sum_{i=1}^{\ell} \left( \frac{1}{r_i} \sum_{d|\frac{n}{r_i}} \frac{\mu(d)}{d} \sum_{\chi^{r_i d} = \chi_0} \chi(a) \right) = \begin{cases} 1 & \text{if } a \in \mathcal{S}; \\ 0 & \text{otherwise,} \end{cases}$$

where  $\mu$  is the Möbius function and the inner sum runs over the multiplicative characters  $\chi$  of  $G$  of order at most  $r_i d$ .

*Proof.* Suppose  $a \in \mathcal{S}$  and let  $r_j$  be the index of  $a$  for some integer  $j \in \{1, \dots, \ell\}$ . Then by Lemma 2.4, we get

$$\frac{1}{r_i} \sum_{d|\frac{n}{r_i}} \frac{\mu(d)}{d} \sum_{\chi^{r_i d} = \chi_0} \chi(a) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, we have

$$\sum_{i=1}^{\ell} \left( \frac{1}{r_i} \sum_{d|(n/r_i)} \frac{\mu(d)}{d} \sum_{\chi^{r_i d} = \chi_0} \chi(a) \right) = 1.$$

Now, let  $b \in G \setminus \mathcal{S}$  and let  $q$  be the index of  $b$ . Then, we shall show that

$$\frac{1}{r_i} \sum_{d|\frac{n}{r_i}} \frac{\mu(d)}{d} \sum_{\chi^{r_i d} = \chi_0} \chi(b) = 0$$

for all  $1 \leq i \leq \ell$ .

To prove this, it suffices to show that  $q \notin \{r_1, r_2, \dots, r_\ell\}$ . Since  $G$  is a finite cyclic group, there exists a unique subgroup  $H_q$  of index  $q$ . Since the index of  $b$  is  $q$ , we conclude that the subgroup generated by  $b$  is equal to  $H_q$ . Also, note that any element in  $G$ , which is of index  $q$ , is a generator of  $H_q$ . Since  $b \in G \setminus \mathcal{S}$  and by hypothesis  $G \setminus \mathcal{S}$  is a subgroup, we conclude that  $b \in H_q \subset G \setminus \mathcal{S}$ . Since  $b$  is arbitrary, we conclude that any element of index  $q$  lies in  $G \setminus \mathcal{S}$ . Therefore,  $q \notin \{r_1, r_2, \dots, r_\ell\}$  and proves the lemma.

### 3. Proof of Theorem 1.1

By Lemma 2.4, we have

$$\frac{1}{f} \sum_{d|\frac{\phi(n)}{f}} \frac{\mu(d)}{d} \sum_{\chi^{fd}=\chi_0} \chi(a) = \begin{cases} 1 & \text{if } a \in \mathcal{S}_{f,n} \\ 0 & \text{otherwise.} \end{cases}$$

Let  $\mathcal{S}_{f,n} = \{g_1, \dots, g_{|\mathcal{S}_{f,n}|}\}$  and  $m \geq 1$  be a given integer. Then consider

$$\begin{aligned} \sum_{k=1}^{|\mathcal{S}_{f,n}|} B_m\left(\frac{g_k}{n}\right) &= \sum_{k=1}^n B_m\left(\frac{k}{n}\right) \left( \frac{1}{f} \sum_{d|\frac{\phi(n)}{f}} \frac{\mu(d)}{d} \sum_{\chi^{fd}=\chi_0} \chi(k) \right) \\ &= \frac{1}{f} \sum_{d|\frac{\phi(n)}{f}} \frac{\mu(d)}{d} \left( \sum_{k=1}^n B_m\left(\frac{k}{n}\right) \sum_{\chi^{fd}=\chi_0} \chi(k) \right) \\ &= \frac{1}{f} \sum_{d|\frac{\phi(n)}{f}} \frac{\mu(d)}{d} \left( \sum_{\chi^{fd}=\chi_0} \sum_{k=1}^n \chi(k) B_m\left(\frac{k}{n}\right) \right) \\ &= \frac{1}{f} \sum_{d|\frac{\phi(n)}{f}} \frac{\mu(d)}{d} \left( \frac{1}{n^{m-1}} \sum_{\chi^{fd}=\chi_0} B_{m,\chi} \right). \end{aligned}$$

By Lemma 2.1, it is enough to show that for each integer  $m \geq 1$ , we have

$$\frac{1}{|\mathcal{S}_{f,n}|} \sum_{k=1}^{|\mathcal{S}_{f,n}|} B_m\left(\frac{g_k}{n}\right) \rightarrow 0 \text{ as } n \rightarrow \infty.$$

Also, by Lemma 2.2 (1), for any character  $\chi$ , we have  $L(1-m, \chi) = -\frac{B_{m,\chi}}{m}$ . Therefore, we get,

$$\begin{aligned} \frac{1}{|\mathcal{S}_{f,n}|} \left| \sum_{k=1}^{|\mathcal{S}_{f,n}|} B_m\left(\frac{g_k}{n}\right) \right| &= \frac{1}{|\mathcal{S}_{f,n}|} \left| \frac{1}{f} \sum_{d|\frac{\phi(n)}{f}} \frac{\mu(d)}{d} \left( \frac{1}{n^{m-1}} \sum_{\chi^{fd}=\chi_0} (-m)L(1-m, \chi) \right) \right| \\ &\leq \frac{1}{|\mathcal{S}_{f,n}|} \frac{1}{f} \sum_{d|\frac{\phi(n)}{f}} \frac{|\mu(d)|}{d} \left( \frac{m}{n^{m-1}} \sum_{\chi^{fd}=\chi_0} |L(1-m, \chi)| \right) \\ &= \frac{m}{|\mathcal{S}_{f,n}| n^{m-1}} \frac{1}{f} \sum_{d|\frac{\phi(n)}{f}} \frac{|\mu(d)|}{d} \left( \sum_{\chi^{fd}=\chi_0} |L(1-m, \chi)| \right) \\ &\leq \frac{C'(m)}{|\mathcal{S}_{f,n}| n^{m-1}} \frac{1}{f} \sum_{d|\frac{\phi(n)}{f}} \frac{1}{d} \left( \sum_{\chi^{fd}=\chi_0} n^{m-\frac{1}{2}} \right), \end{aligned}$$

for some positive constant  $C'(m)$  that depends only on  $m$  by Lemma 2.2 (2). Therefore, we get,

$$\begin{aligned} \left| \frac{1}{|\mathcal{S}_{f,n}|} \sum_{k=1}^{|\mathcal{S}_{f,n}|} B_m \left( \frac{g_k}{n} \right) \right| &\leq \frac{C'(m)\sqrt{n}}{|\mathcal{S}_{f,n}|} \frac{1}{f} \sum_{d|\frac{\phi(n)}{f}} \frac{1}{d} \left( \sum_{\chi^{fd}=\chi_0} 1 \right) \\ &\leq \frac{C'(m)\sqrt{n}}{|\mathcal{S}_{f,n}|} \frac{1}{f} \sum_{d|\frac{\phi(n)}{f}} \frac{1}{d} (fd) = \frac{C'(m)\sqrt{n}}{|\mathcal{S}_{f,n}|} \left( \sum_{d|\frac{\phi(n)}{f}} 1 \right) \\ &= \frac{C'(m)\sqrt{n}}{|\mathcal{S}_{f,n}|} \sigma_0 \left( \frac{\phi(n)}{f} \right). \end{aligned}$$

Since the set  $\mathcal{S}_{f,n}$  precisely contains the generators of the cyclic subgroup of order  $\frac{\phi(n)}{f}$ , the cardinality of the set  $\mathcal{S}_{f,n}$  is  $\phi \left( \frac{\phi(n)}{f} \right)$ . Therefore, we have

$$\begin{aligned} \left| \frac{1}{|\mathcal{S}_{f,n}|} \sum_{k=1}^{|\mathcal{S}_{f,n}|} B_m \left( \frac{g_k}{n} \right) \right| &\leq \frac{C'(m)\sqrt{n}}{|\mathcal{S}_{f,n}|} \sigma_0 \left( \frac{\phi(n)}{f} \right) \\ &= \frac{C'(m)\sqrt{n}}{\phi \left( \frac{\phi(n)}{f} \right)} \sigma_0 \left( \frac{\phi(n)}{f} \right). \end{aligned}$$

For a given  $\epsilon > 0$ , we know that  $\sigma_0(n) = O(n^\epsilon)$  and  $\phi(n) > n^{1-\epsilon}$  for all sufficiently large integers  $n$ . Hence, since  $\sigma_0 \left( \frac{\phi(n)}{f} \right) \leq C \left( \frac{\phi(n)}{f} \right)^\epsilon$  for some positive constant  $C$  and  $\phi \left( \frac{\phi(n)}{f} \right) > \left( \frac{\phi(n)}{f} \right)^{1-\epsilon}$ . Thus, we get,

$$\left| \frac{1}{|\mathcal{S}_{f,n}|} \sum_{k=1}^{|\mathcal{S}_{f,n}|} B_m \left( \frac{g_k}{n} \right) \right| < \frac{C'(m)C\sqrt{n}f^{1-2\epsilon}}{\phi(n)^{1-2\epsilon}}.$$

By hypothesis, we know that  $\frac{\phi(n)}{f} \geq n^{1/2+3\epsilon}$ , we see that

$$\left| \frac{1}{|\mathcal{S}_{f,n}|} \sum_{k=1}^{|\mathcal{S}_{f,n}|} B_m \left( \frac{g_k}{n} \right) \right| < \frac{C'(m)C}{n^{2\epsilon-6\epsilon^2}}$$

and hence as  $n \rightarrow \infty$ , we get the desired result, as the given  $\epsilon$  satisfies  $0 < \epsilon < \frac{1}{12}$ . □

### 4. Proof of Theorem 1.2

For each integer  $n = p^k$  or  $2p^k$ , where  $p$  is an odd prime and  $k \geq 1$  is an integer, we let  $\mathcal{S}_n$  be a given subset of  $(\mathbb{Z}/n\mathbb{Z})^*$  such that its complement is a subgroup of  $(\mathbb{Z}/n\mathbb{Z})^*$ . Note that for these values of  $n$ , the group of coprime residue classes modulo  $n$  is cyclic.

Let  $n$  be one such natural number and we consider  $\mathcal{S}_n$ . Suppose  $r_1, r_2, \dots, r_\ell$  be the indices of the elements of  $\mathcal{S}_n$ . By lemma 2.4, we have

$$\sum_{i=1}^{\ell} \left( \frac{1}{r_i} \sum_{d|\frac{n}{r_i}} \frac{\mu(d)}{d} \sum_{\chi^{r_i d}=\chi_0} \chi(a) \right) = \begin{cases} 1 & \text{if } a \in \mathcal{S}_n \\ 0 & \text{otherwise.} \end{cases}$$

Let  $\mathcal{S}_n = \{g_1, \dots, g_{|\mathcal{S}_n|}\}$  and  $m \geq 1$  be a given integer. Then consider

$$\begin{aligned}
\sum_{k=1}^{|\mathcal{S}_n|} B_m \left( \frac{g_k}{n} \right) &= \sum_{k=1}^n B_m \left( \frac{k}{n} \right) \sum_{i=1}^{\ell} \left( \frac{1}{r_i} \sum_{d|\frac{\phi(n)}{r_i}} \frac{\mu(d)}{d} \sum_{\chi^{r_i d}=\chi_0} \chi(k) \right) \\
&= \sum_{i=1}^{\ell} \frac{1}{r_i} \sum_{d|\frac{\phi(n)}{r_i}} \frac{\mu(d)}{d} \left( \sum_{k=1}^n B_m \left( \frac{k}{n} \right) \sum_{\chi^{r_i d}=\chi_0} \chi(k) \right) \\
&= \sum_{i=1}^{\ell} \frac{1}{r_i} \sum_{d|\frac{\phi(n)}{r_i}} \frac{\mu(d)}{d} \left( \sum_{\chi^{r_i d}=\chi_0} \sum_{k=1}^n \chi(k) B_m \left( \frac{k}{n} \right) \right) \\
&= \sum_{i=1}^{\ell} \frac{1}{r_i} \sum_{d|\frac{\phi(n)}{r_i}} \frac{\mu(d)}{d} \left( \frac{1}{n^{m-1}} \sum_{\chi^{r_i d}=\chi_0} B_{m,\chi} \right).
\end{aligned}$$

By Lemma 2.1, it is enough to show that for each integer  $m \geq 1$ , we have

$$\frac{1}{|\mathcal{S}_n|} \sum_{k=1}^{|\mathcal{S}_n|} B_m \left( \frac{g_k}{n} \right) \rightarrow 0 \text{ as } n \rightarrow \infty.$$

Also, by Lemma 2.2 (1), for any character  $\chi$ , we know that  $L(1-m, \chi) = -\frac{B_{m,\chi}}{m}$ . Thus, we need to estimate the following

$$\frac{1}{|\mathcal{S}_n|} \sum_{k=1}^{|\mathcal{S}_n|} B_m \left( \frac{g_k}{n} \right) = \frac{1}{|\mathcal{S}_n|} \sum_{i=1}^{\ell} \frac{1}{r_i} \sum_{d|\frac{\phi(n)}{r_i}} \frac{\mu(d)}{d} \left( \frac{1}{n^{m-1}} \sum_{\chi^{r_i d}=\chi_0} (-m)L(1-m, \chi) \right).$$

Therefore, by Lemma 2.2 (2), we get

$$\begin{aligned}
\left| \frac{1}{|\mathcal{S}_n|} \sum_{k=1}^{|\mathcal{S}_n|} B_m \left( \frac{g_k}{n} \right) \right| &\leq \frac{1}{|\mathcal{S}_n|} \sum_{i=1}^{\ell} \frac{1}{r_i} \sum_{d|\frac{\phi(n)}{r_i}} \frac{|\mu(d)|}{d} \left( \frac{m}{n^{m-1}} \sum_{\chi^{r_i d}=\chi_0} |L(1-m, \chi)| \right) \\
&= \frac{m}{|\mathcal{S}_n| n^{m-1}} \sum_{i=1}^{\ell} \frac{1}{r_i} \sum_{d|\frac{\phi(n)}{r_i}} \frac{|\mu(d)|}{d} \left( \sum_{\chi^{r_i d}=\chi_0} |L(1-m, \chi)| \right) \\
&\leq \frac{C'(m)}{|\mathcal{S}_n| n^{m-1}} \sum_{i=1}^{\ell} \frac{1}{r_i} \sum_{d|\frac{\phi(n)}{r_i}} \frac{1}{d} \left( \sum_{\chi^{r_i d}=\chi_0} n^{m-\frac{1}{2}} \right) \\
&= \frac{C'(m)\sqrt{n}}{|\mathcal{S}_n|} \sum_{i=1}^{\ell} \frac{1}{r_i} \sum_{d|\frac{\phi(n)}{r_i}} \frac{1}{d} \left( \sum_{\chi^{r_i d}=\chi_0} 1 \right) \\
&\leq \frac{C'(m)\sqrt{n}}{|\mathcal{S}_n|} \sum_{i=1}^{\ell} \frac{1}{r_i} \sum_{d|\frac{\phi(n)}{r_i}} \frac{1}{d} (r_i d) = \frac{C'(m)\sqrt{n}}{|\mathcal{S}_n|} \sum_{i=1}^{\ell} \left( \sum_{d|\frac{\phi(n)}{r_i}} 1 \right) \\
&= \frac{C'(m)\sqrt{n}}{|\mathcal{S}_n|} \sum_{i=1}^{\ell} \sigma_0 \left( \frac{\phi(n)}{r_i} \right) \leq \frac{C'(m)\sqrt{n}}{|\mathcal{S}_n|} \ell \sigma_0(\phi(n)),
\end{aligned}$$



where  $\sigma_0(n)$  stands for the number of divisors of  $n$  and  $C'(m)$  is a positive constant depending only on  $m$ . By Lemma 2.3, for any given  $\epsilon > 0$ , we have  $\sigma_0(n) = O(n^\epsilon)$ . Also, since  $\phi(n) \leq n$ , we get,  $\sigma_0(\phi(n)) = O(\phi(n)^\epsilon) = O(n^\epsilon)$ .

Also, since  $r_1, r_2, \dots, r_l$  are the indices of elements of  $\mathcal{S}_n$  and each  $r_i$  divides  $\phi(n)$ , we have

$$l \leq \sigma_0(\phi(n)) = O(\phi(n)^\epsilon) = O(n^\epsilon).$$

Thus,

$$\left| \frac{1}{|\mathcal{S}_n|} \sum_{k=1}^{|\mathcal{S}_n|} B_m \left( \frac{g_k}{n} \right) \right| \leq \frac{C'(m)n^{\frac{1}{2}+2\epsilon}}{|\mathcal{S}_n|},$$

which holds for any  $\epsilon > 0$ . This proves the theorem. □

### 5. Proof of Corollary 1.3

Let  $H_p$  be the given subgroup of  $(\mathbb{Z}/p\mathbb{Z})^*$  of cardinality  $(p-1)/r$  and  $\mathcal{S}_p$  is the complement of  $H_p$ . Then,

$$|\mathcal{S}_p| = p - 1 - \frac{p-1}{r} \geq \frac{p-1}{2} \geq (p-1)^{\frac{1}{2}+\epsilon},$$

for all sufficiently large  $p$  and for any  $\epsilon$  with  $0 < \epsilon < \frac{1}{2}$ . Therefore, by Theorem 1.2, the assertion follows. □

### 6. Proof of Theorem 1.4

For any integer  $n \geq 2$ , we are given a subgroup  $H'_n$  of the group  $(\mathbb{Z}/n\mathbb{Z})^*$  and we take the elements of  $H'_n$  as integers  $m$  such that  $1 \leq m \leq n$  and  $(m, n) = 1$ . Also, it is given that for each integer  $n \geq 2$ , the element  $g_n \in (\mathbb{Z}/n\mathbb{Z})^*$ . Then consider the subset  $H_n = H'_n/n$  of  $[0, 1]$ .

We want to prove that the sets  $g_n H_n$  are set equidistributed mod 1. For each integer  $n \geq 2$ , we denote  $\widehat{H}_n$  the group of all Dirichlet characters of  $(\mathbb{Z}/n\mathbb{Z})^*$  which are trivial on the subgroup  $H'_n$ . Therefore, we have a canonical isomorphism

$$\widehat{H}_n \cong (\mathbb{Z}/n\mathbb{Z})^*/H'_n$$

and so,

$$|\widehat{H}_n| = \frac{\phi(n)}{|H'_n|} = \frac{\phi(n)}{|g_n H_n|}.$$

Then, we see that

$$\frac{1}{|\widehat{H}_n|} \sum_{\chi \in \widehat{H}_n} \chi(a)\chi(g_n^{-1}) = \begin{cases} 1 & \text{if } a \in g_n H_n \\ 0 & \text{otherwise.} \end{cases}$$

By letting  $H'_n = \{a_1, \dots, a_{|H_n|}\}$ , for each integer  $m \geq 1$ , we see that

$$\begin{aligned} \sum_{k=1}^{|H_n|} B_m \left( \frac{a_k g_n}{n} \right) &= \frac{1}{|\widehat{H}_n|} \sum_{k=1}^n B_m \left( \frac{k}{n} \right) \sum_{\chi \in \widehat{H}_n} \chi(k) \chi(g_n^{-1}) \\ &= \frac{1}{|\widehat{H}_n|} \sum_{k=1}^n B_m \left( \frac{k}{n} \right) \sum_{\chi \in \widehat{H}_n} \chi(k g_n^{-1}) \\ &= \frac{1}{|\widehat{H}_n|} \sum_{\chi \in \widehat{H}_n} \chi(g_n^{-1}) \left( \sum_{k=1}^n B_m \left( \frac{k}{n} \right) \chi(k) \right) \\ &= \frac{1}{n^{m-1} |\widehat{H}_n|} \sum_{\chi \in \widehat{H}_n} \chi(g_n^{-1}) B_{m, \chi}. \end{aligned}$$

By Lemma 2.1, it is enough to show that for each  $m \geq 1$

$$\frac{1}{|g_n H_n|} \sum_{k=1}^{|g_n H_n|} B_m \left( \frac{a_k g_n}{n} \right) \rightarrow 0 \text{ as } n \rightarrow \infty.$$

Since  $|g_n H_n| = |H_n|$ , the rest of the proof goes along the proof of subgroup  $H_n$  proved in [MuTh10]. Hence, we omit the proof here.  $\square$

**Acknowledgements:** We would like to acknowledge the Department of Atomic Energy, Govt. of India and Harish-Chandra Research Institute for providing the excellent financial support and many facilities to carry out this research. This work was completed when the third author was visiting the Department of Mathematics, University of Toronto for which he is grateful to Professor V. Kumar Murty. We are thankful to the referee for going through the earlier draft very carefully and suggesting many useful comments to make the article more readable.

## References

- [Apo76] T. M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976.
- [Jo73] J. Johnsen, On the distribution of powers in finite fields, *J. Reine Angew. Math.* **253** (1973), 10-19.
- [Mu08] M. Ram Murty, *Problems in Analytic Number Theory*, Second edition, Graduate Texts in Mathematics, **206**, Springer-Verlag, New York, 2008.
- [MuSi09] M. Ram Murty and K. Sinha, Effective equidistribution of eigenvalues of Hecke operators, *J. Number Theory* **129** (2009), 681-714.
- [MuTh10] M. Ram Murty and R. Thangadurai, The class number of  $\mathbb{Q}(\sqrt{-p})$  and digits of  $1/p$ , *Proc. Amer. Math. Soc.* **139** (2010), 1277-1289.
- [Wa97] L. Washington, *Introduction to cyclotomic fields*, Second edition, Graduate Texts in Mathematics, **83**, Springer-Verlag, New York, 1997, 487pp.

**J. Chattopadhyay, V. Kumar and R. Thangadurai**

Harish-Chandra Research Institute, HBNI

Chhatnag Road, Jhansi

Allahabad - 211019, INDIA

*e-mail:* jaitrachattopadhyay@hri.res.in

*e-mail:* veekeshkumar@hri.res.in

*e-mail:* thanga@hri.res.in