PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 139, Number 4, April 2011, Pages 1277–1289
S 0002-9939(2010)10560-9
Article electronically published on August 30, 2010

THE CLASS NUMBER OF $\mathbb{Q}(\sqrt{-p})$ AND DIGITS OF $1/p$

M. RAM MURTY AND R. THANGADURAI

(Communicated by Wen-Ching Winnie Li)

Abstract. Let p be a prime number such that $p \equiv 1 \pmod r$ for some integer $r > 1$. Let $g > 1$ be an integer such that g has order r in $(\mathbb{Z}/p\mathbb{Z})^*$. Let

$$\frac{1}{p} = \sum_{k=1}^{\infty} \frac{x_k}{g^k}$$

be the g-adic expansion. Our result implies that the "average" digit in the g-adic expansion of $1/p$ is $(g-1)/2$ with error term involving the generalized Bernoulli numbers $B_{1,\chi}$ (where χ is a character modulo p of order r with $\chi(-1) = -1$). Also, we study, using Bernoulli polynomials and Dirichlet L-functions, the set equidistribution modulo 1 of the elements of the subgroup H_n of $(\mathbb{Z}/n\mathbb{Z})^*$ as $n \to \infty$ whenever $|H_n|/\sqrt{n} \to \infty$.

1. Introduction

Let p be a prime number and g a natural number satisfying $1 < g < p$. Suppose that g is a primitive root (mod p). In 1994, K. Girstmair [2] [3] wrote two papers connecting the digits of the g-adic expansion of $1/p$ with the class number of $\mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \pmod 4$ and $p \geq 7$. More precisely, let

$$\frac{1}{p} = \sum_{k=1}^{\infty} \frac{x_k}{g^k},$$

with $0 \leq x_k \leq g-1$, be the g-adic expansion of $1/p$. Then, Girstmair proved that

$$(x_2 + x_4 + \cdots + x_{p-1}) - (x_1 + x_3 + \cdots + x_{p-2}) = (g+1)h$$

where h is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. In this paper, we will obtain various generalizations of this formula. In particular, we will study what kind of formulas can be derived if g is not necessarily a primitive root (mod p) but has order r (say) mod p. Thus, $p \equiv 1 \pmod r$. In this context, it is easily seen that $1/p$ has a periodic g-adic expansion with period r.

Here is an example of the type of results we derive. Let $p \equiv 11 \pmod{12}$ be a prime number and suppose that 3 has order $(p-1)/2$ in $(\mathbb{Z}/p\mathbb{Z})^*$. Then we will see

Received by the editors January 18, 2010 and, in revised form, April 26, 2010.
2010 *Mathematics Subject Classification.* Primary 11A07, 11R29.
Key words and phrases. Digits, Bernoulli polynomials, Dirichlet L-functions, equidistribution modulo 1.

that the class number $h(\mathbb{Q}(\sqrt{-p}))$ can be given by the following formula

$$h(\mathbb{Q}(\sqrt{-p})) = \frac{p-1}{2} - \sum_{i=1}^{(p-1)/2} x_i$$

where x_k is defined to be the digits $\frac{1}{p} = \sum_{k=1}^{\infty} \frac{x_k}{3^k}$. One can re-write this as

$$h(\mathbb{Q}(\sqrt{-p})) = \sum_{i=1}^{(p-1)/2} (1 - x_i).$$

In particular, the sum on the right is strictly positive, indicating that there are more 0's than 2's in the ternary expansion of $1/p$. The difference is measured by the class number. From this formula, we also see that the complexity of computing $h(\mathbb{Q}(\sqrt{-p}))$ is equivalent to the complexity of computing the digits up to $(p-1)/2$ terms of $1/p$ in base 3. In this article, we will see this fact in some generality. Our first theorem is:

Theorem 1. *Let p be a prime and $r|(p-1)$. Suppose that a character χ of order r is odd and that g has order $(p-1)/r \pmod p$. Let*

$$\frac{1}{p} = \sum_{k=1}^{\infty} \frac{x_k}{g^k}$$

be the g-adic expansion of $1/p$. Then,

$$\sum_{i=1}^{(p-1)/r} x_i = \frac{g-1}{2}\left(\frac{p-1}{r}\right) + \frac{g-1}{r} \sum_{\chi^r=1,\, \chi\,\mathrm{odd}} B_{1,\chi}$$

where $B_{1,\chi}$ is the generalized Bernoulli number.

The sum on the left hand side of the equation in Theorem 1 can be viewed as the trace of $B_{1,\chi}$ for a fixed character χ of order r. Let us also note that if one character χ of order r is odd, then all characters of order r are odd since they are of the form χ^s with $(s, p-1) = 1$ and s is necessarily odd.

Corollary 1. *If $g = 3$ has order $(p-1)/r$ mod p, then*

$$-\sum_{\chi^r=1,\chi\,\mathrm{odd}} B_{1,\chi} = \frac{r}{2} \sum_{i=1}^{(p-1)/r} (1 - x_i).$$

Corollary 2. *Let $p \equiv 3 \pmod 4$ be a prime number and g be an integer such that $(g,p) = 1$ and whose order in $(\mathbb{Z}/p\mathbb{Z})^*$ is $(p-1)/2$. Then we have*

$$\left(\frac{g-1}{2}\right)\left(\frac{p-1}{2} - h\right) = \sum_{i=1}^{(p-1)/2} x_i$$

where x_i's are the digits in the g-adic expansion of $1/p$.

Corollary 2 also appears as Satz 11 in [4]. These results suggest the natural question of how reduced residue classes of subgroups of the group of coprime residue classes (mod n) are distributed. Using the theory of generalized Bernoulli polynomials, we can show they are "equidistributed" in the interval $[1, n]$, provided that the size of the subgroup is sufficiently large. To be precise, we will say, following [7], that a sequence of finite multisets A_n with $|A_n| \to \infty$ is set equidistributed mod 1 with respect to a probability measure μ if for every continuous function f on $[0,1]$, we have

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

In order to verify this condition, it suffices to check that these limits exist on a dense family of functions f in $C[0,1]$. In our context, we will use Bernoulli polynomials to establish the equidistribution result.

Theorem 2. *Let H_n be a subgroup of the coprime residue classes mod n. Take representatives $h \in H$ with $1 \leq h < n$ and consider the set $\{h/n : h \in H_n\}$ contained in $[0,1]$. If $|H_n|/n^{1/2}$ tends to infinity as n tends to infinity, then the H_n's are set equidistributed in $[0,1]$ with respect to the Lebesgue measure.*

The methods used to prove this theorem are classical. The results can be substantially improved if we invoke recent results of Bourgain [1]. We have:

Theorem 3. *The result in Theorem 2 holds provided that $|H_n| > n^{\epsilon}$ for some $\epsilon > 0$.*

Corollary 3. *Let H_n be a subgroup of the coprime residue classes mod n and $\widehat{H_n}$ be the dual of $(\mathbb{Z}/n\mathbb{Z})^*/H_n$. If*

$$\sum_{\chi\in\widehat{H_n}} L(1-m,\chi) = O\left(n^{m-1}(\log n)^c|\widehat{H_n}|\right)$$

holds true for some constant $c > 0$, then as $n \to \infty$, all subgroups H_n such that $|H_n|/(\log n)^c \to \infty$ are set equidistributed modulo 1.

In the final section of our paper, we discuss the general problem of the distribution of digits of $1/p$. This entails the derivation of explicit formulas for the moment sums of the digits and leads to several interesting questions.

2. Preliminary lemmas

We begin with the following lemma, essentially contained in [2].

Lemma 1. *Let $g > 1$ be any integer such that $(g,p) = 1$. For any non-negative integer k, we define g_k to be the least positive integer t such that $t \equiv g^k \pmod{p}$. If $\frac{1}{p} = \sum_{k=1}^{\infty} \frac{x_k}{g^k}$, where $0 \leq x_k \leq g-1$, and $y_k = \frac{gg_{k-1} - g_k}{p}$ for all integers $k \geq 1$, then*

$$y_k = x_k \text{ for all } k.$$

Proof. Consider

$$\begin{aligned}\sum_{k=1}^{\infty}\frac{y_k}{g^k} &= \frac{1}{p}\left[\sum_{k=1}^{\infty}\frac{gg_{k-1}}{g^k}-\sum_{k=1}^{\infty}\frac{g_k}{g^k}\right]\\ &= \frac{1}{p}\left[\sum_{k=1}^{\infty}\frac{g_{k-1}}{g^{k-1}}-\sum_{k=1}^{\infty}\frac{g_k}{g^k}\right]\\ &= \frac{g_0}{p}=\frac{1}{p}=\sum_{k=1}^{\infty}\frac{x_k}{g^k}.\end{aligned}$$

One may notice that $y_k \geq 0$ for every k. Thus the lemma follows from the uniqueness of the g-ary representation. □

For all primes $11 \leq p \equiv 3 \pmod 4$, we have by Dirichlet's class number formula (see, for example, [2]), that the class number of $\mathbb{Q}(\sqrt{-p})$ is given by

$$h := h(\mathbb{Q}(\sqrt{-p})) = -\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\frac{k}{p}. \tag{2}$$

We shall use this information later in the proof.

3. Proof of Theorem 1

Let $r > 2$ be any integer. Let $p \equiv 1 \pmod r$ be any prime. Suppose $g \geq 2$ is any integer such that $(g,p)=1$ and order of g in $(\mathbb{Z}/p\mathbb{Z})^*$ is $(p-1)/r$. Let χ be a Dirichlet character modulo p of order r such that $\chi(-1)=-1$. Then the generalized Bernoulli number $B_{1,\chi}$ is defined as

$$B_{1,\chi} = \frac{1}{p}\sum_{k=1}^{p-1}\chi(k)k. \tag{3}$$

Since $B_{1,\chi}$ is a non-zero multiple of $L(1,\chi)$ (see p. 38 of [8]), we see that it is non-zero if χ is odd. If $\chi(-1)=1$ and χ is non-trivial, then the sum in (3) is zero, as is easily seen by pairing k and $p-k$ in the sum.

If χ is an even Dirichlet character mod p, of order r, then, on the one hand, the sum

$$\frac{1}{r}\sum_{k=1}^{p-1}(\chi(k)+\chi^2(k)+\cdots+\chi^r(k))\frac{k}{p} = \frac{p-1}{2r},$$

since all the characters in the sum are even and the resulting sum over k is zero for all non-trivial characters and the contribution from the trivial character is $(p-1)/2r$. On the other hand, the sum is

$$\sum_{k\equiv u^r \pmod p}\frac{k}{p} = \sum_{k=1}^{(p-1)/r}\frac{g_k}{p},$$

since the group generated by g has order $(p-1)/r$ and consists of the r-th powers (mod p). Thus, by an easy calculation,

$$(g-1)\left(\frac{p-1}{2r}\right) = \sum_{k=1}^{(p-1)/r}\frac{gg_{k-1}-g_k}{p},$$

which by Lemma 1 gives that the sum of the first $(p-1)/r$ digits of $1/p$ in its g-adic expansion is $(g-1)(p-1)/2r$. Hence, in this situation, there is nothing interesting happening. One can interpret this result as saying that the "average" digit in the g-adic expansion of $1/p$ is $(g-1)/2$. If χ is an odd character, this average result has to be modified by an "error" term involving generalized Bernoulli numbers, which in the quadratic character case reduces to a class number.

Now we prove Theorem 1.

Proof of Theorem 1. Let χ be a Dirichlet character modulo p of order r with $\chi(-1)=-1$. Consider

$$\begin{aligned} S &= \frac{1}{r}\sum_{k=1}^{p-1}(\chi(k)+\chi^2(k)+\cdots+\chi^r(k))\frac{k}{p} \\ &= \sum_{k\equiv u^r \pmod p}\frac{k}{p} \\ &= \sum_{k=1}^{(p-1)/r}\frac{g_k}{p} \qquad (4) \end{aligned}$$

as

$$\frac{1}{r}\sum_{i=1}^{r}\chi^i(k) = \begin{cases} 1 & \text{if } k=u^r \text{ for some } u\in(\mathbb{Z}/p\mathbb{Z})^* \\ 0 & \text{otherwise} \end{cases}$$

and $g_k \equiv g^k \pmod p$ for every $k\geq 0$. We compute $2S$ as follows:

$$\begin{aligned} 2S &= \frac{1}{r}\sum_{k=1}^{p-1}(\chi(k)+\cdots+\chi^r(k))\frac{k}{p} + \frac{1}{r}\sum_{k=1}^{p-1}(\chi(-k)+\cdots+\chi^r(-k))\frac{p-k}{p} \\ &= \frac{1}{r}\sum_{k=1}^{p-1}\left(\sum_{i=1}^{r}\left[\chi^i(k)\frac{k}{p}+\chi^i(-k)\frac{p-k}{p}\right]\right) \\ &= \frac{1}{r}\sum_{k=1}^{p-1}\left(\sum_{i\,\text{odd}}+\sum_{i\,\text{even}}\right). \end{aligned}$$

When i is odd, $\chi^i(-k)=-\chi^i(k)$ as $\chi(-1)=-1$. Therefore,

$$\chi^i(k)\frac{k}{p}+\chi^i(-k)\frac{p-k}{p} = \begin{cases} 2\chi^i(k)\dfrac{k}{p}-\chi^i(k) & \text{if } i \text{ is odd} \\ \chi^i(k) & \text{if } i \text{ is even.} \end{cases}$$

Therefore,

$$\begin{aligned} 2S &= \frac{1}{r}\sum_{k=1}^{p-1}\left(\sum_{i\,\text{odd}}\left(2\chi^i(k)\frac{k}{p}-\chi^i(k)\right)+\sum_{i\,\text{even}}\chi^i(k)\right) \\ &= \frac{2}{r}\sum_{i\,\text{odd}}\frac{1}{p}\sum_{k=1}^{p-1}\chi^i(k)k + \sum_{k=1}^{p-1}\frac{1}{r}\sum_{i=1}^{r}\chi^i(-k) \\ &= \frac{2}{r}\sum_{i\,\text{odd}}B_{1,\chi^i}+\frac{p-1}{r}, \end{aligned}$$

by (3) and the contribution from the trivial character. Now, by (4), we have

$$\begin{aligned}(g-1)S = gS - S &= \sum_{k=1}^{(p-1)/r} \frac{gg_k}{p} - \sum_{k=1}^{(p-1)/r} \frac{g_k}{p} \\ &= \sum_{k=2}^{(p-1)/r+1} \frac{gg_{k-1}-g_k}{p} - \frac{g_1}{p} + \frac{gg_{(p-1)/r}}{p} \\ &= \sum_{k=1}^{(p-1)/r} \frac{gg_{k-1}-g_k}{p} \\ &= \sum_{k=1}^{(p-1)/r} x_k, \qquad (5)\end{aligned}$$

by Lemma 1. On the other hand, by $2S$, we can compute $(g-1)S$ as

$$(g-1)S = \frac{g-1}{r}\sum_{i\,\mathrm{odd}} B_{1,\chi^i} + \frac{g-1}{2}\left(\frac{p-1}{2}\right). \qquad (6)$$

From (5) and (6), Theorem 1 follows. □

Proof of Corollary 1. By putting $g = 3$ in Theorem 1, we get the corollary. □

Proof of Corollary 2. By putting $r = 2$ in Theorem 1, we see that g is an element of order $(p-1)/2$ and hence χ is a quadratic character mod p. Therefore,

$$\chi(a) = \left(\frac{a}{p}\right),$$

the Legendre symbol. Since χ is odd, we see that

$$\left(\frac{-1}{p}\right) = -1 = (-1)^{(p-1)/2} \implies p \equiv 3 \pmod 4.$$

Therefore, by Theorem 1, we get

$$\sum_{i=1}^{(p-1)/2} x_i = \left(\frac{g-1}{2}\right)\left(\frac{p-1}{2} + B_{1,\chi}\right)$$

where

$$B_{1,\chi} = \frac{1}{p}\sum_{k=1}^{p-1}\chi(k)k = \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\frac{k}{p} = -h(\sqrt{-p}),$$

by (1). Therefore, we arrive at

$$\sum_{i=1}^{(p-1)/2} x_i = \left(\frac{g-1}{2}\right)\left(\frac{p-1}{2} - h\right).$$

This complete the proof of Corollary 2. □

Now let $p \equiv 11 \pmod{12}$ be a prime. Then, 3 is a quadratic residue modulo p. For

$$\left(\frac{3}{p}\right) \equiv (-1)^{(p-1)/2}\left(\frac{p}{3}\right) = (-1)(-1) = +1,$$

as $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$. If the order of 3 is $(p-1)/2$, then Theorem 1 implies that

$$\frac{p-1}{2} - h = \sum_{i=1}^{(p-1)/2} x_i$$

where x_i's are ternary digits in $1/p$. Thus, we get the example stated in the introduction.

4. Equidistribution of residue classes of subgroups

There are two questions that emerge from the above investigation. The first concerns the distribution of the reduced residue classes (mod p) of the elements of any subgroup of the coprime residue classes. The second is whether interesting formulas can be derived for the sums of the squares or higher powers of the digits x_i studied in Theorem 1. We will address both these questions below.

The first question can be studied in a general context. We can consider the coprime residue classes mod n and look at the distribution of the reduced residue classes of any subgroup. We begin with an arbitrary subgroup H_n of $(\mathbb{Z}/n\mathbb{Z})^*$ and suppose that we have $1 = g_1 < g_2 < \cdots < g_{|H_n|} < n$ with the g_i's being the coset representatives of H_n. A natural question is: how are the numbers g_k, $1 \le k \le |H_n|$, distributed?

For any such question it suffices to determine the behaviour of sums of the form

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

for any suitable family of polynomials f_m with degree m, $m = 1, 2, \ldots$. To this end, it is convenient to take the Bernoulli polynomials and consider the sum

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

where

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

where B_k are the Bernoulli numbers. Thus,

$$B_1(X) = X - \frac{1}{2}, \quad B_2(X) = X^2 - X + \frac{1}{6},$$

etc. Using Bernoulli polynomials, we define for any Dirichlet character χ, the generalized Bernoulli numbers, $B_{m,\chi}$, as follows:

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

Proof of Theorem 2. Let $n > e^{16}$ be an integer. For any subgroup H_n of coprime residue classes modulo n, we denote by $\widehat{H_n}$ the group of Dirichlet characters of $(\mathbb{Z}/n\mathbb{Z})^*$ trivial on H_n. Therefore, we have a canonical isomorphism

$$\widehat{H_n} \cong (\mathbb{Z}/n\mathbb{Z})^*/H_n$$

and so

$$|\widehat{H_n}| = \frac{\phi(n)}{|H_n|}.$$

Also,

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

Therefore, for each $m \geq 1$,

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

Since $\displaystyle\int_0^1 B_m(x)dx = 0$ for every $m \geq 1$ (for instance, see [6], p. 19), by (1), it is enough to show that for each $m \geq 1$

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

Thus, we need to estimate the following:

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

For any character χ of conductor $f|n$, we know that

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

Note that if χ is induced from a primitive character χ^* with conductor f which divides n, then

$$\chi(a) = \begin{cases} \chi^*(a) & \text{if } (a,f) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

In this case, we have

$$L(1-m,\chi) = L(1-m,\chi^*) \prod_{p|(n/f),(p,f)=1} \left(1 - \chi(p)p^{m-1}\right).$$

Also, using the functional equation of $L(1-m,\chi^*)$, we have

$$|L(1-m,\chi^*)| \leq \frac{c_1 m!}{(2\pi)^m} f^{m-\frac{1}{2}}$$

(for instance, see p. 122 of [6]). Using this, we estimate $|L(1-m,\chi)|$ as follows.

Case (*i*) ($m \geq 3$). In this case,

$$\begin{aligned}\left|\prod_{p|(n/f),(p,f)=1}(1-\chi(p)p^{m-1})\right| &= \prod_{p|(n/f),(p,f)=1}\left|p^{m-1}-\overline{\chi(p)}\right| \\ &= \prod_{p|(n/f),(p,f)=1} p^{m-1}\left|1-\frac{\overline{\chi(p)}}{p^{m-1}}\right| \\ &\leq \prod_{p|(n/f),(p,f)=1} p^{m-1}\prod_{p}\left(1+\frac{1}{p^{m-1}}\right) \\ &\leq c_2(n/f)^{m-1},\end{aligned}$$

where c_2 is an absolute constant. Therefore,

$$\begin{aligned}|L(1-m,\chi)| &\leq \frac{c_3 m!}{(2\pi)^m} f^{m-\frac{1}{2}}(n/f)^{m-1} = \frac{c_3 m!}{(2\pi)^m}\sqrt{f}n^{m-1} \\ &\leq c(m)n^{m-\frac{1}{2}},\end{aligned}$$

where $c(m)$ is an absolute constant which depends only on m.

Case (*ii*) ($m = 2$). In this case,

$$\begin{aligned}\left|\prod_{p|(n/f),(p,f)=1}(1-\chi(p)p)\right| &\leq \prod_{p|(n/f)} p \prod_{p|(n/f)}\left(1+\frac{1}{p}\right) \\ &\leq \frac{n}{f}\frac{\sigma(n/f)}{n/f} = \sigma(n/f)\end{aligned}$$

where $\sigma(n) = \sum_{d|n} d$. Therefore,

$$\begin{aligned}|L(-1,\chi)| &\leq \frac{2c_1}{(2\pi)^2} f^{3/2}\sigma(n/f) \\ &= \frac{2c_1}{(2\pi)^2} n^{3/2}\frac{\sigma(n/f)}{(n/f)^{3/2}} \\ &\leq \frac{2c_1}{(2\pi)^2} n^{3/2}\frac{(2.59)(n/f)\log\log(n/f)}{(n/f)^{3/2}} \\ &\leq C(2)n^{3/2} \text{ for all } n \geq e^e,\end{aligned}$$

where $C(2)$ is an absolute constant and in the above we have used the estimate

$$\sigma(n) \leq 2.59n\log\log n \text{ for all } n \geq 7,$$

a result of A. Ivic [5].

Case (*iii*) ($m = 1$). In this case, we have

$$\left|\prod_{p|(n/f),(p,f)=1}(1-\chi(p))\right| \leq \prod_{p|(n/f),(p,f)=1} 2 \leq 2^{\omega(n/f)},$$

where $\omega(n)$ denotes the number of distinct prime factors of n. Therefore,

$$|L(0,\chi)| \leq \frac{c_1}{2\pi}\sqrt{f}2^{\omega(n/f)} = \frac{c_1}{2\pi}\sqrt{n}\frac{2^{\omega(n/f)}}{\sqrt{n/f}}.$$

Note that since $\omega(n) \leq 2\log n/\log\log n$ for all $n \geq 13$, we have

$$2^{\omega(n/f)} \leq 2^{2\log(n/f)/\log\log(n/f)} = (n/f)^{\log 4/\log\log(n/f)}.$$

Therefore,

$$2^{\omega(n/f)} \leq \sqrt{n/f} \text{ for all } n/f > e^{16}.$$

Hence, we get

$$|L(0,\chi)| \leq C(1)\sqrt{n}$$

for all $n > e^{16}$ and $C(1)$ is an absolute constant.

Thus, in all the cases, if χ is a character modulo n, then we have

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

for all $n > e^{16}$ where $C(m)$ is an absolute constant that depends only on m.

Now,

$$\begin{aligned}
\left|\frac{1}{|H_n|}\sum_{k=1}^{|H_n|} B_m\left(\frac{g_k}{n}\right)\right| &\leq \frac{1}{\phi(n)n^{m-1}}\sum_{\chi\in\widehat{H_n}} |B_{m,\chi}| \\
&\leq \frac{1}{\phi(n)n^{m-1}}\sum_{\chi\in\widehat{H_n}} |L(1-m,\chi)| \\
&\leq \frac{|\widehat{H_n}|}{\phi(n)n^{m-1}} C(m)n^{m-\frac{1}{2}} \text{ for all } n > e^{16} \\
&\leq C(m)\frac{\sqrt{n}}{|H_n|} \text{ for all } n > e^{16}.
\end{aligned}$$

Thus the theorem follows. □

Proof of Theorem 3. Let $\epsilon > 0$ be given. Let H be a subgroup of coprime residue classes modulo n such that $|H| > n^\epsilon$. Then the result of Bourgain [1] states that *there is a* $\delta(\epsilon) > 0$ *such that for* $|H| > n^\epsilon$, *we have*

$$\frac{1}{|H|}\max_{(a,n)=1}\left|\sum_{x\in H} e^{2\pi iax/n}\right| < \frac{1}{n^\delta}.$$

Therefore, by Weyl's equidistribution criterion, we get the result. □

Proof of Corollary 3. From the proof of Theorem 2, we see that

$$\begin{aligned}
\left|\frac{1}{|H_n|}\sum_{k=1}^{|H_n|} B_m\left(\frac{g_k}{n}\right)\right| &= \frac{1}{\phi(n)n^{m-1}}\left|\sum_{\chi\in\widehat{H_n}} B_{m,\chi}\right| \\
&= \frac{1}{\phi(n)n^{m-1}}\left|\sum_{\chi\in\widehat{H_n}} L(1-m,\chi)\right| \\
&\leq \frac{1}{\phi(n)n^{m-1}} C_1 n^{m-1}(\log n)^c|\widehat{H_n}| \\
&\qquad \text{by the assumption} \\
&\leq C_1\frac{(\log n)^c}{|H_n|} \to 0
\end{aligned}$$

when $n \to \infty$ as $|H_n|/(\log n)^c \to \infty$. □

5. Concluding remarks

Now we deal with the distribution of the digits x_i where $1/p = 0.x_1x_2\dots x_n\cdots$. This is more difficult, but can be done inductively. We already saw

$$\sum_{i=1}^{(p-1)/r} x_i.$$

Now we will consider $\sum_{i=1}^{(p-1)/r} x_i^2$. By our formula, we see that

$$\begin{aligned}\sum_{i=1}^{(p-1)/r} x_i^2 &= \sum_{i=1}^{(p-1)/r} \left(\frac{gg_{i-1}-g_i}{p}\right)^2 \\ &= \sum_{i=1}^{(p-1)/r} \frac{g^2g_{i-1}^2}{p^2} + \sum_{i=1}^{(p-1)/r} \frac{g_i^2}{p^2} - 2\sum_{i=1}^{(p-1)/r} \frac{gg_ig_{i-1}}{p^2} \\ &= (g^2+1)\sum_{i=1}^{(p-1)/r} \frac{g_i^2}{p^2} - 2\sum_{i=1}^{(p-1)/r} \frac{gg_ig_{i-1}}{p^2}, \end{aligned} \tag{7}$$

$g_0 = g_{(p-1)/r} \equiv 1 \pmod p$. To calculate the other sum, we first observe that

$$gg_{i-1} \equiv g_i \pmod p$$

so that

$$\left\{\frac{gg_{i-1}}{p}\right\} = \frac{g_i}{p}$$

where $\{x\}$ denotes the fractional part of x. Therefore, the sum

$$\begin{aligned} 2\sum_{i=1}^{(p-1)/r} \frac{gg_ig_{i-1}}{p^2} &= 2\sum_{i=1}^{(p-1)/r} \frac{gg_{i-1}}{p}\left\{\frac{gg_{i-1}}{p}\right\} \\ &= 2\sum_{i=1}^{(p-1)/r} \frac{g^2g_{i-1}^2}{p^2} - 2\sum_{i=1}^{(p-1)/r} \frac{gg_{i-1}}{p}\left[\frac{gg_{i-1}}{p}\right]. \end{aligned}$$

Therefore, (7) becomes

$$\sum_{i=1}^{(p-1)/r} x_i^2 = (1-g^2)\sum_{i=1}^{(p-1)/r} \frac{g_i^2}{p^2} + 2\sum_{i=1}^{(p-1)/r} \frac{gg_{i-1}}{p}\left[\frac{gg_{i-1}}{p}\right]. \tag{8}$$

Consider

$$\begin{aligned}(1-g^2)\sum_{i=1}^{(p-1)/r} \frac{g_i^2}{p^2} &= \frac{1-g^2}{r}\sum_{k=1}^{p-1}(\chi(k)+\chi^2(k)+\cdots+\chi^r(k))\frac{k^2}{p^2} \\ &= \frac{1-g^2}{r}\sum_{i=1}^{r}\sum_{k=1}^{p-1}\chi^i(k)\frac{k^2}{p^2}, \end{aligned} \tag{9}$$

where χ is a character of order r. Since $B_2(X) = X^2 - X + 1/6$, we see that for any non-trivial Dirichlet character ψ modulo p,

$$B_{2,\psi} = p\sum_{k=1}^{p-1}\psi(k)\frac{k^2}{p^2} - p\sum_{k=1}^{p-1}\psi(k)\frac{k}{p} + \frac{p}{6}\sum_{k=1}^{p-1}\psi(k) = p\sum_{k=1}^{p-1}\psi(k)\frac{k^2}{p^2} - p\sum_{k=1}^{p-1}\psi(k)\frac{k}{p}.$$

Therefore,

$$\sum_{k=1}^{p-1}\psi(k)\frac{k^2}{p^2}=\frac{1}{p}\left(B_{2,\psi}+B_{1,\psi}\right). \tag{10}$$

By (9) and (10), we get

$$(1-g^2)\sum_{i=1}^{(p-1)/r}\frac{g_i^2}{p^2}=\frac{1-g^2}{pr}\sum_{i=1}^{r}\left(B_{2,\chi^i}+B_{1,\chi^i}\right). \tag{11}$$

Hence, by (8) and (11), we get

$$\begin{aligned}\sum_{i=1}^{(p-1)/r}x_i^2&=\frac{1-g^2}{pr}\sum_{i=1}^{r}\left(B_{2,\chi^i}+B_{1,\chi^i}\right)+2\sum_{i=1}^{(p-1)/r}\frac{gg_{i-1}}{p}\left[\frac{gg_{i-1}}{p}\right]\\&=\frac{1-g^2}{pr}\sum_{i=1}^{r}\left(B_{2,\chi^i}+B_{1,\chi^i}\right)+\frac{2g}{r}\sum_{i=1}^{r}\sum_{k=1}^{p-1}\chi^i(k)\frac{k}{p}\left[\frac{gk}{p}\right].\end{aligned}$$

It is thus clear that sums of the form

$$\sum_{k=1}^{p-1}\chi(k)\frac{k}{p}\left[\frac{gk}{p}\right]$$

enter into the evaluation. Such sums appear in the congruences of Voronoi, extending the celebrated Kummer congruences. For sums of higher powers of the x_i's, similar sums of the form

$$\sum_{k=1}^{p-1}\chi(k)\left(\frac{k}{p}\right)^i\left[\frac{gk}{p}\right]^j$$

appear.

Acknowledgements

The authors would like to thank Kurt Girstmair, Michael Rosen and the referee for their comments on an earlier version of this paper.

References

[1] J. Bourgain, Exponential sum estimates over subgroups of $\mathbb{Z}_q^*$, q arbitrary, *J. Analyse Math.*, **97** (2005), 317-355. MR2274981 (2007j:11103)

[2] K. Girstmair, A "popular" class number formula, *American Math. Monthly,* **101** (1994), no. 10, 997-1001. MR1304325 (95k:11003)

[3] K. Girstmair, The digits of $1/p$ in connection with class number factors, *Acta Arith.,* **67** (1994), no. 4, 381-386. MR1301825 (96g:11134)

[4] K. Girstmair, Periodische Dezimalbrüche - was nicht jeder darüber weiss, Jahrbruch Überblicke Mathematik, 1995, 163-179, Vieweg, Braunschweig, 1995. MR1342348 (96f:11012)

[5] A. Ivić, Two inequalities for the sum of divisors functions, *Univ. u Novom Sadu Zb. Rad. Prirod.-Mat. Fak.*, **7** (1977), 17–22. MR0505991 (58:21911)

[6] M. Ram Murty, Problems in Analytic Number Theory, Graduate Texts in Mathematics, Springer, New York, 2008, 2nd edition. MR2376618 (2008j:11001)

[7] M. Ram Murty and Kaneenika Sinha, Effective equidistribution of eigenvalues of Hecke operators, *Journal of Number Theory,* **129** (2009), 681-714. MR2488597

[8] L. Washington, Introduction to cyclotomic fields, second edition, Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1997. MR1421575 (97h:11130)

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, K7L 3N6, Canada

E-mail address: murty@mast.queensu.ca

Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahbad, 211019, India

E-mail address: thanga@hri.res.in