

Multiplicative Character Sums with the Sum of g -ary Digits Function

WILLIAM D. BANKS *

Department of Mathematics, University of Missouri
Columbia, MO 65211 USA
bbanks@math.missouri.edu

IGOR E. SHPARLINSKI

Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

*Corresponding author

Abstract

We establish upper bounds for multiplicative character sums with the function $\sigma_g(n)$ which computes the sum of the digits of n in a fixed base $g \geq 2$. Our results may be viewed as analogues of some previously known results for exponential sums with sum of g -ary digits function.

MSC Numbers: 11L40, 11A63.

Keywords: Estimate for multiplicative character sums, g -ary digits.

Corresponding Author:

William D. Banks
Department of Mathematics
University of Missouri
201 Mathematical Sciences Bldg.
Columbia, MO 65211 USA
Phone: 1-573-882-4305
Fax: 1-573-882-1869
email: bbanks@math.missouri.edu

1 Introduction

Arithmetic properties of integers characterized by their digits in various bases have been studied in many papers; for instance, see [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 14, 15] and the references therein. In this paper, we consider the problem of obtaining nontrivial bounds for multiplicative character sums with the sum of g -ary digits function $\sigma_g(n)$. Previously, results of this kind have been obtained only for exponential sums (that is, for additive character sums), and although both problems are somewhat related, the estimation of multiplicative character sums requires the use of a very different set of techniques.

Let $g \geq 2$ be a fixed integer base. We consider the base g representation of any arbitrary nonnegative integer n :

$$n = \sum_{j \geq 0} a_j(n)g^j, \quad 0 \leq a_j(n) \leq g - 1,$$

and we denote by $\sigma_g(n)$ the sum of the base- g digits of n ; that is,

$$\sigma_g(n) = \sum_{j \geq 0} a_j(n).$$

In this paper, we obtain nontrivial upper bounds for the character sums

$$\mathcal{S}(r, \chi, f) = \sum_{n=0}^{g^r-1} \chi(f(\sigma_g(n))),$$

where χ is a non-principal multiplicative character for the finite field \mathbb{F}_p with p elements, and $f(X)$ is an irreducible polynomial in $\mathbb{F}_p[X]$. Our results are based on the Weil bound for incomplete character sums; see [17].

Throughout the paper, the implied constants in the symbols “ O ” and “ \ll ” may depend on g but are absolute otherwise. We recall that the expressions $A \ll B$ and $A = O(B)$ are equivalent to the statement that $|A| \leq cB$ for some constant c . As usual, $\log z$ denotes the natural logarithm of z .

Acknowledgments. The first author would like to thank Macquarie University (Sydney) for its hospitality during the preparation of this paper. This work was supported in part by NSF grant DMS-0070628 (Banks) and by ARC grant DP0211459 (Shparlinski).

2 Preparations

Here we collect several auxiliary statements.

The following statement follows immediately from the Weil bound (cf. [17]) and is well-known; see also Theorem 2 of [16].

Lemma 1. *For any multiplicative character χ modulo p of order $m \geq 2$, any integers M and K with $1 \leq K \leq p$, and any polynomial $F(X) \in \mathbb{F}_p[X]$ with at most $d \geq 1$ distinct roots (of arbitrary multiplicity) such that $F(X)$ is not the m -th power of a rational function, the following estimate holds:*

$$\left| \sum_{n=M+1}^{M+K} \chi(F(n)) \right| \ll dp^{1/2} \log p.$$

We also need the following estimate, which is Corollary 2 of [15].

Lemma 2. *For any integers $K \geq 1$ and $0 \leq S \leq K(g-1)$, let $\Phi(K, S)$ be the number of integers $n \in [0, g^K - 1]$ with $\sigma_g(n) = S$. For $K \rightarrow \infty$ and*

$$\Delta = S - \frac{K(g-1)}{2} = o(K),$$

we have

$$\Phi(K, S) = \sqrt{\frac{6(g^K - 1)^2}{\pi K(g^2 - 1)}} \cdot \exp\left(-\frac{6\Delta^2}{K(g^2 - 1)} + O(\Delta^3 K^{-2} + K^{-1/2})\right).$$

3 Main Result

Theorem 3. *For any integer $r \geq 2$, any non-principal multiplicative character χ modulo p of order $m \geq 2$, and any irreducible polynomial $f(X) \in \mathbb{F}_p[X]$ of degree $1 \leq d < p^{1/2}(\log p)^{-1}$ such that $f(X)$ is not the m -th power of a rational function, the following estimate holds:*

$$|\mathcal{S}(r, \chi, f)| \ll d^{1/2} g^r (p^{-1/4} + p^{1/4} r^{-1/4}) \log^{3/4} p$$

Proof. Let k and ℓ be positive integers such that $k + \ell = r$.

Since every integer $n \in [0, g^r - 1]$ can be uniquely represented in the form $n = a + bg^k$ with $a \in [0, g^k - 1]$ and $b \in [0, g^\ell - 1]$, we have

$$\begin{aligned} \mathcal{S}(r, \chi, f) &= \sum_{a=0}^{g^k-1} \sum_{b=0}^{g^\ell-1} \chi(f(\sigma_g(a + bg^k))) = \sum_{a=0}^{g^k-1} \sum_{b=0}^{g^\ell-1} \chi(f(\sigma_g(a) + \sigma_g(b))) \\ &= \sum_{s=0}^{k(g-1)} \sum_{t=0}^{\ell(g-1)} \Phi(k, s) \Phi(\ell, t) \chi(f(s + t)). \end{aligned}$$

Put $\gamma = k(g-1)/2$ and $\Delta = g(k \log k)^{1/2}$. We observe that $\Phi_k(s) = \Phi(k, s)$ is non-decreasing on the interval $0 \leq s \leq \gamma$, and $\Phi_k(s) = \Phi_k(k(g-1) - s)$ for $0 \leq s \leq k(g-1)$. Consequently, if $|s - \gamma| > \Delta$, Lemma 2 implies the estimate

$$\begin{aligned} \Phi(k, s) &= \sqrt{\frac{6(g^k - 1)^2}{\pi k(g^2 - 1)}} \cdot \exp\left(-\frac{6g^2 \log k}{(g^2 - 1)} + O\left(k^{-1/2} \log^{3/2} k\right)\right) \\ &\ll k^{-2} g^k. \end{aligned}$$

Since

$$\sum_{t=0}^{\ell(g-1)} \Phi(\ell, t) = g^\ell,$$

it follows that

$$|\mathcal{S}(r, \chi, f) - \mathcal{T}| \ll k^{-1} g^r, \quad (1)$$

where

$$\mathcal{T} = \sum_{|s-\gamma| \leq \Delta} \sum_{t=0}^{\ell(g-1)} \Phi(k, s) \Phi(\ell, t) \chi(f(s + t)).$$

Next, we turn to the estimation of \mathcal{T} . By the Cauchy inequality, we have

$$|\mathcal{T}|^2 \leq \sum_{|s-\gamma| \leq \Delta} \Phi(k, s)^2 \cdot \sum_{|s-\gamma| \leq \Delta} \left| \sum_{t=0}^{\ell(g-1)} \Phi(\ell, t) \chi(f(s + t)) \right|^2.$$

First of all, we remark that the simple combinatorial identity

$$\sum_{s=0}^{k(g-1)} \Phi(k, s)^2 = \Phi(2k, k(g-1))$$

together with Lemma 2 imply that

$$\sum_{|s-\gamma|\leq\Delta} \Phi(k, s)^2 \leq \sum_{s=0}^{k(g-1)} \Phi(k, s)^2 = \Phi(2k, k(g-1)) \ll k^{-1/2} g^{2k}.$$

Consequently,

$$\begin{aligned} |\mathcal{T}|^2 &\ll k^{-1/2} g^{2k} \sum_{|s-\gamma|\leq\Delta} \sum_{t,u=0}^{\ell(g-1)} \Phi(\ell, t) \Phi(\ell, u) \chi(f(s+t)) \overline{\chi(f(s+u))} \\ &= k^{-1/2} g^{2k} \sum_{t,u=0}^{\ell(g-1)} \Phi(\ell, t) \Phi(\ell, u) \sum_{|s-\gamma|\leq\Delta} \chi(f(s+t) f(s+u)^{p-2}). \end{aligned}$$

If $t \neq u$, the polynomial

$$F_{t,u}(X) = f(X+t) f(X+u)^{p-2} \quad (2)$$

cannot be the m -th power of a rational function since $f(X)$ is irreducible and not the m -th power of a rational function. Thus, for $t \neq u$, we can use the bound provided by Lemma 1, while for $t = u$ we use the trivial bound; we obtain that

$$\begin{aligned} |\mathcal{T}|^2 &\ll k^{-1/2} g^{2k} \left(\Delta \sum_{t=0}^{\ell(g-1)} \Phi(\ell, t)^2 + \left(\frac{\Delta}{p} + 1 \right) dp^{1/2} \log p \left(\sum_{t=0}^{\ell(g-1)} \Phi(\ell, t) \right)^2 \right) \\ &\ll g^{2k} \left(\ell^{-1/2} g^{2\ell} \log^{1/2} k + dp^{-1/2} g^{2\ell} \log p \log^{1/2} k + dp^{1/2} k^{-1/2} g^{2\ell} \log p \right) \\ &= g^{2r} \left(\ell^{-1/2} \log^{1/2} k + dp^{-1/2} \log p \log^{1/2} k + dp^{1/2} k^{-1/2} \log p \right). \end{aligned}$$

Let us choose $k = \min \{ \lfloor r/2 \rfloor, p^2 \}$. Then $\ell \geq r/2$ and we obtain

$$\begin{aligned} |\mathcal{T}|^2 &\ll g^{2r} \left(r^{-1/2} \log^{1/2} p + dp^{-1/2} \log^{3/2} p + dp^{1/2} r^{-1/2} \log p \right) \\ &\ll dg^{2r} \left(p^{-1/2} + p^{1/2} r^{-1/2} \right) \log^{3/2} p \end{aligned}$$

and from (1) the result follows. \square

4 Remarks

It is easy to see that, when d is fixed, Theorem 3 is nontrivial whenever p and r satisfy $p \log^3 p = o(r)$. This threshold is not very surprising due to the inequality $\sigma_g(n) \leq r(g-1)$ for $0 \leq n \leq g^r - 1$ and it seems to be very hard to extend this bound to larger values of p . One the standard ways to tackle this problem is to consider higher powers of the sum \mathcal{T} and derive an estimate using the Hölder inequality; unfortunately, this approach does not appear to yield any improvement.

A more tractable problem would be to relax the irreducibility condition on the polynomial f . This seems quite feasible but requires a more involved analysis of the roots of the polynomial $F_{t,u}(x)$ given by (2).

References

- [1] C. Dartyge and C. Mauduit, ‘Nombres presque premiers dont l’écriture en base r ne comporte pas certains chiffres’, *J. Number Theory*, **81** (2000), 270–291.
- [2] F. M. Dekking, ‘On the distribution of digits in arithmetic sequences’, *Seminar on number theory, Talence 1982–1983, Exp. No. 32, Univ. Bordeaux I*.
- [3] P. Erdős, C. Mauduit and A. Sárközy, ‘On arithmetic properties of integers with missing digits I: Distribution in residue classes’, *J. Number Theory*, **70** (1998), 99–120.
- [4] P. Erdős, C. Mauduit and A. Sárközy, ‘On arithmetic properties of integers with missing digits II: Prime factors’, *Discrete Math.*, **200** (1999), 149–164.
- [5] N. J. Fine, ‘The distribution of the sum of digits $(\text{mod } p)$ ’, *Bull. Amer. Math. Soc.*, **71** (1965), 651–652.
- [6] E. Fouvry and C. Mauduit, ‘Méthodes de crible et fonctions sommes des chiffres’, *Acta Arith.*, **77** (1996), 339–351.
- [7] J. B. Friedlander and I. E. Shparlinski, ‘On the distribution of Diffie–Hellman triples with sparse exponents’, *SIAM J. Discr. Math.*, **14** (2001), 162–169.

- [8] A. O. Gel'fond, 'Sur les nombres qui ont des propriétés additives et multiplicatives données', *Acta Arith.*, **13** (1968), 259–265.
- [9] A. A. Karatsuba and B. Novak, 'Arithmetic problems with numbers of special type', *Mat. Zametki*, **66** (1999), 315–317 (in Russian), translation in *Mathematical Notes*, **66** (1999), 251–253.
- [10] S. Konyagin, 'Arithmetic properties of integers with missing digits: distribution in residue classes', *Periodica Math. Hungar.*, **42** (2001), 145–162.
- [11] S. Konyagin, C. Mauduit and A. Sárközy, 'On the number of prime factors of integers characterized by digit properties', *Periodica Math. Hungar.*, **40** (2000), 37–52.
- [12] S. V. Konyagin and I. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.
- [13] N. M. Korobov, 'On the distribution of digits in periodic fractions', *Mathem. Sbornik*, **89** (1972), 654–670 (in Russian).
- [14] C. Mauduit and A. Sárközy, 'On the arithmetic structure of sets characterized by sum of digits properties', *J. Number Theory*, **61** (1996), 25–38.
- [15] C. Mauduit and A. Sárközy, 'On the arithmetic structure of the integers whose sum of digits is fixed', *Acta Arith.*, **81** (1997), 145–173.
- [16] C. Mauduit and A. Sárközy, 'On finite pseudorandom binary sequences 1: Measure of pseudorandomness, the Legendre symbol', *Acta Arith.*, **82** (1997), 365–377.
- [17] A. Weil, *Basic number theory*, Springer-Verlag, New York, 1974.