

Character Sums over Integers with Restricted g -ary Digits*

WILLIAM D. BANKS[†]

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

ALESSANDRO CONFLITTI

Dipartimento di Matematica
Università degli Studi di Roma “Tor Vergata”
Via della Ricerca Scientifica
I-00133 Roma, Italy
conflitt@mat.uniroma2.it

IGOR E. SHPARLINSKI

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

*AMS Subject Classification: 11L07, 11L15, 11L40, 11N64

[†]Corresponding author

Abstract

We establish upper bounds for multiplicative character sums and exponential sums over sets of integers that are described by various properties of their digits in a fixed base $g \geq 2$. Our main tools are the Weil and Vinogradov bounds for character sums and exponential sums. Our results can be applied to study the distribution of quadratic non-residues and primitive roots among these sets of integers.

1 Introduction

Arithmetic properties of integers characterized by their digits in various bases have been studied in many papers; see [2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 17, 18] and the references therein. In this paper, using a very general technique, we give nontrivial bounds for short character sums over integers satisfying certain digit properties.

More precisely, let $g \geq 2$ be a fixed base and consider the base g representation of an integer $n \geq 0$:

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

Let $\sigma_g(n)$ denote the sum of the base g digits of n ; that is,

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

For any subset $\mathcal{D} \subset \{0, \dots, g - 1\}$ with $\#\mathcal{D} \geq 2$ and any integer $r \geq 1$, let

$$\mathcal{F}_{\mathcal{D}}(r) = \{0 \leq n < g^r \mid a_j(n) \in \mathcal{D}, 0 \leq j \leq r - 1\}.$$

In other words, $\mathcal{F}_{\mathcal{D}}(r)$ is the set of integers with r digits (in base g) all of which lie in the set \mathcal{D} .

For any integers $0 \leq \ell < q$ such that $\gcd(q, g - 1) = 1$, and for any integer $r \geq 1$, we also define

$$\mathcal{E}_{\ell, q}(r) = \{0 \leq n < g^r \mid \sigma_g(n) \equiv \ell \pmod{q}\}.$$

Thus, $\mathcal{E}_{\ell, q}(r)$ is the set of integers with r digits (in base g) such that the sum of the digits satisfies the congruence condition $\sigma_g(n) \equiv \ell \pmod{q}$.

Finally, for any integers $0 \leq s \leq (g-1)r$, let

$$\mathcal{G}_s(r) = \{0 \leq n < g^r \mid \sigma_g(n) = s\}.$$

Then $\mathcal{G}_s(r)$ is the set of integers with r digits (in base g) such that the sum of the digits is equal to s .

Let p be a fixed prime number. In this paper, we establish nontrivial bounds for certain sums of the form

$$S_{\mathcal{D}}(r, \chi, f) = \sum_{n \in \mathcal{F}_{\mathcal{D}}(r)} \chi(f(n)), \quad S_{\ell, q}(r, \chi, f) = \sum_{n \in \mathcal{E}_{\ell, q}(r)} \chi(f(n)),$$

and

$$S_s(r, \chi, f) = \sum_{n \in \mathcal{G}_s(r)} \chi(f(n)),$$

where χ is a non-principal multiplicative character for the finite field \mathbb{F}_p with p elements, and $f(X)$ is a polynomial in $\mathbb{F}_p[X]$. Our results are based on the Weil bound for incomplete character sums [22].

Using similar techniques, we also obtain nontrivial bounds for exponential sums of the form

$$T_{\mathcal{D}}(r, f) = \sum_{n \in \mathcal{F}_{\mathcal{D}}(r)} \mathbf{e}_p(f(n)), \quad T_{\ell, q}(r, f) = \sum_{n \in \mathcal{E}_{\ell, q}(r)} \mathbf{e}_p(f(n)),$$

and

$$T_s(r, f) = \sum_{n \in \mathcal{G}_s(r)} \mathbf{e}_p(f(n)),$$

where $\mathbf{e}_p(z) = e^{2\pi iz/p}$. Moreover, in this case, using the Vinogradov-type bound from [16], we are able to estimate much shorter sums for certain choices of parameters.

In [9], the sums

$$V_s(r, c, \vartheta) = \sum_{n \in \mathcal{G}_s(r)} \mathbf{e}_p(c\vartheta^n)$$

have been estimated; here, using bounds from [15, 16, 20] for exponential sums with exponential functions, we also estimate the related sums

$$V_{\mathcal{D}}(r, c, \vartheta) = \sum_{n \in \mathcal{F}_{\mathcal{D}}(r)} \mathbf{e}_p(c\vartheta^n) \quad \text{and} \quad V_{\ell, q}(r, c, \vartheta) = \sum_{n \in \mathcal{E}_{\ell, q}(r)} \mathbf{e}_p(c\vartheta^n).$$

In order to simplify our calculations and the formulation of our main results, we consider only the case where the prime p is greater than g^r ; however, our

methods and results can be extended to cover smaller values of p . Moreover, we remark that the most challenging and interesting problem is to obtain nontrivial bounds when the value of g^r is as small as possible relative to p , that is, when the sums are as short as possible.

For our bounds to be nontrivial, the sets $\mathcal{F}_{\mathcal{D}}(r)$, $\mathcal{E}_{\ell,q}(r)$ and $\mathcal{G}_s(r)$ must be of sufficiently large cardinality. We remark that, trivially, $\#\mathcal{F}_{\mathcal{D}}(r) = (\#\mathcal{D})^r$, and $\#\mathcal{E}_{\ell,q}(r)$ is given by Lemma 5 (see §2). The problem of estimating $\#\mathcal{G}_s(r)$ is more complicated. Some asymptotic formulas have been given in [18], but they are too technically complicated to be presented here. Nevertheless, we remark that since

$$\sum_{s=0}^{(g-1)r} \#\mathcal{G}_s(r) = g^r,$$

“on average” the value of $\#\mathcal{G}_s(r)$ is at least $g^{r-1}r^{-1}$. Of course, the largest values of $\#\mathcal{G}_s(r)$ occur for the “middle values” where $s \approx (g-1)r/2$.

We repeatedly use that $\bar{\chi}(z) = \chi(z^{p-2})$ for $z \in \mathbb{F}_p^*$ and a multiplicative character χ .

Throughout the paper, the implied constants in the symbols “ O ” and “ \ll ” can depend on g , on a certain integer parameter ν in the Theorem 1, and occasionally, when the sets $\mathcal{E}_{\ell,q}(r)$ are involved, on q as well. We recall that the expressions $A \ll B$ and $A = O(B)$ are each equivalent to the statement that $|A| \leq cB$ for some constant c . As usual, $\log z$ denotes the natural logarithm of z .

Acknowledgement. The first two authors would like to thank Macquarie University for its hospitality during the preparation of this paper. Work supported in part by NSF grant DMS-0070628 (W. Banks) and by ARC grant A00000184 (I. Shparlinski).

2 Preparations

Here we collect several auxiliary statements.

The following two statements follow immediately from the Weil bound and are well-known; see [22]. The first one is essentially Theorem 2 of [19], and the second one is obtained using similar techniques.

Lemma 1. *For any multiplicative character χ modulo p of order $m \geq 2$, any integers M and K with $1 \leq K < p$, and any polynomial $F(X) \in \mathbb{F}_p[X]$ with d*

distinct roots (of arbitrary multiplicity) such that $F(X)$ is not the m -th power of a rational function, we have

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

Lemma 2. For any polynomial $F(X) \in \mathbb{F}_p[X]$ of degree $d \geq 2$ and any integers M and K with $1 \leq K < p$, we have

$$\max_{\gcd(a,p)=1} \left| \sum_{n=M+1}^{M+K} \mathbf{e}_p(aF(n)) \right| \ll dp^{1/2} \log p.$$

The following result is a special case of Theorem 17 from [16].

Lemma 3. For any polynomial $F(X) \in \mathbb{F}_p[X]$ of degree $d > 2$ and any integers M and K with $p^{1/(d-1)} \leq K < p$, we have

$$\max_{\gcd(a,p)=1} \left| \sum_{n=M+1}^{M+K} \mathbf{e}_p(aF(n)) \right| \ll e^{3d} K^{1-1/9d^2 \log d}.$$

The following result can be found in [15, 16, 20]. In some cases, stronger bounds can be found in [14], but they do not seem to be useful for our purposes.

Lemma 4. Let $\lambda \in \mathbb{F}_p^*$ be an element of multiplicative order T . For any $c \in \mathbb{F}_p^*$ and any integer $H \leq T$, the bound

$$\left| \sum_{u=1}^H \mathbf{e}_p(c\lambda^u) \right| \ll p^{1/2} \log p$$

holds.

Finally, we need the following statement from [10].

Lemma 5. For any integers $0 \leq \ell < q$ such that $\gcd(q, g-1) = 1$, there is a constant $\rho < 1$, depending only on g and q , such that

$$\#\mathcal{E}_{\ell,q}(r) = \frac{g^r}{q} + O(g^{\rho r}).$$

3 Multiplicative Character Sums with Polynomials

Theorem 1. *For any integer $r \geq 1$ with $g^r < p$, any multiplicative character χ modulo p of order $m \geq 2$, and any polynomial $f(X) \in \mathbb{F}_p[X]$ that is not the m -th power of a rational function, we have*

$$|S_{\mathcal{D}}(r, \chi, f)| \ll \#\mathcal{F}_{\mathcal{D}}(r)^{1-\alpha/2(1+\alpha\nu)} \left(dp^{1/2} \log p \right)^{(1+\alpha(\nu-1))/2\nu(1+\alpha\nu)},$$

where $d = \deg f$, $0 < \alpha \leq 1$ is the real number such that $\#\mathcal{D} = g^\alpha$, and ν is an arbitrary positive integer if $f(X)$ is irreducible over \mathbb{F}_p , and $\nu = 1$ otherwise.

Proof. Put $K = g^{r-k}$, where $0 \leq k \leq r$ will be chosen later. For every $n \in \mathcal{F}_{\mathcal{D}}(r)$, write $n = ag^k + b$ with $0 \leq a < g^{r-k}$ and $0 \leq b < g^k$; then

$$S_{\mathcal{D}}(r, \chi, f) = \sum_{a \in \mathcal{F}_{\mathcal{D}}(r-k)} \sum_{b \in \mathcal{F}_{\mathcal{D}}(k)} \chi(f(ag^k + b)).$$

By the Hölder inequality, we have

$$\begin{aligned} |S_{\mathcal{D}}(r, \chi, f)|^{2\nu} &\leq \#\mathcal{F}_{\mathcal{D}}(r-k)^{2\nu-1} \sum_{a=0}^{K-1} \left| \sum_{b \in \mathcal{F}_{\mathcal{D}}(k)} \chi(f(ag^k + b)) \right|^{2\nu} \\ &= \#\mathcal{F}_{\mathcal{D}}(r-k)^{2\nu-1} \sum_{a=0}^{K-1} \sum_{\substack{b_1, \dots, b_\nu \in \mathcal{F}_{\mathcal{D}}(k) \\ c_1, \dots, c_\nu \in \mathcal{F}_{\mathcal{D}}(k)}} \prod_{j=1}^{\nu} \chi(f(ag^k + b_j)) \overline{\chi}(f(ag^k + c_j)) \\ &= \#\mathcal{F}_{\mathcal{D}}(r-k)^{2\nu-1} \sum_{\substack{b_1, \dots, b_\nu \in \mathcal{F}_{\mathcal{D}}(k) \\ c_1, \dots, c_\nu \in \mathcal{F}_{\mathcal{D}}(k)}} \left| \sum_{a=0}^{K-1} \prod_{j=1}^{\nu} \chi(f(ag^k + b_j) f(ag^k + c_j)^{p-2}) \right|. \end{aligned}$$

If $f(X)$ is irreducible, then for any $\beta, \gamma \in \mathbb{F}_p$ with $\beta \neq \gamma$, the polynomials $f(g^k X + \beta)$ and $f(g^k X + \gamma)$ are irreducible as well, hence relatively prime. In particular, these polynomials have no common roots. Now let (b_1, \dots, b_ν) and (c_1, \dots, c_ν) be two ν -tuples in $\mathcal{F}_{\mathcal{D}}(k)^\nu$. After applying a permutation to one these ν -tuples (if necessary), for some integer μ , $0 \leq \mu \leq \nu$, we have that $b_i \neq c_j$ for all $1 \leq i, j \leq \mu$, and $b_i = c_i$ for $\mu + 1 \leq i \leq \nu$. Consequently,

$$\prod_{j=1}^{\nu} f(g^k X + b_j) f(g^k X + c_j)^{p-2} = \prod_{j=1}^{\mu} f(g^k X + b_j) f(g^k X + c_j)^{p-2}.$$

Now we see that this function is the m -th power of a rational function if and only if $\mu \equiv 0 \pmod{m}$ and every value that occurs in the sequence b_1, \dots, b_μ or in the sequence c_1, \dots, c_μ occurs with a multiplicity that is divisible by m (we recall that $m|p-1$ thus $p-2 \equiv 1 \pmod{m}$). In other words, both sequences can be separated into μ/m constant subsequences with m terms each. Thus, there are at most $O(\#\mathcal{F}_{\mathcal{D}}(k)^{2\mu/m}) = O(\#\mathcal{F}_{\mathcal{D}}(k)^\mu)$ possibilities. We also have at most $O(\#\mathcal{F}_{\mathcal{D}}(k)^{\nu-\mu})$ possibilities for the remaining elements $b_i = c_i$, $\mu+1 \leq i \leq \nu$. This shows that there are at most $O(\#\mathcal{F}_{\mathcal{D}}(k)^\nu)$ pairs of ν -tuples (b_1, \dots, b_ν) and (c_1, \dots, c_ν) such that

$$F_k(X) = \prod_{j=1}^{\nu} f(g^k X + b_j) f(g^k X + c_j)^{p-2} \quad (1)$$

is the m -th power of a rational function.

Similarly, when $\nu = 1$, the same statement holds for an arbitrary polynomial $f(X)$ that is not the m -th power of a rational function. To verify this, it is enough to examine the roots and poles of $f(g^k X + b)/f(g^k X + c)$. Indeed, we can assume that the multiplicities of all roots of f are at most $m-1$. Therefore in the representation $f(g^k X + b)/f(g^k X + c) = g(X)/h(X)$ with relatively prime $g(X)$ and $h(X)$, the multiplicities of roots of g and h are at most $m-1$. On the other hand, it is obvious that $f(g^k X + b)/f(g^k X + c)$ is not a constant, and thus is not the m -th power of a rational function.

Thus, we can apply Lemma 1 when the function (1) is not the m -th power of a rational function. For remaining $O(\#\mathcal{F}_{\mathcal{D}}(k)^\nu)$ pairs of ν -tuples (b_1, \dots, b_ν) and (c_1, \dots, c_ν) we apply the trivial bound. Therefore, we obtain that

$$\sum_{\substack{b_1, \dots, b_\nu \in \mathcal{F}_{\mathcal{D}}(k) \\ c_1, \dots, c_\nu \in \mathcal{F}_{\mathcal{D}}(k)}} \left| \sum_{a=0}^{K-1} \prod_{j=1}^{\nu} \chi(f(ag^k + b_j) f(ag^k + c_j)^{p-2}) \right| \\ \ll \#\mathcal{F}_{\mathcal{D}}(k)^\nu K + \#\mathcal{F}_{\mathcal{D}}(k)^{2\nu} dp^{1/2} \log p.$$

Hence

$$|S_{\mathcal{D}}(r, \chi, f)|^{2\nu} \ll \#\mathcal{F}_{\mathcal{D}}(r-k)^{2\nu-1} \#\mathcal{F}_{\mathcal{D}}(k)^\nu \left(g^{r-k} + \#\mathcal{F}_{\mathcal{D}}(k)^\nu dp^{1/2} \log p \right). \quad (2)$$

Since $\#\mathcal{F}_{\mathcal{D}}(k) = (\#\mathcal{D})^k = g^{\alpha k}$, by defining k so that

$$g^{k-1} \leq g^{r/(1+\alpha\nu)} \left(dp^{1/2} \log p \right)^{-1/(1+\alpha\nu)} < g^k$$

(which balances both terms in (2)), it follows that

$$\begin{aligned}
|S_{\mathcal{D}}(r, \chi, f)|^{2\nu} &\ll \#\mathcal{F}_{\mathcal{D}}(r-k)^{2\nu-1} \#\mathcal{F}_{\mathcal{D}}(k)^{2\nu} dp^{1/2} \log p \\
&= \#\mathcal{F}_{\mathcal{D}}(r)^{2\nu} g^{-\alpha(r-k)} dp^{1/2} \log p \\
&\ll \#\mathcal{F}_{\mathcal{D}}(r)^{2\nu} g^{-\alpha^2 \nu r / (1+\alpha\nu)} \left(dp^{1/2} \log p \right)^{(1+\alpha(\nu-1))/(1+\alpha\nu)}.
\end{aligned}$$

Recalling that $\#\mathcal{F}_{\mathcal{D}}(r) = g^{\alpha r}$, the result follows. \square

We see that if d is constant, then for any polynomial $f(X)$ the bound of Theorem 1 is nontrivial provided that $\#\mathcal{F}_{\mathcal{D}}(r) \geq (p^{1/2} \log^2 p)^{1/\alpha}$, with p sufficiently large.

Moreover, if d is constant and $f(X)$ is irreducible (for example, for any linear polynomial), then for any $\varepsilon > 0$ and ν sufficiently large, the bound of Theorem 1 is nontrivial provided that $\#\mathcal{F}_{\mathcal{D}}(r) \geq p^{1/2+\varepsilon}$, with p sufficiently large.

Theorem 2. *Fix q and ℓ with $0 \leq \ell < q$ and such that $\gcd(q, g-1) = 1$. For any integer $r \geq 1$ with $g^r < p$, any multiplicative character χ modulo p of order $m \geq 2$, and any polynomial $f(X) \in \mathbb{F}_p[X]$ of degree d such that $f(X)$ is not the m -th power of a rational function, we have*

$$|S_{\ell, q}(r, \chi, f)| \ll \#\mathcal{E}_{\ell, q}(r) \left(\frac{\#\mathcal{E}_{\ell, q}(r)}{dp^{1/2} \log p} \right)^{-1/4}.$$

Proof. As in Theorem 1, put $K = g^{r-k}$, where $0 \leq k \leq r$. For every $n \in \mathcal{E}_{\ell, q}(r)$, write $n = ag^k + b$ with $0 \leq a < g^{r-k}$ and $0 \leq b < g^k$; then

$$S_{\ell, q}(r, \chi, f) = \sum_{j=0}^{q-1} \sum_{a \in \mathcal{E}_{\ell-j, q}(r-k)} \sum_{b \in \mathcal{E}_{j, q}(k)} \chi(f(ag^k + b)).$$

By the Cauchy inequality, we have

$$\begin{aligned}
|S_{\ell, q}(r, \chi, f)|^2 &\leq q \sum_{j=0}^{q-1} \#\mathcal{E}_{\ell-j, q}(r-k) \sum_{a=0}^{K-1} \left| \sum_{b \in \mathcal{E}_{j, q}(k)} \chi(f(ag^k + b)) \right|^2 \\
&= q \sum_{j=0}^{q-1} \#\mathcal{E}_{\ell-j, q}(r-k) \sum_{a=0}^{K-1} \sum_{b_1, b_2 \in \mathcal{E}_{j, q}(k)} \chi(f(ag^k + b_1)) \overline{\chi}(f(ag^k + b_2)) \\
&\leq q \sum_{j=0}^{q-1} \#\mathcal{E}_{\ell-j, q}(r-k) \sum_{b_1, b_2 \in \mathcal{E}_{j, q}(k)} \left| \sum_{a=0}^{K-1} \chi(f(g^k X + b_1)) \overline{\chi}(f(g^k X + b_2)) \right|^2.
\end{aligned}$$

It is easy to see that if $b_1 \not\equiv b_2 \pmod{p}$, and $f(X)$ is not the m -th power of a rational function, then

$$F_k(X) = f(g^k X + b_1)f(g^k X + b_2)^{p-2}$$

cannot be the m -th power of a rational function (again, for this, it is enough to examine the roots and poles of $f(g^k X + b_1)/f(g^k X + b_2)$). Thus, we can apply Lemma 1 when $b_1 \not\equiv b_2 \pmod{p}$, and we use the trivial bound when $b_1 \equiv b_2 \pmod{p}$; we obtain that

$$\begin{aligned} & \sum_{b_1, b_2 \in \mathcal{E}_{j,q}(k)} \left| \sum_{a=0}^{K-1} \chi(f(ag^k + b_1)) \bar{\chi}(f(ag^k + b_2)) \right| \\ &= \#\mathcal{E}_{j,q}(k)K + \sum_{\substack{b_1, b_2 \in \mathcal{E}_{j,q}(k) \\ b_1 \neq b_2}} \left| \sum_{a=0}^{K-1} \chi(f(ag^k + b_1)f(ag^k + b_2)^{p-2}) \right| \\ &\ll \#\mathcal{E}_{j,q}(k)K + \#\mathcal{E}_{j,q}(k)^2 dp^{1/2} \log p \\ &\leq \#\mathcal{E}_{j,q}(k) \left(g^{r-k} + g^k dp^{1/2} \log p \right). \end{aligned}$$

Since

$$\sum_{j=0}^{q-1} \#\mathcal{E}_{\ell-j,q}(r-k) \#\mathcal{E}_{j,q}(k) = \#\mathcal{E}_{\ell,q}(r),$$

this gives

$$|S_{\ell,q}(r, \chi, f)|^2 \ll \#\mathcal{E}_{\ell,q}(r) \left(g^{r-k} + g^k dp^{1/2} \log p \right). \quad (3)$$

Defining k so that

$$g^{k-1} \leq \left(\frac{g^r}{dp^{1/2} \log p} \right)^{1/2} < g^k$$

(which balances the two terms in (3)), it follows that

$$|S_{\ell,q}(r, \chi, f)|^2 \ll \#\mathcal{E}_{\ell,q}(r) d^{1/2} g^{r/2} p^{1/4} \log^{1/2} p.$$

Recalling Lemma 5, we derive the result. \square

We see that if d is constant, the bound of Theorem 2 is nontrivial provided that $\#\mathcal{E}_{\ell,q}(r) \geq p^{1/2} \log^2 p$, with p sufficiently large.

Theorem 3. *For any integers $1 \leq s \leq (g-1)r$ with $g^r < p$, any multiplicative character χ modulo p of order $m \geq 2$, and any polynomial $f(X) \in \mathbb{F}_p[X]$ of degree d such that $f(X)$ is not the m -th power of a rational function, we have*

$$|S_s(r, \chi, f)| \ll \#\mathcal{G}_s(r)^{1/2} s^{1/2} g^{r/4} d^{1/4} p^{1/8} \log^{1/4} p.$$

Proof. As in Theorem 2, put $K = g^{r-k}$ where $0 \leq k \leq r$ will be chosen later. For every $n \in \mathcal{G}_s(r)$, write $n = ag^k + b$ with $0 \leq a < g^{r-k}$ and $0 \leq b < g^k$; then

$$S_s(r, \chi, f) = \sum_{j=0}^s \sum_{a \in \mathcal{G}_{s-j}(r-k)} \sum_{b \in \mathcal{G}_j(k)} \chi(f(ag^k + b)).$$

By the Cauchy inequality, we have

$$\begin{aligned} |S_s(r, \chi, f)|^2 &\leq (s+1) \sum_{j=0}^s \#\mathcal{G}_{s-j}(r-k) \sum_{a=0}^{K-1} \left| \sum_{b \in \mathcal{G}_j(k)} \chi(f(ag^k + b)) \right|^2 \\ &= (s+1) \sum_{j=0}^s \#\mathcal{G}_{s-j}(r-k) \sum_{a=0}^{K-1} \sum_{b_1, b_2 \in \mathcal{G}_j(k)} \chi(f(ag^k + b_1)) \bar{\chi}(f(ag^k + b_2)) \\ &\leq (s+1) \sum_{j=0}^s \#\mathcal{G}_{s-j}(r-k) \sum_{b_1, b_2 \in \mathcal{G}_j(k)} \left| \sum_{a=0}^{K-1} \chi(f(ag^k + b_1)) \bar{\chi}(f(ag^k + b_2)) \right|. \end{aligned}$$

As in the proof of Theorem 2, we can estimate

$$\begin{aligned} &\sum_{b_1, b_2 \in \mathcal{G}_j(k)} \left| \sum_{a=0}^{K-1} \chi(f(ag^k + b_1)) \bar{\chi}(f(ag^k + b_2)) \right| \\ &= \#\mathcal{G}_j(k)K + \sum_{\substack{b_1, b_2 \in \mathcal{G}_j(k) \\ b_1 \neq b_2}} \left| \sum_{a=0}^{K-1} \chi(f(ag^k + b_1)) \bar{\chi}(f(ag^k + b_2)) \right| \\ &\ll \#\mathcal{G}_j(k) \left(K + \#\mathcal{G}_j(k) dp^{1/2} \log p \right). \end{aligned}$$

Since

$$\sum_{j=0}^s \#\mathcal{G}_{s-j}(r-k) \#\mathcal{G}_j(k) = \#\mathcal{G}_s(r)$$

and $\#\mathcal{G}_j(k) \leq g^k$ for $0 \leq j \leq s$, this gives

$$|S_s(r, \chi, f)|^2 \ll \#\mathcal{G}_s(r) s \left(g^{r-k} + g^k dp^{1/2} \log p \right).$$

Defining k so that

$$g^k \leq \left(\frac{g^r}{dp^{1/2} \log p} \right)^{1/2} < g^{k+1},$$

we obtain

$$|S_s(r, \chi, f)|^2 \ll \#\mathcal{G}_s(r) s \left(g^r d p^{1/2} \log p \right)^{1/2}$$

and the result follows. \square

Taking into account that $s \leq (g-1)r = O(\log p)$, we see that if d is constant, the bound of Theorem 3 is nontrivial provided that $\#\mathcal{G}_s(r) \geq g^{r/2} p^{1/4} \log^2 p$, with p sufficiently large.

4 Exponential Sums with Polynomials

Theorem 4. *For any integer $r \geq 1$ with $g^r < p$ and any polynomial $f(X) \in \mathbb{F}_p[X]$ of degree $d \geq 3$, we have*

$$|T_{\mathcal{D}}(r, f)| \ll \#\mathcal{F}_{\mathcal{D}}(r)^{1-\alpha/2(1+\alpha)} \left(d p^{1/2} \log p \right)^{1/2(1+\alpha)},$$

where $0 < \alpha \leq 1$ is the real number such that $\#\mathcal{D} = g^\alpha$.

Proof. As in Theorem 1, put $K = g^{r-k}$, where $0 \leq k \leq r$. For every $n \in \mathcal{F}_{\mathcal{D}}(r)$, write $n = ag^k + b$ with $0 \leq a < g^{r-k}$ and $0 \leq b < g^k$; then

$$T_{\mathcal{D}}(r, f) = \sum_{a \in \mathcal{F}_{\mathcal{D}}(r-k)} \sum_{b \in \mathcal{F}_{\mathcal{D}}(k)} \mathbf{e}_p(f(ag^k + b)).$$

By the Cauchy inequality, we have

$$\begin{aligned} |T_{\mathcal{D}}(r, f)|^2 &\leq \#\mathcal{F}_{\mathcal{D}}(r-k) \sum_{a=0}^{K-1} \left| \sum_{b \in \mathcal{F}_{\mathcal{D}}(k)} \mathbf{e}_p(f(ag^k + b)) \right|^2 \\ &= \#\mathcal{F}_{\mathcal{D}}(r-k) \sum_{a=0}^{K-1} \sum_{b_1, b_2 \in \mathcal{F}_{\mathcal{D}}(k)} \mathbf{e}_p(f(ag^k + b_1) - f(ag^k + b_2)) \\ &\leq \#\mathcal{F}_{\mathcal{D}}(r-k) \sum_{b_1, b_2 \in \mathcal{F}_{\mathcal{D}}(k)} \left| \sum_{a=0}^{K-1} \mathbf{e}_p(f(ag^k + b_1) - f(ag^k + b_2)) \right|. \end{aligned}$$

If $b_1 \not\equiv b_2 \pmod{p}$, then

$$F(X) = f(g^k X + b_1) - f(g^k X + b_2)$$

is a polynomial of degree $d - 1 \geq 2$. Thus, we can apply Lemma 2 when $b_1 \not\equiv b_2 \pmod{p}$, and we use the trivial bound when $b_1 \equiv b_2 \pmod{p}$; we obtain that

$$\sum_{b_1, b_2 \in \mathcal{F}_{\mathcal{D}}(k)} \left| \sum_{a=0}^{K-1} \mathbf{e}_p(f(ag^k + b_1) - f(ag^k + b_2)) \right| \\ \ll \#\mathcal{F}_{\mathcal{D}}(k) K + \#\mathcal{F}_{\mathcal{D}}(k)^2 dp^{1/2} \log p.$$

Since $\#\mathcal{F}_{\mathcal{D}}(k) = (\#\mathcal{D})^k = g^{\alpha k}$, it follows that

$$|T_{\mathcal{D}}(r, f)|^2 \ll \#\mathcal{F}_{\mathcal{D}}(r) \left(g^{r-k} + g^{\alpha k} dp^{1/2} \log p \right). \quad (4)$$

Defining k so that

$$g^{k-1} \leq g^{r/(1+\alpha)} \left(dp^{1/2} \log p \right)^{-1/(1+\alpha)} < g^k$$

(which balances both terms in (4)), it follows that

$$|T_{\mathcal{D}}(r, f)|^2 \ll \#\mathcal{F}_{\mathcal{D}}(r) g^{\alpha r/(1+\alpha)} \left(dp^{1/2} \log p \right)^{1/(1+\alpha)}.$$

Recalling that $\#\mathcal{F}_{\mathcal{D}}(r) = g^{\alpha r}$, the result follows. \square

We see that if d is constant, the bound of Theorem 4 is nontrivial provided that $\#\mathcal{F}_{\mathcal{D}}(r) \geq (p^{1/2} \log^2 p)^{1/\alpha}$, with p sufficiently large.

For smaller sets, we can use Lemma 3 instead of Lemma 2.

Theorem 5. *For any integers $d \geq 4$ and $r \geq 1$ such that*

$$p^{1/(d-2)} < g^r < p,$$

and for any polynomial $f(X) \in \mathbb{F}_p[X]$ of degree d , we have

$$|T_{\mathcal{D}}(r, f)| \ll \#\mathcal{F}_{\mathcal{D}}(r)^{1/2} e^{3d/2} g^{r(1/2-1/36d^2 \log d)}.$$

Proof. Define k by the inequalities

$$k < \frac{r}{18d^2 \log d} \leq k + 1,$$

and put $K = g^{r-k}$. It is easy to verify that

$$K \geq p^{(1-1/18d^2 \log d)/(d-2)} > p^{1/(d-1)}.$$

Therefore, following the proof of Theorem 4 but using Lemma 3 instead of Lemma 2, we derive that

$$|T_{\mathcal{D}}(r, f)|^2 \ll \#\mathcal{F}_{\mathcal{D}}(r) \left(K + \#\mathcal{F}_{\mathcal{D}}(k) e^{3d} K^{1-1/9d^2 \log d} \right).$$

Clearly, $K \geq g^{r/2}$, hence it follows that

$$\#\mathcal{F}_{\mathcal{D}}(k) \leq g^k < g^{r/18d^2 \log d} \leq K^{1/9d^2 \log d},$$

thus $\#\mathcal{F}_{\mathcal{D}}(k) K^{1-1/9d^2 \log d} \leq K$. Consequently,

$$|T_{\mathcal{D}}(r, f)|^2 \ll \#\mathcal{F}_{\mathcal{D}}(r) e^{3d} K,$$

and the result follows. \square

We see that if d is constant, the bound of Theorem 5 is nontrivial provided that $\#\mathcal{F}_{\mathcal{D}}(r) \geq g^{r(1-1/19d^2 \log d)}$, with $p^{1/(d-2)} < g^r < p$ and p sufficiently large.

Theorem 6. Fix q and ℓ with $0 \leq \ell < q$ and such that $\gcd(q, g-1) = 1$. For any integer $r \geq 1$ with $g^r < p$ and any polynomial $f(X) \in \mathbb{F}_p[X]$ of degree $d \geq 3$, we have

$$|T_{\ell, q}(r, f)| \ll \#\mathcal{E}_{\ell, q}(r) \left(\frac{\#\mathcal{E}_{\ell, q}(r)}{dp^{1/2} \log p} \right)^{-1/4}.$$

Proof. Again, put $K = g^{r-k}$, where $0 \leq k \leq r$. For every $n \in \mathcal{E}_{\ell, q}(r)$, write $n = ag^k + b$ with $0 \leq a < g^{r-k}$ and $0 \leq b < g^k$; then

$$T_{\ell, q}(r, f) = \sum_{j=0}^{q-1} \sum_{a \in \mathcal{E}_{\ell-j, q}(r-k)} \sum_{b \in \mathcal{E}_{j, q}(k)} \mathbf{e}_p(f(ag^k + b)).$$

By the Cauchy inequality, we have

$$\begin{aligned} |T_{\ell, q}(r, f)|^2 &\leq q \sum_{j=0}^{q-1} \#\mathcal{E}_{\ell-j, q}(r-k) \sum_{a=0}^{K-1} \left| \sum_{b \in \mathcal{E}_{j, q}(k)} \mathbf{e}_p(f(ag^k + b)) \right|^2 \\ &= q \sum_{j=0}^{q-1} \#\mathcal{E}_{\ell-j, q}(r-k) \sum_{a=0}^{K-1} \sum_{b_1, b_2 \in \mathcal{E}_{j, q}(k)} \mathbf{e}_p(f(ag^k + b_1) - f(ag^k + b_2)) \\ &\leq q \sum_{j=0}^{q-1} \#\mathcal{E}_{\ell-j, q}(r-k) \sum_{b_1, b_2 \in \mathcal{E}_{j, q}(k)} \left| \sum_{a=0}^{K-1} \mathbf{e}_p(f(ag^k + b_1) - f(ag^k + b_2)) \right|. \end{aligned}$$

As in the proof of Theorem 4, we can estimate

$$\begin{aligned} \sum_{b_1, b_2 \in \mathcal{E}_{j,q}(k)} \left| \sum_{a=0}^{K-1} \mathbf{e}_p(f(ag^k + b_1) - f(ag^k + b_2)) \right| \\ \ll \#\mathcal{E}_{j,q}(k)K + \#\mathcal{E}_{j,q}(k)^2 dp^{1/2} \log p \\ \leq \#\mathcal{E}_{j,q}(k) \left(g^{r-k} + g^k dp^{1/2} \log p \right). \end{aligned}$$

Since

$$\sum_{j=0}^{q-1} \#\mathcal{E}_{\ell-j,q}(r-k) \#\mathcal{E}_{j,q}(k) = \#\mathcal{E}_{\ell,q}(r),$$

this gives

$$|T_{\ell,q}(r, f)|^2 \ll \#\mathcal{E}_{\ell,q}(r) \left(g^{r-k} + g^k dp^{1/2} \log p \right),$$

and the proof can be completed as in Theorem 2. \square

We see that if d is constant, the bound of Theorem 6 is nontrivial provided that $\#\mathcal{E}_{\ell,q}(r) \geq p^{1/2} \log^2 p$, with p sufficiently large.

Similarly, by using Lemma 3 instead of Lemma 2, we obtain the following analogue of Theorem 5.

Theorem 7. *Fix q and ℓ with $0 \leq \ell < q$ and such that $\gcd(q, q-1) = 1$. For any integers $d \geq 4$ and $r \geq 1$ with*

$$p^{1/(d-2)} < g^r < p$$

and any polynomial $f(X) \in \mathbb{F}_p[X]$ of degree $d \geq 3$, we have

$$|T_{\ell,q}(r, f)| \ll e^{3d/2} \#\mathcal{E}_{\ell,q}(r)^{1-1/36d^2 \log d}.$$

We see that if d is constant, the bound of Theorem 7 is always nontrivial.

Theorem 8. *For any integers $1 \leq s \leq (g-1)r$ with $g^r < p$ and any polynomial $f(X) \in \mathbb{F}_p[X]$ of degree $d \geq 3$, we have*

$$|T_s(r, f)| \ll \#\mathcal{G}_s(r)^{1/2} s^{1/2} g^{r/4} d^{1/4} p^{1/8} \log^{1/4} p.$$

Proof. Put $K = g^{r-k}$, where $0 \leq k \leq r$. For every $n \in \mathcal{G}_s(r)$, write $n = ag^k + b$ with $0 \leq a < g^{r-k}$ and $0 \leq b < g^k$; then

$$T_s(r, f) = \sum_{j=0}^s \sum_{a \in \mathcal{G}_{s-j}(r-k)} \sum_{b \in \mathcal{G}_j(k)} \mathbf{e}_p(f(ag^k + b)).$$

By the Cauchy inequality, we have

$$\begin{aligned}
|T_s(r, f)|^2 &\leq (s+1) \sum_{j=0}^s \#\mathcal{G}_{s-j}(r-k) \sum_{a=0}^{K-1} \left| \sum_{b \in \mathcal{G}_j(k)} \mathbf{e}_p(f(ag^k + b)) \right|^2 \\
&= (s+1) \sum_{j=0}^s \#\mathcal{G}_{s-j}(r-k) \sum_{a=0}^{K-1} \sum_{b_1, b_2 \in \mathcal{G}_j(k)} \mathbf{e}_p(f(ag^k + b_1) - f(ag^k + b_2)) \\
&\leq (s+1) \sum_{j=0}^s \#\mathcal{G}_{s-j}(r-k) \sum_{b_1, b_2 \in \mathcal{G}_j(k)} \left| \sum_{a=0}^{K-1} \mathbf{e}_p(f(ag^k + b_1) - f(ag^k + b_2)) \right|.
\end{aligned}$$

As in the proof of Theorem 4, we can estimate

$$\begin{aligned}
\sum_{b_1, b_2 \in \mathcal{G}_j(k)} \left| \sum_{a=0}^{K-1} \mathbf{e}_p(f(ag^k + b_1) - f(ag^k + b_2)) \right| \\
\ll \#\mathcal{G}_j(k) \left(K + \#\mathcal{G}_j(k) dp^{1/2} \log p \right).
\end{aligned}$$

Since

$$\sum_{j=0}^s \#\mathcal{G}_{s-j}(r-k) \#\mathcal{G}_j(k) = \#\mathcal{G}_s(r)$$

and $\#\mathcal{G}_j(k) \leq g^k$ for $0 \leq j \leq s$, this gives

$$|T_s(r, f)|^2 \ll \#\mathcal{G}_s(r) s \left(g^{r-k} + g^k dp^{1/2} \log p \right),$$

and the proof can be completed as in Theorem 3. \square

Taking into account that $s \leq (g-1)r = O(\log p)$, we see that if d is constant, the bound of Theorem 8 is nontrivial provided that $\#\mathcal{G}_s(r) \geq g^{r/2} p^{1/4} \log^2 p$, with p sufficiently large.

Finally, by using Lemma 3 instead of Lemma 2, we obtain the following analogue of Theorems 5 and 7.

Theorem 9. *For any integers $d \geq 4$ and $1 \leq s \leq (g-1)r$ such that*

$$p^{1/(d-2)} < g^r < p,$$

and for any polynomial $f(X) \in \mathbb{F}_p[X]$ of degree d , we have

$$|T_s(r, f)| \ll \#\mathcal{G}_s(r)^{1/2} s^{1/2} e^{3d/2} g^{r(1/2-1/36d^2 \log d)}.$$

As before, we see that if d is constant, the bound of Theorem 9 is nontrivial provided that $\#\mathcal{G}_s(r) \geq g^{r(1-1/19d^2 \log d)}$, with $p^{1/(d-2)} < g^r < p$ and p sufficiently large.

5 Exponential Sums with Exponential Functions

Theorem 10. For any $c \in \mathbb{F}_p^*$, any $\vartheta \in \mathbb{F}_p$ of multiplicative order T , and any integer $r \geq 1$ with $g^r < T$, we have

$$|V_{\mathcal{D}}(r, c, \vartheta)| \ll \#\mathcal{F}_{\mathcal{D}}(r)^{1-\alpha/2(1+\alpha)} \left(p^{1/2} \log p\right)^{1/2(1+\alpha)},$$

where $0 < \alpha \leq 1$ is the real number such that $\#\mathcal{D} = g^\alpha$.

Proof. For every $n \in \mathcal{F}_{\mathcal{D}}(r)$, write $n = ag^k + b$ with $0 \leq a < g^{r-k}$ and $0 \leq b < g^k$, where $0 \leq k \leq r$ will be chosen later; then

$$V_{\mathcal{D}}(r, c, \vartheta) = \sum_{a \in \mathcal{F}_{\mathcal{D}}(r-k)} \sum_{b \in \mathcal{F}_{\mathcal{D}}(k)} \mathbf{e}_p \left(c \vartheta^{ag^k+b} \right).$$

By the Cauchy inequality, we have

$$\begin{aligned} |V_{\mathcal{D}}(r, c, \vartheta)|^2 &\leq \#\mathcal{F}_{\mathcal{D}}(k) \sum_{b=0}^{g^k-1} \left| \sum_{a \in \mathcal{F}_{\mathcal{D}}(r-k)} \mathbf{e}_p \left(c \vartheta^{ag^k+b} \right) \right|^2 \\ &= \#\mathcal{F}_{\mathcal{D}}(k) \sum_{b=0}^{g^k-1} \sum_{a_1, a_2 \in \mathcal{F}_{\mathcal{D}}(r-k)} \mathbf{e}_p \left(c \vartheta^b \left(\vartheta^{a_1 g^k} - \vartheta^{a_2 g^k} \right) \right) \\ &\leq \#\mathcal{F}_{\mathcal{D}}(k) \sum_{a_1, a_2 \in \mathcal{F}_{\mathcal{D}}(r-k)} \left| \sum_{b=0}^{g^k-1} \mathbf{e}_p \left(c \vartheta^b \left(\vartheta^{a_1 g^k} - \vartheta^{a_2 g^k} \right) \right) \right|. \end{aligned}$$

If $a_1, a_2 \in \mathcal{F}_{\mathcal{D}}(r-k)$ with $a_1 \neq a_2$, then $\vartheta^{a_1 g^k} \neq \vartheta^{a_2 g^k}$ (since $T > g^r$), so we can apply the bound from Lemma 4; for $a_1 = a_2$ we use the trivial bound.

Thus, we obtain that

$$\sum_{a_1, a_2 \in \mathcal{F}_{\mathcal{D}}(r-k)} \left| \sum_{b=0}^{g^k-1} \mathbf{e}_p \left(c \vartheta^b \left(\vartheta^{a_1 g^k} - \vartheta^{a_2 g^k} \right) \right) \right| \ll \#\mathcal{F}_{\mathcal{D}}(r-k) g^k + \#\mathcal{F}_{\mathcal{D}}(r-k)^2 p^{1/2} \log p.$$

Since $\#\mathcal{F}_{\mathcal{D}}(k) = (\#\mathcal{D})^k = g^{\alpha k}$, it follows that

$$|V_{\mathcal{D}}(r, c, \vartheta)|^2 \ll \#\mathcal{F}_{\mathcal{D}}(r) \left(g^k + g^{\alpha(r-k)} p^{1/2} \log p \right). \quad (5)$$

Defining k so that

$$g^{k-1} \leq g^{\alpha r / (1+\alpha)} \left(p^{1/2} \log p \right)^{1/(1+\alpha)} < g^k$$

(which balances both terms in (5)), it follows that

$$|V_{\mathcal{D}}(r, c, \vartheta)|^2 \ll \#\mathcal{F}_{\mathcal{D}}(r) g^{\alpha r / (1+\alpha)} \left(dp^{1/2} \log p \right)^{1/(1+\alpha)}.$$

Recalling that $\#\mathcal{F}_{\mathcal{D}}(r) = g^{\alpha r}$, the result follows. \square

We see that the bound of Theorem 10 is nontrivial provided that $\#\mathcal{F}_{\mathcal{D}}(r) \geq (p^{1/2} \log^2 p)^{1/\alpha}$, with p sufficiently large.

Theorem 11. *Fix q and ℓ with $0 \leq \ell < q$ and such that $\gcd(q, g-1) = 1$. For any $c \in \mathbb{F}_p^*$, any $\vartheta \in \mathbb{F}_p$ of multiplicative order T , and any integer $r \geq 1$ with $g^r < T$, we have*

$$|V_{\ell, q}(r, c, \vartheta)| \ll \#\mathcal{E}_{\ell, q}(r) \left(\frac{\#\mathcal{E}_{\ell, q}(r)}{p^{1/2} \log p} \right)^{-1/4}.$$

Proof. For every $n \in \mathcal{E}_{\ell, q}(r)$, write $n = ag^k + b$ with $0 \leq a < g^{r-k}$ and $0 \leq b < g^k$, where $0 \leq k \leq r$ will be chosen later; then

$$V_{\ell, q}(r, c, \vartheta) = \sum_{j=0}^{q-1} \sum_{a \in \mathcal{E}_{j, q}(r-k)} \sum_{b \in \mathcal{E}_{\ell-j, q}(k)} \mathbf{e}_p \left(c \vartheta^{ag^k + b} \right).$$

By the Cauchy inequality, we have

$$\begin{aligned}
|V_{\ell,q}(r, c, \vartheta)|^2 &\leq q \sum_{j=0}^{q-1} \#\mathcal{E}_{\ell-j,q}(k) \sum_{b=0}^{g^k-1} \left| \sum_{a \in \mathcal{E}_{j,q}(r-k)} \mathbf{e}_p \left(c\vartheta^{ag^k+b} \right) \right|^2 \\
&= q \sum_{j=0}^{q-1} \#\mathcal{E}_{\ell-j,q}(k) \sum_{b=0}^{g^k-1} \sum_{a_1, a_2 \in \mathcal{E}_{j,q}(r-k)} \mathbf{e}_p \left(c\vartheta^b \left(\vartheta^{a_1 g^k} - \vartheta^{a_2 g^k} \right) \right) \\
&\leq q \sum_{j=0}^{q-1} \#\mathcal{E}_{\ell-j,q}(k) \sum_{a_1, a_2 \in \mathcal{E}_{j,q}(r-k)} \left| \sum_{b=0}^{g^k-1} \mathbf{e}_p \left(c\vartheta^b \left(\vartheta^{a_1 g^k} - \vartheta^{a_2 g^k} \right) \right) \right|.
\end{aligned}$$

As in the proof of Theorem 10, we can estimate

$$\begin{aligned}
\sum_{a_1, a_2 \in \mathcal{E}_{j,q}(r-k)} \left| \sum_{b=0}^{g^k-1} \mathbf{e}_p \left(c\vartheta^b \left(\vartheta^{a_1 g^k} - \vartheta^{a_2 g^k} \right) \right) \right| \\
\ll \#\mathcal{E}_{j,q}(r-k)g^k + \#\mathcal{E}_{j,q}(r-k)^2 p^{1/2} \log p \\
\leq \#\mathcal{E}_{j,q}(r-k) \left(g^k + g^{r-k} d p^{1/2} \log p \right).
\end{aligned}$$

Since

$$\sum_{j=0}^{q-1} \#\mathcal{E}_{j,q}(r-k) \#\mathcal{E}_{\ell-j,q}(k) = \#\mathcal{E}_{\ell,q}(r),$$

this gives

$$|V_{\ell,q}(r, c, \vartheta)|^2 \ll \#\mathcal{E}_{\ell,q}(r) \left(g^k + g^{r-k} p^{1/2} \log p \right). \quad (6)$$

Defining k so that

$$g^{k-1} \leq \left(\frac{g^r}{p^{1/2} \log p} \right)^{1/2} < g^k$$

(which balances the two terms in (6)), it follows that

$$|V_{\ell,q}(r, c, \vartheta)|^2 \ll \#\mathcal{E}_{\ell,q}(r) g^{r/2} p^{1/4} \log^{1/2} p.$$

Recalling Lemma 5, we derive the result. \square

We see that the bound of Theorem 11 is nontrivial provided that $\#\mathcal{E}_{\ell,q}(r) \geq p^{1/2} \log^2 p$, with p sufficiently large.

6 Remarks

Using standard arguments, one can easily derive from the bounds of Section 3 various results about the distribution of quadratic non-residues and primitive roots in the polynomial values $f(n)$, as n runs over the set $\mathcal{F}_{\mathcal{D}}(r)$, the set $\mathcal{E}_{\ell,q}(r)$, or the set $\mathcal{G}_s(r)$. Accordingly, the bounds of Sections 4 imply results about the uniformity of distribution of fractional parts $\{f(n)/p\}$ for integers n in $\mathcal{F}_{\mathcal{D}}(r)$, $\mathcal{E}_{\ell,q}(r)$, or $\mathcal{G}_s(r)$.

It would be interesting to extend the class of polynomials in which one can take arbitrary $\nu \geq 1$ in Theorem 1.

Using the full power of the Vinogradov method, one can also estimate exponential sums for polynomials with real coefficients whose values are taken over integers in $\mathcal{F}_{\mathcal{D}}(r)$, $\mathcal{E}_{\ell,q}(r)$, or $\mathcal{G}_s(r)$.

We remark that the method of Sections 3, 4, and 5 can be applied to similar sums defined over the residue ring \mathbb{Z}_m modulo an arbitrary integer m . In some cases, the Weil bound must be replaced by Hua Loo Keng type bounds (which, unfortunately, are somewhat weaker; see [1, 21]), but our results based on the Vinogradov bounds do not require any substantial changes.

It would be interesting to obtain analogues of Theorems 2, 6 and 7 when q is allowed to grow along with r and p . Some results of this type can be obtained using the methods presented here (with an extra factor of $q^{1/2}$ in front of the corresponding upper bounds). However, for a more careful treatment, one needs a variant of Lemma 5 that can be applied when q is allowed to grow with r .

We have already remarked that the sums $V_s(r, c, \vartheta)$ have been estimated in [9]. Using the analogue of Lemma 4 for multiplicative characters,

$$\left| \sum_{u=1}^H \chi(\lambda^u + c) \right| \ll p^{1/2} \log p,$$

see [4, 23], one can easily obtain complete analogues of that result of [9] and of Theorems 10 and 11 for sums of multiplicative characters.

References

- [1] T. Cochrane and Z. Y. Zheng, ‘A survey on pure and mixed exponential sums modulo prime powers’, *Proc. Illinois Millennial Conf. on Number*

Theory, (to appear).

- [2] 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.
- [3] F. M. Dekking, ‘On the distribution of digits in arithmetic sequences’, *Seminar on number theory, Talence 1982–1983, Exp. No. 32, Univ. Bordeaux I*.
- [4] E. Dobrowolski and K. S. Williams, ‘An upper bound for the sum $\sum_{n=a+1}^{a+H} f(n)$ for a certain class of functions f ’, *Proc. Amer. Math. Soc.* **114** (1992), 29–35.
- [5] 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.
- [6] P. Erdős, C. Mauduit and A. Sárközy, ‘On arithmetic properties of integers with missing digits II: Prime factors’, *Discrete Math.*, **200** (1999), 149–164.
- [7] N. J. Fine, ‘The distribution of the sum of digits $(\bmod p)$ ’, *Bull. Amer. Math. Soc.*, **71** (1965), 651–652.
- [8] E. Fouvry and C. Mauduit, ‘Méthodes de crible et fonctions sommes des chiffres’, *Acta Arith.*, **77** (1996), 339–351.
- [9] 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.
- [10] A. O. Gel’fond, ‘Sur les nombres qui ont des propriétés additives et multiplicatives données’, *Acta Arith.*, **13** (1968), 259–265.
- [11] 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.
- [12] S. Konyagin, ‘Arithmetic properties of integers with missing digits: distribution in residue classes’, *Periodica Math. Hungar.*, **42** (2001), 145–162.
- [13] 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.

- [14] S. V. Konyagin and I. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.
- [15] N. M. Korobov, ‘On the distribution of digits in periodic fractions’, *Mathem. Sbornik*, **89** (1972), 654–670 (in Russian).
- [16] N. M. Korobov, *Exponential sums and their applications*, Kluwer, Dordrecht, North Holland, 1992.
- [17] C. Mauduit and A. Sárközy, ‘On the arithmetic structure of sets characterized by sum of digits properties’, *J. Number Theory*, **61** (1996), 25–38.
- [18] C. Mauduit and A. Sárközy, ‘On the arithmetic structure of the integers whose sum of digits is fixed’, *Acta Arith.*, **81** (1997), 145–173.
- [19] C. Mauduit and A. Sárközy, ‘On finite pseudorandom binary sequences 1: Measure of pseudorandomness, the Legendre symbol’, *Acta Arith.*, **82** (1997), 365–377.
- [20] H. Niederreiter, ‘Quasi-Monte Carlo methods and pseudo-random numbers’, *Bull. Amer. Math. Soc.*, **84** (1978), 957–1041.
- [21] S. B. Stečkin, ‘An estimate of a complete rational exponential sum’, *Proc. Math. Inst. Acad. Sci. USSR*, Moscow, **143** (1977), 188–207 (in Russian).
- [22] A. Weil, *Basic number theory*, Springer-Verlag, New York, 1974.
- [23] H. B. Yu, ‘Estimates of character sums with exponential function’, *Acta Arith.*, **97** (2001), 211–218.