Rev. Mat. Iberoam. 38 (2022), no. 6, 1901–1925
DOI 10.4171/RMI/1316

On digits of Mersenne numbers

Bryce Kerr, László Mérai and Igor E. Shparlinski

Abstract. Motivated by recently developed interest to the distribution of q-ary digits of Mersenne numbers $M_p = 2^p - 1$, where p is prime, we estimate rational exponential sums with M_p, $p \leqslant X$, modulo a large power of a fixed odd prime q. In turn this immediately implies the normality of strings of q-ary digits amongst about $(\log X)^{3/2+o(1)}$ rightmost digits of M_p, $p \leqslant X$. Previous results imply this only for about $(\log X)^{1+o(1)}$ rightmost digits.

1. Introduction

1.1. Overview

Recently, Cai, Faust, Hildebrand, Li and Zhang [4] have considered various questions on the patterns in leading q-ary digits of *Mersenne numbers* $M_p = 2^p - 1$, where p is prime, see also [5, 10] for some other related questions. In particular, one can find in [4] some numerical results which suggest the leftmost q-ary digits of Mersenne numbers obey the so-called *Benford law*. It has also been mentioned in [4], see Remark 4.4 and Section 7, that the bounds of exponential sums with fractions M_p/m for a large integer m such as in [1, 2] can be used to extract some nontrivial information about the distribution of the rightmost digits of M_p. This conclusion in [4] is based on bounds of exponential sums with an arbitrary modulus m. However, for the case q-ary digits only moduli of the form $m = q^\gamma$ with an integer γ are of interest. Here we show that indeed for such moduli, using some ideas of Korobov [12], one can obtain much stronger results. To emphasise the ideas, we consider the case when q is prime, although there is no doubt that the method extends to any q without too much loss in its power.

For example, our bounds of exponential sums immediately imply the following equidistribution results for q-ary digits of M_p. For any fixed real $\varepsilon > 0$ and for any positive integers $s \leqslant r \leqslant (\log X)^{3/2-\varepsilon}$, on rightmost q-ary positions $r, \ldots, r-s+1$ of M_p, $p \leqslant X$, any block of q-ary digits of length s appears asymptotically the same number of times, that is, $(q^{-s} + o(1))\pi(X)$, where, as usual, $\pi(X)$ denotes the number of primes $p \leqslant X$, see Theorem 1.3.

The generic results of [1, 2] imply this only for positions which are much closer to the right end, namely, only for $r \leqslant c \log X$ for some absolute constant $c > 0$.

2020 Mathematics Subject Classification: 11A63, 11B83, 11L07.
Keywords: Mersenne numbers, q-ary digits, exponential sums.

Let m be an arbitrary natural number, and let a and g be integers that are coprime to m. In this paper, we study exponential sums of the form

$$S_m(a;X) = \sum_{n \leqslant X} \Lambda(n)\, \mathbf{e}_m(ag^n), \tag{1.1}$$

where $\mathbf{e}_m$ is the additive character modulo m defined by

$$\mathbf{e}_m(t) = \exp(2\pi i t/m) \quad (t \in \mathbb{R}),$$

and Λ is the *von Mangoldt function*:

$$\Lambda(n) = \begin{cases} \log p & \text{if } n \text{ is a power of the prime } p, \\ 0 & \text{otherwise.} \end{cases}$$

The sums (1.1) are introduced in Banks et al. [1], where it is shown that

$$\max_{(a,m)=1} |S_m(a;X)| \leqslant \left(X\tau^{-11/32} m^{5/16} + X^{5/6}\tau^{5/48} m^{7/24}\right) X^{o(1)},$$

as $X \to \infty$, where $\tau = \operatorname{ord}_m g$ denotes the multiplicative order of g modulo m, that is, the smallest natural number k such that $g^k \equiv 1 \bmod m$.

Using an idea of Garaev [9] to handle double sums over certain hyperbolic regions, the stronger bound

$$\max_{(a,m)=1} |S_m(a;X)| \leqslant \left(X\tau^{-11/32} m^{5/16} + X^{4/5}\tau^{1/8} m^{7/20}\right) X^{o(1)}$$

is established in Banks et al. [2]. Note that, for either of the above bounds to be nontrivial, one must have $\tau \geqslant m^{10/11} X^{o(1)}$ (to control the first term), hence also

$$m \leqslant X^{22/51+o(1)}$$

(to control the second term), as $X \to \infty$. For shorter sums, new ideas are needed.

In the present paper, we study the exponential sums $S_m(a;X)$ in the special case that $m = q^\gamma$ for some fixed prime q. Our aim is to establish nontrivial bounds for short sums in which X is smaller than the modulus m. Our approach relies on an idea of Korobov [12], coupled with the use of Vinogradov's mean value theorem in the explicit form given by Ford [8].

1.2. Statement of results

Since our main motivation comes from applications to Mersenne numbers, we always assume that $q \geqslant 3$, which simplifies the formulas in Section 2.3 (and can easily be avoided at the cost of some small typographical changes).

Theorem 1.1. *Fix a prime $q \geqslant 3$ and an integer $g \geqslant 2$ not divisible by q. Let γ be a positive integer and let $A > 0$ be an arbitrary constant. Suppose that X satisfies*

$$2 \leqslant X \leqslant q^{A\gamma}. \tag{1.2}$$

Then, for all integers a with $\gcd(a,q)=1$*, we have*

$$\left|S_{q^\gamma}(a;X)\right| \leqslant c(g,q,A)\left(X^{1-\delta(A)\rho^2}\log X + Xq^{-\delta(A)\gamma}\right),$$

where $\delta(A)>0$ *is a constant depending only on* A*,*

$$\rho = \frac{\log X}{\log q^\gamma}, \tag{1.3}$$

and $c(g,q,A)$ *depends only on* g*,* q *and* A*.*

We remark that Theorem 1.1 is nontrivial in the range

$$q^{A\gamma} \geqslant X \geqslant q^{\gamma^{2/3+\varepsilon}},$$

for an arbitrary small $\varepsilon>0$, provided that X is large enough, and with $g=2$ yields (via partial summation) a nontrivial bound on exponential sums with Mersenne numbers $M_p = 2^p-1$, p prime.

Corollary 1.2. *For a prime* $q\geqslant 3$ *and a real* X *satisfying* (1.2)*, we have*

$$\max_{(a,q)=1}\left|\sum_{\substack{p\leqslant X\\ p \text{ prime}}} \mathbf{e}_{q^\gamma}(aM_p)\right| \leqslant c(q,A)\left(X^{1-\delta_0(A)\rho^2} + Xq^{-\delta_0(A)\gamma}\right),$$

where $\delta_0(A)>0$ *is a constant depending only on* A*,* ρ *is as in* (1.3) *and* $c(q,A)$ *depends only on* q *and* A*.*

We are now able to address the question of distribution of rightmost digits of Mersenne numbers. Given a string σ of s digits to base q,

$$\sigma = (a_{s-1},\dots,a_0) \in \{0,\dots,q-1\}^s, \tag{1.4}$$

we denote by $A_r(X,\sigma)$ the number of primes $p\leqslant X$ such that M_p written in base q has σ as the string on s consecutive digits on positions $r,\dots,r-s+1$, counting from the right to the left, where the numbering starts with zero.

We recall that by the prime number theorem (in a very crude form) we have $\pi(X) = (1+o(1))X/\log X$ as $X\to\infty$.

Theorem 1.3. *For a fixed prime* $q\geqslant 3$*, a real* $\varepsilon>0$ *and a string* σ *of length* s *of the form* (1.4)*, uniformly over* $\varepsilon\log X\leqslant r\leqslant(\log X)^{3/2-\varepsilon}$ *and strings* σ *of length* s *of the form* (1.4) *we have*

$$A_r(X,\sigma) = (q^{-s}+o(1))\,\pi(X)$$

as $X\to\infty$*.*

We remark that the lower bound on r can be relaxed, but a condition of this kind is necessary. For example, if 2 is not a primitive root modulo q, the distribution of digits on the rightmost positions cannot be uniform.

2. Preliminaries

2.1. Notation

Throughout the paper, $\mathbb{N}$ is the set of positive integers. The letters k, m and n (with or without subscripts) are always used to denote positive integers; the letter q (with or without subscripts) is always used to denote a prime.

Given a prime q, let ν_q denote the *standard q-adic valuation*. In particular, for every $n \in \mathbb{Z} \setminus \{0\}$ one has $\nu_q(n) = k$, where k is the largest nonnegative integer for which $q^k \mid n$.

Given a sequence of complex weights

$$\boldsymbol{\gamma} = (\gamma_h)_{h \in \mathcal{H}}$$

supported on a finite set $\mathcal{H}$ and $\vartheta \geqslant 1$, we define norms of $\boldsymbol{\gamma}$ in the usual way:

$$\|\boldsymbol{\gamma}\|_\infty = \max_{h \in \mathcal{H}} |\gamma_h| \quad \text{and} \quad \|\boldsymbol{\gamma}\|_\vartheta = \Big(\sum_{h \in \mathcal{H}} |\gamma_h|^\vartheta \Big)^{1/\vartheta}.$$

For given functions F and G, the notations $F \ll G$, $G \gg F$ and $F = O(G)$ are all equivalent to the statement that the inequality $|F| \leqslant c|G|$ holds with some constant $c > 0$. Throughout the paper, any implied constants in symbols O, $\ll$ and $\gg$ may depend on the parameters q and A, and are *absolute* unless specified otherwise.

We write $F \asymp G$ to indicate that $F \ll G$ and $G \ll F$ both hold.

Finally, we use $\#\mathcal{S}$ to denote the cardinality of a finite set $\mathcal{S}$.

2.2. Sums over primes

It is convenient to use a form of *Vaughan's identity* given by the equation (6) in Chapter 24 of [6].

Lemma 2.1. *For any complex-valued function $f(n)$ with $|f(n)| \leqslant 1$ and any real numbers $1 < U, V \leqslant X$ with $UV \leqslant X$, we have*

$$\sum_{n \leqslant X} \Lambda(n) f(n) \ll U + \Sigma_1 \log X + \Sigma_2^{1/2} X^{1/2} (\log X)^3,$$

where

$$\Sigma_1 = \sum_{t \leqslant UV} \max_{w \leqslant X/t} \Big| \sum_{w \leqslant m \leqslant X/t} f(mt) \Big|,$$

$$\Sigma_2 = \max_{U \leqslant w \leqslant X/V} \max_{V \leqslant j \leqslant X/w} \sum_{V < m \leqslant X/w} \Big| \sum_{\substack{w < n \leqslant 2w \\ n \leqslant X/m \\ n \leqslant X/j}} f(jn) \overline{f}(mn) \Big|.$$

2.3. Multiplicative order of integers

Fix a prime $q \geqslant 3$ and an integer $g \neq \pm 1$ with $\gcd(g, q) = 1$. For every $n \in \mathbb{N}$, let $\tau_n = \mathrm{ord}_{q^n} g$ denote the order of g modulo q^n. We write

$$g^{\tau_n} = 1 + h_n q^{n + \mathfrak{g}_n} \quad (n \in \mathbb{N}), \tag{2.1}$$

with some uniquely determined integers h_n and $\mathfrak{g}_n \geqslant 0$ such that $\gcd(h_n, q) = 1$. We also put

$$\tau = \tau_1 \quad \text{and} \quad G = \mathfrak{g}_1 + 1 = \nu_q(g^\tau - 1). \tag{2.2}$$

A simple argument shows

$$\mathfrak{g}_n = \begin{cases} G - n & \text{if } n \leqslant G, \\ 0 & \text{if } n \geqslant G, \end{cases} \quad \text{and} \quad \tau_n = \begin{cases} \tau & \text{if } n \leqslant G, \\ q^{n-G}\,\tau & \text{if } n \geqslant G. \end{cases} \tag{2.3}$$

The following two statements are easy consequences of (2.3).

Lemma 2.2. *For $r \geqslant s \geqslant G$, we have*

$$g^{n_1\tau_s} \equiv g^{n_2\tau_s} \bmod q^r \quad \Longleftrightarrow \quad q^{r-s} \mid (n_1 - n_2).$$

Lemma 2.3. *For $m \in \mathbb{N}$ and nonnegative integers x and y with $x \neq y$, either $q \nmid g^{mx} - g^{my}$, or*

$$\nu_q(g^{mx} - g^{my}) = \nu_q(x - y) + \nu_q(m) + G.$$

Proof. Put $\tau_0 = 1$. For any integer $n \geqslant 0$, we have that $q^n \mid g^{mx} - g^{my}$ if and only if $mx \equiv my \bmod \tau_n$. Consequently,

$$\nu_q(g^{mx} - g^{my}) = \max\{n \geqslant 0 : \ \tau_n \mid m(x - y)\},$$

and the result follows from (2.3) as $\gcd(\tau, q) = 1$. ■

2.4. Explicit form of the Vinogradov mean value theorem

Let $N_{r,k}(P)$ be the number of integral solutions to the system of equations

$$n_1^j + \cdots + n_r^j = m_1^j + \cdots + m_r^j \quad (1 \leqslant j \leqslant k,\ 1 \leqslant n_\ell, m_\ell \leqslant P).$$

Our application of Lemma 2.5 below requires a precise form of the Vinogradov mean value theorem. For this purpose, we use a fully explicit version due to Ford (Theorem 3 in [8]), which is presented here in a weakened and simplified form.

Lemma 2.4. *For any integer $k \geqslant 129$, there is an integer $r \in [2k^2, 4k^2]$ such that for $P > 0$,*

$$N_{r,k}(P) \leqslant k^{3k^3} P^{2r - k(k+1)/2 + k^2/1000}.$$

We note that the condition $r \geqslant 2k^2$ is not explicit in Theorem 3 of [8], but we can always impose this in view of the well-known (and essentially trivial) monotonicity property

$$N_{r+1,k}(P)\, P^{-2(r+1)} \leqslant N_{r,k}(P)\, P^{-2r}.$$

We also observe that the recent striking advances in the Vinogradov mean value theorem due to Bourgain, Demeter and Guth [3] and Wooley [14] are not suitable for our purposes here, as they contain implicit constants that depend on r and k, whereas in our approach r and k grow together with P. On the other hand, a result of Steiner [13] may perhaps be used to improve numerical constants in our estimates in some ranges of parameters.

2.5. Double exponential sums with polynomials

Our main tool to bound the exponential sum $S_m(a, X)$ is the following variation of a result of Korobov (Lemma 3 in [12]); examining the proof of that lemma, one can easily see that one can add complex weights $\alpha(x)$ and $\beta(y)$ without any changes in the proof.

It is convenient to denote

$$\mathbf{e}(t) = \exp(2\pi i t) \quad (t \in \mathbb{R}).$$

Lemma 2.5. *Let $\xi_j \in \mathbb{R}$, for $j = 1, \dots, k$, and suppose that each ξ_j has a rational approximation such that*

$$\left|\xi_j - \frac{b_j}{q_j}\right| \leqslant \frac{1}{q_j^2} \quad \text{with } b_j \in \mathbb{Z},\ q_j \in \mathbb{N}, \text{ and } (b_j, q_j) = 1.$$

Then, for any natural number r and sequences of complex numbers $\alpha(x), \beta(y)$ satisfying

$$|\alpha(x)|, |\beta(y)| \leqslant 1,$$

the sum

$$S = \sum_{x,y=1}^{P} \alpha(x)\beta(y)\,\mathbf{e}(\xi_1 xy + \cdots + \xi_k x^k y^k)$$

admits the upper bound

$$|S|^{2r^2} \leqslant \left(64r^2 \log(3Q)\right)^{k/2} P^{4r^2-2r} N_{r,k}(P) \prod_{j=1}^{k} \min\left\{P^j, P^j q_j^{-1/2} + q_j^{1/2}\right\},$$

where

$$Q = \max_{1 \leqslant j \leqslant k} \{q_j\}.$$

The following result follows from the standard completing technique, see Section 12.2 of [11].

Lemma 2.6. *For an arbitrary function $f\colon \mathbb{R} \to \mathbb{R}$, an interval $\mathcal{I}$ of length N, and integers U and V satisfying*

$$UV \leqslant N/2,$$

there exists some $\alpha \in \mathbb{R}$ such that

$$\sum_{x \in \mathcal{I}} \mathbf{e}(f(x)) \ll \frac{\log N}{UV} \sum_{x \in \mathcal{J}} \sum_{u \leqslant U} \left| \sum_{v \leqslant V} \mathbf{e}(f(x + uv) + \alpha v) \right|,$$

where $\mathcal{J}$ is some interval of length $2N$.

Proof. It is enough to write

$$\sum_{x \in \mathcal{I}} \mathbf{e}(f(x)) = \sum_{\substack{x \in \mathcal{J} \\ x + uv \in \mathcal{I}}} \mathbf{e}(f(x + uv))$$

and the use of the completing technique from Section 12.2 of [11] to encode the condition $x + uv \in \mathcal{I}$ into linear exponential sums, and the use of the bound (8.6) in [11]. ∎

2.6. Bilinear forms with exponential functions

Fix a prime q and an integer $g \neq \pm 1$ with $\gcd(q, g) = 1$. We denote by τ_n the order of g modulo q^n, and recall how G is defined in (2.2).

The following result is the main ingredient for Theorem 1.1. It uses some ideas of Korobov [12], Theorem 4.

Proposition 2.7. *Let $\gamma \in \mathbb{N}$ with $\gamma > 16G$. Given integers $K, L \geqslant 0$ and $M, N \geqslant 1$ with*

$$M \leqslant q^{2\gamma/65},$$

two sequences of complex weights

$$\boldsymbol{\alpha} = (\alpha_m)_{m=K+1}^{K+M} \quad \text{and} \quad \boldsymbol{\beta} = (\beta_n)_{n=L+1}^{L+N}$$

and an integer z not divisible by q, for the sum

$$S = \sum_{m=K+1}^{K+M} \sum_{n=L+1}^{L+N} \alpha_m \beta_n \, \mathbf{e}_{q^\gamma}(z g^{mn}),$$

we have

$$S \ll \|\boldsymbol{\alpha}\|_2 \, \|\boldsymbol{\beta}\|_\infty \left(M^{1/2-10^{-10}\rho^2} N \log M + M^{1/2} N^{1/2}\right) + \|\boldsymbol{\alpha}\|_\infty \, \|\boldsymbol{\beta}\|_\infty \, N q^{8G},$$

where

$$\rho = \frac{\log M}{\log q^\gamma}.$$

Proof. To simplify the notation, we write

$$\mathcal{M} = \{K+1, \ldots, K+M\} \quad \text{and} \quad \mathcal{N} = \{L+1, \ldots, L+N\}.$$

First note we may assume

$$M \geqslant (\log q^\gamma)^{32}, \tag{2.4}$$

as otherwise

$$M^{\rho^2} \ll 1,$$

and hence for the first term in the bound for S,

$$\|\boldsymbol{\alpha}\|_2 \, \|\boldsymbol{\beta}\|_\infty \, M^{1/2-10^{-10}\rho^2} N \log M \gg \|\boldsymbol{\alpha}\|_2 \, \|\boldsymbol{\beta}\|_\infty \, M^{1/2} N \log M,$$

which is worse than trivial. If

$$M \leqslant q^{8G},$$

then we have

$$S \leqslant \sum_{m=K+1}^{K+M} \sum_{n=L+1}^{L+N} |\alpha_m| |\beta_n| \leqslant \|\boldsymbol{\alpha}\|_\infty \, \|\boldsymbol{\beta}\|_\infty \, N q^{8G}.$$

Hence we may assume

$$M \geqslant q^{8G}.$$

By the Cauchy–Schwarz inequality,

$$\begin{aligned}(2.5)\quad |S|^2 &\leqslant \|\boldsymbol{\alpha}\|_2^2 \sum_{m\in\mathcal{M}} \Big|\sum_{n\in\mathcal{N}} \beta_n\, \mathbf{e}_{q^\gamma}(zg^{mn})\Big|^2 \leqslant \|\boldsymbol{\alpha}\|_2^2 \sum_{n_1,n_2\in\mathcal{N}} |\beta_{n_1}||\beta_{n_2}||S(n_1,n_2)| \\ &\leqslant \|\boldsymbol{\alpha}\|_2^2\, \|\boldsymbol{\beta}\|_\infty^2 \sum_{n_1,n_2\in\mathcal{N}} |S(n_1,n_2)|,\end{aligned}$$

where

$$S(n_1,n_2) = \sum_{m\in\mathcal{M}} \mathbf{e}_{q^\gamma}(z(g^{n_1m} - g^{n_2m})).$$

Recall we are assuming

$$(2.6)\qquad \rho \leqslant \frac{2}{65}.$$

Define s by

$$(2.7)\qquad s = \left\lfloor \frac{\rho\gamma}{8} \right\rfloor = \left\lfloor \frac{1}{8}\frac{\log M}{\log q} \right\rfloor \geqslant G,$$

so that from (2.3), we have

$$(2.8)\qquad \tau_s \leqslant q^s \leqslant M^{1/8},$$

and

$$(2.9)\qquad q^s > \frac{M^{1/8}}{q} \gg M^{1/8},$$

with implied constant depending on q. To establish the desired result, we bound $S(n_1,n_2)$ in different ways as the pair (n_1,n_2) varies over $\mathcal{N}\times\mathcal{N}$.

We denote

$$\begin{aligned}\mathcal{A}_1 &= \{(n_1,n_2)\in\mathcal{N}\times\mathcal{N} : \nu_q(n_1) > s \text{ or } \nu_q(n_2) > s\},\\ \mathcal{A}_2 &= \{(n_1,n_2)\in\mathcal{N}\times\mathcal{N} : g^{n_1\tau_s} \equiv g^{n_2\tau_s} \bmod q^{2s}\},\\ \mathcal{A}_3 &= (\mathcal{N}\times\mathcal{N})\setminus(\mathcal{A}_1\cup\mathcal{A}_2).\end{aligned}$$

Clearly,

$$\#\mathcal{A}_1 \leqslant 2N^2/q^s,$$

and Lemma 2.2 implies that

$$\#\mathcal{A}_2 \leqslant N^2/q^s + N.$$

Thus using the trivial bound $|S(n_1,n_2)| \leqslant M$ along with (2.9), we get that

$$(2.10)\qquad \sum_{j=1,2}\ \sum_{(n_1,n_2)\in\mathcal{A}_j} |S(n_1,n_2)| \ll \left(\frac{MN^2}{q^s} + MN\right) \ll (N^2M^{7/8} + MN).$$

For the final set $\mathcal{A}_3$, we need a nontrivial bound on $S(n_1, n_2)$. Let $(n_1, n_2) \in \mathcal{A}_3$ be fixed. Since $|S(n_1, n_2)| = |S(n_2, n_1)|$, without loss of generality we can assume

$$\nu_q(n_1) = a, \quad \nu_q(n_2) = b, \quad a \leqslant b \leqslant s. \tag{2.11}$$

With a and b fixed for the moment, it is convenient to define

$$k = \left\lfloor \frac{\gamma}{s+a} \right\rfloor \quad \text{and} \quad P = q^{s+a}. \tag{2.12}$$

Using the definition of s along with (2.6) and (2.8), we see that

$$k \geqslant 129 \quad \text{and} \quad P \leqslant q^{2s} \leqslant M^{1/4}. \tag{2.13}$$

Now put $\lambda = g^{n_1}$ and $\mu = g^{n_2}$, so that

$$S(n_1, n_2) = \sum_{m \in \mathcal{M}} \mathbf{e}_{q^\gamma}(z(\lambda^m - \mu^m)).$$

Using (2.1), (2.7) and (2.11), it is easy to see that the relations

$$\lambda^{\tau_s} = 1 + uq^{s+a} \quad \text{and} \quad \mu^{\tau_s} = 1 + vq^{s+b} \tag{2.14}$$

hold with some integers u, v coprime to q. Partitioning the summation over m into distinct residue classes modulo τ_s leads to the estimate

$$S(n_1, n_2) = S_0(n_1, n_2) + O(\tau_s) = S_0(n_1, n_2) + O(M^{1/8}) \tag{2.15}$$

by (2.8), where

$$S_0(n_1, n_2) = \sum_{x=1}^{\tau_s} \sum_{y \in \mathcal{Y}} \mathbf{e}_{q^\gamma}(z(\lambda^{x+\tau_s y} - \mu^{x+\tau_s y})),$$

and

$$\mathcal{Y} = (K/\tau_s, (K+M)/\tau_s] \cap \mathbb{Z}.$$

By (2.14) we have

$$\begin{aligned} \lambda^{x+\tau_s y} - \mu^{x+\tau_s y} &= \lambda^x (1 + uq^{s+a})^y - \mu^x (1 + vq^{s+b})^y \\ &= \lambda^x \sum_{i=0}^{y} \binom{y}{i} u^i q^{(s+a)i} - \mu^x \sum_{i=0}^{y} \binom{y}{i} v^i q^{(s+b)i} \\ &\equiv \lambda^x - \mu^x + \sum_{i=1}^{k} q^{(s+a)i} (\lambda^x u^i - \mu^x v^i q^{\Delta i}) \binom{y}{i} \mod q^\gamma, \end{aligned}$$

where we have put $\Delta = b - a$ (note that (2.12) is used in the last step); therefore,

$$|S_0(n_1, n_2)| \leqslant \sum_{x=1}^{\tau_s} \left| \sum_{y \in \mathcal{Y}} \mathbf{e}_{q^\gamma} \left(\sum_{i=1}^{k} q^{(s+a)i} (\lambda^x u^i - \mu^x v^i q^{\Delta i}) \binom{y}{i} \right) \right|.$$

We apply Lemma 2.6 with the function

$$f(y) = \sum_{i=1}^{k} q^{(s+a)i} (\lambda^x u^i - \mu^x v^i q^{\Delta i}) \binom{y}{i}$$

and parameters

$$U = V = P, \quad \mathcal{I} = \mathcal{Y},$$

and note that, by (2.8) and (2.13),

$$P^2 \leqslant M^{1/2} \leqslant M^{7/8} \leqslant \frac{M}{\tau_s} \leqslant \#\mathcal{Y} + 1.$$

It follows that

$$\begin{aligned} S_0(n_1, n_2) &\ll \frac{\log M}{P^2} \sum_{x=1}^{\tau_s} \sum_{y \in \mathcal{Z}} \sum_{z_1=1}^{P} \left| \sum_{z_2=1}^{P} \mathbf{e}(\alpha_x z_2)\, \mathbf{e}_{q^\gamma}(f(y + z_1 z_2)) \right| \\ &\ll \frac{\log M}{P^2} \sum_{x=1}^{\tau_s} \sum_{y \in \mathcal{Z}} \left| \sum_{z_1=1}^{P} \sum_{z_2=1}^{P} \mathbf{e}(\alpha_x z_2)\, \beta_{x,y}(z_1)\, \mathbf{e}_{q^\gamma}(f(y + z_1 z_2)) \right|, \end{aligned} \tag{2.16}$$

where $\mathcal{Z}$ is an interval of length $O(M/\tau_s)$ and α_x may depend on the variable x and $\beta_{x,y}$ may depend on the variables x and y and satisfies

$$|\beta_{x,y}(z_1)| = 1.$$

With the intention of applying Lemmas 2.4 and 2.5 to the right side of (2.16), we fix y for the moment and write

$$k!\, f(y + Z) = \sum_{j=0}^{k} a_j Z^j \quad (a_j \in \mathbb{Z}),$$

and for each $i = 1, \ldots, k$,

$$k!\, q^{(s+a)i} (\lambda^x u^i - \mu^x v^i q^{\Delta i}) \binom{y + Z}{i} = \sum_{j=1}^{i} a_{i,j} Z^j \tag{2.17}$$

with some $a_{i,j} \in \mathbb{Z}$. Clearly,

$$a_j = \sum_{i=j}^{k} a_{i,j},$$

and thus

$$\nu_q(a_j) \geqslant \min\{\nu_q(a_{i,j}) : i = j, \ldots, k\}. \tag{2.18}$$

Moreover, equality holds in (2.18) whenever

$$\nu_q(a_{j,j}) < \nu_q(a_{i,j}) \quad (i > j). \tag{2.19}$$

Denote

$$\bar{\nu} = \min\left\{\nu_q(\lambda^x u^j - \mu^x v^j q^{\Delta j}) : \ j = 1, \dots, k\right\},$$

and let $\bar{j}$ be an index for which

$$\nu_q(\lambda^x u^{\bar{j}} - \mu^x v^{\bar{j}} q^{\Delta \bar{j}}) = \bar{\nu}. \tag{2.20}$$

From (2.17) it is clear that

$$a_{\bar{j},\bar{j}} = \frac{k!}{\bar{j}!} q^{(s+a)\bar{j}} (\lambda^x u^{\bar{j}} - \mu^x v^{\bar{j}} q^{\Delta \bar{j}}),$$

and therefore

$$\nu_q(a_{\bar{j},\bar{j}}) = \nu_q(k!) - \nu_q(\bar{j}!) + (s+a)\bar{j} + \bar{\nu}. \tag{2.21}$$

On the other hand, (2.17) implies

$$\nu_q(a_{i,\bar{j}}) \geqslant \nu_q(k!) - \nu_q(i!) + (s+a)i + \bar{\nu} \quad (i > \bar{j}). \tag{2.22}$$

Before we proceed, we note that the estimate $\bar{j} < i \leqslant k < q^{s+a}$ holds since by (2.4), (2.7) and (2.12) we have

$$k \leqslant \frac{\gamma}{s} \leqslant \frac{2\gamma}{s+1} < \frac{16}{\rho} = \frac{16 \log q^{\gamma}}{\log M} \leqslant M^{1/32} < q^s \leqslant q^{s+a}. \tag{2.23}$$

This implies the inequality

$$(s+a)(i-\bar{j}) > \nu_q(i(i-1)\cdots(\bar{j}+1)) = \nu_q(i!) - \nu_q(\bar{j}!),$$

which together with (2.21) and (2.22) verifies the condition (2.19) for any $\bar{j}$ satisfying (2.20). Hence, (2.18) holds with equality, and thus we have

$$\nu_q(a_{\bar{j}}) = \nu_q(k!) - \nu_q(\bar{j}!) + (s+a)\bar{j} + \bar{\nu} \tag{2.24}$$

for any $\bar{j}$ satisfying (2.20).

If $\Delta > 0$, then clearly

$$\nu_q(\lambda^x u^j - \mu^x v^j q^{\Delta j}) = 0 \quad (j \geqslant 1).$$

For $\Delta = 0$ (that is, $a = b$), we claim that for any two consecutive indices j and $j+1$,

$$\nu_q(\lambda^x u^j - \mu^x v^j) = \bar{\nu} \quad \text{or} \quad \nu_q(\lambda^x u^{j+1} - \mu^x v^{j+1}) = \bar{\nu}. \tag{2.25}$$

To prove the claim, suppose on the contrary that

$$\lambda^x u^j \equiv \mu^x v^j \mod q^{\bar{\nu}+1} \quad \text{and} \quad \lambda^x u^{j+1} \equiv \mu^x v^{j+1} \mod q^{\bar{\nu}+1}$$

for some j. Then, dividing the second congruence by the first one, we get $u \equiv v \mod q^{\bar{\nu}+1}$ and thus

$$\lambda^x u^j \equiv \mu^x v^j \mod q^{\bar{\nu}+1} \quad \text{for all } j,$$

which contradicts the definition of $\bar{\nu}$.

Now let

$$\mathcal{J} = \bigl\{(k+1)/2 \leqslant j \leqslant k : \nu_q(\lambda^x u^j - \mu^x v^j q^\Delta) = \bar{\nu}\bigr\}.$$

In view of (2.25), this implies that $\#\mathcal{J} \geqslant \lfloor k/4 \rfloor$. Since $\lambda^x - \mu^x = g^{n_1 x} - g^{n_2 x}$ and $n_1 \neq n_2$ (in fact, $\nu_q(n_1 - n_2) < s$ by Lemma 2.2 since $(n_1, n_2) \notin \mathcal{A}_2$), by Lemma 2.3 and inequalities (2.7) and (2.8) we have

$$\nu_q(\lambda^x - \mu^x) = 0 \quad \text{or} \quad \nu_q(\lambda^x - \mu^x) = \nu_q(n_1 - n_2) + \nu_q(x) + G \leqslant 3s;$$

this implies that $\bar{\nu} \leqslant 3s$. Thus, for every $j \in \mathcal{J}$ we have by (2.24),

$$(s+a)j \leqslant \nu_q(a_j) \leqslant \nu_q(k!) + (s+a)j + 3s,$$

and so (recalling that $P = q^{s+a}$) we can write

$$\frac{a_j}{k!\,q^\gamma} = \frac{b_j}{q_j} \tag{2.26}$$

with

$$\gcd(b_j, q_j) = 1 \quad \text{and} \quad P^{-j} q^{\gamma - 3s} \leqslant q_j \leqslant k!\,P^{-j} q^\gamma. \tag{2.27}$$

We also define q_j by (2.26) for $j \notin \mathcal{J}$.

We are now in a position to apply Lemmas 2.4 and 2.5 in order to bound the double sum over z_1 and z_2 in (2.16). Writing

$$\begin{aligned} T &= \sum_{z_1, z_2 = 1}^{P} \beta_{x,y}(z_1)\,\alpha_x(z_2)\,\mathbf{e}_{q^\gamma}(f(y + z_1 z_2)) \\ &= \sum_{z_1, z_2 = 1}^{P} \beta_{x,y}(z_1)\,\alpha_x(z_2)\,\mathbf{e}\Bigl(\sum_{j=1}^{k} \frac{b_j}{q_j}(z_1 z_2)^j\Bigr), \end{aligned}$$

Lemma 2.5 shows that for any natural number r, the bound

$$|T|^{2r^2} \leqslant \bigl(64 r^2 \log(3Q)\bigr)^{k/2} P^{4r^2 - 2r} N_{r,k}(P) \prod_{j=1}^{k} \min\{P^j, P^j q_j^{-1/2} + q_j^{1/2}\}$$

holds with $Q = \max_{1 \leqslant j \leqslant k} q_j$. Note that (2.23) and (2.27) imply that

$$\log(3Q) \leqslant \log(3k!\,q^\gamma) \leqslant \gamma \log(kq) \leqslant \gamma k \log q$$

since for $129 \leqslant k \leqslant \gamma$ we have $3k! \leqslant k^k \leqslant k^\gamma$. Moreover, since $k \geqslant 129$ (see (2.13)), Lemma 2.4 shows that we can choose the integer $r \in [2k^2, 4k^2]$ so that

$$N_{r,k}(P) \leqslant k^{3k^3} P^{2r - k(k+1)/2 + k^2/1000}.$$

Hence we find that

$$|T|^{2r^2} \leqslant \bigl(1024 \gamma k^5 \log q\bigr)^{k/2} k^{3k^3 + 3k} P^{4r^2 - k(k+1)/2 + k^2/1000} R, \tag{2.28}$$

where

$$R = \prod_{j=1}^{k} \min\left\{P^j, P^j q_j^{-1/2} + q_j^{1/2}\right\} = P^{k(k+1)/2} \prod_{j=1}^{k} \min\left\{1, q_j^{-1/2} + P^{-j} q_j^{1/2}\right\}.$$

For any $j \in \mathcal{J}$ we have $j \geqslant (k+1)/2$. Recalling (2.12), we have

$$P^{-j} \leqslant P^j q^{-\gamma};$$

thus, using (2.27) we see that

$$q_j^{-1/2} + P^{-j} q_j^{1/2} \leqslant P^{j/2} q^{-\gamma/2+3s/2} + (k!)^{1/2} P^{j/2} q^{-\gamma/2} \leqslant k^k P^{j/2} q^{-\gamma/2+3s/2}.$$

For $j \notin \mathcal{J}$, we use the trivial bound

$$\min\left\{1, q_j^{-1/2} + P^{-j} q_j^{1/2}\right\} \leqslant 1.$$

Therefore, recalling that $\#\mathcal{J} \geqslant \lfloor k/4 \rfloor$, and using the bounds

$$0.24k < \lfloor k/4 \rfloor \leqslant k/4 \quad \text{and} \quad \sum_{j=k-\lfloor k/4 \rfloor+1}^{k} j/2 < 0.11k^2,$$

which hold for $k \geqslant 129$, we see that

$$\begin{aligned} R &\leqslant P^{k(k+1)/2} \prod_{j \in \mathcal{J}} \left(k^k P^{j/2} q^{-\gamma/2+3s/2}\right) \leqslant k^{k^2} P^{k(k+1)/2} \prod_{j=k-\lfloor k/4 \rfloor+1}^{k} \left(P^{j/2} q^{-\gamma/2+3s/2}\right) \\ &\leqslant k^{k^2} P^{k(k+1)/2+0.11k^2} q^{-0.12\gamma k+3sk/8}. \end{aligned}$$

Combining this bound with (2.28), we deduce that

$$|T| \leqslant (ABC)^{1/2r^2} P^2, \tag{2.29}$$

where

$$A = 2^{5k} k^{3k^3+k^2+11k/2}, \quad B = (\gamma \log q)^{k/2} \quad \text{and} \quad C = P^{0.111k^2} q^{-0.12\gamma k+3sk/8}.$$

Since $r \geqslant 2k^2$, it is clear that

$$A^{1/2r^2} \ll 1. \tag{2.30}$$

Next, since $k \asymp \gamma/s \asymp \rho^{-1}$, we have

$$\gamma \log q = \rho^{-1} \log M \ll k \log M,$$

hence

$$B^{1/2r^2} \ll (k \log M)^{1/8k^4} \ll \log M. \tag{2.31}$$

Recalling (2.7) and (2.12), we have

$$\frac{\gamma}{s+a} - 1 < k \leqslant \frac{\gamma}{s+a} \quad \text{and} \quad \frac{\gamma}{s} \geqslant \frac{8}{\rho},$$

and using (2.7), we get that

$$\frac{\log C}{\log q} = 0.111(s+a)k^2 - 0.12\gamma k + 3sk/8 \leqslant -\frac{0.009\gamma^2}{s+a} + 0.12\gamma + \frac{3s\gamma}{8(s+a)}$$
$$\leqslant -\frac{0.009\gamma^2}{s} + 0.12\gamma + \frac{3\gamma}{8} \leqslant -\frac{0.036\gamma}{\rho} + 0.495\gamma \leqslant -\frac{0.02\gamma}{\rho},$$

where we have used the inequality $\rho \leqslant 2/65$ in the last step; thus,

$$C \leqslant M^{-0.02/\rho^2}. \tag{2.32}$$

Since

$$r \leqslant 4k^2,$$

we have

$$\frac{0.02}{2r^2\rho^2} \geqslant \frac{1}{1600\rho^2 k^4}, \tag{2.33}$$

and from (2.7) and (2.12),

$$k \leqslant \frac{\gamma}{s+a} \leqslant \frac{\gamma}{\rho\gamma/8 - 1}. \tag{2.34}$$

Since

$$\rho\gamma = \frac{\log M}{\log q},$$

and we allow the implied constant in the statement of Proposition 2.7 to depend on q, we may assume that $M \geqslant q^{16}$ and thus

$$\rho\gamma \geqslant 16,$$

which combined with (2.34) implies

$$k \leqslant \frac{16}{\rho},$$

and hence by (2.33),

$$\frac{0.02}{2r^2\rho^2} \geqslant \frac{1}{1600k^4\rho^2} \geqslant \frac{1}{25 \cdot 2^{22}}\rho^2 \geqslant 10^{-9}\rho^2.$$

Substituted in (2.32), this gives

$$C^{1/2r^2} \leqslant M^{-10^{-9}\rho^2}.$$

Combining the above with (2.29), (2.30) and (2.31) we get

$$T \ll P^2 M^{-10^{-9}\rho^2} \log M.$$

Inserting the previous bound into (2.16) and using (2.13), we have

$$S_0(n_1,n_2) \ll \tau_s\,\#\mathcal{Y}\,M^{-10^{-9}\rho^2}(\log M)^2 \ll M^{1-10^{-9}\rho^2}(\log M)^2,$$

since

$$\tau_s\,\#\mathcal{Y} \ll M.$$

Combining with (2.15) implies that

$$S(n_1,n_2) \ll M^{1-10^{-9}\rho^2}(\log M)^2. \tag{2.35}$$

Now (2.5), (2.10) and (2.35) together yield the bound

$$S \ll \|\boldsymbol{\alpha}\|_2\,\|\boldsymbol{\beta}\|_\infty\,N\,M^{1/2-10^{-10}\rho^2}\log M + \|\boldsymbol{\alpha}\|_2\,\|\boldsymbol{\beta}\|_\infty\left(M^{7/16}N + M^{1/2}N^{1/2}\right),$$

and since $M^{7/16}N$ never dominates the term $NM^{1/2-10^{-10}\rho^2}\log M$, we obtain the desired result. ∎

We can remove the condition $M \leqslant q^{2\gamma/65}$ in Proposition 2.7 by partitioning the summation over M into short intervals. This is necessary for applications to Theorem 1.3, where we need to consider both long and short ranges of the parameter M.

Corollary 2.8. *Let* $\gamma \in \mathbb{N}$ *with* $\gamma > 16G$ *and let* $A > 0$ *be arbitrary. Given integers* $K, L \geqslant 0$ *and* $M, N \geqslant 1$ *with*

$$M \leqslant q^{A\gamma}, \tag{2.36}$$

two sequences of complex weights

$$\boldsymbol{\alpha} = (\alpha_m)_{m=K+1}^{K+M} \quad \text{and} \quad \boldsymbol{\beta} = (\beta_n)_{n=L+1}^{L+N}$$

and an integer z *not divisible by* q*, for the sum*

$$S = \sum_{m=K+1}^{K+M}\sum_{n=L+1}^{L+N}\alpha_m\,\beta_n\,\mathbf{e}_{q^\gamma}(zg^{mn}),$$

we have

$$S \ll \|\boldsymbol{\alpha}\|_2\,\|\boldsymbol{\beta}\|_\infty\left(M^{1/2-c\rho^2}N\log M + M^{1/2}N^{1/2}\right) + \left(1 + \frac{M}{q^{2\gamma/65}}\right)\|\boldsymbol{\alpha}\|_\infty\,\|\boldsymbol{\beta}\|_\infty\,Nq^{8G},$$

where

$$\rho = \frac{\log M}{\log q^\gamma}$$

and $c > 0$ *is a constant depending on* A*.*

Proof. By Proposition 2.7, we may assume $M \geqslant q^{2\gamma/65}$, and by modifying the coefficients $\boldsymbol{\alpha}$ (appending them with at most $\lfloor q^{2\gamma/65}\rfloor$ zeros), we may assume

$$M = JM_0, \quad \text{with} \quad M_0 = \lfloor q^{2\gamma/65}\rfloor \tag{2.37}$$

for some integer $J \geqslant 1$. Subdividing S into J sums,

$$S_j = \sum_{m=K+1+M_0 j}^{K+M_0(j+1)} \sum_{n=L+1}^{L+N} \alpha_m \beta_n \mathbf{e}_{q^\gamma}(z g^{mn}),$$

by the the Cauchy–Schwarz inequality and Proposition 2.7 (applied for each $0 \leqslant j \leqslant J-1$), and denoting

$$\rho_0 = \frac{\log M_0}{\log q^\gamma}, \tag{2.38}$$

we obtain

$$\begin{aligned}
|S|^2 &\leqslant J \sum_{j=0}^{J-1} |S_j|^2 \\
&\ll J\|\boldsymbol{\beta}\|_\infty^2 \sum_{j=0}^{J-1} \sum_{m=K+1+M_0 j}^{K+M_0(j+1)} |\alpha_m|^2 \left(M_0^{1-2\cdot 10^{-10}\rho_0^2} N^2 \log^2 M + q^{2\gamma/65} N\right) \\
&\quad + J^2 \|\boldsymbol{\alpha}\|_\infty^2 \|\boldsymbol{\beta}\|_\infty^2 N^2 q^{16G} \\
&\ll \|\boldsymbol{\alpha}\|_2^2 \|\boldsymbol{\beta}\|_\infty^2 \left(J q^{2\gamma(1-2\cdot 10^{-10}\rho_0^2)/65} N^2 \log^2 M + J q^{2\gamma/65} N\right) \\
&\quad + J^2 \|\boldsymbol{\alpha}\|_\infty^2 \|\boldsymbol{\beta}\|_\infty^2 N^2 q^{16G} \\
&\ll \|\boldsymbol{\alpha}\|_2^2 \|\boldsymbol{\beta}\|_\infty^2 \left(M q^{-2\cdot 10^{-10}\gamma\rho_0^2/65} N^2 \log^2 M + MN\right) + \|\boldsymbol{\alpha}\|_\infty^2 \|\boldsymbol{\beta}\|_\infty^2 N^2 \frac{q^{16G} M^2}{q^{4\gamma/65}}.
\end{aligned}$$

By (2.36), (2.37) and (2.38), we have

$$q^{10^{10}\gamma\rho_0^2} \geqslant M^{c\rho^2},$$

for some constant c depending on A. Hence

$$|S| \ll \|\boldsymbol{\alpha}\|_2 \|\boldsymbol{\beta}\|_\infty \left(M^{1/2-c\rho^2} N \log^2 M + M^{1/2} N^{1/2}\right) + \|\boldsymbol{\alpha}\|_\infty \|\boldsymbol{\beta}\|_\infty N \frac{q^{8G} M}{q^{2\gamma/65}},$$

which completes the proof. ■

We now estimate double sums with variables limits of summation for one variable.

Lemma 2.9. *Let* $\gamma \in \mathbb{N}$ *with* $\gamma > 16G$ *and let* $A > 0$ *be arbitrary. Given integers* $M, N \geqslant 1$ *and* $L \geqslant 0$ *with*

$$M \leqslant q^{A\gamma},$$

two sequences

$$(K_m)_{m=1}^M \quad \text{and} \quad (N_m)_{m=1}^M$$

of nonnegative integers such that $K_m < N_m \leqslant N$ *for each* m*, two sequences of complex weights*

$$\boldsymbol{\alpha} = (\alpha_m)_{m=1}^M \quad \text{and} \quad \boldsymbol{\beta} = (\beta_n)_{n=1}^N$$

with

$$\|\boldsymbol{\alpha}\|_\infty, \|\boldsymbol{\beta}\|_\infty \ll 1$$

and an integer z *not divisible by* q*, for the sum*

$$\widetilde{S} = \sum_{m=L+1}^{L+M} \sum_{K_m \leqslant n \leqslant N_m} \alpha_m \beta_n \mathbf{e}_{q^\gamma}(zg^{mn})$$

we have

$$\widetilde{S} \ll \left(NM^{1-c\rho^2} + N^{1/2}M\right) \log M \log N + \left(1 + \frac{M}{q^{2\gamma/65}}\right) Nq^{8G} \log N,$$

where

$$\rho = \frac{\log M}{\log q^\gamma}$$

and $c > 0$ *is a constant depending on* A*.*

Proof. Using the standard completing technique, see, for example, Section 12.2 in [11] and the bound (8.6) in [11], it follows that

$$\widetilde{S} = \sum_{-N/2 < r \leqslant N/2} \frac{1}{|r|+1} \sum_{m=L+1}^{L+M} \sum_{n=1}^{N} \widetilde{\alpha}_{m,r} \widetilde{\beta}_{n,r} \mathbf{e}_{q^\gamma}(zg^{mn}),$$

where

$$\widetilde{\alpha}_{m,r} = \alpha_m \eta_{m,r} \quad \text{and} \quad \widetilde{\beta}_{n,r} = \beta_n \mathbf{e}_N(rn),$$

for some complex number $\eta_{m,r} \ll 1$. Applying Corollary 2.8 and noting that

$$\sum_{-N/2 < r \leqslant N/2} \frac{1}{|r|+1} \ll \log N,$$

we derive

$$\widetilde{S} \ll \left(NM^{1-c\rho^2} + N^{1/2}M\right) \log M \log N + \left(1 + \frac{M}{q^{2\gamma/65}}\right) Nq^{8G} \log N,$$

which completes the proof. ∎

2.7. Bounds on double exponential sums over hyperbolic domains

One of our main technical tool is the following result, which gives a bound on double exponential sums over certain "hyperbolic" regions of summation.

We recall the definition of G, given in (2.2).

Lemma 2.10. *Let* $\gamma \in \mathbb{N}$ *with* $\gamma > 16G$ *and* $A > 0$*. Given real numbers* $X, Y, Z \geqslant 1$ *with*

$$Z < Y \leqslant q^{A\gamma},$$

and a sequence $\boldsymbol{\beta} = (\beta_n)_{n \leqslant X/Z}$ *of complex numbers with*

$$\|\boldsymbol{\beta}\|_\infty \leqslant 1,$$

any sequences

$$(K_m)_{m=1}^{M} \quad \text{and} \quad (N_m)_{m=1}^{M}$$

of nonnegative integers such that $K_m < N_m \leqslant X/m$ *for each* m*, and any integer* z *coprime to* q*, we have*

$$\sum_{Z<m\leqslant Y} \Big| \sum_{K_m \leqslant n \leqslant N_m} \beta_n \, \mathbf{e}_{q^\gamma}(zg^{mn}) \Big|$$
$$\ll \big(XZ^{-c\zeta^2} + (YX)^{1/2}\big)(\log X)^2 + \Big(\frac{1}{Z} + \frac{1}{q^{2\gamma/65}}\Big) X q^{8G} \log X,$$

where

$$\zeta = \frac{\log Z}{\log q^\gamma} \tag{2.39}$$

and $c > 0$ *is a constant depending only* A*.*

Proof. Clearly there are complex numbers α_m such that $|\alpha_m| = 1$ for $Z < m \leqslant Y$ and $\alpha_m = 0$ otherwise, such that

$$\sum_{Z<m\leqslant Y} \Big| \sum_{K_m \leqslant n \leqslant N_m} \beta_n \, \mathbf{e}_{q^\gamma}(zg^{mn}) \Big| = \sum_{Z<m\leqslant Y} \alpha_m \sum_{K_m \leqslant n \leqslant N_m} \beta_n \, \mathbf{e}_{q^\gamma}(zg^{mn}).$$

Furthermore,

$$\sum_{Z<m\leqslant Y} \alpha_m \sum_{K_m \leqslant n \leqslant N_m} \beta_n \, \mathbf{e}_{q^\gamma}(zg^{mn})$$
$$= \sum_{\log Z - 1 \leqslant j \leqslant \log Y} \; \sum_{e^j < m \leqslant e^{j+1}} \; \sum_{K_m \leqslant n \leqslant N_m} \alpha_m \beta_n \, \mathbf{e}_{q^\gamma}(zg^{mn})$$

and we have set $\alpha_m = 0$ if $m \leqslant Z$ or $m \geqslant Y$. We observe that for each j within the summation range, we have

$$\frac{\log(e^{j+1} - e^j)}{\log q^\gamma} \geqslant \frac{\log(Z-1)}{\log q^\gamma} \geqslant \frac{\zeta}{2},$$

where ζ is given by (2.39). Hence

$$\sum_{e^j < m \leqslant e^{j+1}} \; \sum_{K_m \leqslant n \leqslant N_m} \alpha_m \beta_n \, \mathbf{e}_{q^\gamma}(zg^{mn})$$
$$\ll \Big(\frac{X}{e^j} e^{j(1-c\zeta^2/4)} + e^j \Big(\frac{X}{e^j}\Big)^{1/2}\Big)(\log X)^2 + \Big(1 + \frac{2^j}{q^{2\gamma/65}}\Big) \frac{X}{2^j} q^{8G} \log N$$

by Lemma 2.9, and the result follows after renaming c, summing the above over j satisfying $\log Z - 1 \leqslant j \leqslant \log Y$, and using the estimates

$$\sum_{\log Z \leqslant j \leqslant \log Y} e^{-\alpha j} \ll Z^{-\alpha} \quad \text{and} \quad \sum_{\log Z \leqslant j \leqslant \log Y} e^{j\alpha} \ll Y^\alpha.$$

provided $\alpha > 0$ is bounded away from 0. ■

2.8. Bounds on single exponential sums

We observe that combining Proposition 2.7 with Lemma 2.6 allows us to estimate sums over an interval which has previously been considered by Korobov [12], Theorem 4. We present a proof for completeness.

Lemma 2.11. *With notation as in* (2.2) *and Proposition* 2.7, *suppose* M *satisfies*

$$M \leqslant q^{2\gamma/65}.$$

Then we have

$$\sum_{m=K+1}^{K+M} \mathbf{e}_{q^\gamma}(zg^m) \ll M^{1-10^{-11}\rho^2}(\log M)^2 + M^{10^{-10}\rho^2} q^{8G}(\log M)^2,$$

where

$$\rho = \frac{\log M}{\log q^\gamma}\cdot$$

Proof. Let

$$S = \sum_{m=K+1}^{K+M} \mathbf{e}_{q^\gamma}(zg^m),$$

and apply Lemma 2.6 with

$$U = M^{1-10^{-10}\rho^2} \quad \text{and} \quad V = 0.5\,M^{10^{-10}\rho^2}$$

to get

$$S \ll \frac{\log N}{M} \sum_{m=K+1}^{K+M} \sum_{u \leqslant U} \Big| \sum_{v \leqslant V} \mathbf{e}(\alpha v)\, \mathbf{e}_{q^\gamma}(zg^m g^{uv}) \Big|.$$

Taking a maximum over m in the above, we get

$$S \ll \log M \sum_{u \leqslant U} \sum_{v \leqslant V} \alpha(u)\beta(v)\, \mathbf{e}_{q^\gamma}(z_0 g^{uv}),$$

for some $\gcd(z_0, p) = 1$ and complex numbers α, β satisfying

$$|\alpha(u)|, |\beta(v)| \leqslant 1.$$

With

$$\rho_0 = \frac{\log U}{\log q^\gamma},$$

we have

$$\rho_0 = \rho(1 - 10^{-10}\rho^2),$$

hence by Proposition 2.7,

$$\begin{aligned} S &\ll (\log M)^2 \left(V(U^{1-10^{-10}\rho_0^2} + q^{8G}) + UV^{1/2}\right) \\ &\ll (\log M)^2 M \left(M^{-10^{-10}\rho^2(1-10^{-10}\rho^2)^2} + M^{-\frac{1}{2}10^{-10}\rho^2}\right) + M^{10^{-10}\rho^2} q^{8G}(\log M)^2. \end{aligned}$$

Note the assumption

$$M \leqslant q^{2\gamma/65}$$

implies that

$$\rho \leqslant \frac{2}{65},$$

and hence

$$(1 - 10^{-10}\rho^2)^2 \geqslant \left(1 - 10^{-10}\left(\frac{2}{65}\right)^2\right)^2 \geqslant \frac{1}{10},$$

which completes the proof. ■

Partitioning the summation into small intervals as in the proof of Corollary 2.8 allows us again to remove the restriction $M \leqslant q^{2\gamma/65}$ in Lemma 2.11.

Corollary 2.12. *With notation as in* (2.2) *and Proposition* 2.7, *suppose* M *satisfies*

$$M \leqslant q^{A\gamma}.$$

Then we have

$$\sum_{m=K+1}^{K+M} \mathbf{e}_{q^\gamma}(zg^m) \ll M^{1-c\rho^2}\log M + M^{1-c}q^{8G},$$

where

$$\rho = \frac{\log M}{\log q^\gamma}$$

and $c > 0$ *is a constant depending only* A.

Proof. Arguing as in the proof of Corollary 2.8, we may partition the summation over m into intervals of length at most $q^{2\gamma/65}$ and apply Lemma 2.11 to each of these intervals. This produces a bound of the form

$$\sum_{m=K+1}^{K+M} \mathbf{e}_{q^\gamma}(zg^m) \ll M^{1-c\rho^2}(\log M)^2 + M^{1-c}q^{8G}\log M, \tag{2.40}$$

for a constant c depending on A. Unless we have $M^{c\rho^2} \geqslant (\log M)^2$ the estimate (2.40) is trivial. Under this condition we have

$$M^{-c\rho^2}(\log M)^2 \leqslant \sqrt{M^{-c\rho^2}(\log M)^2},$$

which allows us to replace $(\log M)^2$ with $\log M$ after changing the constant $c > 0$. Reducing c if necessary, we can also discard $\log M$ in the second term. ■

3. Proofs of main results

3.1. Proof of Theorem 1.1

We apply Lemma 2.1 with

$$U = X^{1/4} \quad \text{and} \quad V = X^{1/4} \tag{3.1}$$

to get

$$S_{q^\gamma}(a; X) \ll X^{1/4} + \Sigma_1 (\log X) + \Sigma_2^{1/2} X^{1/2} (\log X)^3, \tag{3.2}$$

where

$$\Sigma_1 = \sum_{t \leqslant UV} \max_{w \leqslant X/t} \Bigl| \sum_{w \leqslant m \leqslant X/t} \mathbf{e}_{q^\gamma}(a g^{tm}) \Bigr|,$$

and

$$\Sigma_2 = \max_{U \leqslant w \leqslant X/V} \max_{V \leqslant j \leqslant X/w} \sum_{V < m \leqslant X/w} \Bigl| \sum_{\substack{w < n \leqslant 2w \\ n \leqslant X/m \\ n \leqslant X/j}} \alpha_n \, \mathbf{e}_{q^\gamma}(a g^{mn}) \Bigr|,$$

for some $|\alpha_n| \leqslant 1$. Considering Σ_1, for each fixed $t \leqslant UV = X^{1/2}$, define

$$G_t = \nu_q(g^{t \operatorname{ord}_q(g^t)} - 1)$$

and

$$\rho_t = \frac{\log (X/t)}{\log q^\gamma}.$$

By (3.1) and $t \leqslant UV = X^{1/2}$ we have

$$\rho_t \geqslant \frac{\rho}{2}. \tag{3.3}$$

We claim that the following inequality holds:

$$\max_{w \leqslant X/t} \Bigl| \sum_{w \leqslant m \leqslant X/t} \mathbf{e}_{q^\gamma}(a g^{tm}) \Bigr| \ll \left(\frac{X}{t}\right)^{1 - c\rho_t^2} \log X + \left(\frac{X}{t}\right)^{1-c} q^{8G_t}. \tag{3.4}$$

Indeed, if $\gamma > 16 G_t$, this follows from Corollary 2.12.

If $\gamma \leqslant 16 G_t$, then

$$\left(\frac{X}{t}\right)^{1-c} q^{8G_t} \geqslant \left(\frac{X}{t}\right)^{1-c} q^{\gamma/2} \geqslant \left(\frac{X}{t}\right),$$

so (3.4) is trivially true as well since

$$\max_{w \leqslant X/t} \Bigl| \sum_{w \leqslant m \leqslant X/t} \mathbf{e}_{q^\gamma}(a g^{tm}) \Bigr| \ll \frac{X}{t}, \tag{3.5}$$

which proves (3.4).

Summing (3.4) over $t \leqslant UV$ and using (3.4), (3.3) and (3.5) gives

$$\Sigma_1 \ll \sum_{t \leqslant X^{1/2}} \left(\frac{X}{t}\right)^{1-c\rho_t^2} \log X + \widetilde{\Sigma}_1, \tag{3.6}$$

where

$$\widetilde{\Sigma}_1 = \sum_{t \leqslant X^{1/2}} \min\left\{\frac{X}{t}, \left(\frac{X}{t}\right)^{1-c} q^{8G_t}\right\}.$$

For $t \leqslant X^{1/2}$ we have $(X/t)^{1-c\rho_t^2/4} \leqslant X^{1-c\rho^2/8} t^{-1}$, thus

$$\sum_{t \leqslant X^{1/2}} \left(\frac{X}{t}\right)^{1-c\rho_t^2} \leqslant \sum_{t \leqslant X^{1/2}} \left(\frac{X}{t}\right)^{1-c\rho^2/4} \ll X^{1-c\rho^2/8} \log X.$$

This, together with (3.6), implies

$$\Sigma_1 \ll X^{1-c\rho^2/8} \log X + \widetilde{\Sigma}_1. \tag{3.7}$$

Considering $\widetilde{\Sigma}_1$, we partition summation over t into dyadic intervals to obtain

$$\begin{aligned} \widetilde{\Sigma}_1 &\ll \sum_{k \leqslant \frac{\log X}{2\log 2}} \sum_{2^k \leqslant t < 2^{k+1}} \min\left\{\frac{X}{t}, \left(\frac{X}{t}\right)^{1-c} q^{8G_t}\right\} \\ &\ll \sum_{k \leqslant \frac{\log X}{2\log 2}} \sum_{2^k \leqslant t < 2^{k+1}} \min\left\{\frac{X}{2^k}, \left(\frac{X}{2^k}\right)^{1-c} q^{8G_t}\right\}. \end{aligned}$$

Let k_0 be an index with $k_0 \leqslant (\log X)/(2\log 2)$ such that the maximum of the inner sums over t is attained, and write

$$Z = \frac{X}{2^{k_0}}.$$

Then

$$X^{1/2} \leqslant Z \leqslant X,$$

and

$$\widetilde{\Sigma}_1 \ll (\log X) \sum_{X/Z \leqslant t \leqslant 2X/Z} \min\left\{Z, Z^{1-c} q^{8G_t}\right\}.$$

Recalling the definition of G, given by (2.2), we see that

$$\operatorname{ord}_q(g^t) = \frac{\tau}{\gcd(\tau, t)},$$

and by Lemma 2.3, used with $m = 1$, $x = \tau t/\gcd(\tau, t)$ and $y = 0$,

$$G_t = \nu_q\left(g^{\tau t/\gcd(\tau,t)} - 1\right) = G + \nu_q(t).$$

As g and q are fixed, $G = O(1)$, and hence

$$\widetilde{\Sigma}_1 \ll \log X \sum_{X/Z \leqslant t \leqslant 2X/Z} \min\left\{Z, Z^{1-c} q^{8\nu_q(t)}\right\}.$$

For $O(XZ^{-1-c/9})$ values of $t \leqslant 2X/Z$ with $q^{\nu_q(t)} > Z^{c/9}$, we use

$$\min\left\{Z, Z^{1-c}q^{8\nu_q(t)}\right\} \leqslant Z.$$

Their total contribution is $O(XZ^{-c/9})$. For the remaining values of t, we use

$$\min\left\{Z, Z^{1-c}q^{8\nu_q(t)}\right\} \leqslant Z^{1-c+8c/9} = Z^{1-c/9},$$

which gives the same total contribution $O(XZ^{-c/9})$. Hence, recalling $Z \geqslant X^{1/2}$, we obtain

$$\widetilde{\Sigma}_1 \ll XZ^{-c/9}\log X \leqslant X^{1-c/18}\log X.$$

Using the above in (3.7) gives

$$\Sigma_1 \ll X^{1-c\rho^2/8}\log X + X^{1-c/18}\log X \ll X^{1-\delta(A)\rho^2}(\log X)^2, \tag{3.8}$$

for some constant $\delta(A) > 0$ that depends only on A.

To estimate Σ_2, we apply Lemma 2.10 to get

$$\Sigma_2 \ll \left(X^{1-\delta(A)\rho^2} + X^{7/8} + \frac{X}{q^{2\gamma/65}}\right)(\log X)^2,$$

for a suitably reduced $\delta(A)$ if necessary. By the above bounds (3.2) and (3.8),

$$S_{q^\gamma}(a; X) \ll X^{1-\delta(A)\rho^2}(\log X)^3 + \frac{X}{q^{2\gamma/65}}(\log X)^4.$$

Now, using the same argument as in the proof of Corollary 2.12, and reducing $\delta(A)$ if necessary, we see that we can replace $(\log X)^3$ with $\log X$ (or any other power of $\log X$) in the first term, and also discard completely $(\log X)^4$ in the second term.

3.2. Proof of Theorem 1.3

We observe that the property of having σ on positions $r, \dots, r-s+1$ of M_p is equivalent to the property of the fractional part of M_p/q^{r+1} falling in a prescribed half-open interval of length $1/q^s$, namely, to

$$\left\{\frac{M_p}{q^{r+1}}\right\} \in \left[\frac{\bar{\sigma}}{q^s}, \frac{\bar{\sigma}+1}{q^s}\right), \tag{3.9}$$

(we recall that the numbering starts from zero), where

$$\bar{\sigma} = \sum_{i=0}^{s-1} a_i q^i,$$

is the integer which q-ary digits are given by σ. We now combine the bound of Corollary 1.2 with the *Erdős–Turán inequality* (see Theorem 1.21 in [7]), which gives a bound of the discrepancy via exponential sums, and conclude that for any integer parameter $H \geqslant 1$,

$$A_r(X,\sigma) - q^{-s}\pi(X) \ll \pi(X)H^{-1} + \sum_{h=1}^{H}\frac{1}{h}\left|\sum_{\substack{p \leqslant X\\ p \text{ prime}}} \mathbf{e}_{q^{r+1}}(hM_p)\right|.$$

We now set

$$H = \lfloor X^{\varepsilon/2} \rfloor.$$

Below we use very crude bounds, many of them can be done in a more refined way; however, this does not improve the final result.

Namely, for any positive integer $h \leqslant H$, writing

$$q^{\gamma} = \frac{q^{r+1}}{\gcd(h, q^{r+1})},$$

since $r \geqslant \varepsilon \log X$, we see that

$$q^{\gamma} \geqslant q^{r+1}/H \geqslant e^{r}/H \geqslant X^{\varepsilon/2}. \tag{3.10}$$

We now use Corollary 1.2 with $A = 2/\varepsilon$ and note by (3.10) that the condition (1.2) is satisfied. This implies that (3.9) happens for

$$A_r(X, \sigma) = q^{-s}\pi(X) + O\big(X^{1-\varepsilon/2} + X^{1-c\varrho^2} \log X + X q^{-c\gamma} \log X\big) \tag{3.11}$$

primes $p \leqslant X$, where

$$\varrho = \frac{\log X}{\log q^{r+1}} \leqslant \frac{\log X}{\log q^{\gamma}},$$

and $c > 0$ is some constant that depends on ε and q.

Using that $r \leqslant (\log X)^{3/2-\varepsilon}$, we obtain $\varrho \geqslant (\log X)^{-1/2+\varepsilon/2}$. Thus,

$$X^{1-c\varrho^2} \log X \leqslant X \exp\left(-c(\log X)^{\varepsilon}\right) \log X.$$

We also have by (3.10),

$$X q^{-c\gamma} \leqslant X^{1-c\varepsilon/2},$$

and then (3.11) implies

$$A_r(X, \sigma) = q^{-s}\pi(X) + O\left(X \exp\left(-0.5c(\log X)^{\varepsilon}\right)\right),$$

which concludes the proof.

Acknowledgements. The authors would like to thank Bill Banks for many useful discussions and for his contribution to an early version of the paper. The authors also would like to thank Olivier Bordelles for his interest and very important comments and suggestions.

The authors are grateful to the anonymous referees for the very careful reading of the manuscript and very useful comments.

Funding. During the preparation of this work, B. K. was supported by the Australian Research Council Grant DP160100932, L. M. was supported by the Austrian Science Fund Project P31762, and I. S. was supported by the Australian Research Council Grant DP170100786.

References

[1] Banks, W., Conflitti, A., Friedlander, J. and Shparlinski, I. E.: Exponential sums over Mersenne numbers. *Compos. Math.* **140** (2004), no. 1, 15–30.

[2] Banks, W., Friedlander, J., Garaev, M. and Shparlinski, I. E.: Exponential and character sums with Mersenne numbers. *J. Aust. Math. Soc.* **92** (2012), no. 1, 1–13.

[3] Bourgain, J., Demeter, C. and Guth, L.: Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three. *Ann. of Math. (2)* **184** (2016), no. 2, 633–682.

[4] Cai, Z., Faust, M., Hildebrand, A. J., Li, J. and Zhang, Y.: Leading digits of Mersenne numbers. *Exp. Math.* **30** (2021), no. 3, 405–421.

[5] Cai, Z., Hildebrand, A. J. and Li, J.: A local Benford law for a class of arithmetic sequences. *Int. J. Number Theory* **15** (2019), no. 3, 613–638.

[6] Davenport, H.: *Multiplicative number theory*. Second edition. Graduate Texts in Mathematics 74, Springer-Verlag, New York-Berlin, 1980.

[7] Drmota, M. and Tichy, R. F.: *Sequences, discrepancies and applications*. Lecture Notes in Mathematics 1651, Springer-Verlag, Berlin, 1997.

[8] Ford, K.: Vinogradov's integral and bounds for the Riemann zeta function. *Proc. London Math. Soc. (3)* **85** (2002), no. 3, 565–633.

[9] Garaev, M.: Estimation of Kloosterman sums with primes and its application. *Mat. Zametki* **88** (2010), no. 3, 365–373. Translation in *Math. Notes* **88** (2010), no. 3-4, 330–337.

[10] He, X., Hildebrand, A. J., Li, J. and Zhang, Y.: Complexity of leading digit sequences. *Discrete Math. Theor. Comput. Sci.* **22** (2020), no. 1, Paper no. 14, 30 pp.

[11] Iwaniec, H. and Kowalski, E.: *Analytic number theory*. American Mathematical Society Colloquium Publications 53, American Mathematical Society, Providence, RI, 2004.

[12] Korobov, N.: The distribution of digits in periodic fractions. *Mat. Sb. (N.S.)* **89** (1972), 654–670. Translation in *Math. USSR-Sb.* **18** (1972), no. 4, 659–676.

[13] Steiner, R. S.: Effective Vinogradov's mean value theorem via efficient boxing. *J. Number Theory* **204** (2019), 354–404.

[14] Wooley, T.: The cubic case of the main conjecture in Vinogradov's mean value theorem. *Adv. Math.* **294** (2016), 532–561.

Received February 17, 2021; revised September 24, 2021. Published online December 16, 2021.

Bryce Kerr
Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany;
bryce.kerr89@gmail.com

László Mérai
Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences, Altenberger Straße 69, 4040 Linz, Austria;
laszlo.merai@oeaw.ac.at

Igor E. Shparlinski
Department of Pure Mathematics, University of New South Wales,
Sydney, NSW 2052, Australia;
igor.shparlinski@unsw.edu.au