J. Aust. Math. Soc. **92** (2012), 1–13
doi:10.1017/S1446788712000109

EXPONENTIAL AND CHARACTER SUMS WITH MERSENNE NUMBERS

WILLIAM D. BANKS, JOHN B. FRIEDLANDER, MOUBARIZ Z. GARAEV and IGOR E. SHPARLINSKI✉

(Received 23 December 2010; accepted 16 January 2012)

Communicated by F. Papparlardi and J. Shallit

Dedicated to the memory of Alf van der Poorten

Abstract

We give new bounds on sums of the form $\sum_{n\le N}\Lambda(n)\exp(2\pi iag^n/m)$ and $\sum_{n\le N}\Lambda(n)\chi(g^n+a)$, where Λ is the von Mangoldt function, m is a natural number, a and g are integers coprime to m, and χ is a multiplicative character modulo m. In particular, our results yield bounds on the sums $\sum_{p\le N}\exp(2\pi iaM_p/m)$ and $\sum_{p\le N}\chi(M_p)$ with Mersenne numbers $M_p=2^p-1$, where p is prime.

2010 *Mathematics subject classification*: primary 11L07; secondary 11L20.

Keywords and phrases: Mersenne number, exponential sums, character sums.

1. Introduction

Let m be an arbitrary natural number, and let a and g be integers that are coprime to m. Our aim in the present note is to give bounds on exponential sums and multiplicative character sums of the form

$$S_m(a;N)=\sum_{n\le N}\Lambda(n)e_m(ag^n) \quad \text{and} \quad T_m(\chi,a;N)=\sum_{n\le N}\Lambda(n)\chi(g^n+a),$$

where e_m is the additive character modulo m defined by

$$e_m(x)=\exp(2\pi ix/m) \quad (x\in\mathbb{R}),$$

and χ is a nontrivial multiplicative character modulo m. As usual, Λ denotes the von Mangoldt function given by

$$\Lambda(n)=\begin{cases}\log p & \text{if } n \text{ is a power of the prime } p,\\ 0 & \text{if } n \text{ is not a prime power.}\end{cases}$$

Friedlander was partially supported by NSERC Grant A5123 and Shparlinski was partially supported by ARC Grant DP1092835.

Let t denote the multiplicative order of g modulo m, that is, the smallest natural number such that $g^t \equiv 1 \bmod m$. For the exponential sums defined above, Banks *et al.* [1] have established the following bound as $N \to \infty$:

$$\max_{\gcd(a,m)=1} |S_m(a;N)| \le \begin{cases} (Nt^{-11/32}m^{5/16} + N^{5/6}t^{5/48}m^{7/24})N^{o(1)} & \text{for all } m \ge 1, \\ (Nt^{-1/6}q^{1/8} + N^{5/6}t^{2/9}q^{1/6})N^{o(1)} & \text{if } m = q \text{ is prime.} \end{cases} \tag{1.1}$$

Furthermore, as previously observed in [2, Lemma 2], using a bound of Garaev [7] one can improve (1.1) for a prime $m = q$ as follows:

$$\max_{\gcd(a,q)=1} |S_q(a;N)| \le (Nt^{-1/4}q^{1/8} + N^{5/6}t^{2/9}q^{1/6})N^{o(1)}. \tag{1.2}$$

We remark that an even stronger bound which is valid for *almost all* primes q has been obtained by Garaev and Shparlinski [10].

In this paper, using bounds for single and bilinear exponential sums from [1] and exploiting an idea of Garaev [8] to handle double sums over a certain 'hyperbolic' region, we give improvements of both (1.1) and (1.2).

As for the multiplicative character sums defined above, in an earlier work [3] we presented a bound on $T_m(\chi, a; N)$ in the case where $m = q$ is prime, but our proof contains a gap (see [3, Theorem 12]; the condition that the intervals of summation in our double sums contain distinct elements modulo t does not necessary hold). In the present note, although we do not completely recover [3, Theorem 12], we derive a bound that is nontrivial over a range that is only slightly shorter.

We note that, using our results in the case $g = 2$ together with partial summation, one obtains nontrivial bounds on the sums

$$\sum_{\substack{p \le N \\ p \text{ prime}}} e_m(aM_p) \quad \text{and} \quad \sum_{\substack{p \le N \\ p \text{ prime}}} \chi(M_p) \tag{1.3}$$

with *Mersenne numbers* $M_p = 2^p - 1$, where p is prime.

In particular, we see from (1.1) and (1.2) that the sums $S_m(a;N)$ admit a nontrivial estimate if, for some fixed $\varepsilon > 0$,

$$t \ge m^{10/11+\varepsilon} \quad \text{and} \quad N \ge t^{5/8}m^{7/4+\varepsilon} \tag{1.4}$$

for general m, and we improve this to

$$t \ge q^{1/2+\varepsilon} \quad \text{and} \quad N \ge t^{4/3}q^{1+\varepsilon} \tag{1.5}$$

for the case of prime $m = q$.

By comparison, our new estimates for $S_m(a;N)$ given herein are, for general m, stronger than those given previously, although they are nontrivial only under the same condition (1.4). For the case of prime $m = q$ they are not only stronger but also extend

https://doi.org/10.1017/S1446788712000109 Published online by Cambridge University Press

the region (1.5) to

$$t \geq q^{1/2+\varepsilon} \quad \text{and} \quad N \geq t^{1/2} q^{5/4+\varepsilon}. \tag{1.6}$$

Our bound on $T_q(\chi, a; N)$ is also nontrivial under the same condition (1.6).

Throughout the paper, the implied constants in the symbol '$\ll$' may depend on the parameter ε (when present) but are absolute otherwise (we recall that the notation $A \ll B$ is equivalent to the assertion that $|A| \leq cB$ for some constant $c > 0$). As a consequence, all of our results below are uniform in all parameters other than ε. In particular, our bounds are uniform over all integers a coprime to the modulus m and over all integers g with the same multiplicative order t modulo m.

2. Preparation

2.1. Vaughan's bound. We need the following result of Vaughan [15], which is stated here in the form given in [4, Ch. 24].

LEMMA 2.1. *For any complex-valued function $f(n)$ and any real numbers $U, V > 1$ with $UV \leq N$,*

$$\sum_{n \leq N} \Lambda(n) f(n) \ll \Sigma_1 + \Sigma_2 + \Sigma_3 + \Sigma_4,$$

where

$$\Sigma_1 = \Big| \sum_{n \leq U} \Lambda(n) f(n) \Big|,$$

$$\Sigma_2 = (\log UV) \sum_{k \leq UV} \Big| \sum_{\ell \leq N/k} f(k\ell) \Big|,$$

$$\Sigma_3 = (\log N) \sum_{k \leq V} \max_{w \geq 0} \Big| \sum_{w < \ell \leq N/k} f(k\ell) \Big|,$$

$$\Sigma_4 = \Big| \sum_{\substack{k\ell \leq N \\ k > V, \ell > U}} \Lambda(\ell) \Big(\sum_{\substack{d \mid k \\ d \leq V}} \mu(d) \Big) f(k\ell) \Big|.$$

2.2. Bounds on exponential sums. As in [1], we need bounds on exponential sums with exponential functions over consecutive integers. The following statement is [1, Lemma 2.2]; it follows immediately from a result of Korobov [14, Theorem 10, Ch. 1] (see also the proof of [13, Lemma 2]).

LEMMA 2.2. *Suppose that ϑ is coprime to m, and let T be the multiplicative order of ϑ modulo m. Then, for any $H_1 < H_2$ and any integer a coprime to m,*

$$\sum_{H_1 < n \leq H_2} e_m(a\vartheta^n) \ll ((H_2 - H_1)T^{-1} + 1) m^{1/2+\varepsilon}.$$

We also need the following bound on bilinear exponential sums with exponential functions, which is a special case of [1, Lemma 2.5].

https://doi.org/10.1017/S1446788712000109 Published online by Cambridge University Press

LEMMA 2.3. *Suppose that g is coprime to m, and let t be the multiplicative order of g modulo m. Let K, L be natural numbers. Then, for any two sequences $(\alpha_k)_{k=1}^K$ and $(\beta_\ell)_{\ell=1}^L$ of complex numbers and any integer a coprime to m,*

$$\sum_{k\le K}\sum_{\ell\le L}\alpha_k\beta_\ell e_m(ag^{k\ell}) \ll AB(Kt^{-1/2}+K^{1/2})(Lt^{-1/2}+L^{1/2})t^{21/32}m^{5/16+\varepsilon},$$

where

$$A=\max_{k\le K}|\alpha_k| \quad \textit{and} \quad B=\max_{\ell\le L}|\beta_\ell|. \tag{2.1}$$

In the special case where $m=q$ is a prime number, a stronger bound follows immediately from [1, Lemma 2.7], but one can do better using an improved version of that estimate due to Garaev and Karatsuba [9].

LEMMA 2.4. *Suppose that $q \nmid g$, and let t be the multiplicative order of g modulo q. Let K, L be natural numbers. Then, for any two sequences $(\alpha_k)_{k=1}^K$ and $(\beta_\ell)_{\ell=1}^L$ of complex numbers and any integer a not divisible by q,*

$$\sum_{k\le K}\sum_{\ell\le L}\alpha_k\beta_\ell e_q(ag^{k\ell}) \ll AB(Kt^{-1/2}+K^{1/2})(Lt^{-1/4}+L^{3/4})t^{1/2}q^{1/8+\varepsilon},$$

where A and B are defined by (2.1).

PROOF. In the case where $K, L \le t$, an application of [9, Corollary 3] (with the choice $k=1$) yields the bound

$$\sum_{k\le K}\sum_{\ell\le L}\alpha_k\beta_\ell e_q(ag^{k\ell}) \ll ABK^{1/2}L^{3/4}t^{1/2}q^{1/8+\varepsilon}.$$

For arbitrary K and L, we split the double sums into at most $(Kt^{-1}+1)(Lt^{-1}+1)$ double sums with at most $\min\{K,t\}\cdot\min\{L,t\}$ terms, deriving the bound

$$\sum_{k\le K}\sum_{\ell\le L}\alpha_k\beta_\ell e_q(ag^{k\ell}) \ll (Kt^{-1}+1)(Lt^{-1}+1)\min\{K,t\}^{1/2}\min\{L,t\}^{3/4}t^{1/2}q^{1/8+\varepsilon}.$$

Since

$$(Kt^{-1}+1)\min\{K,t\}^{1/2} \le Kt^{-1/2}+K^{1/2}$$

and

$$(Lt^{-1}+1)\min\{L,t\}^{3/4} \le Lt^{-1/4}+L^{3/4},$$

the result follows. □

Next, we use an idea of Garaev [8] to derive a variant of Lemma 2.3 in which the summation limits over ℓ depend on the parameter k.

LEMMA 2.5. *Let the notation be as in Lemma 2.3. For any two sequences $(L_k)_{k=1}^K$ and $(M_k)_{k=1}^K$ of nonnegative integers such that $M_k < L_k \le L$ for each k,*

$$\sum_{k\le K}\sum_{M_k<\ell\le L_k}\alpha_k\beta_\ell e_m(ag^{k\ell}) \ll AB(Kt^{-1/2}+K^{1/2})(Lt^{-1/2}+L^{1/2})t^{21/32}m^{5/16}(mL)^{\varepsilon}.$$

https://doi.org/10.1017/S1446788712000109 Published online by Cambridge University Press

PROOF. For each inner sum,

$$\sum_{M_k<\ell\le L_k}\beta_\ell e_m(ag^{k\ell}) = \sum_{\ell\le L}\sum_{M_K<s\le L_k}\beta_\ell e_m(ag^{k\ell})\cdot\frac{1}{L}\sum_{-\frac12 L<r\le\frac12 L} e_L(r(\ell-s))$$
$$= \frac{1}{L}\sum_{-\frac12 L<r\le\frac12 L}\sum_{M_k<s\le L_k} e_L(-rs)\sum_{\ell\le L}\beta_\ell e_L(r\ell)e_m(ag^{k\ell}).$$

In view of [12, bound (8.6)], for each $k\le K$ and every integer r such that $|r|\le\frac12 L$ we can write

$$\sum_{M_k<s\le L_k} e_L(-rs) = \sum_{s\le L_k} e_L(-rs) - \sum_{s\le M_k} e_L(-rs) = \eta_{k,r}\frac{L}{|r|+1}$$

for some complex number $\eta_{k,r}\ll 1$. Thus, if we put

$$\widetilde{\alpha}_{k,r} = \alpha_k\eta_{k,r} \quad\text{and}\quad \widetilde{\beta}_{\ell,r} = \beta_\ell e_L(r\ell),$$

it follows that

$$\sum_{k\le K}\sum_{M_k<\ell\le L_k}\alpha_k\beta_\ell e_m(ag^{k\ell}) = \sum_{-\frac12 L<r\le\frac12 L}\frac{1}{|r|+1}\sum_{k\le K}\sum_{\ell\le L}\widetilde{\alpha}_{k,r}\widetilde{\beta}_{\ell,r}e_m(ag^{k\ell}).$$

Applying Lemma 2.3 with the sequences $(\widetilde{\alpha}_{k,r})_{k=1}^K$ and $(\widetilde{\beta}_{\ell,r})_{\ell=1}^L$, and noting that

$$\sum_{-\frac12 L<r\le\frac12 L}\frac{1}{|r|+1}\ll\log L\ll L^\varepsilon,$$

we derive the stated bound. □

Similarly, using Lemma 2.4 instead of Lemma 2.3, we obtain our next result.

LEMMA 2.6. *Let the notation be as in Lemma 2.4. For any two sequences $(L_k)_{k=1}^K$ and $(M_k)_{k=1}^K$ of nonnegative integers such that $M_k<L_k\le L$ for each k,*

$$\sum_{k\le K}\sum_{M_k<\ell\le L_k}\alpha_k\beta_\ell e_q(ag^{k\ell})\ll AB(Kt^{-1/2}+K^{1/2})(Lt^{-1/4}+L^{3/4})t^{1/2}q^{1/8}(qL)^\varepsilon.$$

Our main technical tool is the following lemma, which is used to bound double exponential sums over a certain 'hyperbolic' region of summation.

LEMMA 2.7. *Suppose that g is coprime to m, and let t be the multiplicative order of g modulo m. Let X, Y, Z be real numbers such that $Z>Y>X\ge 2$. Then, for any two sequences $(\alpha_k)_{X<k\le Y}$ and $(\beta_\ell)_{\ell\le Z/X}$ of complex numbers, any sequence $(M_k)_{k=1}^K$ of nonnegative integers such that $M_k<Z/k$ for each k, and any integer a coprime to m,*

$$\sum_{X<k\le Y}\sum_{M_k<\ell\le Z/k}\alpha_k\beta_\ell e_m(ag^{k\ell})$$
$$\ll AB(Zt^{-1}+Y^{1/2}Z^{1/2}t^{-1/2}+X^{-1/2}Zt^{-1/2}+Z^{1/2})t^{21/32}m^{5/16}(mZ)^\varepsilon,$$

where A and B are defined by (2.1).

https://doi.org/10.1017/S1446788712000109 Published online by Cambridge University Press

PROOF. Let $\alpha_k = 0$ if $k \le X$ or $k > Y$. Then

$$\sum_{X<k\le Y} \sum_{M_k<\ell\le Z/k} \alpha_k\beta_\ell e_m(ag^{k\ell}) = \sum_{\log X\le j\le \log Y} \sum_{e^j<k\le e^{j+1}} \sum_{M_k<\ell\le Z/k} \alpha_k\beta_\ell e_m(ag^{k\ell}).$$

Using Lemma 2.5, each inner double sum satisfies the bound

$$\sum_{e^j<k\le e^{j+1}} \sum_{M_k<\ell\le Z/k} \alpha_k\beta_\ell e_m(ag^{k\ell}) \ll AB(e^j t^{-1/2} + e^{j/2})(Ze^{-j}t^{-1/2} + Z^{1/2}e^{-j/2})t^{21/32}m^{5/16}(mZ)^\varepsilon.$$

Taking into account that

$$\sum_{\log X\le j\le \log Y} (e^j t^{-1/2} + e^{j/2})(Ze^{-j}t^{-1/2} + Z^{1/2}e^{-j/2}) \ll Zt^{-1}\log Y + Y^{1/2}Z^{1/2}t^{-1/2} + X^{-1/2}Zt^{-1/2} + Z^{1/2}\log Y,$$

and $\log Y \le \log Z \ll Z^\varepsilon$, we obtain the stated bound. □

For prime moduli $m = q$, Lemma 2.7 can be strengthened by using Lemma 2.6 instead of Lemma 2.5 in the proof; the details are omitted.

LEMMA 2.8. *Suppose that $q \nmid g$, and let t be the multiplicative order of g modulo q. Let X, Y, Z be real numbers such that $Z > Y > X \ge 2$. Then, for any two sequences $(\alpha_k)_{X<k\le Y}$ and $(\beta_\ell)_{\ell\le Z/X}$ of complex numbers, any sequence $(M_k)_{k=1}^K$ of nonnegative integers such that $M_k < Z/k$ for each k, and any integer a not divisible by q,*

$$\sum_{X<k\le Y} \sum_{M_k<\ell\le Z/k} \alpha_k\,\beta_\ell\, e_q(ag^{k\ell}) \ll AB(Zt^{-3/4} + Y^{1/4}Z^{3/4}t^{-1/2} + X^{-1/2}Zt^{-1/4} + X^{-1/4}Z^{3/4})t^{1/2}q^{1/8}(qZ)^\varepsilon,$$

where A and B are defined by (2.1).

2.3. Bounds on multiplicative character sums. Here we collect analogues of bounds given in Section 2.2. Unfortunately, these are only available in the case where our nontrivial multiplicative character χ has a prime modulus q, and we assume throughout that χ is such a character.

The following statement, an analogue of Lemma 2.2, follows immediately from results given in [5, 16].

LEMMA 2.9. *Suppose that $q \nmid \vartheta$, and let T be the multiplicative order of ϑ modulo q. Then, for any $H_1 < H_2$ and any integer a not divisible by q,*

$$\sum_{H_1<n\le H_2} \chi(\vartheta^n + a) \ll ((H_2 - H_1)T^{-1} + 1)q^{1/2+\varepsilon}.$$

https://doi.org/10.1017/S1446788712000109 Published online by Cambridge University Press

Next, we give an analogue of Lemma 2.4 with the character χ. This result is also an improvement of [3, Theorem 10]. Our proof is based on the following statement (which can be extended in many ways but is stated here in the simplest form that suffices for our purposes).

LEMMA 2.10. *Let $\overline{\mathbb{F}}_q$ denote the algebraic closure of $\mathbb{F}_q$, and let $\overline{\mathbb{F}}_q(Z)$ be the field of rational functions over $\overline{\mathbb{F}}_q$. For any integers d and a and any primes $v_1, v_2, v_3, v_4 > 3$ such that $\gcd(dav_1v_2v_3v_4, q) = 1$, the rational function*

$$F(Z) = \frac{(Z^{dv_1} + a)(Z^{dv_2} + a)}{(Z^{dv_3} + a)(Z^{dv_4} + a)}$$

cannot be expressed in the form $H(Z)^\delta$, where $H \in \overline{\mathbb{F}}_q(Z)$ and $\delta > 1$, unless each value in the sequence v_1, v_2, v_3, v_4 occurs an even number of times.

PROOF. We first observe that whenever $\gcd(u, v) = 1$ the polynomials $Z^{du} + a$ and $Z^{dv} + a$ have at most d common roots in $\overline{\mathbb{F}}_q$. Indeed, if r and s are integers such that $ur + vs = 1$, then every common root ρ satisfies the equation $\rho^d = (-a)^{r+s}$.

Now, if some value in the sequence v_1, v_2, v_3, v_4 occurs an odd number of times, then one of the primes, say v_1, is different from the others. By the argument above, $Z^{dv_1} + a$ has at most $3d < dv_1$ roots in common with $Z^{dv_2} + a$, $Z^{dv_3} + a$ or $Z^{dv_4} + a$; let ρ be one of the other roots. Since $\gcd(dav_1, q) = 1$, the roots of $Z^{dv_1} + a$ in $\overline{\mathbb{F}}_q$ are all distinct and nonzero; hence ρ is a root of $F(Z)$ of multiplicity one, and the result follows. □

LEMMA 2.11. *Suppose that $q \nmid g$, and let t be the multiplicative order of g modulo q. Let K, L be natural numbers. Then, for any two sequences $(\alpha_k)_{k=1}^K$ and $(\beta_\ell)_{\ell=1}^L$ of complex numbers and any integer a not divisible by q,*

$$\sum_{k \le K} \sum_{\ell \le L} \alpha_k \beta_\ell \chi(g^{k\ell} + a) \ll AB(Kt^{-1/2} + K^{1/2})(Lt^{-1/4} + L^{3/4})t^{1/2}q^{1/8+\varepsilon},$$

where A and B are defined by (2.1).

PROOF. In the case where $K, L \le t$, our argument is almost identical to that given in [9, Section 3] (with $k = 1$, and excluding the prime 3 from the set $\mathcal{V}$ considered there). However, instead of proving that the polynomial $aZ^{dv_1} + aZ^{dv_2} - aZ^{dv_3} - aZ^{dv_4}$ is not constant unless the sequence of primes v_1, v_2, v_3, v_4 satisfies $\{v_1, v_2\} = \{v_3, v_4\}$, in our setting we justify the application of the Weil bound for all other quadruples, by using Lemma 2.10. In this way, we obtain for $K, L \le t$ the bound

$$\sum_{k \le K} \sum_{\ell \le L} \alpha_k \beta_\ell \chi(g^{k\ell} + a) \ll ABK^{1/2}L^{3/4}t^{1/2}q^{1/8+\varepsilon}.$$

Now the argument in the proof of Lemma 2.4 gives the desired extension to arbitrary K and L. □

https://doi.org/10.1017/S1446788712000109 Published online by Cambridge University Press

In turn, following the arguments of Section 2.2, we derive from Lemma 2.11 the following analogue of Lemma 2.8.

LEMMA 2.12. *Suppose that $q \nmid g$, and let t be the multiplicative order of g modulo q. Let X, Y, Z be real numbers such that $Z > Y > X \ge 2$. Then, for any two sequences $(\alpha_k)_{X<k\le Y}$ and $(\beta_\ell)_{\ell\le Z/X}$ of complex numbers, any sequence $(M_k)_{k=1}^K$ of nonnegative integers such that $M_k < Z/k$ for each k, and any integer a not divisible by q,*

$$\sum_{X<k\le Y}\sum_{M_k<\ell\le Z/k}\alpha_k\beta_\ell\chi(g^{k\ell}+a) \ll AB(Zt^{-3/4}+Y^{1/4}Z^{3/4}t^{-1/2}+X^{-1/2}Zt^{-1/4}+X^{-1/4}Z^{3/4})t^{1/2}q^{1/8}(qZ)^{\varepsilon},$$

where A and B are defined by (2.1).

3. Main results

3.1. Exponential sums over primes.

THEOREM 3.1. *Suppose that g is coprime to m, and let t be the multiplicative order of g modulo m. Then, as $N \to \infty$,*

$$\max_{\gcd(a,m)=1}\left|\sum_{n\le N}\Lambda(n)e_m(ag^n)\right| \le (Nt^{-11/32}m^{5/16}+N^{4/5}t^{1/8}m^{7/20})N^{o(1)}.$$

PROOF. For convenience we put

$$S_m = \max_{\gcd(a,m)=1}\left|\sum_{n\le N}\Lambda(n)e_m(ag^n)\right|.$$

The desired bound is trivial unless

$$t \ge m^{10/11} \quad \text{and} \quad N \ge t^{5/8}m^{7/4}, \tag{3.1}$$

hence we assume that these inequalities hold in what follows. In particular, any estimates involving $t^{o(1)}$ or $m^{o(1)}$ can be expressed as $N^{o(1)}$ with $N \to \infty$.

Let $U, V > 1$ with $UV \le N$ and apply Lemma 2.1 with the function $f(n) = e_m(ag^n)$. Estimating Σ_1 trivially,

$$\Sigma_1 = \left|\sum_{n\le U}\Lambda(n)e_m(ag^n)\right| \le \sum_{n\le U}\Lambda(n) \ll U. \tag{3.2}$$

To bound

$$\Sigma_2 = (\log UV)\sum_{k\le UV}\left|\sum_{\ell\le N/k}e_m(ag^{k\ell})\right|,$$

https://doi.org/10.1017/S1446788712000109 Published online by Cambridge University Press

note that for any $k \le UV$ the number $\vartheta = g^k$ is of multiplicative order $T = t/\gcd(t,k)$ modulo m, hence an application of Lemma 2.2 yields the bound

$$\Sigma_2 \le \Big(\frac{N}{t}\sum_{k\le UV}\frac{\gcd(t,k)}{k} + UV\Big)m^{1/2}N^{o(1)}.$$

Moreover,

$$\begin{aligned}\sum_{k\le UV}\frac{\gcd(t,k)}{k} &= \sum_{d\mid t}\sum_{\substack{k\le UV\\ \gcd(t,k)=d}}\frac{d}{k} \le \sum_{d\mid t}\sum_{\substack{k\le UV\\ d\mid k}}\frac{d}{k}\\ &= \sum_{d\mid t}\sum_{w\le UV/d}\frac{1}{w} \le \tau(t)\sum_{w\le UV}\frac{1}{w} \ll \tau(t)\log UV,\end{aligned}$$

where τ is the divisor function. Since $UV \le N$ and $\tau(t) = t^{o(1)}$ as $t \to \infty$ (see, for example, [11, Theorem 315]), it follows that

$$\sum_{k\le UV}\frac{\gcd(t,k)}{k} \le N^{o(1)}.$$

Consequently,

$$\Sigma_2 \le (Nt^{-1} + UV)m^{1/2}N^{o(1)}. \tag{3.3}$$

The method used to bound Σ_2 can also be applied to Σ_3, and one obtains that

$$\Sigma_3 \le (Nt^{-1} + V)m^{1/2}N^{o(1)}. \tag{3.4}$$

Finally, let us write

$$\Sigma_4 = \Big|\sum_{V<k\le N/U}\sum_{U<\ell\le N/k}\alpha_k\beta_\ell e_m(ag^{k\ell})\Big|$$

with

$$\alpha_k = \sum_{\substack{d\mid k\\ d\le V}}\mu(d) \quad \text{and} \quad \beta_\ell = \Lambda(\ell).$$

Clearly, both A and B are of size $N^{o(1)}$ as $N \to \infty$, hence Lemma 2.7 yields the bound

$$\Sigma_4 \le (Nt^{-1} + U^{-1/2}Nt^{-1/2} + V^{-1/2}Nt^{-1/2} + N^{1/2})t^{21/32}m^{5/16}N^{o(1)}. \tag{3.5}$$

We now choose

$$U = V = N^{2/5}t^{1/16}m^{-3/40}$$

to balance the terms that depend on U and V in (3.3) and (3.5). One sees that the bounds of (3.2), (3.3) and (3.4) are all dominated by our bound for Σ_4 on the right-hand side of (3.5). Therefore, upon combining these bounds we obtain that

$$S_m \le (Nt^{-11/32}m^{5/16} + N^{4/5}t^{1/8}m^{7/20} + N^{1/2}t^{21/32}m^{5/16})N^{o(1)}.$$

https://doi.org/10.1017/S1446788712000109 Published online by Cambridge University Press

To conclude the proof, it remains to observe that the inequality

$$N^{4/5}t^{1/8}m^{7/20} \ge N^{1/2}t^{21/32}m^{5/16}$$

is equivalent to

$$N \ge t^{85/48}m^{-1/8},$$

which follows from the second inequality in (3.1) since $t \le m$. □

We remark that the range of t in (3.1) for which the result is nontrivial is the same as that given by the earlier bound (1.1) but the new result begins to detect cancellation in the sum for smaller values of N. The same remark applies to the improvement over (1.2) in the prime modulus case, which we give now.

Using partial summation, we immediately derive from Theorem 3.1 the following bound for the exponential sums with Mersenne numbers in (1.3): for any odd $m \ge 1$, as $N \to \infty$,

$$\max_{\gcd(a,m)=1} \Bigg| \sum_{\substack{p \le N \\ p \text{ prime}}} e_m(aM_p) \Bigg| \le (Nt^{-11/32}m^{5/16} + N^{4/5}t^{1/8}m^{7/20})N^{o(1)},$$

where t is the multiplicative order of 2 modulo m.

THEOREM 3.2. *Suppose that $q \nmid g$, and let t be the multiplicative order of g modulo q. Then*

$$\max_{\gcd(a,q)=1} \Bigg| \sum_{n \le N} \Lambda(n) e_q(ag^n) \Bigg| \le (Nt^{-1/4}q^{1/8} + N^{6/7}t^{1/14}q^{5/28})N^{o(1)}.$$

PROOF. Note that the desired bound is trivial unless

$$t \ge q^{1/2} \quad \text{and} \quad N \ge t^{1/2}q^{5/4}. \tag{3.6}$$

Proceeding as in the proof of Theorem 3.1 with the function $f(n) = e_q(ag^n)$, but using Lemma 2.8 instead of Lemma 2.7 to bound the sum Σ_4,

$$\begin{aligned}
&\Sigma_1 \ll U,\\
&\Sigma_2 \le (Nt^{-1} + UV)q^{1/2}N^{o(1)},\\
&\Sigma_3 \le (Nt^{-1} + V)q^{1/2}N^{o(1)},\\
&\Sigma_4 \le (Nt^{-3/4} + U^{-1/4}Nt^{-1/2} + V^{-1/2}Nt^{-1/4} + V^{-1/4}N^{3/4})t^{1/2}q^{1/8}N^{o(1)}.
\end{aligned}$$

Since $t > q^{1/2}$, we have $Nt^{-1}q^{1/2} < Nt^{-1/4}q^{1/8}$, and it follows that S_q is at most

$$(Nt^{-1/4}q^{1/8} + (UVq^{1/2} + U^{-1/4}Nq^{1/8} + V^{-1/2}Nt^{1/4}q^{1/8}) + V^{-1/4}N^{3/4}t^{1/2}q^{1/8})N^{o(1)}.$$

We balance only the three terms in the inner set of parentheses and then show that the resulting quantity dominates the final term $V^{-1/4}N^{3/4}t^{1/2}q^{1/8}$. Thus, we choose

$$U = N^{4/7}t^{-2/7}q^{-3/14} \quad \text{and} \quad V = N^{2/7}t^{5/14}q^{-3/28}.$$

https://doi.org/10.1017/S1446788712000109 Published online by Cambridge University Press

Inserting these values of U, V into the above bound on S_q, we get

$$S_q \le (Nt^{-1/4}q^{1/8} + N^{6/7}t^{1/14}q^{5/28} + N^{19/28}t^{23/56}q^{17/112})N^{o(1)}.$$

To conclude the proof, it remains to observe that the inequality

$$N^{6/7}t^{1/14}q^{5/28} \ge N^{19/28}t^{23/56}q^{17/112}$$

is equivalent to

$$N \ge t^{19/10}q^{-3/20},$$

which follows from the second inequality in (3.6) since $t \le q$. □

Using partial summation we immediately derive from Theorem 3.2 the following bound for the exponential sums with Mersenne numbers in (1.3): for any prime $q \ge 3$, as $N \to \infty$,

$$\max_{\gcd(a,q)=1} \left| \sum_{\substack{p \le N \\ p \text{ prime}}} e_q(aM_p) \right| \le (Nt^{-1/4}q^{1/8} + N^{6/7}t^{1/14}q^{5/28})N^{o(1)},$$

where t is the multiplicative order of 2 modulo q.

3.2. Character sums over primes. Using Lemma 2.12 instead of Lemma 2.8 in the proof of Theorem 3.2, we derive the following statement.

THEOREM 3.3. *Suppose that g is coprime to q, and let t be the multiplicative order of g modulo q. Then, as $N \to \infty$,*

$$\max_{\gcd(a,q)=1} \max_{\chi \in \mathcal{X}_q^*} \left| \sum_{n \le N} \Lambda(n)\chi(g^n + a) \right| \le (Nt^{-1/4}q^{1/8} + N^{6/7}t^{1/14}q^{5/28})N^{o(1)},$$

where $\mathcal{X}_q^*$ is the set of all nonprincipal multiplicative characters modulo q.

As compared to the bound erroneously claimed in [3, Theorem 12], the bound of Theorem 3.3 is nontrivial for the same range of t, but only for somewhat larger N than before.

Finally, as before, using partial summation we immediately derive the following bound for the exponential sums with Mersenne numbers in (1.3) from Theorem 3.3: for any prime $q \ge 3$, as $N \to \infty$,

$$\max_{\gcd(a,q)=1} \max_{\chi \in \mathcal{X}_q^*} \left| \sum_{\substack{p \le N \\ p \text{ prime}}} \chi(M_p + a) \right| \le (Nt^{-1/4}q^{1/8} + N^{6/7}t^{1/14}q^{5/28})N^{o(1)},$$

where t is the multiplicative order of 2 modulo q.

https://doi.org/10.1017/S1446788712000109 Published online by Cambridge University Press

4. Remarks

Lemma 2.10 immediately extends to more general rational functions having products of $\nu \geq 1$ similar binomial terms in the numerator and denominator. In turn, this more general statement can be used to establish full analogues of the results of [9] for bilinear sums with multiplicative characters (Lemma 2.11 is a special case of such a result with $\nu = 2$).

Our estimates clearly lead to various improvements and generalisations of the results of [2] (although specific details have yet to be worked out). Lemma 2.11 and its aforementioned generalisations also allow us to improve [3, Theorem 14]; however, using the approach of [6], one can derive even stronger estimates.

For the interested reader, we leave open the problem of getting nontrivial bounds on the sums $T_m(\chi, a; N)$ for an arbitrary composite m.

References

[1] W. Banks, A. Conflitti, J. B. Friedlander and I. E. Shparlinski, 'Exponential sums over Mersenne numbers', *Compositio Math.* **140** (2004), 15–30.
[2] W. D. Banks, J. B. Friedlander, M. Z. Garaev and I. E. Shparlinski, 'Character sums with exponential functions over smooth numbers', *Indag. Math.* **17** (2006), 157–168.
[3] W. D. Banks, J. B. Friedlander, M. Z. Garaev and I. E. Shparlinski, 'Double character sums over elliptic curves and finite fields', *Pure Appl. Math. Q.* **2** (2006), 179–197.
[4] H. Davenport, *Multiplicative Number Theory*, 2nd edn (Springer, New York, 1980).
[5] 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.
[6] E. El Mahassni and I. E. Shparlinski, 'On the distribution of the elliptic curve power generator', *Proc. 8th Conf. on Finite Fields and Appl.*, Contemporary Mathematics, 461 (American Mathematical Society, Providence, RI, 2008), pp. 111–119.
[7] M. Z. Garaev, 'Double exponential sums related to Diffie–Hellman distributions', *Int. Math. Res. Not.* **17** (2005), 1005–1014.
[8] M. Z. Garaev, 'An estimate of Kloosterman sums with prime numbers and an application', *Mat. Zametki* **88** (2010), 365–373 (in Russian).
[9] M. Z. Garaev and A. A. Karatsuba, 'New estimates of double trigonometric sums with exponential functions', *Arch. Math.* **87** (2006), 33–40.
[10] M. Z. Garaev and I. E. Shparlinski, 'The large sieve inequality with exponential functions and the distribution of Mersenne numbers modulo primes', *Int. Math. Res. Not.* **39** (2005), 2391–2408.
[11] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Oxford University Press, Oxford, 1979).
[12] H. Iwaniec and E. Kowalski, *Analytic Number Theory* (American Mathematical Society, Providence, RI, 2004).
[13] N. M. Korobov, 'On the distribution of digits in periodic fractions', *Mat. Sb.* **89** (1972), 654–670 (in Russian); English translation in *Math. USSR–Sb.* **18** (1972), 659–676.
[14] N. M. Korobov, *Exponential Sums and their Applications* (Kluwer Academic Publishers, Dordrecht, 1992).
[15] R. C. Vaughan, 'An elementary method in prime number theory', *Acta Arith.* **37** (1980), 111–115.
[16] H. B. Yu, 'Estimates of character sums with exponential function', *Acta Arith.* **97** (2001), 211–218.

https://doi.org/10.1017/S1446788712000109 Published online by Cambridge University Press

WILLIAM D. BANKS, Department of Mathematics, University of Missouri, Columbia, MO 65211, USA
e-mail: bankswd@missouri.edu

JOHN B. FRIEDLANDER, Department of Mathematics, University of Toronto, Toronto, Ontario M5S 3G3, Canada
e-mail: frdlndr@math.toronto.edu

MOUBARIZ Z. GARAEV, Instituto de Matemáticas, Universidad Nacional Autónoma de México, C. P. 58089, Morelia, Michoacán, México
e-mail: garaev@matmor.unam.mx

IGOR E. SHPARLINSKI, Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
e-mail: igor.shparlinski@mq.edu.au

https://doi.org/10.1017/S1446788712000109 Published online by Cambridge University Press