Compositio Math. 140 (2004) 15–30
DOI: 10.1112/S0010437X03000022

Exponential sums over Mersenne numbers

William D. Banks, Alessandro Conflitti, John B. Friedlander and Igor E. Shparlinski

Abstract

We give estimates for exponential sums of the form $\sum_{n\leqslant N}\Lambda(n)\exp(2\pi iag^n/m)$, where m is a positive integer, a and g are integers relatively prime to m, and Λ is the von Mangoldt function. In particular, our results yield bounds for exponential sums of the form $\sum_{p\leqslant N}\exp(2\pi iaM_p/m)$, where M_p is the Mersenne number; $M_p = 2^p - 1$ for any prime p. We also estimate some closely related sums, including $\sum_{n\leqslant N}\mu(n)\exp(2\pi iag^n/m)$ and $\sum_{n\leqslant N}\mu^2(n)\exp(2\pi iag^n/m)$, where μ is the Möbius function.

1. Introduction

It is well-known that methods originating with Vinogradov [Vin54] have been used successfully to find non-trivial estimates for a wide variety of exponential sums taken over the values of an integer polynomial at prime numbers. Certain modern and more convenient variants of these methods are due to Vaughan [Vau80] and to Heath-Brown [Hea82]. In this paper, we use such arguments to estimate exponential sums, taken again at prime values, where the integer polynomial is now replaced by an exponential function.

All of these methods employ a variant of the sieve of Eratosthenes to reduce the problem of estimating exponential sums over primes to that of deriving estimates for sums over consecutive integers and for a certain double sum with weights. For the case that we are considering here, in the literature there are already a number of bounds for similar sums taken over consecutive integer values [KS99, Kor72, Kor92, Nie78, Nie92]. The corresponding double sums have not been previously studied, however. In § 2, we obtain such bounds as a generalization of those in [FK02, FS01].

Let m be an arbitrary positive integer. Put $\mathbf{e}(\alpha) = \exp(2\pi i\alpha)$ for any real number α, and $\mathbf{e}_m(\alpha) = \mathbf{e}(\alpha/m)$. Our goal is to estimate exponential sums of the form

$$\sum_{n\leqslant N}\Lambda(n)\,\mathbf{e}_m(ag^n), \tag{1}$$

where a and g are integers relatively prime to m. As usual,

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

is the von Mangoldt function, and $\log z$ denotes the natural logarithm of z. Let t denote the multiplicative order of g modulo m. We show that, for any given $\delta > 0$, the exponential sum above is small whenever $t \geqslant m^{10/11+\delta}$ and $N \geqslant t^{5/8+\delta}m^{7/4}$.

Received 1 September 2002, accepted in final form 13 February 2003.
2000 Mathematics Subject Classification 11L07, 11L20.
Keywords: exponential sums over primes, Mersenne numbers.
The first author was supported in part by NSF grant DMS-0070628 and by Macquarie University (Sydney). The third author was supported in part by NSERC grant A5123 and by the Max Planck Institut für Mathematik (Bonn). The fourth author was supported in part by ARC grant A00000184.

Applying these considerations to the case $g = 2$, we deduce that, under the same conditions,

$$\sum_{p \leqslant N} \mathbf{e}_m(aM_p) = o(\pi(N)), \tag{2}$$

where, for any prime p, M_p is the *Mersenne number* defined by $M_p = 2^p - 1$. Here $\pi(N)$ denotes the number of primes $p \leqslant N$.

Certainly, it seems an interesting goal to ease the above restrictions so as to obtain estimates when the period t is smaller and also to treat shorter sums where the method given in our principal arguments (§ 3) seems to fail. Ironically, that method also fails to apply to the very long sums, which should be the easier ones, and so, to achieve the full range of uniformity stated above, we need to add (in § 4) some refinements and further ingredients which depend on the distribution of primes in arithmetic progressions.

It seems natural to consider the analogous exponential sums wherein the von Mangoldt function in (1) is replaced by another function of arithmetic interest, or the set of primes in (2) is replaced by another interesting set of integers. In § 5, we consider the exponential sum

$$\sum_{n \leqslant N} \mu(n)\, \mathbf{e}_m(ag^n)$$

and obtain precisely the same bounds as for the original sum (1). Because of the extremely close similarities in proof, we only sketch the argument. In § 6, we consider the corresponding sum

$$\sum_{n \leqslant N} \mu^2(n)\, \mathbf{e}_m(ag^n)$$

over square-free integers. For this sum, the argument is much easier, and our results are considerably stronger.

Throughout the paper, the implied constants in symbols 'O' and '$\ll$' may depend, where obvious, on one of the small positive parameters ε or δ, and are absolute otherwise (we recall that $A \ll B$ is equivalent to $A = O(B)$). For example, the well-known bound

$$\tau(n) \ll n^{\varepsilon} \tag{3}$$

holds for any $\varepsilon > 0$, where $\tau(n)$ denotes the number of positive integer divisors of $n \in \mathbb{N}$.

All of our results below are uniform in all parameters except (when present) ε or δ. In particular, our bounds are uniform over all integers a relatively prime to the modulus and over all integers g with the same multiplicative order modulo m or q.

2. Preparation

We use the following result of [Vau80] in the form given in [Dav80, ch. 24].

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

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

where

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

$$\Sigma_2 = (\log UV) \sum_{v \leqslant UV} \Big| \sum_{s \leqslant N/v} f(sv) \Big|,$$

https://doi.org/10.1112/S0010437X03000022 Published online by Cambridge University Press

$$\Sigma_3 = (\log N) \sum_{v \leqslant V} \max_{w \geqslant 1} \Big| \sum_{w \leqslant s \leqslant N/v} f(sv) \Big|,$$

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

The next result is essentially Theorem 10 in [Kor92, ch. 1]; see also the proof of Lemma 2 in [Kor72].

Lemma 2.2. *Let ϑ be of multiplicative order T modulo a positive integer m. Then, for any $H_1 < H_2$ and any integer a relatively prime to m,*

$$\sum_{H_1 < x \leqslant H_2} \mathbf{e}_m(a\vartheta^x) \ll \left(\frac{H_2 - H_1}{T} + 1 \right) m^{1/2} \log m.$$

In fact, the statement referred to in [Kor92] is the corresponding bound

$$\left| \sum_{x=1}^{T} \mathbf{e}_m(a\vartheta^x)\, \mathbf{e}_T(bx) \right| \leqslant m^{1/2} \tag{4}$$

for the relevant complete sum, which is valid for any integer b. Lemma 2.2 follows from this by the standard method of 'completing the sum'. Thus, the factor $\log m$ occurring in Lemma 2.2 is really only necessary for the second term on the right-hand side, not the first.

We also need the following variant of the bound (4).

Lemma 2.3. *Let ϑ be of multiplicative order T modulo a positive integer m. Then, for any integer a relatively prime to m,*

$$\sum_{\substack{x=1 \\ \gcd(x,T)=1}}^{T} \mathbf{e}_m(a\vartheta^x) \ll 2^{\nu(T)} m^{1/2},$$

where $\nu(T)$ is the number of distinct prime divisors of T.

Proof. Using the inclusion–exclusion principle to detect the coprimality condition $\gcd(x, T) = 1$, we obtain

$$\sum_{\substack{x=1 \\ \gcd(x,T)=1}}^{T} \mathbf{e}_m(a\vartheta^x) = \sum_{d \mid T} \mu(d) \sum_{\substack{x=1 \\ x \equiv 0 \pmod d}}^{T} \mathbf{e}_m(a\vartheta^x) = \sum_{d \mid T} \mu(d) \sum_{x=1}^{T/d} \mathbf{e}_m(a\vartheta^{dx}),$$

where, as usual, μ denotes the Möbius function. Because ϑ^d is of multiplicative order T/d, we can use the bound (4), which gives

$$\left| \sum_{\substack{x=1 \\ \gcd(x,T)=1}}^{T} \mathbf{e}_m(a\vartheta^x) \right| \leqslant m^{1/2} \sum_{d \mid T} |\mu(d)| = 2^{\nu(T)} m^{1/2}. \qquad \square$$

The following statement is the most important special case of Theorem 9 from [FK02].

Lemma 2.4. *Let ϑ be of multiplicative order T modulo a positive integer m. Then, for any integers a and b with $\gcd(a, m) = 1$, we have*

$$\sum_{y=1}^{T} \left| \sum_{x=1}^{T} \mathbf{e}_m(a\vartheta^x + b\vartheta^{xy}) \right|^4 \ll T^{9/4} m^{5/2+\varepsilon}.$$

https://doi.org/10.1112/S0010437X03000022 Published online by Cambridge University Press

We are now ready to prove our basic estimate for weighted double sums that is needed for the Vaughan combinatorial lemma. For any sequence $\alpha = (\alpha_k)$ of complex numbers with finite support, we denote its ℓ_2 norm by

$$\|\alpha\| = \Bigg(\sum_k |\alpha_k|^2 \Bigg)^{1/2}.$$

Lemma 2.5. *Let m be a positive integer, g an integer relatively prime to m, and t the multiplicative order of g modulo m. Let K, L, X, Y be real numbers with $X, Y > 0$. Then, for any two sequences of complex numbers $\alpha = (\alpha_k)$ supported on the interval $[K, K+X]$ and $\beta = (\beta_\ell)$ supported on $[L, L+Y]$, and for any integer a relatively prime to m, we have*

$$\sum_{\substack{K<k\leqslant K+X \\ L<\ell\leqslant L+Y}} \alpha_k \beta_\ell \, \mathbf{e}_m(ag^{k\ell}) \ll \|\alpha\|\|\beta\|(X/t+1)^{1/2}(Y/t+1)^{1/2} t^{21/32} m^{5/16+\varepsilon}.$$

Proof. First we group together terms in the sum in accordance with the greatest common divisor of ℓ and t. By the triangle inequality,

$$\left| \sum_{\substack{K<k\leqslant K+X \\ L<\ell\leqslant L+Y}} \alpha_k \beta_\ell \, \mathbf{e}_m(ag^{k\ell}) \right| \leqslant \sum_{d \mid t} \sigma_d(a),$$

where

$$\sigma_d(a) = \left| \sum_{K<k\leqslant K+X} \sum_{\substack{L<\ell\leqslant L+Y \\ \gcd(\ell,t)=d}} \alpha_k \beta_\ell \, \mathbf{e}_m(ag^{k\ell}) \right|.$$

Using the Cauchy inequality, we find

$$\begin{aligned}
\sigma_d(a)^2 &\leqslant \sum_{K<k\leqslant K+X} |\alpha_k|^2 \sum_{K<k\leqslant K+X} \left| \sum_{\substack{L<\ell\leqslant L+Y \\ \gcd(\ell,t)=d}} \beta_\ell \, \mathbf{e}_m(ag^{k\ell}) \right|^2 \\
&\leqslant \|\alpha\|^2 (X/t+1) \sum_{k=1}^{t} \left| \sum_{\substack{L<\ell\leqslant L+Y \\ \gcd(\ell,t)=d}} \beta_\ell \, \mathbf{e}_m(ag^{k\ell}) \right|^2 \\
&= \|\alpha\|^2 (X/t+1) \sum_{\substack{L<\ell,r\leqslant L+Y \\ \gcd(\ell,t)=\gcd(r,t)=d}} \beta_\ell \overline{\beta_r} \sum_{k=1}^{t} \mathbf{e}_m(a(g^{k\ell} - g^{kr})).
\end{aligned}$$

Since $2|\beta_\ell \overline{\beta_r}| \leqslant |\beta_\ell|^2 + |\beta_r|^2$, we deduce that

$$\begin{aligned}
\sigma_d(a)^2 &\leqslant \frac{1}{2}\|\alpha\|^2 (X/t+1) \sum_{\substack{L<\ell,r\leqslant L+Y \\ \gcd(\ell,t)=\gcd(r,t)=d}} |\beta_\ell|^2 \left| \sum_{k=1}^{t} \mathbf{e}_m(a(g^{k\ell} - g^{kr})) \right| \\
&\quad + \frac{1}{2}\|\alpha\|^2 (X/t+1) \sum_{\substack{L<\ell,r\leqslant L+Y \\ \gcd(\ell,t)=\gcd(r,t)=d}} |\beta_r|^2 \left| \sum_{k=1}^{t} \mathbf{e}_m(a(g^{k\ell} - g^{kr})) \right|
\end{aligned}$$

https://doi.org/10.1112/S0010437X03000022 Published online by Cambridge University Press

$$= \|\alpha\|^2 (X/t+1) \sum_{\substack{L<\ell,r\leqslant L+Y\\ \gcd(\ell,t)=\gcd(r,t)=d}} |\beta_\ell|^2 \left| \sum_{k=1}^{t} \mathbf{e}_m(a(g^{k\ell}-g^{kr}))\right|$$

$$\leqslant \|\alpha\|^2 (X/t+1)(Y/t+1) \sum_{\substack{L\leqslant\ell\leqslant L+Y\\ \gcd(\ell,t)=d}} |\beta_\ell|^2 \sum_{\substack{1\leqslant r\leqslant t\\ \gcd(r,t)=d}} \left| \sum_{k=1}^{t} \mathbf{e}_m(a(g^{k\ell}-g^{kr}))\right|.$$

Since each element ℓ with $\gcd(\ell,t)=d$ can be represented in the form $\ell = dw$ with $\gcd(w,t/d)=1$, and $\vartheta_d = g^d$ is of multiplicative order t/d, it follows that the inner double sum over r and k does not depend on ℓ (to see this, make the change of variables $k \mapsto kw^{-1}$, $r \mapsto rw$). Therefore,

$$\sigma_d(a)^2 \leqslant \|\alpha\|^2 (X/t+1)(Y/t+1) \sum_{\substack{L\leqslant\ell\leqslant L+Y\\ \gcd(\ell,t)=d}} |\beta_\ell|^2 \sum_{\substack{1\leqslant r\leqslant t\\ \gcd(r,t)=d}} \left| \sum_{k=1}^{t} \mathbf{e}_m(a(g^{kd}-g^{kr}))\right|$$

$$\leqslant \|\alpha\|^2 (X/t+1)(Y/t+1) \sum_{\substack{L\leqslant\ell\leqslant L+Y\\ \gcd(\ell,t)=d}} |\beta_\ell|^2 \sum_{r=1}^{t/d} \left| \sum_{k=1}^{t} \mathbf{e}_m(a(\vartheta_d^k-\vartheta_d^{kr}))\right|$$

$$= \|\alpha\|^2 (X/t+1)(Y/t+1) dS \sum_{\substack{L\leqslant\ell\leqslant L+Y\\ \gcd(\ell,t)=d}} |\beta_\ell|^2,$$

where

$$S = \sum_{r=1}^{t/d} \left| \sum_{k=1}^{t/d} \mathbf{e}_m(a(\vartheta_d^k-\vartheta_d^{kr}))\right|.$$

By the Hölder inequality and Lemma 2.4, we see that

$$S^4 \leqslant (t/d)^3 \sum_{r=1}^{t/d} \left| \sum_{k=1}^{t/d} \mathbf{e}_m(a(\vartheta_d^k-\vartheta_d^{kr}))\right|^4 \ll (t/d)^3 (t/d)^{9/4} m^{5/2+\varepsilon},$$

so that

$$dS \ll t^{21/16} d^{-5/16} m^{5/8+\varepsilon} \ll t^{21/16} m^{5/8+\varepsilon}.$$

Consequently,

$$\sigma_d(a) \ll \|\alpha\| (X/t+1)^{1/2} (Y/t+1)^{1/2} t^{21/32} m^{5/16+\varepsilon} \left(\sum_{\substack{L\leqslant\ell\leqslant L+Y\\ \gcd(\ell,t)=d}} |\beta_\ell|^2 \right)^{1/2}$$

for every divisor $d|t$. Summing over d and using the Cauchy inequality, we obtain

$$\sum_{d|t} \left(\sum_{\substack{L\leqslant\ell\leqslant L+Y\\ \gcd(\ell,t)=d}} |\beta_\ell|^2 \right)^{1/2} \leqslant (\tau(t))^{1/2} \|\beta\|.$$

Applying the bound (3) and taking into account the fact that $t \leqslant m$, we obtain the stated result. □

In the special case where $m = q$ is a prime number one can improve upon the preceding results. In this case, instead of Lemma 2.4, we use the following stronger bound from [CFKLLS00] (see also [CFS99] for an earlier result of this type).

https://doi.org/10.1112/S0010437X03000022 Published online by Cambridge University Press

Lemma 2.6. *Let ϑ be of multiplicative order T modulo a prime number q. Then, for any integers a and b with $\gcd(a,q)=1$, we have*

$$\sum_{y=1}^{T}\Bigg|\sum_{x=1}^{T}\mathbf{e}_q(a\vartheta^x+b\vartheta^{xy})\Bigg|^4 \ll T^{11/3}q.$$

Using Lemma 2.6 in place of Lemma 2.4, we obtain the following stronger analogue of Lemma 2.5.

Lemma 2.7. *Let q be a prime number, a and g integers not divisible by q, and t the multiplicative order of g modulo q. Let K, L, X, Y be real numbers with $X,Y>0$. Then, for any two sequences of complex numbers $\alpha=(\alpha_k)$ supported on the interval $[K,K+X]$ and $\beta=(\beta_\ell)$ supported on $[L,L+Y]$, we have*

$$\sum_{\substack{K<k\leqslant K+X\\ L<\ell\leqslant L+Y}}\alpha_k\beta_\ell\,\mathbf{e}_m(ag^{k\ell}) \ll \|\alpha\|\|\beta\|(X/t+1)^{1/2}(Y/t+1)^{1/2}t^{5/6}q^{1/8+\varepsilon}.$$

Finally, we need the following result.

Lemma 2.8. *For $K^{1/2}\leqslant X\leqslant K$, we have the bounds*

$$\sum_{K<k\leqslant K+X}\tau(k)\ll X\log K \quad \text{and} \quad \sum_{K<k\leqslant K+X}\tau^2(k)\ll X(\log K)^3.$$

These bounds, actually valid in a larger range, may be found for example as special cases of Theorem 2 from [Shi80].

3. Main results

Theorem 3.1. *Fix $\varepsilon>0$. Let m be a positive integer, g an integer relatively prime to m, and t the multiplicative order of g modulo m. Then we have the bound*

$$\max_{\gcd(a,m)=1}\Bigg|\sum_{n\leqslant N}\Lambda(n)\,\mathbf{e}_m(ag^n)\Bigg| \ll (Nt^{-11/32}m^{5/16}+N^{5/6}t^{5/48}m^{7/24})N^{\varepsilon},$$

where the implied constant depends only on ε.

Proof. Let $U,V>1$ with $UV\leqslant N$ and apply Lemma 2.1 with the function $f(n)=\mathbf{e}_m(ag^n)$. In the notation of that lemma we have, by Chebyshev's bound,

$$\Sigma_1=\Bigg|\sum_{1\leqslant n\leqslant U}\Lambda(n)f(n)\Bigg|\leqslant\sum_{1\leqslant n\leqslant U}\Lambda(n)\ll U. \tag{5}$$

Next, since the multiplicative order of $\vartheta=g^v$ is $t/\gcd(t,v)$, Lemma 2.2 yields the bound

$$\begin{aligned}\Sigma_2&\leqslant\log N\sum_{1\leqslant v\leqslant UV}\left(\frac{N\gcd(t,v)}{vt}+1\right)m^{1/2}\log m\\ &\leqslant Nt^{-1}m^{1/2}\log N\log m\sum_{1\leqslant v\leqslant UV}\frac{\gcd(t,v)}{v}+UVm^{1/2}\log N\log m.\end{aligned}$$

https://doi.org/10.1112/S0010437X03000022 Published online by Cambridge University Press

Moreover,

$$\sum_{1\leqslant v\leqslant UV}\frac{\gcd(t,v)}{v}=\sum_{d\mid t}\sum_{\substack{1\leqslant v\leqslant UV\\ \gcd(t,v)=d}}\frac{d}{v}\leqslant\sum_{d\mid t}\sum_{\substack{1\leqslant v\leqslant UV\\ d\mid v}}\frac{d}{v}$$
$$=\sum_{d\mid t}\sum_{1\leqslant w\leqslant UV/d}\frac{1}{w}\ll\sum_{d\mid t}\log UV\leqslant\tau(t)\log N.$$

Therefore, we obtain the estimate

$$\Sigma_2\ll(Nt^{-1}m^{1/2}+UVm^{1/2})N^{\varepsilon}. \tag{6}$$

Similarly, we obtain the stronger bound

$$\Sigma_3\ll(Nt^{-1}m^{1/2}+Vm^{1/2})N^{\varepsilon}. \tag{7}$$

It remains only to estimate Σ_4. Let us denote

$$A(k)=\Big|\sum_{d\mid k,\ d\leqslant V}\mu(d)\Big|,$$

so that, using (3), we obtain

$$A(k)\leqslant\tau(k)\ll k^{\varepsilon/4}\quad\text{and}\quad\Lambda(\ell)\leqslant\log\ell\ll\ell^{\varepsilon/4}. \tag{8}$$

Now, let Δ be fixed in the range $1/V<\Delta<1/2$, and define the set

$$\Omega=\{V(1+\Delta)^i\mid 0\leqslant i\leqslant R\},$$

where

$$R=\left\lfloor\frac{\log(N/V)}{\log(1+\Delta)}\right\rfloor\ll\Delta^{-1}\log N.$$

Then

$$\Sigma_4=\sum_{\substack{k\ell\leqslant N\\ k>V,\,\ell>U}}A(k)\Lambda(\ell)\,\mathbf{e}_m(ag^{k\ell})=\sum_{K\in\Omega}\sigma(K),$$

where

$$\sigma(K)=\sum_{\substack{K<k\leqslant K(1+\Delta)\\ k<N/U}}\ \sum_{U<\ell\leqslant N/k}A(k)\Lambda(\ell)\,\mathbf{e}_m(ag^{k\ell}).$$

For any k in the range $K<k\leqslant K(1+\Delta)$, we have $N/k=N/K+O(\Delta N/K)$. Assuming that

$$\Delta N\geqslant K \tag{9}$$

and using (8), it follows that

$$\sigma(K)=\widetilde{\sigma}(K)+O(\Delta^2N^{1+3\varepsilon/4}),$$

where

$$\widetilde{\sigma}(K)=\sum_{\substack{K<k\leqslant K(1+\Delta)\\ k<N/U}}\ \sum_{U<\ell\leqslant N/K}A(k)\Lambda(\ell)\,\mathbf{e}_m(ag^{k\ell}).$$

Because Ω has at most $O(\Delta^{-1}\log N)$ elements, it follows that

$$\Sigma_4=\sum_{K\in\Omega}\widetilde{\sigma}(K)+O(\Delta N^{1+\varepsilon}). \tag{10}$$

We can estimate each $\widetilde{\sigma}(K)$, using Lemma 2.5 together with (8), obtaining

$$\widetilde{\sigma}(K)\ll N^{\varepsilon}(\Delta K)^{1/2}(N/K)^{1/2}(\Delta K/t+1)^{1/2}(N/Kt+1)^{1/2}t^{21/32}m^{5/16}.$$

https://doi.org/10.1112/S0010437X03000022 Published online by Cambridge University Press

We write this as

$$\widetilde{\sigma}(K) \ll \widetilde{\sigma}_1(K) + \widetilde{\sigma}_2(K) + \widetilde{\sigma}_3(K) + \widetilde{\sigma}_4(K), \tag{11}$$

where

$$\widetilde{\sigma}_1(K) = \Delta N^{1+\varepsilon} t^{-11/32} m^{5/16}, \quad \widetilde{\sigma}_2(K) = \Delta N^{1/2+\varepsilon} K^{1/2} t^{5/32} m^{5/16},$$
$$\widetilde{\sigma}_3(K) = \Delta^{1/2} N^{1+\varepsilon} K^{-1/2} t^{5/32} m^{5/16}, \quad \widetilde{\sigma}_4(K) = \Delta^{1/2} N^{1/2+\varepsilon} t^{21/32} m^{5/16}.$$

For any real number α we trivially have

$$\sum_{\substack{K \in \Omega \\ A \leqslant K \leqslant B}} K^\alpha \ll \Delta^{-1}(B^\alpha + A^\alpha) \log N.$$

In particular, we derive that

$$\sum_{K \in \Omega} \widetilde{\sigma}_1(K) \ll N^{1+\varepsilon} t^{-11/32} m^{5/16}, \quad \sum_{K \in \Omega} \widetilde{\sigma}_2(K) \ll N^{1+\varepsilon} U^{-1/2} t^{5/32} m^{5/16},$$
$$\sum_{K \in \Omega} \widetilde{\sigma}_3(K) \ll \Delta^{-1/2} N^{1+\varepsilon} V^{-1/2} t^{5/32} m^{5/16}, \quad \sum_{K \in \Omega} \widetilde{\sigma}_4(K) \ll \Delta^{-1/2} N^{1/2+\varepsilon} t^{21/32} m^{5/16},$$

which are valid for every $\varepsilon > 0$. Putting these results together with (10) and (11), and then with (5), (6), and (7), we find that

$$\Sigma_4 \ll (B_1 + B_2 + B_3 + B_4 + B_5) N^\varepsilon,$$

and

$$\sum_{n \leqslant N} \Lambda(n)\, \mathbf{e}_m(a g^n) \ll |\Sigma_4| + \Sigma_1 + \Sigma_2 + \Sigma_3$$
$$\ll (B_1 + B_2 + B_3 + B_4 + B_5 + B_6 + B_7) N^\varepsilon,$$

where

$$B_1 = N t^{-11/32} m^{5/16}, \quad B_2 = N U^{-1/2} t^{5/32} m^{5/16},$$
$$B_3 = \Delta^{-1/2} N V^{-1/2} t^{5/32} m^{5/16}, \quad B_4 = \Delta^{-1/2} N^{1/2} t^{21/32} m^{5/16},$$
$$B_5 = \Delta N, \quad B_6 = N t^{-1} m^{1/2}, \quad B_7 = UV m^{1/2}.$$

Note that the result is trivial unless $B_1 \leqslant N$ and so we can assume that $t \geqslant m^{10/11}$. From this it follows that $B_6 \leqslant B_1$, thus B_6 can be neglected.

Next we choose U and V. We balance B_2 and B_3 by setting $U = \Delta V$, and then we balance both of these with B_7 by choosing $U = \Delta^{2/5} N^{2/5} t^{1/16} m^{-3/40}$, which gives $B_2 = B_3 = B_7 = \Delta^{-1/5} N^{4/5} t^{1/8} m^{7/20}$. It is easy to see these choices are optimal.

Now we choose Δ to balance these with B_5, the appropriate choice being $\Delta = N^{-1/6} t^{5/48} m^{7/24}$; this gives $B_2 = B_3 = B_5 = B_7 = N^{5/6} t^{5/48} m^{7/24}$. This would certainly be an optimal choice for Δ were it not for the presence of B_4. Fortunately, this term does not present any real difficulty. Indeed, it can now be seen that, for a non-trivial bound, we require $N \geqslant t^{5/8} m^{7/4}$. Using this together with the trivial bound $t \leqslant m$ and the above choice of Δ, one verifies that $B_4 = N^{7/12} t^{29/48} m^{1/6} < B_5$.

It remains only to check that our choices of U, V, Δ satisfy the mild size restrictions imposed earlier. Since we can assume $N \geqslant 64 t^{5/8} m^{7/4}$, else the theorem is trivial, this implies $\Delta \leqslant 1/2$ as required. We also have $\Delta V \geqslant \Delta U = N^{1/6} t^{5/24} m^{1/3} > 1$ so that $\Delta > 1/U > 1/V$ and $U, V > 1$. In particular, since $K \leqslant N/U$, we see that the assumption (9) is satisfied for this choice of parameters. Finally, $UV = \Delta^{-3}(\Delta U)^2 = N^{5/6} t^{5/48} m^{-5/24} \leqslant N$ since $t \leqslant m$. The result follows. □

https://doi.org/10.1112/S0010437X03000022 Published online by Cambridge University Press

Theorem 3.2. *Fix $\varepsilon > 0$. Let q be a prime number, g an integer not divisible by q, and t the multiplicative order of g modulo q. We have*

$$\max_{\gcd(a,q)=1} \left| \sum_{n \leqslant N} \Lambda(n)\, \mathbf{e}_q(ag^n) \right| \ll (Nt^{-1/6}q^{1/8} + N^{5/6}t^{2/9}q^{1/6})N^{\varepsilon},$$

where the implied constant depends only on ε.

Proof. We follow the proof of Theorem 3.1 and keep the same notation. Applying Lemma 2.7 instead of Lemma 2.5, together with the estimate (8), we obtain that

$$\widetilde{\sigma}(K) \ll N^{\varepsilon}(\Delta K)^{1/2}(N/K)^{1/2}(\Delta K/t + 1)^{1/2}(N/Kt + 1)^{1/2}t^{5/6}q^{1/8}.$$

This improvement leads to the bound

$$\sum_{n \leqslant N} \Lambda(n)\, \mathbf{e}_m(ag^n) \ll (B_1 + B_2 + B_3 + B_4 + B_5 + B_6 + B_7)N^{\varepsilon},$$

where

$$B_1 = Nt^{-1/6}q^{1/8}, \quad B_2 = NU^{-1/2}t^{1/3}q^{1/8},$$
$$B_3 = \Delta^{-1/2}NV^{-1/2}t^{1/3}q^{1/8}, \quad B_4 = \Delta^{-1/2}N^{1/2}t^{5/6}q^{1/8},$$
$$B_5 = \Delta N, \quad B_6 = Nt^{-1}q^{1/2}, \quad B_7 = UVq^{1/2}.$$

Balancing these expressions as before leads to the choice $U = \Delta V = \Delta^{2/5}N^{2/5}t^{2/15}q^{-3/20}$, then to $\Delta = N^{-1/6}t^{2/9}q^{1/6}$. Since the result is otherwise trivial we can assume that $t \geqslant q^{3/4}$ and that $N \geqslant 64t^{4/3}q$; then $B_j \leqslant N$ for $j = 1, \dots, 6$, $B_5 < B_1$, and $B_4 < B_2 = B_3 = B_6 = B_7$. Since we can also check that $1/V < 1/U < \Delta \leqslant 1/2$, and that $U, V > 1$, $UV < N$, the result follows. □

4. Longer sums

The results of the previous section are not quite sufficient to give the range of uniformity claimed in the introduction. It is easy to see that, as stated, the above estimates become trivial when N becomes extremely large in relation to m. Indeed, the factor N^{ε}, which is not important when N and m are of the same logarithmic order, becomes crucial for larger values of N. Nevertheless, it is possible to overcome this problem by a slightly more careful treatment which we now describe.

Theorem 4.1. *Let m be a positive integer and g an integer relatively prime to m. For each $\delta > 0$, there exists $\eta > 0$ such that if the multiplicative order t of g modulo m satisfies $t \geqslant m^{10/11+\delta}$, then for all $N \geqslant t^{5/8+\delta}m^{7/4}$ we have the bound*

$$\max_{\gcd(a,m)=1} \left| \sum_{n \leqslant N} \Lambda(n)\, \mathbf{e}_m(ag^n) \right| \ll Nt^{-\eta},$$

where the implied constant depends only on δ.

Proof. Let us fix a large constant $A > 0$. For $N \leqslant m^A$, the desired result follows immediately from Theorem 3.1.

We now extend the range of N for which our bound is non-trivial from m^A up to $\exp(m^{\gamma})$ for some fixed $\gamma > 0$. To do this, it suffices to replace the factor N^{ε} in Theorem 3.1 by any expression of the form $m^{\varepsilon}(\log N)^c$, where $c > 0$ is an absolute constant. Examining our earlier treatment, we see at once that, in our bounds for Σ_1, Σ_2, and Σ_3, the factor N^{ε} can easily be replaced by $m^{\varepsilon}(\log N)^2$.

For Σ_4, the matter is a bit more complicated. To estimate Σ_4 we apply Lemma 2.8 to the sums

$$\sum_{K < k \leqslant K(1+\Delta)} A(k), \qquad \sum_{K < k \leqslant K(1+\Delta)} (A(k))^2, \quad K \in \Omega,$$

https://doi.org/10.1112/S0010437X03000022 Published online by Cambridge University Press

using the trivial bound $A(k) \leqslant \tau(k)$. To verify that Lemma 2.8 is applicable note that

$$\frac{\log(\Delta K)}{\log K} = 1 + \frac{\log \Delta}{\log K} \geqslant 1 + \frac{\log \Delta}{\log V}.$$

When $N > m^A$ and $A > 0$ is large, which we can assume to be the case, it is easily checked that with our earlier choice of the parameters the right-hand side is $2/3 + o(1)$ as A increases. We choose A sufficiently large so that the right-hand side is at least $1/2$.

Tracing through the reasoning in our earlier treatment of Σ_4, the first change required is in the approximation of $\sigma(K)$. To this end we require the first part of Lemma 2.8 which together with trivial bound $\Lambda(\ell) \leqslant \log N$ yields

$$\begin{aligned}\sum_{\substack{K<k\leqslant K(1+\Delta)\\ k<N/U}} \sum_{N/k<\ell\leqslant N/K} A(k)\Lambda(\ell) &\ll \Delta N K^{-1} \log N \sum_{\substack{K<k\leqslant K(1+\Delta)\\ k<N/U}} A(k)\\ &\ll \Delta^2 N (\log N)^2.\end{aligned}$$

The approximation now becomes

$$\sigma(K) = \widetilde{\sigma}(K) + O(\Delta^2 N (\log N)^2),$$

so that (10) is sharpened to

$$\Sigma_4 = \sum_{K\in\Omega} \widetilde{\sigma}(K) + O(\Delta N (\log N)^3).$$

Next, in the application of Lemma 2.5 that provides bounds for each $\widetilde{\sigma}_j(K)$, $1 \leqslant j \leqslant 4$, we now use the second part of Lemma 2.8 to estimate the sum over k, and we use the trivial bound $\Lambda(\ell) \leqslant \log N$ together with the Chebyshev bound to estimate the sum over ℓ. We find that N^ε can here be replaced by $m^\varepsilon (\log N)^2$. A further factor of $\log N$ is introduced when these bounds are summed over $K \in \Omega$.

Thus, without even bothering to optimize the final exponent of $\log N$, we can choose it to be $c = 3$ and take U, V, and Δ as before. As a result, we obtain the bound of Theorem 3.1 but with N^ε replaced by $m^\varepsilon (\log N)^3$, and this extends the range for N (for which the results save a power of t) up to $\exp(m^\gamma)$ for any fixed $\gamma < 3$.

By refining our method in the manner indicated above, we can dispense with the case $m > (\log N)^C$ for any $C > 3$, so that in the remaining case we may assume $m \leqslant (\log N)^C$, say with $C = 4$, which can be treated (as if the period m of the exponential sum is essentially fixed) by appealing to the Siegel–Walfisz theorem for the distribution of primes in arithmetic progressions modulo t. Thus

$$\psi(N; t, b) = \sum_{\substack{n\leqslant N\\ n\equiv b \pmod t}} \Lambda(n) = \chi_0(b) N/\varphi(t) + O(N(\log N)^{-8}),$$

where φ is the Euler function, χ_0 is the principal character modulo t, and where 8 can be replaced by whatever we like. This result may be found (in more general form) in many places. It occurs for example in [Dav80, ch. 22], albeit not under the name Siegel–Walfisz (although see the footnote on p. 133).

We can write our exponential sum in the form

$$\sum_{n\leqslant N} \Lambda(n)\, \mathbf{e}_m(ag^n) = \sum_{b=1}^{t} \mathbf{e}_m(ag^b)\psi(N; t, b).$$

On insertion of this in the asymptotic formula for ψ, the error term therein gives a contribution E

https://doi.org/10.1112/S0010437X03000022 Published online by Cambridge University Press

which satisfies the bound $E \ll tN(\log N)^{-8} \ll Nt^{-1}$. The main term gives a contribution

$$M = \frac{N}{\varphi(t)} \sum_{\substack{b=1 \\ \gcd(b,t)=1}}^{t} \mathbf{e}_m(ag^b)$$

and to complete the argument it remains to recall Lemma 2.3, the inequality $2^{\nu(t)} \leqslant \tau(t)$, and the bound (3). □

Theorem 4.1 implies that, for any $\delta > 0$, there exists positive real η such that if $N \geqslant t^{5/8+\delta}m^{7/4}$ and $t \geqslant m^{10/11+\delta}$, then

$$\max_{\gcd(a,m)=1} \left| \sum_{p \leqslant N} \mathbf{e}_m(ag^p) \right| \ll \pi(N)t^{-\eta}, \tag{12}$$

where the sum runs over all primes $p \leqslant N$. In particular, this bound holds for exponential sums over Mersenne numbers, hence we obtain (2) under the stated conditions (with t equal to the order of $g = 2$ modulo m). Indeed,

$$\left| \sum_{p \leqslant N} \mathbf{e}_m(a(g^p - 1)) \right| = \left| e_m(-a) \sum_{p \leqslant N} \mathbf{e}_m(ag^p) \right| = \left| \sum_{p \leqslant N} \mathbf{e}_m(ag^p) \right|$$

and, applying partial summation, we obtain

$$\begin{aligned}
\sum_{p \leqslant N} \mathbf{e}_m(ag^p) &= \sum_{2 \leqslant n \leqslant N} \frac{1}{\log n} \Lambda(n)\, \mathbf{e}_m(ag^n) + O(N^{1/2}) \\
&= \frac{1}{\log N} \sum_{n=2}^{N} \Lambda(n)\, \mathbf{e}_m(ag^n) + \sum_{M=2}^{N-1} \left(\frac{1}{\log M} - \frac{1}{\log(M+1)} \right) \sum_{n=2}^{M} \Lambda(n)\, \mathbf{e}_m(ag^n) + O(N^{1/2}) \\
&\ll \frac{1}{\log N} \left| \sum_{n=2}^{N} \Lambda(n)\, \mathbf{e}_m(ag^n) \right| + \sum_{M=2}^{N-1} \frac{1}{M \log^2 M} \left| \sum_{n=2}^{M} \Lambda(n)\, \mathbf{e}_m(ag^n) \right| + N^{1/2}.
\end{aligned}$$

After simple calculations, we obtain (12). Also, by Theorem 3.1 we see that

$$\max_{\gcd(a,m)=1} \left| \sum_{p \leqslant N} \mathbf{e}_m(aM_p) \right| \ll (Nt^{-11/32}m^{5/16} + N^{5/6}t^{5/48}m^{7/24})N^{\varepsilon}$$

for any $\varepsilon > 0$.

Analogously, for sums with prime denominators, we obtain the following result.

THEOREM 4.2. *Let q be a prime number, g an integer relatively prime to q. For each $\delta > 0$, there exists $\eta > 0$ such that if the multiplicative order t of g modulo q satisfies $t \geqslant q^{3/4+\delta}$, then for all $N \geqslant t^{4/3+\delta}q$ we have*

$$\max_{\gcd(a,q)=1} \left| \sum_{n \leqslant N} \Lambda(n)\, \mathbf{e}_q(ag^n) \right| \ll Nt^{-\eta},$$

where the implied constant depends only on δ.

Theorem 4.2 implies that, for any $\delta > 0$, there exists positive real η such that if $N \geqslant t^{4/3+\delta}q$ and $t \geqslant q^{3/4+\delta}$, then

$$\max_{\gcd(a,q)=1} \left| \sum_{p \leqslant N} \mathbf{e}_q(ag^p) \right| \ll \pi(N)t^{-\eta}.$$

In particular, this bound also holds for exponential sums over Mersenne numbers and implies (2) when $m = q$ is prime and the above conditions hold.

https://doi.org/10.1112/S0010437X03000022 Published online by Cambridge University Press

From Theorem 3.2 we also have

$$\max_{\gcd(a,q)=1} \Big| \sum_{p\leqslant N} \mathbf{e}_q(aM_p) \Big| \ll (Nt^{-1/6}q^{1/8} + N^{5/6}t^{2/9}q^{1/6})N^{\varepsilon}$$

for any $\varepsilon > 0$.

5. Sums weighted by the Möbius function

As is the case with many other sums over primes, the corresponding sums weighted by the Möbius function can be treated by essentially the same techniques. In this section we give such results. Because the methods are so very close to those in the previous sections we give only the briefest of sketches.

Theorem 5.1. *Theorems 3.1 and 4.1 hold under precisely the same conditions with the sum*

$$\sum_{n\leqslant N} \mu(n)\,\mathbf{e}_m(ag^n) \quad \textit{in place of} \quad \sum_{n\leqslant N} \Lambda(n)\,\mathbf{e}_m(ag^n),$$

as do Theorems 3.2 and 4.2 in the case where $m = q$ is prime.

Sketch of Proof. Our starting point before was Lemma 2.1. To prove the results in this case we need a similar combinatorial decomposition for μ. We may start, for example, with the following formula from § 3 of [FI98]. Let h be any arithmetic function, and let H be the summatory function $H(n) = \sum_{d|n} h(d)$. Then, if U, $V > 1$ and $n > U$, we have

$$h(n) = \sum_{\substack{b|n\\ b\leqslant V}} \mu(b)H(n/b) - \sum_{\substack{bc|n\\ b\leqslant V,\ c\leqslant U}} \mu(b)h(c) + \sum_{\substack{bc|n\\ b>V,\ c>U}} \mu(b)h(c).$$

Here, if we take $h = \Lambda$ so that $H(n) = \log n$, multiply by f, and then sum over n, we are led to a proof of Lemma 2.1. If instead we take $h = \mu$, so that (provided $n > V$) we have $H(n/b) = 0$ for all $b|n$ with $b \leqslant V$, then we are led to the analogous bound

$$\sum_{n\leqslant N} \mu(n)f(n) \ll \Sigma_1' + \Sigma_2' + \Sigma_3' + |\Sigma_4'|,$$

where

$$\Sigma_1' = \Big| \sum_{n\leqslant \max\{U,V\}} \mu(n)f(n) \Big|, \quad \Sigma_2' = \sum_{v\leqslant UV} \tau(v) \Big| \sum_{s\leqslant N/v} f(sv) \Big|,$$
$$\Sigma_3' = 0, \quad \Sigma_4' = \sum_{\substack{k\ell\leqslant N\\ k>V,\ \ell>U}} \mu(\ell) \Big| \sum_{d|k,\ d\leqslant V} \mu(d) \Big| f(k\ell).$$

Let us compare these with the corresponding sums Σ_j. We find that Σ_1' can again be bounded trivially, now by $\Sigma_1' \leqslant \max\{U, V\}$ which is worse than before but still very small, for example, when compared to the bound we gave for Σ_2. In estimating Σ_2' the extra factor $\tau(v)$ causes only a little trouble. Arguing as before in the proof of Theorem 3.1, we find that

$$\sum_{1\leqslant v\leqslant UV} \tau(v)\frac{\gcd(t,v)}{v} \ll \tau_3(t)\log^2 N,$$

so that the bound for Σ_2' is worse only in that $\tau(t)$ has been replaced by $\tau_3(t)$, the number of ways t can be written as the product of three positive integers. Since $\tau_3(t) \ll t^{\varepsilon} \leqslant m^{\varepsilon}$, none of the theorems is weakened at all. Obviously Σ_3' is easier than before. A little thought discloses that Σ_4' is virtually

https://doi.org/10.1112/S0010437X03000022 Published online by Cambridge University Press

the same as before, being a bit easier in one or two places where we can take advantage of the fact that the trivial bound for μ is better than the trivial bound for Λ.

Finally, for the very largest values of N, we replace the earlier Siegel–Walfisz bound by its Möbius function analogue:

$$\sum_{\substack{n\leqslant N\\ n\equiv b \pmod t}} \mu(n) \ll N(\log N)^{-8},$$

and, since there is no main term here, this part of the proof is somewhat simpler than before. □

6. Sums over square-free numbers

In this section, we show that much simpler arguments, which combine only the sieve of Eratosthenes with Lemma 2.2, can be used to treat the corresponding exponential sum over square-free numbers.

THEOREM 6.1. *Let m be a positive integer, g an integer relatively prime to m, and t the multiplicative order of g modulo m. Then we have the bound*

$$\max_{\gcd(a,m)=1} \left| \sum_{n\leqslant N} \mu^2(n)\, \mathbf{e}_m(ag^n) \right| \ll (Nt^{-1}m^{1/2} + N^{1/2}m^{1/4})t^{\varepsilon},$$

where the implied constant depends only on ε.

Proof. We have

$$\begin{aligned}\sum_{n\leqslant N} \mu^2(n)\, \mathbf{e}_m(ag^n) &= \sum_{d\leqslant N^{1/2}} \mu(d) \sum_{\substack{n\leqslant N\\ d^2\mid n}} \mathbf{e}_m(ag^n)\\ &= \sum_{d\leqslant N^{1/2}} \mu(d) \sum_{n\leqslant N/d^2} \mathbf{e}_m(ag^{nd^2}).\end{aligned}$$

If t is the multiplicative order of g modulo m, then the multiplicative order of g^{d^2} modulo m is $t/\gcd(t,d^2)$. Fix some $D \geqslant 1$. Using Lemma 2.2 for $d \leqslant D$ (assuming that $\gcd(a,m)=1$) and the trivial upper bound N/d^2 for $d > D$, we obtain

$$\begin{aligned}\sum_{n\leqslant N} \mu^2(n)\, \mathbf{e}_m(ag^n) &\ll \sum_{d\leqslant D} \left(\frac{N\gcd(t,d^2)}{td^2} + 1\right) m^{1/2}\log m + \sum_{d>D} \frac{N}{d^2}\\ &\ll Nt^{-1}m^{1/2}\log m \sum_{d\leqslant D} \frac{\gcd(t,d^2)}{d^2} + Dm^{1/2}\log m + ND^{-1}.\end{aligned}$$

Now, collecting together all numbers d with the same value of $\gcd(t,d) = f$ (thus $\gcd(t,d^2) \leqslant f^2$), we derive

$$\sum_{d\leqslant D} \frac{\gcd(t,d^2)}{d^2} = \sum_{f\mid t} \sum_{\substack{d\leqslant D\\ \gcd(t,d)=f}} \frac{\gcd(t,d^2)}{d^2} \leqslant \sum_{f\mid t} \sum_{d\leqslant D/f} \frac{1}{d^2} \leqslant 2\tau(t).$$

Choose $D = N^{1/2}m^{-1/4}\log^{-1/2} m$ to balance the other two terms. Note that for this choice we have $D \geqslant 1$ else the theorem is trivial. We obtain

$$\sum_{n\leqslant N} \mu^2(n)\, \mathbf{e}_m(ag^n) \ll Nt^{-1}\tau(t)m^{1/2}\log m + N^{1/2}m^{1/4}\log^{1/2} m.$$

Using (3) and remarking that the bound of the theorem is trivial for $t < m^{1/2}$, we obtain the result. □

https://doi.org/10.1112/S0010437X03000022 Published online by Cambridge University Press

Theorem 6.1 is non-trivial for $N \geqslant m^{1/2+\delta}$ and $t \geqslant m^{1/2+\delta}$ with any fixed $\delta > 0$. This is the same range in which the underlying Lemma 2.2 is non-trivial. We remark that in the case of prime denominators better bounds are known; see [KS99], which can be used to improve Theorem 6.1 in the case where $n = q$ is prime.

The same arguments also apply to sums over k-free numbers (that is, over numbers that are not divisible by the kth power of any prime number). In this situation, the second term in our estimate is improved to $N^{1/k}m^{(k-1)/2k}$ (after balancing $Dm^{1/2}\log m$ with N/D^{k-1}). The range in which this estimate is non-trivial remains the same, however.

7. Remarks

Our results are non-trivial provided that the multiplicative order t of g modulo m (or q) is sufficiently large. Although this should frequently be the case, unconditional results in this direction are still rather weak (see [EM99, IT02, KR01, MRS96, Pap96]) and only guarantee that when g is fixed, then, for any fixed ε, we have that t is at least $m^{1/2-\varepsilon}$ for almost all integers m, and is at least $q^{1/2-\varepsilon}$ for almost all primes q. We recall, however, that under the Extended Riemann Hypothesis, it is known that, provided again that g is fixed, t is at least $m^{1-\varepsilon}$ for almost all integers m and is at least $q^{1-\varepsilon}$ for almost all primes q; see [EM99, Kur01, LP]. We also remark that the results of [BH98] show that, for many primes q, the order t of g modulo q is substantially larger than $q^{1/2}$. In particular, it follows from [BH98] that $t \geqslant q^{0.677}$ for at least $cx/\log^2 x$ primes $q \leqslant x$ with a positive constant c.

Using some of the results of [FK02], which hold for an arbitrary modulus m, one can estimate exponential sums over *Fermat numbers* $F_n = 2^{2^n}+1$. Unfortunately, proving that there are members of this sequence of sufficiently large period modulo m appears to be quite difficult, and it is not clear whether there are any values of m for which the corresponding bound is non-trivial, although one certainly would expect this to be the case. Even for sums with a prime denominator q, the bounds from [FHS00] (which are stronger than those for the general case of [FK02]) do not overlap with what is currently known about the period of F_n modulo q; see [FPS01].

We have already mentioned that when $n = q$ is prime stronger variants of Lemma 2.2 are available which can be used to improve Theorem 6.1. These do not, however, yield any further improvement of our other results, as Lemma 2.7 remains a bottleneck for our approach.

We note that it would be of very great interest to estimate the sums

$$\sum_{n \leqslant N} \Lambda(n)\chi(g^n + a), \quad \gcd(a, m) = 1,$$

with multiplicative characters χ modulo m. Unfortunately, analogues of our underlying results, that is, those of [CFKLLS00] and [FK02], are not known for multiplicative characters. On the other hand, character sum analogues of Lemma 2.2 are known [DW92, Yu01]; thus one can extend Theorem 6.1 to character sums over square-free numbers.

Finally, studying similar exponential and character sums over various other interesting subsets of the integers $n \leqslant N$ leads to other challenging questions. In particular, one can consider the sums

$$\sum_{\substack{n \leqslant N \\ n \text{ is } r\text{-smooth}}} \mathbf{e}_m(ag^n) \quad \text{and} \quad \sum_{\substack{n \leqslant N \\ n \text{ is } r\text{-smooth}}} \chi(g^n + a),$$

over r-smooth integers (recall that $n \geqslant 1$ is called r-smooth if every prime divisor of n does not exceed r). Another tempting choice would be the sum over all integers up to N which can be expressed as the sum of two squares.

https://doi.org/10.1112/S0010437X03000022 Published online by Cambridge University Press

References

BH98 R. C. Baker and G. Harman, *Shifted primes without large prime factors*, Acta Arith. **83** (1998), 331–361.

CFKLLS00 R. Canetti, J. B. Friedlander, S. Konyagin, M. Larsen, D. Lieman and I. E. Shparlinski, *On the statistical properties of Diffie–Hellman distributions*, Israel J. Math. **120** (2000), 23–46.

CFS99 R. Canetti, J. Friedlander and I. Shparlinski, *On certain exponential sums and the distribution of Diffie-Hellman triples*, J. London Math Soc. **59** (1999), 799–812.

Dav80 H. Davenport, *Multiplicative number theory*, 2nd edn (Springer-Verlag, New York, 1980).

DW92 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.

EM99 P. Erdős and R. Murty, *On the order of a (mod p)*, in *Proc. 5th Canadian Number Theory Association Conf.* (American Mathematical Society, Providence, RI, 1999), 87–97.

FHS00 J. B. Friedlander, J. Hansen and I. E. Shparlinski, *On character sums with exponential functions*, Mathematika, **47** (2000), 75–85.

FI98 J. B. Friedlander and H. Iwaniec, *Asymptotic sieve for primes*, Annals of Math. **148** (1998), 1041–1065.

FK02 J. B. Friedlander, S. V. Konyagin and I. E. Shparlinski, *Some doubly exponential sums over* $\mathbb{Z}_m$, Acta Arith. **105** (2002), 349–370.

FPS01 J. B. Friedlander, C. Pomerance and I. E. Shparlinski, *Period of the power generator and small values of Carmichael's function*, Math. Comp. **70** (2001), 1591–1605 (see also Math. Comp. **71** (2002), 1803–1806).

FS01 J. B. Friedlander and I. E. Shparlinski, *Double exponential sums over thin sets*, Proc. Amer. Math. Soc. **129** (2001), 1617–1621.

Hea82 D. R. Heath-Brown, *Prime numbers in short intervals and a generalized Vaughan identity*, Canad. J. Math. **34** (1982), 1365–1377.

IT02 H.-K. Indlekofer and N. M. Timofeev, *Divisors of shifted primes*, Publ. Math. Debrecen, **60** (2002), 307–345.

Kor72 N. M. Korobov, *On the distribution of digits in periodic fractions*, Matem. Sbornik **89** (1972), 654–670 (in Russian) (English translation Math. USSR–Sb. **18** (1972), 659–676).

Kor92 N. M. Korobov, *Exponential sums and their applications* (Kluwer Academic, Dordrecht, 1992).

KR01 P. Kurlberg and Z. Rudnick, *On quantum ergodicity for linear maps of the torus*, Commun. Math. Phys. **222** (2001), 201–227.

KS99 S. V. Konyagin and I. Shparlinski, *Character sums with exponential functions and their applications* (Cambridge University Press, Cambridge, 1999).

Kur01 P. Kurlberg, *On the order of unimodular matrices modulo integers*, Acta Arith. (to appear).

LP S. Li and C. Pomerance, *On generalizing Artin's conjecture on primitive roots to composite moduli*, J. Reine Angew. Math. **556** (2003), 205–224.

MRS96 M. R. Murty, M. Rosen and J. H. Silverman, *Variations on a theme of Romanoff*, Int. J. Math. **7** (1996), 373–391.

Nie78 H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. **84** (1978), 957–1041.

Nie92 H. Niederreiter, *Random number generation and Quasi-Monte Carlo methods* (SIAM Press, 1992).

Pap96 F. Pappalardi, *On the order of finitely generated subgroups of* $\mathbb{Q}^*$ *(mod p) and divisors of* $p-1$, J. Number Theory **57** (1996), 207–222.

Shi80 P. Shiu, *A Brun–Titchmarsh theorem for multiplicative functions*, J. Reine Angew. Math. **313** (1980), 161–170.

Vau80 R. C. Vaughan, *An elementary method in prime number theory*, Acta Arith. **37** (1980), 111–115.

Vin54 I. M. Vinogradov, *The method of trigonometric sums in the theory of numbers* (Interscience, London, 1954).

Yu01 H. B. Yu, *Estimates of character sums with exponential function*, Acta Arith. **97** (2001), 211–218.

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

Alessandro Conflitti conflitt@mat.uniroma2.it
Dip. di Matematica, Università degli Studi di Roma 'Tor Vergata', Via della Ricerca Scientifica, I-00133 Roma, Italy

John B. Friedlander frdlndr@math.toronto.edu
Department of Mathematics, University of Toronto, Toronto, Ontario M5S 3G3, Canada

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

https://doi.org/10.1112/S0010437X03000022 Published online by Cambridge University Press