Exponential Sums over Mersenne Numbers

William D. Banks
Dept. of Mathematics, University of Missouri
Columbia, MO 65203, USA
bbanks@math.missouri.edu

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

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

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

Abstract

We give estimates for exponential sums of the form

$$\sum_{n \le N} \Lambda(n) \exp(2\pi i a g^n/m),$$

where m is a positive integer, a and g are integers relatively prime to m, and $\Lambda(n)$ is the von Mangoldt function. We also discuss some applications of our results. In particular, our results yield bounds for exponential sums of the form

$$\sum_{p \le N} \exp(2\pi i a M_p/m),$$

where M_p is the Mersenne number $M_p = 2^p - 1$ for any prime p.

AMS Subject Classification Numbers: 11L07, 11L20.

1 Introduction

It is well-known that methods originating with Vinogradov [24] have been used successfully to find nontrivial 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 [23] and to Heath-Brown [10]. 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 there are already in the literature a number of bounds for similar sums taken over consecutive integer values [12, 13, 14, 19, 20]. The corresponding double sums have not been previously studied, however. In Section 2, we obtain such bounds as a generalization of those in [7, 9].

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

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

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 $t \ge m^{10/11+\delta}$ and $N \ge t^{5/8+\delta} m^{7/4}$.

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

$$\sum_{p \le N} \mathbf{e}_m(aM_p) = o(\pi(N)), \tag{1}$$

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 $p \le N$.

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 (Section 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 Section 4) some refinements and further ingredients which depend on the distribution of primes in arithmetic progressions.

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

$$\tau(n) \ll n^{\varepsilon} \tag{2}$$

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 [23] in the form given in Chapter 24 of [4]:

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

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

where

$$\begin{aligned}
\Sigma_1 &= \left|\sum_{n\le U}\Lambda(n)f(n)\right|,\\
\Sigma_2 &= (\log UV)\sum_{v\le UV}\left|\sum_{s\le N/v}f(sv)\right|,\\
\Sigma_3 &= (\log N)\sum_{v\le V}\max_{w\ge 1}\left|\sum_{w\le s\le N/v}f(sv)\right|,\\
\Sigma_4 &= \sum_{\substack{k\ell\le N\\ k>V,\ \ell>U}}\Lambda(\ell)\left|\sum_{d\mid k,\ d\le V}\mu(d)\right| f(k\ell).
\end{aligned}$$

The next result is essentially Theorem 10 in Chapter 1 of [14]; see also the proof of Lemma 2 in [13].

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,*

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

In fact, the statement referred to in [14] is the corresponding bound

$$\left|\sum_{x=1}^{T}\mathbf{e}_m(a\vartheta^x)\,\mathbf{e}_T(bx)\right| \le m^{1/2} \tag{3}$$

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 side, not the first.

We also need the following variant of the bound (3).

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 (3), which gives

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

□

The following statement is the most important special case of Theorem 9 from [7].

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*

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

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

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

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*

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

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

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

where

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

Using the Cauchy inequality, we find

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

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

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

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,

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

where

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

By the Hölder inequality and Lemma 2.4, we see that

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

so that

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

Consequently,

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

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

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

Applying the bound (2) and taking into account the fact that $t \le m$, 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 [2] (see also [3] for an earlier result of this type).

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*

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

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*

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

Finally, we need the following result.

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

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

These bounds, actually valid in a larger range, may be found for example as special cases of Theorem 2 from [22].

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*

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

where the implied constant depends only on ε.

Proof. Let U, $V > 1$ with $UV \le N$ 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,

$$\Sigma_1 = \left| \sum_{1\le n\le U} \Lambda(n) f(n) \right| \le \sum_{1\le n\le U} \Lambda(n) \ll U. \tag{4}$$

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

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

Moreover,

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

Therefore, we obtain the estimate

$$\Sigma_2\ll\left(Nt^{-1}m^{1/2}+UVm^{1/2}\right)N^{\varepsilon}. \tag{5}$$

Similarly, we obtain the stronger bound

$$\Sigma_3\ll\left(Nt^{-1}m^{1/2}+Vm^{1/2}\right)N^{\varepsilon}. \tag{6}$$

It remains only to estimate Σ_4. Let us denote

$$A(k)=\left|\sum_{d|k,\ d\le V}\mu(d)\right|,$$

so that using (2), we obtain

$$A(k)\le\tau(k)\ll k^{\varepsilon/4}\qquad\text{and}\qquad\Lambda(\ell)\le\log\ell\ll\ell^{\varepsilon/4}. \tag{7}$$

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

$$\Omega=\left\{V(1+\Delta)^i\ \middle|\ 0\le i\le R\right\},$$

where

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

Then

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

where

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

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

$$\Delta N \ge K \tag{8}$$

and using (7), it follows that

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

where

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

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

$$\Sigma_4 = \sum_{K\in\Omega} \widetilde{\sigma}(K) + O(\Delta N^{1+\varepsilon}). \tag{9}$$

We can estimate each $\widetilde{\sigma}(K)$, using Lemma 2.5 together with (7), obtaining

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

We write this as

$$\widetilde{\sigma}(K) \ll \widetilde{\sigma}_1(K) + \widetilde{\sigma}_2(K) + \widetilde{\sigma}_3(K) + \widetilde{\sigma}_4(K), \tag{10}$$

where

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

For any real number α we trivially have

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

In particular, we derive that

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

which is valid for every $\varepsilon > 0$. Putting these results together with (9) and (10), and then with (4), (5) and (6), we find that

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

and

$$\begin{aligned}
\sum_{n\le N} \Lambda(n)\,\mathbf{e}_m(ag^n) &\ll |\Sigma_4| + \Sigma_1 + \Sigma_2 + \Sigma_3 \\
&\ll (B_1 + B_2 + B_3 + B_4 + B_5 + B_6 + B_7)\, N^{\varepsilon},
\end{aligned}$$

where

$$\begin{aligned}
B_1 &= Nt^{-11/32}m^{5/16}, \\
B_2 &= NU^{-1/2}t^{5/32}m^{5/16}, \\
B_3 &= \Delta^{-1/2}NV^{-1/2}t^{5/32}m^{5/16}, \\
B_4 &= \Delta^{-1/2}N^{1/2}t^{21/32}m^{5/16}, \\
B_5 &= \Delta N, \\
B_6 &= Nt^{-1}m^{1/2}, \\
B_7 &= UVm^{1/2}.
\end{aligned}$$

Note that the result is trivial unless $B_1 \le N$ and so we can assume that $t \ge m^{10/11}$. From this it follows that $B_6 \le B_1$, 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 nontrivial bound, we require $N \geq t^{5/8} m^{7/4}$. Using this together with the trivial bound $t \leq m$ 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 $N \geq 64 t^{5/8} m^{7/4}$, else the theorem is trivial, this implies $\Delta \leq 1/2$ as required. We also have

$$\Delta V \geq \Delta U = N^{1/6} t^{5/24} m^{1/3} > 1$$

so that $\Delta > 1/U > 1/V$ and $U, V > 1$. In particular, since $K \leq N/U$, we see that the assumption (8) is satisfied for this choice of parameters. Finally,

$$UV = \Delta^{-3} (\Delta U)^2 = N^{5/6} t^{5/48} m^{-5/24} \leq N$$

since $t \leq m$. The result follows. $\square$

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*

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

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 (7), 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

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

where

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

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 $t \ge q^{3/4}$ and that $N \ge 64t^{4/3}q$; then $B_j \le N$ 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 $1/V < 1/U < \Delta \le 1/2$, and that U, $V > 1$, $UV < N$, the result follows. $\square$

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 $t \ge m^{10/11+\delta}$, then for all $N \ge t^{5/8+\delta} m^{7/4}$ we have the bound*

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

where the implied constant depends only on δ.

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

We now extend the range of N for which our bound is nontrivial 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

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

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

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

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 $\Lambda(\ell) \le \log N$ yields

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

The approximation now becomes

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

so that (9) 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 $\widetilde{\sigma}_j(K)$, $1 \le j \le 4$, we now use the second part of Lemma 2.8 to estimate the sum over k, and we use the trivial bound $\Lambda(\ell) \le \log N$ 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 $m \le (\log N)^C$, 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

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

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 Chapter 22 of [4], albeit not under the name Siegel–Walfisz.

We can write our exponential sum in the form

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

On insertion of this in the asymptotic formula for ψ the error term therein gives a contribution E 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 $2^{\nu(t)} \le \tau(t)$ and the bound (2). $\square$

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

$$\max_{\gcd(a,m)=1} \left| \sum_{p\le N} \mathbf{e}_m\left(ag^p\right) \right| \ll \pi(N)t^{-\eta}, \tag{11}$$

where the sum runs over all primes $p \le N$. In particular, this bound holds for exponential sums over Mersenne numbers, hence we obtain (1) under the stated conditions (with t equal to the order of $g = 2$ modulo m). Indeed,

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

and, applying partial summation, we obtain

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

After simple calculations, we obtain (11). Also, by Theorem 3.1 we see that

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

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 $t \ge q^{3/4+\delta}$, then for all $N \ge t^{4/3+\delta}q$ we have*

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

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 $N \ge t^{4/3+\delta}q$ and $t \ge q^{3/4+\delta}$, then

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

In particular, this bound also holds for exponential sums over Mersenne numbers and implies (1) when $m = q$ is prime and the above conditions hold.

From Theorem 3.2 we also have

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

for any $\varepsilon > 0$.

5 Remarks

Our results are nontrivial 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 [5, 11, 16, 18, 21]) and only guarantee that when g is fixed, t is of order at least $m^{1/2}$ for almost all integers m, and of order at least $q^{1/2}$ for almost all primes q. We recall, however, that under the Extended Riemann Hypothesis, it is known that t is of order m for almost all integers m and of order q for almost all primes q; see [5, 15, 17]. We also remark that the results of [1] 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 [1] that $t \ge q^{0.677}$ for at least $cx/\log^2 x$ primes $q \le x$ with a positive constant c.

Using some of the results of [7], 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 nontrivial, although one certainly would expect this to be the case. Even for sums with a prime denominator q, the bounds from [6] (which are stronger than those for the general case of [7]) do not overlap with what is currently known about the period of F_n modulo q; see [8].

Finally, we note that it would be of very great interest to estimate the sums

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

with multiplicative characters χ modulo m. Unfortunately, analogues of our underlying results, that is, those of [2] and [7], are not known for multiplicative characters.

6 Acknowledgements

During the preparation of this paper, W. B. was supported in part by NSF grant DMS-0070628 and by Macquarie University (Sydney), J. F. was supported in part by NSERC grant A5123 and by the Max Planck Institut für Mathematik (Bonn), and I. S. was supported in part by ARC grant A00000184.

References

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

[2] 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.

[3] 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.

[4] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Springer-Verlag, New York 1980.

[5] P. Erdős and R. Murty, 'On the order of $a \pmod p$', *Proc. 5th Canadian Number Theory Association Conf.* Amer. Math. Soc., Providence, RI, 1999, 87–97.

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

[7] J. B. Friedlander, S. V. Konyagin and I. E. Shparlinski, 'Some doubly exponential sums over $\mathbb{Z}_m$', *Acta Arith.*, (to appear).

[8] 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.

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

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

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

[12] S. V. Konyagin and I. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.

[13] N. M. Korobov, 'On the distribution of digits in periodic fractions', *Matem. Sbornik*, **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 Acad. Publ., Dordrecht, 1992.

[15] P. Kurlberg,'On the order of unimodular matrices modulo integers', *Preprint*, 2001, 1–12.

[16] P. Kurlberg and Z. Rudnick, 'On quantum ergodicity for linear maps of the torus', *Comm. Math. Phys.*, **222** (2001), 201–227.

[17] S. Li and C. Pomerance, 'On generalizing Artin's conjecture on primitive roots to composite moduli,' *J. Reine Angew. Math.*, (to appear).

[18] M. R. Murty, M. Rosen and J. H. Silverman, 'Variations on a theme of Romanoff', *Intern. J. Math. Soc.*, **7** (1996), 373–391.

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

[20] H. Niederreiter, *Random number generation and Quasi–Monte Carlo methods*, SIAM Press, 1992.

[21] 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.

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

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

[24] I. M. Vinogradov, *The method of trigonometric sums in the theory of numbers*, Interscience Publisher, 1954.