Fields Institute Communications
Volume **00**, 0000

Congruences and Exponential Sums with the Euler Function

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

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

Dedicated to Hugh Williams on his sixtieth birthday

Abstract. We give upper bounds for the number of solutions to congruences with the Euler function $\varphi(n)$ and with the Carmichael function $\lambda(n)$. We also give nontrivial bounds for certain exponential sums involving $\varphi(n)$. Analogous results can also be obtained for the sum of divisors function and similar arithmetic functions.

1 Introduction

Let $\varphi(n)$ denote the Euler function:

$$\varphi(n) = \#\{1 \le a \le n \mid \gcd(a,n) = 1\}.$$

Let p be a prime number, fixed throughout, and put $\mathbf{e}_p(x) = \exp(2\pi i x/p)$ for all $x \in \mathbb{R}$. In this paper, we give upper bounds for exponential sums of the form

$$S_p(a,N) = \sum_{n=1}^{N} \mathbf{e}_p\left(a\varphi(n)\right),$$

where $\gcd(a,p) = 1$, and N is sufficiently large. Our bounds are nontrivial for a wide range of values of p, starting with $p \ge \log^9 N$. We remark that although it might be possible to improve on this power of $\log N$, for very small values of p relative to N, it is simply not possible to obtain nontrivial bounds. In fact, it has been shown in Theorem 3.5 of [5] that for any prime number p of size

$$p = o(\log\log N), \tag{1.1}$$

2000 *Mathematics Subject Classification.* Primary 11L07, 11N69; Secondary 11N37, 11L20.

the congruence $\varphi(n) \equiv 0 \pmod p$ holds for all positive integers $n \le N$ with at most $o(N)$ exceptions; see (2.3) below for a more precise formulation of this statement. Thus, for primes of this size, one has $S_p(a, N) = N + o(N)$.

We also estimate more general sums of the form

$$S_p(f, N) = \sum_{n=1}^{N} \mathbf{e}_p(f(\varphi(n))),$$

where $f(x)$ is a polynomial with integer coefficients and degree $d \ge 2$ that is not constant modulo p. In fact, our methods can be used without any further modifications to estimate the similar sums when $f(x)$ is a rational function (one only needs to deal appropriately with the poles).

We also expect that our methods can be applied to exponential sums with p replaced by an arbitrary positive integer m, although certain arguments would be more complicated. One should also be able to work with various other arithmetic functions, including the sum of divisors function $\sigma(n)$.

We also give bounds for the number $T_p(a, N)$ of positive integers $n \le N$ such that $\varphi(n) \equiv a \pmod p$ and for the number $L_p(a, N)$ of positive integers $n \le N$ such that $\lambda(n) \equiv a \pmod p$, where $\lambda(n)$ denotes the Carmichael function. We recall that $\lambda(n)$ is defined to be the largest possible order of any element in the unit group of the residue ring modulo $n \ge 1$. More precisely, for a prime power q^k, one has

$$\lambda\big(q^k\big) = \begin{cases} q^{k-1}(q-1) & \text{if } q \ge 3 \text{ or } k \le 2, \\ 2^{k-2} & \text{if } q = 2 \text{ and } k \ge 3, \end{cases}$$

and for arbitrary $n \ge 2$,

$$\lambda(n) = \operatorname{lcm}\left(\lambda\big(q_1^{k_1}\big), \ldots, \lambda\big(q_\nu^{k_\nu}\big)\right),$$

where $n = q_1^{k_1} \ldots q_\nu^{k_\nu}$ is the prime factorization of n. Of course, $\lambda(1) = 1$.

Throughout the paper, the implied constants in the symbols "O", "$\gg$" and "$\ll$" may occasionally, where obvious, depend on a real parameter $\varepsilon > 0$ and an integer $d \ge 1$ but are absolute otherwise. We recall that the notations $U \ll V$ and $V \gg U$ are equivalent to the statement that $U = O(V)$ for positive functions U and V. We also use the symbol "o" with its usual meaning: the statement $U = o(V)$ is equivalent to $U/V \to 0$.

Acknowledgements. Most of this work was done during a visit by W. B. to Macquarie University, whose hospitality and support are gratefully acknowledged. Work also supported in part, for W. B. by NSF grant DMS-0070628, and for I. S. by ARC grant DP0211459.

2 Preparations

Here we collect some known number-theoretic estimates which are used in the sequel.

For any integer $n \ge 2$, let $P(n)$ denote the largest prime divisor of n, and put $P(1) = 1$. As usual, we say that an integer $n \ge 1$ is Y-smooth if and only if $P(n) \le Y$. Let

$$\psi(X, Y) = \#\{1 \le n \le X \mid n \text{ is } Y\text{-smooth}\}.$$

The following estimate is a substantially relaxed and simplified version of Corollary 1.3 of [13]; see also [3].

Lemma 2.1 *Let $u = \log X/\log Y$. For any $u \to \infty$ with $u \le Y^{1/2}$, we have*

$$\psi(X,Y) \ll Xu^{-u+o(u)}.$$

Throughout the sequel, we denote by $\mathcal{P}$ the set of all prime numbers, $\mathcal{P}[Y,X]$ the set of $\ell \in \mathcal{P}$ with $Y < \ell \le X$, and $\mathcal{P}[X] = \mathcal{P}[1,X]$.

We also need the following simplified form of the Brun-Titchmarsh theorem; see Theorem 1 in Section 2.3.1 of [9] or Theorem 3.7 in Chapter 3 of [10].

Lemma 2.2 *For any $X > k$, let $\pi(X;k,a)$ be the number of primes $\ell \in \mathcal{P}[X]$ such that $\ell \equiv a \pmod k$. Then*

$$\pi(X;k,a) \ll \frac{X}{\varphi(k)\log(2X/k)}.$$

Finally, our principal tool is the following bound for exponential sums with prime numbers, which follows immediately from Theorem 2 of [16].

Lemma 2.3 *For any $X \ge 2$, the following bound holds:*

$$\max_{\gcd(c,p)=1} \left| \sum_{\ell \in \mathcal{P}[X]} \mathbf{e}_p(c\ell) \right| \ll (p^{-1/2} + X^{-1/4}p^{1/8} + p^{1/2}X^{-1/2})X\log^3 X.$$

Proof Let $\Lambda(n)$ denote the von Mangoldt function:

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

According to Theorem 2 of [16], we have for any integer $m \ge 2$:

$$\max_{\gcd(c,p)=1} \left| \sum_{n=2}^{m} \Lambda(n)\,\mathbf{e}_p(cn) \right| \ll (p^{-1/2} + m^{-1/4}p^{1/8} + p^{1/2}m^{-1/2})m\log^4 m.$$

Taking $M = \lfloor X \rfloor$, we apply partial summation:

$$\begin{aligned} \sum_{\ell \in \mathcal{P}[X]} \mathbf{e}_p(c\ell) &= \sum_{n=2}^{M} \frac{1}{\log n}\Lambda(n)\,\mathbf{e}_p(cn) + O(M^{1/2}) \\ &= \frac{1}{\log M}\sum_{n=2}^{M} \Lambda(n)\,\mathbf{e}_p(cn) \\ &\qquad + \sum_{m=2}^{M-1} \left(\frac{1}{\log m} - \frac{1}{\log(m+1)} \right) \sum_{n=2}^{m} \Lambda(n)\,\mathbf{e}_p(cn) + O(X^{1/2}) \\ &\ll \frac{1}{\log M}\left| \sum_{n=2}^{M} \Lambda(n)\,\mathbf{e}_p(cn) \right| + \sum_{m=2}^{M-1} \frac{1}{m\log^2 m}\left| \sum_{n=2}^{m} \Lambda(n)\,\mathbf{e}_p(cn) \right| + M^{1/2}. \end{aligned}$$

The result follows. □

Let $\mathcal{F}_{d,p}$ denote the set of polynomials with integer coefficients of degree d whose leading coefficient is relatively prime to p; that is,

$$\mathcal{F}_{d,p} = \big\{ f(x) = a_d x^d + \ldots + a_1 x + a_0 \in \mathbb{Z}[x] \,\big|\, a_d \not\equiv 0 \pmod p \big\}. \tag{2.1}$$

For exponential sums over primes with polynomials from $\mathcal{F}_{d,p}$, $d \ge 2$, we use the following bound of [7]. We remark that the condition $d \ge 2$ is important; thus Lemma 2.3 and Lemma 2.4 do not overlap.

Lemma 2.4 *For any $\varepsilon > 0$, $d \ge 2$ and $X \ge 2$, the following bound holds:*

$$\max_{g \in \mathcal{F}_{d,p}} \left| \sum_{\ell \in \mathcal{P}[X]} \mathbf{e}_p(g(\ell)) \right| \ll p^{3/16+\varepsilon} X^{25/32}.$$

For any integer a, let

$$\mathcal{T}_p(a, N) = \{1 \le n \le N \,|\, \varphi(n) \equiv a \pmod p\}, \tag{2.2}$$

and put $T_p(a, N) = \#\mathcal{T}_p(a, N)$. In the special case where $a \equiv 0 \pmod p$, we have the following bound, which is a partial case of Theorem 3.5 of [5].

Lemma 2.5 *For any $N \ge 2$, we have*

$$T_p(0, N) \ll \frac{N \log\log N}{p}.$$

We remark that the bound of Lemma 2.5 becomes trivial when $p = O(\log\log N)$, which is very close to the threshold (1.1) below which it is not possible to obtain nontrivial upper bounds. Indeed, for p satisfying (1.1), we have by inequality (4.2) of [5]:

$$T_p(0, N) = N + O(N \exp(-cp^{-1} \log\log N)), \tag{2.3}$$

for some absolute constant $c > 0$.

To study congruences with the Carmichael function, we need the following statement, which is Theorem 5 of [8].

Lemma 2.6 *For all sufficiently large numbers N and any $\Delta \ge (\log\log N)^3$, the number of positive integers $n \le N$ with*

$$\lambda(n) \le n \exp(-\Delta)$$

is at most $N \exp\left(-0.69\,(\Delta \log \Delta)^{1/3}\right)$.

3 Congruences with $\varphi(n)$

As in Section 2, let $\mathcal{T}_p(a, N)$ be defined by (2.2), and let $T_p(a, N) = \#\mathcal{T}_p(a, N)$. In this section, we consider the problem of estimating $T_p(a, N)$ in the case where $a \not\equiv 0 \pmod p$.

Theorem 3.1 *The following bound holds:*

$$\max_{\gcd(a,p)=1} T_p(a, N) \ll N w^{-w/2+o(w)} + \frac{Nw}{p},$$

where $w = \log N / \log p$. Moreover, if $p \le \exp\left(\sqrt{0.5 \log N \log\log N}\right)$, then

$$\max_{\gcd(a,p)=1} T_p(a, N) \ll N p^{-1+o(1)}.$$

Proof Without loss of generality, we can assume that $p \to \infty$ as $N \to \infty$, since the bounds are trivial otherwise. Throughout the proof, let a be fixed with $\gcd(a, p) = 1$. We define

$$u = \begin{cases} \dfrac{\log N}{2 \log p} & \text{if } p \ge \exp\left(\sqrt{0.5 \log N \log\log N}\right), \\ \dfrac{\log p}{\log\log p} & \text{if } p < \exp\left(\sqrt{0.5 \log N \log\log N}\right). \end{cases}$$

We also define a smoothness bound $K = N^{1/u}$. Note that $p \le K^{2/3}$ and $u \le K^{1/2}$ for sufficiently large values of N, and that $u \to \infty$ as $N \to \infty$.

Let $\mathcal{E}_1$ be the set of integers $n \in [1, N]$ such that n is K-smooth. Since all of the conditions of Lemma 2.1 hold, we have

$$\#\mathcal{E}_1 \ll Nu^{-u+o(u)}.$$

Next, let $\mathcal{E}_2$ be the set of integers $n \in [1, N]$ such that $P(n) > K$ and $P(n)^2 \mid n$. Then

$$\#\mathcal{E}_2 \ll \sum_{\ell \in \mathcal{P}[K, N^{1/2}]} \sum_{\substack{K < n \le N \\ \ell^2 \mid n}} 1 \le \sum_{\ell \in \mathcal{P}[K, N^{1/2}]} N/\ell^2 \le N \sum_{k > K} \frac{1}{k^2} \ll N/K.$$

Now define $\mathcal{N} = \{1, \dots, N\} \setminus (\mathcal{E}_1 \cup \mathcal{E}_2)$. Using the results above, we obtain that

$$T_p(a, N) \ll Nu^{-u+o(u)} + N/K + \sum_{\substack{n \in \mathcal{N} \\ \varphi(n) \equiv a \pmod p}} 1.$$

Since every $n \in \mathcal{N}$ can be expressed in the form $n = \ell m$ with $\ell \in \mathcal{P}[K, N/m]$ and $\gcd(\ell, m) = 1$, and since $\gcd(a, p) = 1$, it follows that

$$\sum_{\substack{n \in \mathcal{N} \\ \varphi(n) \equiv a \pmod p}} 1 \le \sum_{\substack{1 < m \le N/K \\ \varphi(m) \not\equiv 0 \pmod p}} \sum_{\substack{\ell \in \mathcal{P}[K, N/m] \\ \ell \equiv a_m \pmod p}} 1,$$

where $a_m \equiv 1 + a\varphi(m)^{-1} \pmod p$. By Lemma 2.2,

$$\sum_{\substack{\ell \in \mathcal{P}[K, N/m] \\ \ell \equiv a_m \pmod p}} 1 \ll \frac{N}{mp \log(2N/mp)} \le \frac{N}{mp \log(2K/p)} \ll \frac{N}{mp \log K},$$

since $p \le K^{2/3}$. Hence,

$$\sum_{\substack{n \in \mathcal{N} \\ \varphi(n) \equiv a \pmod p}} 1 \le \frac{N}{p \log K} \sum_{1 < m \le N/K} \frac{1}{m} \ll \frac{N \log(N/K)}{p \log K} < \frac{Nu}{p}.$$

Therefore

$$T_p(a, N) \ll Nu^{-u+o(u)} + N/K + Nu/p.$$

Because $p \le K^{2/3}$, we see that the second term never dominates, and the result follows. □

The bound (2.3) suggests that when p is very small relative to N, one might expect that $T_p(a, N) = o(N/p)$. By refining the arguments in Theorem 3.1 in order to make use of (2.3), we show that this is indeed the case in the following quantitative form:

Theorem 3.2 *There exists an absolute constant $C > 0$, such that for*

$$p \le C \frac{\log\log N}{\log\log\log N},$$

the following bound holds:

$$\max_{\gcd(a,p)=1} T_p(a, N) \ll \frac{N}{p} \exp(-Cp^{-1} \log\log N).$$

Proof Without loss of generality, we can assume that $p \to \infty$ as $N \to \infty$ since otherwise the result follows trivially from (2.3). Let a be fixed with $\gcd(a,p) = 1$. Put $u = \exp(0.5cp^{-1}\log\log N)$, where $c > 0$ is the constant from (2.3); by our hypothesis on the size of p, we see that $u \to \infty$ as $N \to \infty$. Finally, define the smoothness bound $K = N^{1/u}$. Since $u = (\log N)^{o(1)}$, we have that $K = \exp((\log N)^{1+o(1)})$, hence $u \le K^{1/2}$ and $p \le K^{1/2}$ if N is sufficiently large.

Proceeding as in Theorem 3.1 with these choices for u and K, we obtain the estimate

$$T_p(a,N) \ll Nu^{-u+o(u)} + N/K + \frac{N}{p\log K} \sum_{\substack{1<m\le N/K\\ \varphi(m)\not\equiv 0 \pmod p}} \frac{1}{m}.$$

Using partial summation together with the estimate (2.3), we also have (with $M = \lfloor N/K \rfloor$):

$$\begin{aligned}
&\sum_{\substack{1<m\le N/K\\ \varphi(m)\not\equiv 0 \pmod p}} \frac{1}{m} \\
&\qquad = \frac{1}{M}\,(M - T_p(0,M)) + \sum_{m=2}^{M-1}\left(\frac{1}{m} - \frac{1}{m+1}\right)(m - T_p(0,m)) \\
&\qquad \ll 1 + \sum_{m=3}^{M-1} \frac{\exp(-cp^{-1}\log\log m)}{m} = 1 + \sum_{m=3}^{M-1} \frac{1}{m(\log m)^{cp^{-1}}} \\
&\qquad \ll 1 + (\log M)^{1-cp^{-1}} \ll (\log N)^{1-cp^{-1}}.
\end{aligned}$$

Since

$$\frac{N}{p\log K}\,(\log N)^{1-cp^{-1}} = \frac{N}{p}\,\exp(-0.5cp^{-1}\log\log N),$$

we derive the estimate

$$T_p(a,N) \ll Nu^{-u+o(u)} + NK^{-1} + Np^{-1}\exp(-0.5cp^{-1}\log\log N).$$

Now let $C = c/3$, and suppose that p satisfies the hypothesis of the theorem. It is easily seen that

$$K = \exp((\log N)^{1+o(1)}) \gg p\exp(0.5cp^{-1}\log\log N).$$

Also,

$$\begin{aligned}
u = \exp(0.5cp^{-1}\log\log N) &\ge (\log\log N)^{1.5} \\
&\gg \log C + \log\log N - \log\log\log N \ge \log p,
\end{aligned}$$

thus

$$-u\log u\,(1+o(1)) \ll (1-u/2)\log u \ll \log u - \log p,$$

and therefore

$$u^{-u+o(u)} \ll up^{-1} = p^{-1}\exp(-0.5cp^{-1}\log\log N).$$

The result follows. □

4 Congruences with $\lambda(n)$

Let us define

$$\mathcal{L}_p(a,N) = \{1 \le n \le N \,|\, \lambda(n) \equiv a \pmod p\},$$

and put $L_p(a,N) = \#\mathcal{L}_p(a,N)$. Since the integers $\lambda(n)$ and $\varphi(n)$ always have the same set of prime divisors, it follows that $L_p(0,N) = T_p(0,N)$; thus the estimate for $T_p(0,N)$ in Lemma 2.5 applies to $L_p(0,N)$ as well.

In this section, we combine Theorem 3.1 with Lemma 2.6 to estimate $L_p(a,N)$ in certain ranges when $a \not\equiv 0 \pmod p$.

Theorem 4.1 *For*

$$\exp\left(3(\log\log N)^3\right) \le p \le \exp\left(\frac{\log N \log\log\log N}{5(\log\log N)^3}\right),$$

the following bound holds:

$$\max_{\gcd(a,p)=1} L_p(a,N) \ll N\left(\exp\left(-0.4w^{1/3}\left(\log w\right)^{2/3}\right) + \exp\left(-0.5\left(\log p \log\log p\right)^{1/3}\right)\right),$$

where $w = \log N/\log p$.

Proof Denote $h(n) = \varphi(n)/\lambda(n)$. For any $\eta \ge 1$, we have

$$L_p(a,N) \le \sum_{1\le h<\eta} \sum_{\substack{n\in\mathcal{L}_p(a,N)\\ h(n)=h}} 1 + \sum_{\substack{n\in\mathcal{L}_p(a,N)\\ h(n)\ge\eta}} 1 \le \sum_{1\le h<\eta} T_p(ah,N) + \sum_{\substack{n\in\mathcal{L}_p(a,N)\\ h(n)\ge\eta}} 1.$$

Then, provided that

$$\eta \ge \exp\left(\left(\log\log N\right)^3\right), \tag{4.1}$$

Theorem 3.1 and Lemma 2.6 together imply

$$L_p(a,N) \ll \eta\left(Nw^{-w/2+o(w)} + \frac{Nw}{p}\right) + N\exp\left(-0.69\left(\log\eta\log\log\eta\right)^{1/3}\right).$$

Now put

$$\eta = \min\left\{w^{w/4},\, p^{1/2}\right\}.$$

It follows from the conditions of the theorem that (4.1) is satisfied and also that $w = p^{o(1)}$; consequently,

$$\begin{aligned} L_p(a,N) &\ll N\eta^{-1/2+o(1)} + N\exp\left(-0.69\left(\log\eta\log\log\eta\right)^{1/3}\right) \\ &\ll N\exp\left(-0.69\left(\log\eta\log\log\eta\right)^{1/3}\right), \end{aligned}$$

and the result follows. □

It is easy to see that one can slightly improve the constants that occur in the statement of Theorem 4.1, both in the range specified for p and in the bound, but we have not done so in order to provide a cleaner statement.

5 Exponential Sums with $\varphi(n)$

We now show that the same arguments used in the proof of Theorem 3.1, combined with the bound of Lemma 2.5, can be used to estimate exponential sums with the Euler function.

Theorem 5.1 *The following bound holds:*

$$\max_{\gcd(a,p)=1} |S_p(a,N)| \ll N\left(\frac{\log^4 N}{p^{1/2}} + w^{-2w/5+o(w)}\right),$$

where $w = \log N/\log p$.

Proof Without loss of generality, we can assume that $p \ge \log^8 N$ since the bound is trivial otherwise. In particular, we can assume that p is sufficiently large for our purposes. Throughout the proof, fix a with $\gcd(a,p) = 1$. We define $K = p^{2.5}$ and denote by $\mathcal{E}_1$ the set of $n \in [1,N]$ which are K-smooth. Let

$$u = \frac{\log N}{\log K} = 2w/5.$$

It is easy to see that if $w \ge p^{1/3}$, then $p \le \log^3 N$ and the bound is trivial; thus we can assume that $u \le p^{1/2} \le K^{1/2}$. By Lemma 2.1, we have that

$$\#\mathcal{E}_1 \ll Nu^{-u+o(u)}.$$

Denote by $\mathcal{E}_2$ the set of $n \in [1,N]$ for which $P(n) > K$ and $P(n)^2 \mid n$. Then

$$\#\mathcal{E}_2 \ll \sum_{\ell \in \mathcal{P}[K,N]} N/\ell^2 \ll N/K.$$

Denote by $\mathcal{E}_3$ the set of $n \in [1,N]$ such that $P(n)^2 \not\mid n$ and $p \mid \varphi(m)$, where $m = n/P(n)$. Since $p \mid \varphi(n)$ for every $n \in \mathcal{E}_3$, Lemma 2.5 yields the estimate

$$\#\mathcal{E}_3 \ll \frac{N\log\log N}{p} \ll \frac{N\log p}{p}.$$

Finally, let $\mathcal{N} = \{1,\dots,N\} \setminus (\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3)$. From the preceding bounds, it follows that

$$\begin{aligned} S_p(a,N) &= \sum_{n\in\mathcal{N}} \mathbf{e}_p(a\varphi(n)) + O\left(N\left(\frac{\log p}{p} + u^{-u+o(u)} + K^{-1}\right)\right) \\ &= \sum_{n\in\mathcal{N}} \mathbf{e}_p(a\varphi(n)) + O\left(N\left(\frac{\log p}{p} + w^{-2w/5+o(w)}\right)\right). \end{aligned}$$

Now, every integer $n \in \mathcal{N}$ has a unique representation of the form $n = m\ell$, where $\ell \in \mathcal{P}[K,N]$, $\ell > P(m)$, and $p \not\mid \varphi(m)$. Conversely, if $L_m = \max\{K, P(m)\}$, then for any $m \le N/K$ such that $p \not\mid \varphi(m)$ and any $\ell \in \mathcal{P}[L_m, N/m]$, we have $n = m\ell \in \mathcal{N}$. Observing that $\varphi(n) = \varphi(m)(\ell-1)$, we obtain

$$\begin{aligned} \sum_{n\in\mathcal{N}} \mathbf{e}_p(a\varphi(n)) &= \sum_{\substack{m\le N/K \\ p\not\mid\varphi(m)}} \sum_{\ell\in\mathcal{P}[L_m,N/m]} \mathbf{e}_p(a\varphi(m\ell)) \\ &= \sum_{\substack{m\le N/K \\ p\not\mid\varphi(m)}} \mathbf{e}_p(-a\varphi(m)) \sum_{\ell\in\mathcal{P}[L_m,N/m]} \mathbf{e}_p(a\varphi(m)\ell). \end{aligned}$$

Write

$$\sum_{\ell \in \mathcal{P}[L_m, N/m]} \mathbf{e}_p(a\varphi(m)\ell) = \sum_{\ell \in \mathcal{P}[N/m]} \mathbf{e}_p(a\varphi(m)\ell) - \sum_{\ell \in \mathcal{P}[L_m]} \mathbf{e}_p(a\varphi(m)\ell),$$

and observe that the right hand side of the bound in Lemma 2.3 is a monotonically increasing function of X. Then it follows that

$$\sum_{\ell \in \mathcal{P}[L_m, N/m]} \mathbf{e}_p(a\varphi(m\ell)) \ll \frac{N}{m}\left(p^{-1/2} + N^{-1/4}m^{1/4}p^{1/8} + p^{1/2}m^{1/2}N^{-1/2}\right)\log^3 N.$$

Recalling that $m \le N/K = Np^{-5/2}$, we see that the first term always dominates the other two. Hence,

$$\sum_{\ell \in \mathcal{P}[L_m, N/m]} \mathbf{e}_p(a\varphi(m\ell)) \ll \frac{N\log^3 N}{mp^{1/2}},$$

Therefore,

$$\sum_{n \in \mathcal{N}} \mathbf{e}_p(a\varphi(n)) \ll \frac{N\log^3 N}{p^{1/2}} \sum_{m=1}^{N} \frac{1}{m} \ll \frac{N\log^4 N}{p^{1/2}},$$

and we obtain the stated result. □

It is easy to see that the bound of Theorem 5.1 is nontrivial when the conditions

$$\log N = o(p^{1/8}) \qquad \text{and} \qquad p = N^{o(1)}$$

both hold.

We now turn our attention to sums with polynomials f from the class $\mathcal{F}_{d,p}$ given by (2.1), with $d \ge 2$. As before, we remark that the condition $d \ge 2$ is important, thus Theorem 5.1 and Theorem 5.2 do not overlap.

Theorem 5.2 *For any $\varepsilon > 0$ and $d \ge 2$, the following bound holds:*

$$\max_{f \in \mathcal{F}_{d,p}} |S_p(f, N)| \ll N\left(p^{-1/4+\varepsilon} + w^{-w/2+o(w)}\right),$$

for $p \ge \log N$, where $w = \log N/\log p$.

Proof We use the same notation as in the proof of Theorem 5.1 except that we put $K = p^2$; thus $u = \log N/\log K = w/2 \le p = K^{1/2}$. As in the proof of Theorem 5.1 we obtain

$$\begin{aligned} S_p(f, N) &= \sum_{n \in \mathcal{N}} \mathbf{e}_p(f(\varphi(n))) + O\left(N\left(\frac{\log p}{p} + u^{-u+o(u)} + K^{-1}\right)\right) \\ &= \sum_{\substack{m \le N/K \\ p \nmid \varphi(m)}} \sum_{\ell \in \mathcal{P}[L_m, N/m]} \mathbf{e}_p(f(\varphi(m)(\ell-1))) + O\left(N\left(\frac{\log p}{p} + w^{-w/2+o(w)}\right)\right). \end{aligned}$$

It is clear that for each m in the sum above, the polynomial $f(\varphi(m)(x-1)) \in \mathcal{F}_{d,p}$. Therefore using Lemma 2.4 instead of Lemma 2.3, as in the proof of Theorem 5.1, we derive that

$$\begin{aligned} \sum_{\substack{m \le N/K \\ p \nmid \varphi(m)}} \sum_{\ell \in \mathcal{P}[L_m, N/m]} \mathbf{e}_p(f(\varphi(m)(\ell-1))) &\ll p^{3/16+\varepsilon} \sum_{m \le N/K} (N/m)^{25/32} \\ &\ll p^{3/16+\varepsilon} N K^{-7/32} = Np^{-1/4+\varepsilon}, \end{aligned}$$

and we obtain the stated result. □

Clearly, there are many possible admissible choices for K and thus a trade-off between the exponent of p and w^w (and the required bottom range of p).

6 Remarks

As we have already remarked, our approach should work in principle for exponential sums with $f(\varphi(n))$, where f is a polynomial with integer coefficients. Appropriate analogues of Lemma 2.3 can be found in [7, 11, 12]. It would also be interesting to consider such sums when f is a polynomial with irrational coefficients, however our methods do not seem to extend to this case. One can also fix an integer $g \ge 1$ of multiplicative order t modulo $m \ge 2$ and consider the rather exotic sums

$$V_m(a, g, N) = \sum_{n=1}^{N} \mathbf{e}_m\left(ag^{\varphi(n)}\right).$$

At least when t is prime, our method, combined with the upper bounds from [1] on sums with ag^ℓ taken over primes ℓ, should work in principle to estimate such sums. It would also be interesting to estimate exponential sums with the Euler function over integers taken from various special sets $\mathcal{S}$, such as shifted primes.

It would also be interesting to extend our results in another direction, namely to sums with arbitrary integer denominator m. In this case, as well as in the estimate of sums $V_m(a, g, N)$ for composite multiplicative orders t, one would need an analogue of Lemma 2.5 for arbitrary m. Clearly, proving such an analogue seems possible, but it requires some additional arguments. The problem of estimating the number of solutions to the congruence $\varphi(n) \equiv a \pmod m$, $1 \le n \le N$, is an interesting question in its own right, and it certainly deserves more attention. For moduli that are products of a fixed number of primes (not necessarily distinct), a generalization of Lemma 2.5 is given in [2]; in fact, it also applies to iterations of the Euler function. In the case where the modulus m is fixed and N is growing, rather detailed information about the distribution of $\varphi(n)$, $1 \le n \le N$, in residue classes modulo m can be found in [4, 6, 15]. However, this question remains open in the general case.

We also remark that by Lemma 2 of [14], almost all values of $\varphi(n)$, $1 \le n \le N$, are divisible by all prime powers

$$p^\alpha \ll \frac{\log\log N}{\log\log\log N}.$$

Therefore, for some constant $c > 0$ and some integer

$$m \ge (\log N)^{c/\log\log\log N}$$

one has $T_m(0, N) = N + o(N)$.

Sums with multiplicative characters might also be considered; in principle, our methods should provide nontrivial bounds in certain ranges, similar to those of Theorem 5.1.

Finally, we mention that our methods can be applied to the sum of divisors function $\sigma(n)$. However, it is still not clear how to estimate exponential sums with the Carmichael function $\lambda(n)$, even given its close relationship to the Euler function.

References

[1] W. Banks, A. Conflitti, J. B. Friedlander and I. E. Shparlinski, 'Exponential sums with Mersenne numbers', *Compositio Math.*, (to appear).

[2] N. L. Bassily, I. Kátai and M. Wijsmuller, 'On the prime power divisors of the iterates of the Euler-ϕ function', *Publ. Math. Debrecen* **55** (1999), 17–32.

[3] E. R. Canfield, P. Erdős and C. Pomerance, 'On a problem of Oppenheim concerning "Factorisatio Numerorum"', *J. Number Theory*, **17** (1983), 1–28.

[4] T. Dence and C. Pomerance, 'Euler's function in residue classes', *The Ramanujan J.* **2** (1998), 7–20.

[5] P. Erdős, A. Granville, C. Pomerance and C. Spiro, 'On the normal behaviour of the iterates of some arithmetic functions', in *Analytic Number Theory*, Birkhäuser, Boston, 1990, 165–204.

[6] K. Ford, S. Konyagin, and C. Pomerance, 'Residue classes free of values of Euler's function', *Number theory in progress, (Zakopane-Kościelisko, 1997)*, Vol. 2, de Gruyter, Berlin, 1999, 805–812.

[7] É. Fouvry and P. Michel, 'Sur certaines sommes d'exponentielles sur les nombres premiers', *Ann. Sci. École Norm. Sup.*, **31** (1998), 93–130.

[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] G. Greaves, *Sieves in number theory*, Springer-Verlag, Berlin, 2001.

[10] H. Halberstam and H.–E. Richert, *Sieve methods*, Academic Press, London, 1974.

[11] G. Harman, 'Trigonometric sums over primes, I', *Mathematika*, **28** (1981), 249–254.

[12] G. Harman, 'Trigonometric sums over primes, II', *Glasgow Math. J.*, **24** (1983), 23–37.

[13] A. Hildebrand and G. Tenenbaum, 'Integers without large prime factors', *J. de Théorie des Nombres de Bordeaux*, **5** (1993), 411–484.

[14] F. Luca and C. Pomerance, 'On some problems of Mąkowski–Schinzel and Erdős concerning the arithmetical functions φ and σ', *Colloq. Math.*, **92** (2002), 111–130.

[15] W. Narkiewicz, *Uniform distribution of sequences of integers in residue classes*, Lecture Notes in Math., Vol. 1087, Springer-Verlag, Berlin, 1984.

[16] R. C. Vaughan, 'Mean value theorems in prime number theory', *J. Lond. Math. Soc.*, **10** (1975), 153–162.