Canad. J. Math. Vol. **61** (3), 2009 pp. 481–502

Uniform Distribution of Fractional Parts Related to Pseudoprimes

William D. Banks, Moubariz Z. Garaev, Florian Luca, and Igor E. Shparlinski

Abstract. We estimate exponential sums with the Fermat-like quotients

$$f_g(n) = \frac{g^{n-1}-1}{n} \quad \text{and} \quad h_g(n) = \frac{g^{n-1}-1}{P(n)},$$

where g and n are positive integers, n is composite, and $P(n)$ is the largest prime factor of n. Clearly, both $f_g(n)$ and $h_g(n)$ are integers if n is a Fermat pseudoprime to base g, and if n is a Carmichael number, this is true for all g coprime to n. Nevertheless, our bounds imply that the fractional parts $\{f_g(n)\}$ and $\{h_g(n)\}$ are uniformly distributed, on average over g for $f_g(n)$, and individually for $h_g(n)$. We also obtain similar results with the functions $\widetilde{f}_g(n) = gf_g(n)$ and $\widetilde{h}_g(n) = gh_g(n)$.

1 Introduction

Throughout the paper, we use $P(n)$ to denote the largest prime divisor of the integer $n \ge 2$, and we put $P(1) = 1$.

For every integer $g \ge 1$, let $f_g(\cdot)$ and $h_g(\cdot)$ be the arithmetic functions defined by

$$f_g(n) = \frac{g^{n-1}-1}{n} \quad \text{and} \quad h_g(n) = \frac{g^{n-1}-1}{P(n)} \quad (n \ge 1).$$

Clearly, $f_g(n)$ and $h_g(n)$ are *integers* if n is a prime number and $n \nmid g$. On the other hand, if n takes only *composite* values, the problem of understanding the distribution of the fractional parts of $f_g(n)$ and $h_g(n)$ is rather involved. To approach this problem, we consider exponential sums of the form:

$$S_g(a;N) = \sum_{\substack{n=1 \\ n \text{ composite}}}^{N} \mathbf{e}(ah_g(n)),$$

$$W(a;N) = \sum_{\substack{n=1 \\ n \text{ composite}}}^{N} \left| \sum_{\substack{g=1 \\ \gcd(g,n)=1}}^{n} \mathbf{e}(af_g(n)) \right|,$$

Received by the editors May 26, 2006; revised November 15, 2006.

During the preparation of this paper, F. L. was also supported in part by grants PAPIIT IN104505, SEP-CONACyT 46755 and a Guggenheim Fellowship, and I. S. was supported in part by ARC grant DP0556431.

AMS subject classification: Primary: 11L07; secondary: 11N37, 11N60.

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

where the additive character $\mathbf{e}(\cdot)$ is defined (as usual) by $\mathbf{e}(x) = \exp(2\pi i x)$ for all $x \in \mathbb{R}$, and $a \neq 0$ is an integer.

We also consider the arithmetic functions

$$\widetilde{f}_g(n) = \frac{g^n - g}{n} \quad \text{and} \quad \widetilde{h}_g(n) = \frac{g^n - g}{P(n)} \quad (n \geq 1)$$

and the corresponding exponential sums

$$\widetilde{S}_g(a;N) = \sum_{\substack{n=1 \\ n \text{ composite}}}^{N} \mathbf{e}(a\widetilde{h}_g(n)),$$

$$\widetilde{W}(a;N) = \sum_{\substack{n=1 \\ n \text{ composite}}}^{N} \left| \sum_{\substack{g=1 \\ \gcd(g,n)=1}}^{n} \mathbf{e}(a\widetilde{f}_g(n)) \right|.$$

Clearly, $\widetilde{S}_g(a;N) = S_g(ag;N)$; the sums $\widetilde{W}(a;N)$, however, require an independent treatment.

Our results imply that the fractional parts $\{f_g(n)\}$, $\{\widetilde{f}_g(n)\}$, $\{h_g(n)\}$, and $\{\widetilde{h}_g(n)\}$ are uniformly distributed over the interval $[0,1)$, on average over $g \in (\mathbb{Z}/n\mathbb{Z})^*$ for $f_g(n)$ and $\widetilde{f}_g(n)$, and individually (that is, with $g > 1$ fixed) for $h_g(n)$ and $\widetilde{h}_g(n)$. Of course, one can either include or exclude the prime numbers in the preceding statement since their contribution cannot change the property of uniform distribution.

We remark that if n is a Fermat pseudoprime to base g, then both $f_g(n)$ and $h_g(n)$ are integers. If n is a Carmichael number, then it is a Fermat pseudoprime to base g for every g coprime to n, hence $f_g(n)$ and $h_g(n)$ are integers for all such g. Since it is expected that there are

$$C(N) = N^{1-(1+o(1))\log\log\log N/\log\log N}$$

Carmichael numbers $n \leq N$ (see [1,16]), their contribution to the sums $S_g(a;N)$ and $W(a;N)$ is substantial; therefore, one cannot expect to obtain very strong bounds for those sums. In particular, it is unlikely that one can obtain upper bounds for $S_g(a;N)$ and $W(a;N)$ of the form $O(N^\theta)$ and $O(N^{1+\theta})$, respectively, for any fixed constant $\theta < 1$. Indeed, using the *Erdős-Turán inequality*, which relates exponential sums to uniformity of distribution, we show that the lower bound $S_g(a;N) \gg N\log\log N/\log N$ holds for at least one integer a in the range $1 \leq a \leq \log N$; thus, our upper bound for $S_g(a;N)$ (cf. Theorem 3.1) is rather tight. The same comments certainly apply to $\widetilde{S}_g(a;N)$ and $\widetilde{W}(a;N)$ as well.

Problems of a similar flavor concerning the integrality and the distribution of fractional parts of ratios formed with various number theoretic functions have been treated previously in [2,4,29,31,37,38]. In part, our motivation also stems from the results of [17,18] on bounds for exponential sums with *Fermat quotients*.

It is perhaps surprising that, in order to establish our upper bounds for $S_g(a;N)$ and $W(a;N)$, we need to apply tools from very different and seemingly unrelated

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

areas of number theory, including several recent results. For instance, we not only apply an asymptotic formula for the number of solutions to a symmetric equation with an exponential function, which dates historically back to 1962 (see the corollary to [35, Lemma 1, Chapter 15]), but we also use very recent results on "individual" bounds of short exponential sums from [5, 6], together with bounds "on average" from [13] (see also [15]). In the course of our proofs, we also establish several new auxiliary results which may be of independent interest; see, for example, Lemmas 2.3 and 2.10.

In what follows, we use the Landau symbols O and o, as well as the Vinogradov symbols $\ll$ and $\gg$, with their usual meanings. Any implied constants may depend, where obvious, on the parameter g but are absolute otherwise, as for example Sections 4 and 5. We recall that the notations $A \ll B$, $B \gg A$, and $A = O(B)$ are all equivalent, and $A = o(B)$ means that A/B tends to zero. Throughout, we use the letters p and q exclusively to denote prime numbers, while m and n always denote positive integers. For a positive real number x we write $\log x$ for the maximum between the natural logarithm of x and 1.

2 Preliminary Results

2.1 Arithmetic Estimates

Recall that a positive integer n is said to be *y-smooth* if $P(n) \le y$. For real numbers $x \ge y \ge 2$, let

$$\Psi(x, y) = \#\{n \le x \,:\, P(n) \le y\}.$$

Lemma 2.1 *Let $u = (\log x)/(\log y)$, where $x \ge y \ge 2$. If $u \to \infty$ as $x \to \infty$ and $u \le y^{1/2}$, then the following estimate holds: $\Psi(x, y) = xu^{-u+o(u)}$.*

For a proof of the Lemma 2.1, we refer the reader to [39, Section III.5.4]; we remark that the condition $u \le y^{1/2}$ can be relaxed slightly, but the statement of Lemma 2.1 is sufficient for our purposes.

For every positive integer n, let $\rho(n)$ denote the largest squarefree divisor r of n for which $\gcd(r, n/r) = 1$; then $s = n/\rho(n)$ is the largest *powerful* divisor of n (recall that a positive integer m is said to be powerful if $p^2 \mid m$ for every prime p that divides m).

We need the following statement, which is [8, Lemma 7].

Lemma 2.2 *Uniformly for $x \ge y \ge 1$, the bound $\rho(n) > n/y$ holds for all $n \le x$ with at most $O(x/y^{1/2})$ exceptions.*

For every positive integer n, let

$$\gamma(n) = \prod_{p \mid n} \gcd(n - 1, p - 1).$$

We note that this function also gives the cardinality of the set of the so-called *false witnesses* modulo n, that is, of the set

$$\{u \in \mathbb{Z}/n\mathbb{Z} \,:\, u^{n-1} \equiv 1 \pmod{n}\},$$

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

and has been studied in the literature (see [11] and the references therein). The average value, the normal order, and the number of prime factors of $\gamma(n)$ are estimated in [11]; however, these bounds do not seem to be enough for our purposes.

Our next result shows for almost all composite integers n, the value of $\gamma(n)$ is very small. Although several bounds on the number of composite integers $n \le x$ such that $\gamma(n) > z$ can be extracted from [11], our estimate appears to be new. More precisely, [11, Theorem 2.2] implies such a bound for large values of z, and [11, Theorem 6.5] treats the case of small values of z. In our applications, however, we need a bound in the medium range. For our application, it is convenient to formulate this result in the following two-parametric form.

Lemma 2.3 *Uniformly for $x \ge y \ge 1$ and $\log\log\log x = o(\log k)$, the number of composite integers $n \le x$ such that $\gamma(n) > y^k$ is at most*

$$O\Big(\frac{x\log\log x}{y} + \frac{x}{\exp((1+o(1))k\log k)}\Big).$$

Proof Let $\omega(m)$ be the number of distinct prime factors of the m, and put $\mathcal{E}_1 = \{n \le x : \omega(n) \ge k\}$. If $n \in \mathcal{E}_1$, there exists a divisor $m \mid n$ with $\omega(m) = k$. For fixed m, there are at most x/m integers $n \in \mathcal{E}_1$ such that $m \mid n$. Therefore, by unique factorization and the Stirling formula for $k!$, we see that

$$\#\mathcal{E}_1 \le x \sum_{\substack{m\le x\\ \omega(m)=k}} \frac{1}{m} \le \frac{x}{k!}\Big(\sum_{p^\alpha\le x}\frac{1}{p^\alpha}\Big)^k = \frac{x}{k!}\,(\log\log x + O(1))^k \tag{2.1}$$

$$\le x\Big(\frac{e\log\log x + O(1)}{k}\Big)^k = x\exp\big(-(1+o(1))k\log k\big),$$

where the last estimate above uses the fact that $\log\log\log x = o(\log k)$.

Let $\varphi(\,\cdot\,)$ denote the Euler function. We recall the estimate

$$\sum_{\substack{p\le t\\ p\equiv 1 \pmod d}} \frac{1}{p} \ll \frac{\log\log t}{\varphi(d)}, \tag{2.2}$$

which holds uniformly for $1 \le d \le t$ (see [3, Lemma 1] or [9, Bound (3.1)]). We also note that the bound

$$\sum_{d>t} \frac{1}{d\varphi(d)} \ll \frac{1}{t} \tag{2.3}$$

follows by partial summation from the asymptotic formula of Landau [27]:

$$\sum_{d\le t}\frac{1}{\varphi(d)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)}\Big(\log t + \gamma - \sum_p \frac{\log p}{p^2-p+1}\Big) + O\left(\frac{\log t}{t}\right),$$

where $\zeta(s)$ is the Riemann zeta-function, and γ is the Euler-Mascheroni constant (a more recent reference is [32]).

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

Now let $\mathcal{E}_2$ be the set of composite $n \le x$ for which there exists $p \mid n$ with $d = \gcd(n-1, p-1) > y$. Write $n = pm$. Since $n \equiv p \equiv 1 \pmod{d}$, it follows that $m \equiv 1 \pmod{d}$; moreover, $m > 1$ since n is not prime. For each p and d, we have $1 < m \le x/p$ and also $m \equiv 1 \pmod{d}$, hence the number of such m is at most x/pd. Summing first over primes $p \equiv 1 \pmod{d}$, then over all $d > y$, we derive from (2.2) and (2.3) that

$$\#\mathcal{E}_2 \le \sum_{d>y} \sum_{\substack{p \le x \\ p \equiv 1 \pmod{d}}} \frac{x}{pd} \ll x \sum_{d>y} \frac{\log\log x}{d\varphi(d)} \ll \frac{x \log\log x}{y}. \tag{2.4}$$

The result now follows from the estimates (2.1) and (2.4) by observing that

$$\gamma(n) = \prod_{p \mid n} \gcd(n-1, p-1) \le y^{\omega(n)} \le y^k$$

if $n \le x$ is composite and not in the set $\mathcal{E}_1 \cup \mathcal{E}_2$. ■

By optimizing the choice of y and k for each given z, one can reformulate Lemma 2.3 as the following more concise (albeit weaker) statement.

Corollary 2.4 *Uniformly for $x \ge z \ge 1$ and $\log\log\log x = o(\log\log z)$, the number of composite integers $n \le x$ such that $\gamma(n) > z$ does not exceed*

$$x \exp\left(-\sqrt{(0.5 + o(1)) \log z \log\log z}\right).$$

Proof Choose k as the largest integer with $k^2 \log k \le \log z$, and put $y = z^{1/k}$. Then, using our hypotheses on x and z, we see that the conditions of Lemma 2.3 are met, and the corollary follows immediately. ■

For a fixed base $g \ge 2$ and any prime $p \nmid g$, let t_p denote the multiplicative order of g modulo p. As usual, we use $\tau(n)$ to denote the number of positive integer divisors of n.

Let $\mathcal{Q}$ be the set of primes p satisfying the conditions

$$\tau(p-1) \le (\log p)^2 \quad \text{and} \quad t_p > p^{1/2} (\log p)^{-10}, \tag{2.5}$$

and let

$$\mathcal{R} = \{p \text{ prime} : p \notin \mathcal{Q}\}. \tag{2.6}$$

Lemma 2.5 *Uniformly for $x \ge 2$, the following bound holds:*

$$\#\{p \le x : p \in \mathcal{R}\} \ll \frac{x}{(\log x)^2}.$$

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

Proof Since all primes with $t_p \le x^{1/2}(\log x)^{-10}$ are divisors of

$$U = \prod_{t \le x^{1/2}(\log x)^{-10}} (g^t - 1) = \exp\left(O(x(\log x)^{-20})\right),$$

there are no more than $\log U = O(x(\log x)^{-20})$ such primes. (See also [10, 12, 19] for several more results in this direction which apply to even larger values of t_p but which unfortunately give very large exceptional sets that are of no use for us.) The result now follows immediately from the Titchmarsh bound: $\sum_{p \le x} \tau(p-1) \ll x$, (see [36, Theorem 7.1, Chapter 5]). ∎

Finally, we need the following estimate:

Lemma 2.6 *There exists a positive constant c such that for $x \ge y \ge 2$ and $\Delta > 0$, the following bound holds:*

$$\#\{n \le x : y < P(n) \le y(1+\Delta)\} \ll \frac{x \log(1+\Delta)}{\log y} + x \exp\left(-c(\log y)^{3/5}\right).$$

Proof We apply the following precise version of the Mertens formula, which is given in [40]:

$$\sum_{p \le t} \frac{1}{p} = \log\log t + a + O\left(\exp\left(-c(\log t)^{3/5}\right)\right) \tag{2.7}$$

for some constants a and $c > 0$. Applying (2.7) with $t = y$ and $t = y(1+\Delta)$, and observing that for each prime p in the interval $\left(y, y(1+\Delta)\right]$, the number of integers $n \le x$ with $P(n) = p$ does not exceed x/p, we obtain that

$$\begin{aligned}
\frac{1}{x} \cdot \#\{n \le x : y < P(m) \le y(1+\Delta)\} &\le \sum_{y < p \le y(1+\Delta)} \frac{1}{p} \\
&= \log\left(\log y + \log(1+\Delta)\right) - \log\log y + O\left(\exp\left(-c(\log y)^{3/5}\right)\right) \\
&= \log\left(1 + \frac{\log(1+\Delta)}{\log y}\right) + O\left(\exp\left(-c(\log y)^{3/5}\right)\right),
\end{aligned}$$

and the result follows. ∎

2.2 Estimates for Exponential Sums

We begin with some well known and elementary results.

The following result, based on the Chinese Remainder Theorem, allows one to reduce exponential sums with polynomials and with arbitrary denominators to exponential sums with prime power denominators; this has been discussed, for example, in [41, Problem 12.d, Chapter 3].

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

Lemma 2.7 *Let $n = n_1 n_2$, where $n_1, n_2 \geq 2$ are coprime, and suppose that the integers r_1, r_2 satisfy:*

$$r_1 n_2 \equiv 1 \pmod{n_1} \quad \text{and} \quad r_2 n_1 \equiv 1 \pmod{n_2}.$$

Then, for any polynomial $F(X) \in \mathbb{Z}[X]$ with integer coefficients, we have

$$\sum_{\substack{g=0 \\ \gcd(g,n)=1}}^{n-1} \mathbf{e}\left(F(g)/n\right) = \sum_{\substack{g_1=0 \\ \gcd(g_1,n_1)=1}}^{n_1-1} \mathbf{e}\left(r_1 F(g_1)/n_1\right) \sum_{\substack{g_2=0 \\ \gcd(g_2,n_2)=1}}^{n_2-1} \mathbf{e}\left(r_2 F(g_2)/n_2\right).$$

Lemma 2.8 *For integers a, n, k with $n, k \geq 1$, we have*

$$\left| \sum_{\substack{g=0 \\ \gcd(g,n)=1}}^{n-1} \mathbf{e}\left(ag^k/n\right) \right| \leq n d^{1/2} \gamma(n) \rho(n)^{-1/2},$$

where $d = \gcd(a, n)$.

Proof The proof is similar to that of [8, Lemma 4]. We recall the Weil bound, which asserts that for every integer b and prime $p \nmid b$, the inequality

$$\left| \sum_{g=1}^{p-1} \mathbf{e}\left(bg^k/p\right) \right| \leq \gcd(k, p-1) p^{1/2}$$

holds (see, for example, [28, Theorem 5.41]).

Let $\rho(n) = p_1 \cdots p_\nu$ be the factorization of $\rho(n)$ as a product of (distinct) primes, and put $s = n/\rho(n)$. Then, by Lemma 2.7, we have

$$\sum_{\substack{g=0 \\ \gcd(g,n)=1}}^{n-1} \mathbf{e}\left(ag^k/n\right) = \prod_{j=1}^{\nu} \Big(\sum_{g_j=1}^{p_j-1} \mathbf{e}_{p_j}\left(ab_j g_j^k/p_j\right) \Big) \Big(\sum_{\substack{h=0 \\ \gcd(h,s)=1}}^{s-1} \mathbf{e}\left(ach^k/s\right) \Big)$$

for some integers $b_1, \ldots, b_\nu$ and c such that $\gcd(b_j, p_j) = 1$ for $j = 1, \ldots, \nu$ and $\gcd(c, s) = 1$. For each j such that $p_j \mid a$, the sum over g_j is equal to $p_j - 1$. We estimate the sum over h trivially as s. Therefore,

$$\left| \sum_{\substack{g=0 \\ \gcd(g,n)=1}}^{n-1} \mathbf{e}\left(ag^k/n\right) \right| \leq s \prod_{\substack{j=1 \\ p_j \nmid a}}^{\nu} \left(\gcd\left(k, (p_j - 1)\right) p_j^{1/2} \right) \prod_{\substack{j=1 \\ p_j \mid a}}^{\nu} p_j,$$

and the result follows. ∎

The next result appears in [5]; it can also be deduced from [6, Theorem 5] in an even more explicit form.

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

Lemma 2.9 *For every $\delta > 0$, there exists $\eta > 0$, such that if $p^\delta \le M \le t_p$, then for every integer a not divisible by p, the following bound holds:*

$$\Big| \sum_{m \le M} \mathbf{e}(ag^m/p) \Big| \le Mp^{-\eta}.$$

The following bound on short exponential sums with an exponential function appears to be new and may be of independent interest. To prove this bound, we use the well known method of estimating double exponential sums via the number to solutions of certain symmetric systems of equations, which can be found in [14, 20–22,24–26] and in many other places (for example, [23]). In fact, although the result is conveniently summarized in [23, Lemma 4], no proof is given there. Here, we supply a proof for the sake of completeness.

Lemma 2.10 *For a real number $V \ge 2$ and positive integers M, k, ℓ satisfying the inequalities*

$$2^k k!\, \pi(V) \le M^{k+1} \quad \text{and} \quad 2^\ell \ell!\, \pi(V) \le M^{(\ell+1)/2},$$

the following bound holds:

$$\sum_{\substack{p \le V \\ p \nmid ag}} \max_{L \le M} \Big| \sum_{m=1}^{L} \mathbf{e}(ag^m/p) \Big| \ll \pi(V) M \left(\frac{V^{1/2} M^{3/4}}{\pi(V)} \right)^{1/k\ell},$$

where the implied constant depends only on g.

Proof For each prime $p \le V$ such that $p \nmid ag$, let L_p denote the smallest positive integer such that

$$\max_{L \le M} \Big| \sum_{m=1}^{L} \mathbf{e}(ag^m/p) \Big| = \Big| \sum_{m=1}^{L_p} \mathbf{e}(ag^m/p) \Big|.$$

Put $H = \lfloor M^{1/2} \rfloor$; then,

$$\sum_{\substack{p \le V \\ p \nmid ag}} \Big| \sum_{m=1}^{L_p} \mathbf{e}(ag^m/p) \Big| = \frac{W}{H} + O(\pi(V)H), \tag{2.8}$$

where

$$W = \sum_{\substack{p \le V \\ p \nmid ag}} \sum_{h=1}^{H} \Big| \sum_{m=1}^{L_p} \mathbf{e}(ag^{m+h}/p) \Big|.$$

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

By the Hölder inequality, it follows that

$$W^k \le \pi(V)^{k-1} H^{k-1} \sum_{\substack{p \le V \\ p \nmid ag}} \sum_{h=1}^{H} \Big| \sum_{m=1}^{L_p} \mathbf{e}(ag^{m+h}/p) \Big|^k$$

$$= \pi(V)^{k-1} H^{k-1} \sum_{\substack{p \le V \\ p \nmid ag}} \sum_{h=1}^{H} \vartheta_{p,h} \Big(\sum_{m=1}^{L_p} \mathbf{e}(ag^{m+h}/p) \Big)^k$$

for some complex numbers $\vartheta_{p,h}$ of absolute value 1.

Now, let $R_{p,s}(K, \lambda)$ denote the number of solutions of the congruence

$$\sum_{i=1}^{s} g^{r_i} \equiv \lambda \pmod{p} \qquad (1 \le r_1, \dots, r_s \le K).$$

Then

$$\Big(\sum_{m=1}^{L_p} \mathbf{e}(ag^{m+h}/p) \Big)^k = \sum_{\lambda=0}^{p-1} R_{p,k}(L_p, \lambda)\, \mathbf{e}(a\lambda g^h/p).$$

Therefore, after changing the order of summation, we derive that

$$W^k \le \pi(V)^{k-1} H^{k-1} \sum_{\substack{p \le V \\ p \nmid ag}} \sum_{\lambda=0}^{p-1} R_{p,k}(L_p, \lambda) \sum_{h=1}^{H} \vartheta_{p,h}\, \mathbf{e}(a\lambda g^h/p).$$

Writing

$$R_{p,k}(L_p, \lambda) = \big(R_{p,k}(L_p, \lambda)^2 \big)^{1/2\ell} R_{p,k}(L_p, \lambda)^{(\ell-1)/\ell}$$

and using the Hölder inequality for a sum of products of three terms, we have

$$W^{2k\ell} \le \pi(V)^{2\ell(k-1)} H^{2\ell(k-1)} \sum_{\substack{p \le V \\ p \nmid ag}} \sum_{\lambda=0}^{p-1} R_{p,k}(L_p, \lambda)^2$$

$$\times \quad \Bigg(\sum_{\substack{p \le V \\ p \nmid ag}} \sum_{\lambda=0}^{p-1} R_{p,k}(L_p, \lambda) \Bigg)^{2\ell-2} \quad \times \quad \sum_{\substack{p \le V \\ p \nmid ag}} \sum_{\lambda=0}^{p-1} \Big| \sum_{h=1}^{H} \vartheta_{p,h}\, \mathbf{e}(a\lambda g^h/p) \Big|^{2\ell}.$$

Clearly,

$$\sum_{\lambda=0}^{p-1} R_{p,k}(L_p, \lambda) = L_p^k \le M^k,$$

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

and

$$\sum_{\lambda=0}^{p-1} R_{p,k}(L_p, \lambda)^2 = T_{p,k}(L_p),$$

where $T_{p,s}(K)$ denotes the number of solutions of the congruence

$$\sum_{i=1}^{2s} (-1)^i g^{r_i} \equiv 0 \pmod{p} \qquad (1 \le r_1, \dots, r_s \le K).$$

Thus,

$$W^{2k\ell} \le \pi(V)^{2\ell(k-1)+2\ell-2} H^{2\ell(k-1)} M^{2k(\ell-1)} \sum_{\substack{p \le V \\ p \nmid ag}} T_{p,k}(L_p) \times \sum_{\substack{p \le V \\ p \nmid ag}} \sum_{\lambda=0}^{p-1} \Big| \sum_{h=1}^{H} \vartheta_{p,h}\, \mathbf{e}(a\lambda g^h/p) \Big|^{2\ell}.$$

Furthermore,

$$\begin{aligned} \sum_{\lambda=0}^{p-1} \Big| \sum_{h=1}^{H} \vartheta_{p,h}\, \mathbf{e}(a\lambda g^h/p) \Big|^{2\ell} &= \sum_{h_1,\dots,h_{2\ell}=1}^{H} \prod_{i=1}^{2\ell} \vartheta_{p,h_i} \sum_{\lambda=0}^{p-1} \mathbf{e}\Big(\frac{\lambda}{p} \sum_{i=1}^{2\ell} (-1)^i g^{h_i} \Big) \\ &\le \sum_{h_1,\dots,h_{2\ell}=1}^{H} \Big| \sum_{\lambda=0}^{p-1} \mathbf{e}\Big(\frac{\lambda}{p} \sum_{i=1}^{2\ell} (-1)^i g^{h_i} \Big) \Big| = p\, T_{p,\ell}(H). \end{aligned}$$

Hence,

$$W^{2k\ell} \le \pi(V)^{2k\ell-2} H^{2\ell(k-1)} M^{2k(\ell-1)} \sum_{\substack{p \le V \\ p \nmid ag}} T_{p,k}(L_p) \sum_{\substack{p \le V \\ p \nmid ag}} p\, T_{p,\ell}(H).$$

We remark that

$$\sum_{\substack{p \le V \\ p \nmid ag}} T_{p,k}(L_p) \le \sum_{p \le V} T_{p,k}(M)$$

is equal to the number of primes $p \le V$ which divide all possible expressions of the form

$$\sum_{i=1}^{2k} (-1)^i g^{m_i} \qquad (1 \le m_1, \dots, m_{2k} \le M).$$

Clearly, any nonzero sum above has at most $\log(2kg^M)/\log 2$ prime divisors. Also, by the corollary to [35, Lemma 1, Chapter 15], there are at most $2^k k! M^k$ such sums which vanish (see also [7] for a survey of recent results in this direction). For these

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

ones, we estimate the number of prime divisors trivially as $\pi(V)$. Thus, using the inequality $2^k k!\,\pi(V) \le M^{k+1}$, we deduce that

$$\sum_{p\le V} T_{p,k}(M) \ll M^{2k}\log(2kg^M) + 2^k k! M^k \pi(V)$$
$$\ll M^{2k}\log k + M^{2k+1} + 2^k k! M^k \pi(V) \ll M^{2k+1}.$$

Similarly,

$$\sum_{\substack{p\le V\\ p\nmid ag}} pT_{p,\ell}(H) \le V \sum_{p\le V} T_{p,\ell}(H) \ll VH^{2\ell+1}.$$

Consequently,

$$W^{2k\ell} \ll \pi(V)^{2k\ell-2} VH^{2k\ell+1} M^{2k\ell+1}.$$

Substituting this estimate into (2.8), we obtain that

$$\sum_{\substack{p\le V\\ p\nmid ag}} \Big|\sum_{m=1}^{L_p} \mathbf{e}(ag^m/p)\Big| \ll \pi(V)^{1-1/k\ell} V^{1/2k\ell} M^{1+3/4k\ell} + \pi(V) M^{1/2}.$$

It now remains only to observe that, since $2^k k!\,\pi(V) \le M^{k+1}$, the last term never dominates. ∎

It is important to remark that the implied constant in the bound of Lemma 2.10 depends on g but not on the parameters k, ℓ (nor on a, M, V). In particular, in our applications we can choose k and ℓ to be growing functions of M and V. Of course, we use Lemma 2.10 only to deal with the case that M is suitably small with respect to V, and in the remaining range, we apply Lemma 2.9.

We also need the following bound, which is a special case of the more general results of [13].

Lemma 2.11 *For any positive real number U, any positive integer M, and any subset $\mathcal{M} \subseteq \{1,\dots,M\}$ of cardinality $\#\mathcal{M} = T$, we have the uniform bound:*

$$\sum_{\substack{p\in\mathcal{Q}\\ U\le p\le 2U}} \max_{(a,p)=1} \Big|\sum_{m\in\mathcal{M}} \mathbf{e}\left(ag^m/p\right)\Big|^2 \ll UT(MU^{-0.04}+U)(\log U)^2,$$

where $\mathcal{Q}$ is the set defined by (2.5).

Proof Indeed, if we enumerate the elements of $\mathcal{M}$ as $s_1 < s_2 < \dots < s_T$ and apply [13, Theorem 1] with

$$X = 2U, \qquad \Delta = U^{1/2}(\log U)^{-10}, \qquad L = U^{2/77}$$

and take into account that $T \le s_T \le M$, then we obtain

$$\sum_{p\in\mathcal{L}} \frac{1}{\tau(p-1)} \max_{(a,p)=1} \Big|\sum_{m\in\mathcal{M}} \mathbf{e}\left(ag^m/p\right)\Big|^2 \ll UT(MU^{-1/22}(\log U)^5 + U),$$

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

where $\mathcal{L}$ is the set of prime numbers $p \le 2U$ with $t_p > U^{1/2}(\log U)^{-10}$. Since

$$\{p : \ p \in \mathcal{Q}, \ U \le p \le 2U\} \subseteq \mathcal{L}$$

and $\tau(p-1) \ll (\log U)^2$ for any $p \in \mathcal{Q}$, $U \le p \le 2U$, the result follows. ∎

3 Single Exponential Sums with $h_g(n)$

Theorem 3.1 *Fix $g > 1$ and $\varepsilon > 0$. Then for every integer a such that $\log|a| \le \exp\left((\log N)^{1-\varepsilon}\right)$, the inequality*

$$S_g(a;N) \ll \frac{N}{\sqrt{\log N}}$$

holds, where the implied constant depends only on g and ε.

Proof We may assume that $\varepsilon < 1/2$. Put $Q = \exp\left(2(\log N)^{1-\varepsilon}\right)$, and let $\mathcal{E}_1$ denote the set of Q-smooth integers $n \le N$. Then, applying Lemma 2.1 with $u = 0.5(\log N)^{\varepsilon}$, we obtain the bound

$$\begin{aligned} \#\mathcal{E}_1 &= \Psi(N,Q) = Nu^{-u+o(u)} \\ &= N\exp\left(-\left(0.5\,\varepsilon + o(1)\right)(\log N)^{\varepsilon}\log\log N\right). \end{aligned} \tag{3.1}$$

Next, let $\mathcal{E}_2$ be the set of the integers $n \le N$, $n \notin \mathcal{E}_1$, such that $P(n) \mid ag$. We have

$$\#\mathcal{E}_2 \le \sum_{\substack{p>Q \\ p \mid ag}} \frac{N}{p} \ll \frac{N}{Q}\sum_{p \mid ag} 1 \ll \frac{N}{Q}\log|a| \le N\exp\left(-(\log N)^{1-\varepsilon}\right). \tag{3.2}$$

Let $\mathcal{E}_3$ be the set of the positive integers $n \le N$ not in $\mathcal{E}_1$ such that $P(n) \in \mathcal{R}$ where the set $\mathcal{R}$ is defined by (2.6). We have

$$\#\mathcal{E}_3 \le \sum_{\substack{Q<p\le N \\ p\in\mathcal{R}}} \sum_{\substack{n\le N \\ P(n)=p}} 1 \le N \sum_{\substack{Q<p\le N \\ p\in\mathcal{R}}} \frac{1}{p}. \tag{3.3}$$

By Lemma 2.5 and partial summation, we obtain that

$$\#\mathcal{E}_3 \ll \frac{N}{\log Q} \le \frac{N}{\sqrt{\log N}}.$$

Let us now denote

$$X = N^{1/2}(\log N)^{-5}, \quad Y = N^{3/4} \quad \text{and} \quad Z = N\exp\left(-\sqrt{\log N}\right).$$

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

Let $\mathcal{E}_4$ be the set of the positive integers $n \le N$ such that either $X < P(n) \le N^{1/2}$, or $Z < P(n) \le N$. By Lemma 2.6, it follows that

$$\mathcal{E}_4 \ll \frac{N}{\sqrt{\log N}}. \tag{3.4}$$

Let $\mathcal{N}$ be the set of integers $n \le N$ such that $n \notin \mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3 \cup \mathcal{E}_4$. Then, from the estimates (3.1), (3.2), (3.3), and (3.4), we conclude that

$$S_g(a;N) = \sum_{n=1}^{N} \mathbf{e}(ah_g(n)) + O\left(\frac{N}{\log N}\right) = \sum_{n\in\mathcal{N}} \mathbf{e}(ah_g(n)) + O\left(\frac{N}{\sqrt{\log N}}\right).$$

Note that the error term in the middle expression comes from prime values of $n \le N$, which are not included in the sum $S_g(a;N)$.

Every $n \in \mathcal{N}$ has a unique representation of the form $n = pm$, with a prime $p \ge Q$ and an integer $m \le N/p$ such that $P(m) \le p$. Also, remarking that for $p > N^{1/2}$ the condition $P(m) \le p$ is automatically satisfied, we see that

$$\sum_{n\in\mathcal{N}} \mathbf{e}(ah_g(n)) = W_1 + W_2 + W_3,$$

where, since $g^{pm} \equiv g^m \pmod{p}$, we have

$$|W_1| = \Big| \sum_{\substack{Q<p\le X\\ p\in\mathcal{Q}}} \sum_{\substack{m\le N/p\\ P(m)\le p}} \mathbf{e}(ah_g(pm)) \Big| \le \sum_{\substack{Q<p\le X\\ p\in\mathcal{Q}}} \Big| \sum_{\substack{m\le N/p\\ P(m)\le p}} \mathbf{e}(ag^{m-1}/p) \Big|,$$

$$|W_2| = \Big| \sum_{\substack{N^{1/2}<p\le Y\\ p\in\mathcal{Q}}} \sum_{m\le N/p} \mathbf{e}(ah_g(pm)) \Big| \le \sum_{\substack{N^{1/2}<p\le Y\\ p\in\mathcal{Q}}} \Big| \sum_{m\le N/p} \mathbf{e}(ag^{m-1}/p) \Big|,$$

$$|W_3| = \Big| \sum_{\substack{Y<p\le Z\\ p\in\mathcal{Q}}} \sum_{m\le N/p} \mathbf{e}(ah_g(pm)) \Big| \le \sum_{\substack{Y<p\le Z\\ p\in\mathcal{Q}}} \Big| \sum_{m\le N/p} \mathbf{e}(ag^{m-1}/p) \Big|.$$

To estimate $|W_1|$, put $\Delta = 1/\log N$ and consider the sequence of real numbers:

$$U_j = \min\{Q(1+\Delta)^j, X\} \qquad (0 \le j \le J),$$

where

$$J = \left\lceil \frac{\log(X/Q)}{\log(1+\Delta)} \right\rceil \ll \Delta^{-1}\log N = (\log N)^2. \tag{3.5}$$

We denote the set of primes $p \in \mathcal{Q}$ in the half-open interval $(U_j, U_{j+1}]$ by $\mathcal{U}_j$, $j = 0, \dots, J-1$.

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

From the above, we infer that

$$|W_1| \le \sum_{j=0}^{J-1} |\sigma_j|, \tag{3.6}$$

where

$$\sigma_j = \sum_{p \in \mathcal{U}_j} \sum_{\substack{m \le N/p \\ P(m) \le p}} \mathbf{e}(ag^{m-1}/p) \qquad (0 \le j \le J-1).$$

We have

$$\begin{aligned} \sigma_j &= \sum_{p \in \mathcal{U}_j} \Bigg(\sum_{\substack{m \le N/U_j \\ P(m) \le p}} \mathbf{e}(ag^{m-1}/p) + O\big(|N/p - N/U_j|\big) \Bigg) \\ &= \sum_{p \in \mathcal{U}_j} \Bigg(\sum_{\substack{m \le N/U_j \\ P(m) \le p}} \mathbf{e}(ag^{m-1}/p) + O(N\Delta/p) \Bigg). \end{aligned}$$

Applying Lemma 2.6 with $x = N/U_j$ and $y = U_{j-1} \ge Q$, together with the fact that $\log(1+\Delta) \le \Delta$ and

$$2\log(1+\Delta) \ge \Delta = (\log N)^{-1} \ge (\log Q)^{-2} \ge (\log U_j)^{-2},$$

(which means that only the first term on the right hand side of the inequality of Lemma 2.6 matters) we obtain that

$$\begin{aligned} \sigma_j &= \sum_{p \in \mathcal{U}_j} \Bigg(\sum_{\substack{m \le N/U_j \\ P(m) \le U_j}} \mathbf{e}(ag^{m-1}/p) + O\big(N\Delta/p + N\Delta/(U_j \log U_j)\big) \Bigg) \\ &= \widetilde{\sigma}_j + O\Bigg(N\Delta \sum_{p \in \mathcal{U}_j} 1/p\Bigg), \end{aligned}$$

where

$$\widetilde{\sigma}_j = \sum_{p \in \mathcal{U}_j} \sum_{\substack{m \le N/U_j \\ P(m) \le U_j}} \mathbf{e}(ag^{m-1}/p) \qquad (0 \le j \le J-1).$$

Thus, from (3.6), we have

$$|W_1| \le \sum_{j=0}^{J-1} |\widetilde{\sigma}_j| + O\Bigg(N\Delta \sum_{p \le N} 1/p\Bigg) = \sum_{j=0}^{J-1} |\widetilde{\sigma}_j| + O\Bigg(\frac{N \log\log N}{\log N}\Bigg). \tag{3.7}$$

Using the trivial bound $\#\mathcal{U}_j \le \Delta U_j$ (in fact, the stronger bound

$$\#\mathcal{U}_j \ll \Delta U_j / \log U_j \le \Delta U_j / \log Q$$

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

also holds (see [34], for example), but this does not lead to an improvement in the final bound for $S_g(a;N)$) and the Cauchy inequality, we derive that

$$\widetilde{\sigma}_j^2 \le \Delta U_j \sum_{p\in\mathcal{U}_j} \Big| \sum_{\substack{m\le N/U_j\\ P(m)\le U_j}} \mathbf{e}(ag^{m-1}/p)\Big|^2.$$

Applying Lemma 2.11 and estimating the number of $m \le N/U_j$ such that $P(m) \le U_j$ trivially as N/U_j, we see that

$$\begin{aligned}|\widetilde{\sigma}_j|^2 &\ll \Delta N U_j (N U_j^{-1.04} + U_j)(\log U_j)^2\\ &= \Delta N^2 U_j^{-0.04} + \Delta N U_j^2 (\log U_j)^2\\ &\le \Delta N^2 Q^{-0.04} + \Delta N X^2 (\log N)^2 \le 2N^2 (\log N)^{-9}.\end{aligned}$$

Therefore, from (3.5) and (3.7) it follows that

$$|W_1| \ll \frac{N \log\log N}{\log N}.$$

To estimate W_2, we simply apply Lemma 2.9 with $\delta = 1/6$ to each sum over m, getting

$$\sum_{m\le N/p} \mathbf{e}(ag^{m-1}/p) \ll \frac{N}{p} p^{-\eta}$$

with some absolute constant $\eta > 0$. Here, recall that $t_p \ge p^{1/2}(\log p)^{-10}$ for every prime $p \in \mathcal{Q}$; hence, the above bound follows from Lemma 2.9 regardless of whether $t_p \ge N/p$ or not. Consequently,

$$|W_2| \ll \sum_{N^{1/2}<p\le N} \frac{N}{p} p^{-\eta} \le N^{1-\eta/2} \sum_{N^{1/2}<p\le N} \frac{1}{p} \ll N^{1-\eta/2} \log\log N.$$

To estimate W_3, consider the sequence of real numbers:

$$V_i = \max\{Y, e^{-i}Z\} \qquad (0 \le i \le I),$$

where $I = \lceil \log(Z/Y) \rceil$. We denote the set of primes $p \in \mathcal{Q}$ in the half-open interval $(V_{i+1}, V_i]$ by $\mathcal{V}_i$, $i = 0, \dots, I-1$. Then

$$|W_3| \le \sum_{i=0}^{I-1} |\Sigma_i|, \tag{3.8}$$

where

$$\Sigma_i = \sum_{p\in\mathcal{V}_i} \sum_{m\le N/p} \mathbf{e}(ag^{m-1}/p).$$

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

For each $i = 0, \dots, I-1$, we apply Lemma 2.10 with the parameter choices

$$k = \ell = \left\lceil \frac{4 \log N}{i + \sqrt{\log N}} \right\rceil, \quad V = V_{i+1} \quad \text{and} \quad M = \lceil N/V_i \rceil .$$

In particular,

$$M \ge \exp\left(i - 1 + \sqrt{\log N}\right),$$

and also

$$\frac{N}{\log N} \ll \pi(V) M \ll \frac{N}{\log N}.$$

Since, for sufficiently large N, the inequality

$$\frac{M^{(\ell+1)/2}}{2^\ell \ell!} \ge \frac{M^{k/2}}{2^k k!} \ge \left(\frac{M^{1/2}}{2k}\right)^k \ge M^{k/3} \ge e^{(i+\sqrt{\log N})k/4} \ge N$$

holds, one easily verifies that the conditions of Lemma 2.10 are satisfied if N is large enough. Since $V > N^{3/4}$ and $M < N^{1/4}$, we have

$$M^{3/4} V^{-1/2} \log V \ll N^{-3/16} \log N \ll N^{-1/6}.$$

Thus, an application of Lemma 2.10 yields the bound

$$\begin{aligned} |\Sigma_i| &\ll \frac{N}{\log N} \left(N^{-1/6}\right)^{1/k\ell} = \frac{N}{\log N} \exp\Big(-\frac{1}{150}\left(i + \sqrt{\log N}\right)^2 / \log N\Big) \\ &\le \frac{N}{\log N} \exp\Big(-\frac{i^2}{150 \log N}\Big). \end{aligned}$$

From (3.8), we now derive that

$$|W_3| \le \frac{N}{\log N} \sum_{i=0}^{\infty} e^{-i^2/150 \log N} \ll \frac{N}{\log N} \int_0^\infty e^{-t^2/150 \log N} dt \ll \frac{N}{(\log N)^{1/2}},$$

and the proof is complete. ∎

Next, we obtain a lower bound which shows that the upper bound of Theorem 3.1 is quite tight.

Theorem 3.2 *Let $g > 1$ be a fixed integer base. Then the inequality*

$$\max_{1 \le a \le \log N} |S_g(a; N)| \gg \frac{N \log\log N}{\log N}$$

holds, where the implied constant depends only on g.

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

Proof Let $\mathcal{T}$ be the set of positive integers $n \le N$ which can be expressed in the form $n = mp$, where the prime p and integer m satisfy the inequalities

$$m \le \frac{\log N}{6 \log g}, \quad N^{2/3} < p \le N/m.$$

Clearly, for each m there are $(1 + o(1))N/(m \log N)$ primes p such that $n = mp$ lies in $\mathcal{T}$, and the pair (m, p) is uniquely determined by n. Therefore,

$$\#\mathcal{T} \gg \sum_{m \le (\log N)/(6 \log g)} \frac{N}{m \log N} \gg \frac{N \log\log N}{\log N}.$$

Next, observe that for every $n \in \mathcal{T}$,

$$\{h_g(n)\} = \left\{ \frac{g^{mp-1} - 1}{p} \right\} = \left\{ \frac{g^{m-1} - 1}{p} \right\} < \frac{N^{1/6}}{N^{2/3}} = N^{-1/2}.$$

Thus, the numbers $\{h_g(n)\}$ with $n \in \mathcal{T}$ all lie in the interval $[0, N^{-1/2})$.

On the other hand, by [33, Theorem 1, Chapter 1] for the number of points $A(\gamma)$ in an interval $[0, \gamma) \subseteq [0, 1)$, we have

$$\max_{0 \le \gamma \le 1} |A(\gamma) - \gamma N| \ll \frac{N}{H} + \sum_{a=1}^{H} \left(\frac{1}{H} + \min\left\{ \gamma, \frac{1}{a} \right\} \right) \left| S_g(a, N) \right|$$

for any integer $H \ge 1$. Therefore, applying this inequality with $\gamma = N^{-1/2}$, we derive

$$\frac{N \log\log N}{\log N} \ll \#\mathcal{T} \ll \frac{N}{H} + \left(\frac{1}{H} + \frac{1}{N^{1/2}} \right) \sum_{a=1}^{H} \left| S_g(a, N) \right|.$$

Hence, by taking $H = \lfloor c \log N/(\log\log N) \rfloor$, with some large but fixed positive number $c > 0$ (depending only on g) and assuming that N is large enough, we obtain

$$\frac{N \log\log N}{\log N} \ll \frac{1}{H} \sum_{a=1}^{H} \left| S_g(a, N) \right|,$$

whence the stated result follows even for a smaller range of a. ∎

4 Double Exponential Sums with $f_g(n)$

Theorem 4.1 *For any integer a such that $\log |a| = o\left(\sqrt{\log N \log\log N}\right)$, the following inequality holds:*

$$W(a; N) \le N^2 \exp\left(-(0.5 + o(1)) \sqrt{\log N \log\log N} \right).$$

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

Proof Let N be sufficiently large, and suppose that k (a positive integer parameter that depends only on N) is such that $\log\log\log N = o(\log k)$. Put $y = \exp(k\log k)$, and let $\mathcal{E}$ be the set of composite integers $n \le N$ such that either $\rho(n) \le n/y^2$ or $\gamma(n) > y^k$. By Lemmas 2.2 and 2.3, it follows that

$$W(a;N) \le \sum_{\substack{n\le N,\ n\notin\mathcal{E}\\ n \text{ composite}}} \Bigg| \sum_{\substack{g=1\\ \gcd(g,n)=1}}^{n} \mathbf{e}(af_g(n))\Bigg| + O\Big(\frac{N^2}{\exp((1+o(1))k\log k)}\Big).$$

If $n \notin \mathcal{E}$, then $\rho(n) > n/y^2$ and $\gamma(n) \le y^k$; hence, by Lemma 2.8, we see that

$$\begin{aligned} W(a;N) &\ll |a|y^{k+1}N^{3/2} + \frac{N^2}{\exp\big((1+o(1))k\log k\big)} \\ &= |a|N^{3/2}\exp(k(k+1)\log k) + \frac{N^2}{\exp((1+o(1))k\log k)}. \end{aligned}$$

Choosing k such that $k(k+2)\log k \sim 0.5\log N$ (to balance the two terms above), we obtain the stated estimate. ∎

5 Double Exponential Sums with $\widetilde{f}_g(n)$

Theorem 5.1 *For any nonzero integer a with $|a| < (\log\log\log N)^3$ the bound*

$$\widetilde{W}(a;N) \ll \frac{N^2\log\log\log\log N}{\log\log\log N}$$

holds as $N \to \infty$.

Proof Let $\lambda(\cdot)$ denote the Carmichael function. We recall that if $n = \prod_{\nu=1}^{s} p_\nu^{\alpha_\nu}$ is the prime factorization of n, then $\lambda(n) = \operatorname{lcm}[\lambda(p_1^{\alpha_1}),\dots,\lambda(p_s^{\alpha_s})]$, where $\lambda(p^\alpha) = p^{\alpha-1}(p-1)$ for a prime power except when $p = 2$ and $\alpha \ge 3$, in which case $\lambda(2^\alpha) = 2^{\alpha-2}$.

Put

$$y = (\log\log\log N)^2 \quad \text{and} \quad z = \frac{\log\log N}{(\log\log\log N)^2},$$

and let $\mathcal{I}$ be the interval $[y,z]$.

The proof of [30, Lemma 2] shows that if $\mathcal{E}_1$ is the set of integers $n \le N$ for which there exists a prime number $q \in \mathcal{I}$ such that $q \nmid \lambda(n)$, then

$$\#\mathcal{E}_1 \ll \frac{N}{\log\log N}. \tag{5.1}$$

Let $\mathcal{E}_2$ be the set of $n \le N$ such that $q^2 \mid n$ for some prime $q > y$. Then

$$\#\mathcal{E}_2 \le \sum_{q\ge y}\frac{N}{q^2} \ll \frac{N}{y} \ll \frac{N}{(\log\log\log N)^2}. \tag{5.2}$$

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

Let $\mathcal{E}_3$ be the set of $n \le N$ such that n is not divisible by any prime in $\mathcal{I}$. By the inclusion-exclusion principle, we have

$$\#\mathcal{E}_3 = N \prod_{y \le q \le z} \Big(1 - \frac{1}{q}\Big) + O(2^z) \ll N \frac{\log y}{\log z} + 2^z \ll \frac{N \log\log\log\log N}{\log\log\log N}. \tag{5.3}$$

Finally, let $\mathcal{N}$ be the set of integers $n \le N$ such that $n \notin \mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3$. Thus, from (5.1), (5.2), and (5.3), we deduce that

$$\widetilde{W}(a;N) = \sigma + O\Big(\frac{N^2 \log\log\log\log N}{\log\log\log N}\Big), \tag{5.4}$$

where

$$\sigma = \sum_{n \in \mathcal{N}} \Big| \sum_{\substack{g=1 \\ \gcd(g,n)=1}}^{n} \mathbf{e}(a\widetilde{f}_g(n)) \Big|.$$

To handle this sum, write $d_n = \gcd(n, \lambda(n))$, and put $s_n = \lambda(n)/d_n$. Then

$$\begin{aligned}
\sigma &= \sum_{n \in \mathcal{N}} \Big| \sum_{\substack{g=1 \\ \gcd(g,n)=1}}^{n} \mathbf{e}(a(g^n - g)/n) \Big| \\
&= \sum_{n \in \mathcal{N}} \frac{1}{\varphi(n)} \Big| \sum_{\substack{1 \le h \le n \\ \gcd(h,n)=1}} \sum_{\substack{g=1 \\ \gcd(g,n)=1}}^{n} \mathbf{e}(a((gh^{s_n})^n - gh^{s_n})/n) \Big| \\
&= \sum_{n \in \mathcal{N}} \frac{1}{\varphi(n)} \Big| \sum_{\substack{g=1 \\ \gcd(g,n)=1}}^{n} \sum_{\substack{1 \le h \le n \\ \gcd(h,n)=1}} \mathbf{e}(a(g^n - gh^{s_n})/n) \Big|.
\end{aligned}$$

Using first the Cauchy inequality, and then extending the range of summation over g, we derive that

$$\begin{aligned}
\Big| \sum_{\substack{g=1 \\ \gcd(g,n)=1}}^{n} \sum_{\substack{1 \le h \le n \\ \gcd(h,n)=1}} \mathbf{e}(a(g^n - gh^{s_n})/n) \Big|^2 &\le \varphi(n) \sum_{g=1}^{n} \Big| \sum_{\substack{1 \le h \le n \\ \gcd(h,n)=1}} \mathbf{e}(agh^{s_n}/n) \Big|^2 \\
&= \varphi(n)\, n M_a(n, s_n),
\end{aligned}$$

where

$$M_a(n,s) = \#\{(x,y) : ax^s \equiv ay^s \pmod n,\ x,\ y \in (\mathbb{Z}/n\mathbb{Z})^*\}.$$

Now, clearly $M_a(n,s) = \varphi(n) L_a(n,s)$, where

$$L_a(n,s) = \#\{x : ax^s \equiv a \pmod n,\ x \in (\mathbb{Z}/n\mathbb{Z})^*\}.$$

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

Therefore,

$$|\sigma| \le \sum_{n \in \mathcal{N}} \sqrt{n L_a(n, s_n)}. \tag{5.5}$$

Since $n \in \mathcal{N}$, there exists a prime $q \in \mathcal{I}$ such that $q \mid d_n$ but $q^2 \nmid n$. Let $\alpha \ge 1$ be the largest power of q dividing $\lambda(n)$. Then there exists a prime $p \mid n$ such that $q^\alpha \mid p-1$. It is also clear that $q^\alpha \nmid s_n$. This immediately shows that $\gcd(s_n, p-1) \mid (p-1)/q$. Since, by the Chinese Remainder Theorem, $L_a(n,s)$ is a multiplicative function with respect to n (and since $p > q > y$ we also have both $\gcd(n/p, p) = 1$ and $\gcd(a, p) = 1$), we derive that

$$\begin{aligned} L_a(n, s_n) &= L_a(n/p, s_n) L_a(p, s_n) \le \varphi(n/p) L_a(p, s_n) = \varphi(n/p) L_1(p, s_n) \\ &= \varphi(n/p) \gcd(s_n, p-1) \le \varphi(n/p)(p-1)/q = \varphi(n)/q \le n/y. \end{aligned}$$

Now relation (5.5) immediately shows that $\sigma \ll N^2 y^{-1/2}$, which together with (5.4) concludes the proof. ∎

6 Open Questions

Clearly, the range over a in Theorems 3.1, 4.1, and 5.1 can easily be extended. However, we do not see how to improve the corresponding bounds, even at the cost of reducing the range of a. Neither can we see any approaches toward estimating the single exponential sums

$$T_g(a; N) = \sum_{\substack{n=1 \\ n \text{ composite}}}^{N} \mathbf{e}(a f_g(n)),$$

$$\widetilde{T}_g(a; N) = \sum_{\substack{n=1 \\ n \text{ composite}}}^{N} \mathbf{e}(a \widetilde{f}_g(n)),$$

and we would like to leave these as open problems.

Acknowledgment The authors would like to thank the referee for a patient and careful reading which revealed a number of minor inaccuracies in the original version of the paper.

References

[1] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers.* Ann. of Math. **139**(1994), no. 3, 703–722.

[2] W. D. Banks, M. Z. Garaev, F. Luca, and I. E. Shparlinski, *Uniform distribution of the fractional part of the average prime divisor.* Forum Math. **17**(2005), no. 6, 885–901.

[3] 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), no. 1-2, 17–32.

[4] P. T. Bateman, P. Erdös, C. Pomerance, and E. G. Straus, *The arithmetic mean of the divisors of an integer.* In: Analytic number theory, Lecture Notes in Math. 899, Springer, Berlin-New York, 1981, pp. 197–220.

[5] J. Bourgain, *New bounds on exponential sums related to Diffie-Hellman distributions.* C. R. Math. Acad. Sci. Paris **338**(2004), no. 11, 825–830.

[6] J. Bourgain, A. A. Glibichuk, and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order.* J. London Math. Soc. **73**(2006), no. 2, 380–398.

[7] R. N. Boyarinov, I. S. Ngongo, and V. N. Chubarikov, *On new metric theorems in the method of A. G. Postnikov.* In: IV International conference: modern problems of number theory and its pplications, Current problems III, Mosk. Gos. Univ. im. Lomonosova Mekh.-Mat. Fak., Moscow, 2002, pp. 5–31.

[8] E. D. El-Mahassni, I. E. Shparlinski, and A. Winterhof, *Distribution of nonlinear congruential pseudorandom numbers modulo almost squarefree integers.* Monatsh. Math. **148**(2006), no. 4, 297–307.

[9] P. Erdös, A. Granville, C. Pomerance, and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions.* In: Analytic number theory, Progr. Math. 85, Birkhäuser, Boston, MA, 1990, pp. 165–204.

[10] P. Erdős and R. Murty, *On the order of a* $\pmod p$. CRM Proc. Lecture Notes 19, American Mathematical Society, Providence, RI, 1999, 87–97.

[11] P. Erdős and C. Pomerance, *On the number of false witnesses for a composite number.* Math. Comp.**46**(1986), no. 173, 259–279.

[12] K. Ford, *The distribution of integers with a divisorin a given interval.* Ann. of Math. **168**(2008), no. 2, 367–433.

[13] M. Z. Garaev, *The large sieve inequality for the exponential sequence* $\lambda^{[O(n^{15/14+o(1)})]}$ *modulo primes.* Canad. J. Math., **61**(2009), 336–350.

[14] M. Z. Garaev, F. Luca, and I. E. Shparlinski, *Exponential sums and congruences with factorials.* J. Reine Angew. Math. **584**(2005), 29–44.

[15] M. Z. Garaev and I. E. Shparlinski, *The large sieve inequality with exponential functions and the distribution of Mersenne numbers modulo primes.* Int. Math. Res. Not. **2005**(2005), no. 39, 2391–2408.

[16] A. Granville and C. Pomerance, *Two contradictory conjectures concerning Carmichael numbers.* Math. Comp. **71**(2002), no. 238, 883–908.

[17] D. R. Heath-Brown, *An estimate for Heilbronn's exponential sum.* In: Analytic number theory 2, Progr. Math. 139, Birkhäuser, Boston, MA, 1996, pp. 451–463.

[18] D. R. Heath-Brown and S. V. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum.* Q. J. Math. **51**(2000), no. 2, 221–235.

[19] K.-H. Indlekofer and N. M. Timofeev, *Divisors of shifted primes.* Publ. Math. Debrecen **60**(2002), no. 3-4, 307–345.

[20] A. A. Karatsuba, *Fractional parts of functions of a special form.* Izv. Math. **59**(1995), no. 4, 721–740.

[21] ———, *Analogues of Kloosterman sums.* Izv. Math. **59**(1995), no. 5, 971–981.

[22] ———, *Double Kloosterman sums.* Math. Notes **66**(1999), no. 5-6, 565–569.

[23] S. V. Konyagin, *Estimates of trigonometric sums over subgroups and Gauss sums.* In: IV International Conference, Modern problems of number theory and its applications, Mosk. Gos. Univ. im. Lomonosova Mekh.-Mat. Fak., Moscow, 2002, pp. 86–114.

[24] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications.* Cambridge Tracts in Mathematics 136, Cambridge University Press, Cambridge, 1999.

[25] N. M. Korobov, *Estimates of trigonometric sums and their applications.* Uspehi Mat. Nauk **13**(1958), no. 4, 185–192.

[26] ———, *Double trigonometric sums and their applications to the estimation of rational sums.* Mat. Zametki **6**(1969), 25–34.

[27] E. Landau, *Über die Zahlentheoretische Function* $\varphi(n)$ *und ihre Beziehung zum Goldbachschen Satz.* Nachr. Königlichen Ges. Wiss. Göttingen, Math.-Phys. Klasse, Göttingen, 1900, 177–186.

[28] R. Lidl and H. Niederreiter, *Finite fields.* In: Encyclopedia of mathematics and its applications 20, second edition, Cambridge University Press, Cambridge, 1997.

[29] F. Luca, *On* $f(n)$ *modulo* $\omega(n)$ *and* $\Omega(n)$ *when* f *is a polynomial.* J. Aust. Math. Soc. **77**(2004), no. 2, 149–164.

[30] F. Luca and C. Pomerance, *On some problems of Makowski-Schinzel and Erdős concerning the arithmetical functions* ϕ *and* σ. Colloq. Math. **92**(2002), no. 1, 111–130.

[31] F. Luca and A. Sankaranarayanan, *The distribution of integers n divisible by* $l^{\omega(n)}$. Publ. Inst. Math. **76(90)**(2004), 89–99.

[32] H. L. Montgomery, *Primes in arithmetic progressions.* Michigan Math. J. **17**(1970), 33–39.

https://doi.org/10.4153/CJM-2009-025-2 Published online by Cambridge University Press

[33] ———, *Ten lectures on the interface between analytic number theory and harmonic analysis.* CMBS Regional Conference Series in Mathematics 84, American Mathematical Society, Providence, RI, 1994.
[34] H. L. Montgomery and R. C. Vaughan, *The large sieve.* Mathematika **20**(1973), 119–134.
[35] A. G. Postnikov, *Ergodic aspects of the theory of congruences and of the theory of Diophantine approximations.* Trudy Mat. Inst. Steklov **82**(1966), 3–112.
[36] K. Prachar, *Primzahlverteilung.* Springer-Verlag, Berlin, 1957.
[37] C. Spiro, *How often is the number of divisors of n a divisor of n?* J. Number Theory **21**(1985), no. 1, 81–100.
[38] ———, *Divisibility of the k-fold iterated divisor function of n into n.* Acta Arith. **68**(1994), no. 4, 307–339.
[39] G. Tenenbaum, *Introduction to analytic and probabilistic number theory.* Studies in Advanced Mathematics 46, Cambridge University Press, 1995.
[40] A. I. Vinogradov, *On the remainder in Merten's formula.* Dokl. Akad. Nauk SSSR **148**(1963), 262–263.
[41] I. M. Vinogradov, *Elements of number theory.* Dover Publications, New York, 1954.

Department of Mathematics, University of Missouri, Columbia, MO 65211 USA
e-mail: bbanks@math.missouri.edu

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

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