

ON GAUSS SUMS AND THE EVALUATION OF STECHKIN'S CONSTANT

WILLIAM D. BANKS AND IGOR E. SHPARLINSKI

ABSTRACT. For the Gauss sums which are defined by

$$S_n(a, q) := \sum_{x \bmod q} \mathbf{e}(ax^n/q),$$

Stechkin (1975) conjectured that the quantity

$$A := \sup_{n, q \geq 2} \max_{\gcd(a, q) = 1} \frac{|S_n(a, q)|}{q^{1-1/n}}$$

is finite. Shparlinski (1991) proved that A is finite, but in the absence of effective bounds on the sums $S_n(a, q)$ the precise determination of A has remained intractable for many years. Using recent work of Cochrane and Pinner (2011) on Gauss sums with prime moduli, in this paper we show that with the constant given by

$$A = |S_6(\hat{a}, \hat{q})|/\hat{q}^{1-1/6} = 4.709236\dots,$$

where $\hat{a} := 4787$ and $\hat{q} := 4606056 = 2^3 \cdot 3^2 \cdot 7 \cdot 13 \cdot 19 \cdot 37$, one has the sharp inequality

$$|S_n(a, q)| \leq A q^{1-1/n}$$

for all $n, q \geq 2$ and all $a \in \mathbb{Z}$ with $\gcd(a, q) = 1$. One interesting aspect of our method is that we apply effective lower bounds for the center density in the sphere packing problem due to Cohn and Elkies (2003) to derive new effective bounds on the sums $S_n(a, q)$ in order to make the task computationally feasible.

1. INTRODUCTION

1.1. Background. In this paper we study the Gauss sums defined by

$$S_n(a, q) := \sum_{x \bmod q} \mathbf{e}(ax^n/q) \quad (n, q \geq 2, a \in \mathbb{Z})$$

where $\mathbf{e}(t) := \exp(2\pi it)$ for all $t \in \mathbb{R}$. Since $S_n(a, q) = dS_n(a/d, q/d)$ for any integer $d \geq 1$ that divides both a and q , for given n and q it is natural to investigate the quantity

$$G_n(q) := \max_{\gcd(a, q) = 1} |S_n(a, q)|,$$

which is the largest absolute value of the “irreducible” Gauss sums for a given modulus q and exponent n . It is well known (see Stechkin [11]) that for some constant $C(n)$ that depends only on n one has a bound of the form

$$G_n(q) \leq C(n) q^{1-1/n} \quad (q \geq 2),$$

Received by the editor August 13, 2014 and, in revised form, March 7, 2015.
 2010 *Mathematics Subject Classification*. Primary 11-XX.

and therefore the number

$$A(n) := \sup_{q \geq 2} G_n(q)/q^{1-1/n}$$

is well defined and finite for each $n \geq 2$. Stechkin [11] showed that the bound

$$(1) \quad A(n) \leq \exp(O(\log \log 3n^2)) \quad (n \geq 2)$$

holds, and he conjectured that for some absolute constant C one has

$$(2) \quad A(n) \leq C \quad (n \geq 2).$$

Shparlinski [10] proved Stechkin's conjecture in the stronger form

$$(3) \quad A(n) = 1 + O(n^{-1/4+\varepsilon}) \quad (n \geq 2).$$

We remark that the estimate (3) has been subsequently strengthened by Konyagin and Shparlinski (see [7, Theorem 6.7]) to

$$(4) \quad A(n) = 1 + O(n^{-1}\tau(n) \log n) \quad (n \geq 2),$$

where $\tau(\cdot)$ is the divisor function. In the opposite direction, it has been shown in [7, Theorem 6.7] that for infinitely many integers n one has the lower bound

$$(5) \quad A(n) > 1 + n^{-1} \exp\left(\frac{0.43 \log n}{\log \log n}\right).$$

We also note that the lower bound

$$(6) \quad A(n) \geq 1$$

holds for all $n \geq 2$ as one sees by applying [7, Lemma 6.4] with $m := n$ and $q := p$ for some prime $p \nmid n$.

1.2. Main result. The validity of (3) leads naturally to the problem of determining the exact value of *Stechkin's constant*

$$A := \max_{n \geq 2} A(n).$$

The argument of [10] is based on results that involve effectively computable constants, and it implies that A can be determined explicitly. Furthermore, even stronger bounds with explicit constants are available now thanks to Cochrane and Pinner [1]. However, even applying these new bounds in the argument of [10] one is still faced with an entirely infeasible computational task. To circumvent this problem, we derive new theoretical bounds by modifying an argument borrowed from [7, Chapter 4]. Our bounds also incorporate state of the art results on the sphere packing problem due to Cohn and Elkies [3]. These new theoretical bounds allow us to bring the overall amount of computation to a tractable level, enabling the explicit determination of A .

Theorem 1. *We have $A(n) < A(6)$ for all $n \geq 2$, $n \neq 6$. In particular, with the constant*

$$A := A(6) = \frac{|S_6(4787, 4606056)|}{4606056^{5/6}} = 4.70923685314526794358\dots$$

one has

$$|S_n(a, q)| \leq Aq^{1-1/n}$$

for all $n, q \geq 2$ and $a \in \mathbb{Z}$ with $\gcd(a, q) = 1$.

1.3. General approach. The results described above have all been obtained by reducing bounds for the general sums $G_n(q)$ to bounds on sums $G_n(p)$ with a prime modulus. There are several different (and elementary) ways to show that the bound $G_n(p) \leq np^{1/2}$ holds (see, for example, Lidl and Niederreiter [8, Theorem 5.32]), a result that plays the key role in Stechkin's proof of (1) in [11]. Stechkin [11] observed that in order to prove the conjecture (2) one simply needs a bound on $G_n(p)$ which remains nontrivial for all $n \leq p^\vartheta$ with some fixed $\vartheta > 1/2$. The first bound of this type, valid for any fixed $\vartheta < 4/7$, is given in [10]; taken together with the argument of Stechkin [11] this leads to (3). An improvement by Heath-Brown and Konyagin (see [5, Theorem 1]) of the principal result of [10], along with some additional arguments, leads to the stronger estimate (4); see [7, Chapter 6] for details.

The problem of determining A explicitly involves much more effort than that of simply performing a single direct computation. The starting point in our proof of Theorem 1 is the replacement of the bound of [5, Theorem 1] with a more recent *effective* bound on Gauss sums due to Cochrane and Pinner [1]; see (7) below. Using this bound one sees that each number $A(n)$ can be computed in a finite number of steps. However, the number of steps required is quite huge even for small values of n , and the direct computation of $A(n)$ is therefore exceedingly slow (especially when n is prime). It is infeasible to compute $A(n)$ over the entire range of values of n that are needed to yield the proof of Theorem 1 directly from the bound of [1] combined with the argument of [10]. Instead, to obtain Theorem 1 we establish the upper bound $A(n) < 4.7$ for all $n > 6$ using a combination of previously known bounds and some new bounds.

Our underlying approach has been to modify and extend the techniques of [7, Chapter 6] to obtain an effective version of [7, Theorem 6.7]. More precisely, in Propositions 1 and 2 we give general conditions under which one can disregard the value of $G_n(p)$ in the computation of $A(n)$. Special cases of these results, stated as Corollaries 1–4, have been used to perform the main computation described at the beginning of §2.2.

An interesting aspect of our method is that Corollary 4, which shows that $G_n(p)$ can be disregarded if $n \geq 2000$, $p \geq 8.5 \times 10^6$, and $(p-1)/\gcd(n, p-1) \geq 173$, essentially relies on effective lower bounds for the *center density in the sphere packing* problem due to Cohn and Elkies [3]. In the absence of these lower bounds, the running time of our primary computational algorithm would have increased by a factor of at least one thousand. We also remark that the criteria presented in Corollaries 1–3 allow for early termination of the program as the sums over x in (16), (17) and (18) are monotonically increasing and avoid the use of complex numbers.

2. PROOF OF THEOREM 1

2.1. Theoretical results. In what follows, the letter n always denotes a natural number, and the letter p always denotes a prime number.

We recall that $G_n(p) = G_d(p)$ holds whenever $\gcd(n, p-1) = d$; see [7, Lemma 6.6]. Our main technical tool for proving Theorem 1 is the bound

$$(7) \quad G_d(p) \leq B(d, p) := \min\{(d-1)p^{1/2}, \lambda d^{5/8} p^{5/8}, \lambda d^{3/8} p^{3/4}\} + 1,$$

where

$$\lambda := 2 \cdot 3^{-1/4} = 1.519671 \dots;$$

this is the main result of Cochrane and Pinner [1, Theorem 1.2].

For a given prime p and natural number n , let $v_p(n)$ denote the greatest integer m for which $p^m \mid n$ (that is, $v_p(\cdot)$ is the usual p -adic valuation). Arguing as in [7, Chapter 6], but using [2, Theorem 1.1] instead of [7, Lemma 6.3], we have

$$(8) \quad A(n) = A_1(n)A_2(n),$$

where

$$A_1(n) := \prod_{p \mid n} \max_{1 \leq m \leq v_p(n)+1} \left\{ G_n(p)/p^{m(1-1/n)}, 1 \right\},$$

$$A_2(n) := \prod_{d \mid n} \prod_{\substack{p \nmid n \\ \gcd(n,p-1)=d \\ B(d,p) > p^{1-1/n}}} \max \left\{ G_d(p)/p^{1-1/n}, 1 \right\}.$$

(Using [2, Theorem 1.1] allows us to replace $v_p(n) + 2$ with $v_p(n) + 1$ in the formula for $A_1(n)$ from [7, Chapter 6], but this has no influence on our result.)

Note that for fixed d and n there are only finitely many primes p for which $B(d, p) > p^{1-1/n}$. For our purposes below, we recall that the bound

$$(9) \quad A(n) \leq n^{3/n} A_2(n)$$

holds; see [7, p. 42].

Lemma 1. *Let b_1, \dots, b_m be real numbers with $|b_j| < p/2$ for each j , and suppose that*

$$\sum_{j=1}^m b_j^2 \geq C.$$

Then

$$(10) \quad \Re \sum_{j=1}^m \mathbf{e}(b_j/p) \leq m - \frac{8C}{p^2},$$

where $\Re z$ denotes the real part of $z \in \mathbb{C}$. Moreover, if $|b_j| < p/4$ for each j , then

$$(11) \quad \Re \sum_{j=1}^m \mathbf{e}(b_j/p) \leq m - \frac{16C}{p^2}.$$

Proof. The first bound (10) is [7, Lemma 4.1]; the proof is based on the inequality $\cos(2\pi u) \leq 1 - 8u^2$ for $u \in [-\frac{1}{2}, \frac{1}{2}]$. The second bound (11) is proved similarly using the inequality $\cos(2\pi u) \leq 1 - 16u^2$ for $u \in [-\frac{1}{4}, \frac{1}{4}]$. \square

To state the next result, we introduce some notation. As usual, we denote by $\varphi(\cdot)$ the Euler function. In what follows, for a fixed odd prime p and any $b \in \mathbb{Z}$ we denote by $\llbracket b \rrbracket_p$ the unique integer such that $b \equiv \llbracket b \rrbracket_p \pmod{p}$ and $-p/2 < \llbracket b \rrbracket_p < p/2$. We also denote by g a fixed generator of the multiplicative group \mathbb{F}_p^* of the finite field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

For any $r \geq 2$ let

$$C_r := \left(r \gamma_{r-1}^{r-1} \right)^{-1/r} \quad \text{and} \quad K_r := 4(1 - 1/f_r)C_r$$

where γ_k denotes the k -th Hermite constant (see Conway and Sloane [4]) and f_r is the least natural number such that $\varphi(f_r) \geq r$.

Finally, for fixed n and p we put $d := \gcd(n, p - 1)$ and $t := (p - 1)/d$.

Proposition 1. *Fix n, p and $\Theta \geq 1$. Suppose that $\varphi(t) \geq r \geq 2$, that the inequalities*

$$(12) \quad \sum_{x=1}^t \llbracket g^{dx+y} \rrbracket_p^2 \geq \Theta F_r(t, p) \quad (1 \leq y \leq d)$$

hold with

$$F_r(t, p) := \left(\frac{p^{2(r-1)t}}{r \gamma_{r-1}^{r-1}} \right)^{1/r} = C_r p^{2-2/r} t^{1/r},$$

and that the inequality

$$(13) \quad p^{1-1/n} \geq 1 + \lambda \left(\frac{p^5 \log p}{\Theta K_r (p-1)^{1/r}} \right)^{3r/(16r-8)}$$

holds. Then $G_d(p) \leq p^{1-1/n}$.

Proof. We can assume that $B(d, p) > p^{1-1/n}$, for otherwise the result follows immediately from (7).

We have

$$G_d(p) \leq 1 + d \max_{1 \leq y \leq d} \left| \sum_{x=1}^t e(g^{dx+y}/p) \right|.$$

Replacing $F_r(t, p)$ with $\Theta F_r(t, p)$ in the proof of [7, Theorem 4.2], taking into account (12) and our hypothesis that $\varphi(t) \geq r \geq 2$, we see that

$$(14) \quad G_d(p) \leq 1 + d(t - 4\Theta F_r(t, p)(1 - 1/t)p^{-2}).$$

Since $t \geq f_r$ it follows that

$$G_d(p) \leq 1 + d(t - 4\Theta C_r p^{-2/r} t^{1/r} (1 - 1/t)) \leq p - \Theta K_r d p^{-2/r} t^{1/r},$$

and recalling that $t := (p - 1)/d$ this leads to the bound

$$(15) \quad G_d(p) \leq p - \Theta K_r d^{1-1/r} p^{-2/r} (p - 1)^{1/r}.$$

On the other hand, combining (7) and (13) we have

$$1 + \lambda d^{3/8} p^{3/4} \geq B(d, p) > p^{1-1/n} \geq 1 + \lambda \left(\frac{p^5 \log p}{\Theta K_r (p-1)^{1/r}} \right)^{3r/(16r-8)},$$

which in turn yields the inequality

$$\Theta K_r d^{1-1/r} p^{-2/r} (p - 1)^{1/r} \geq d^{-1} p \log p.$$

In view of (15) we deduce that

$$G_d(p) \leq p - d^{-1} p \log p \leq p^{1-1/d} \leq p^{1-1/n}$$

as required. □

Corollary 1. *Suppose that $n \geq 2000$, $\varphi(t) \geq 25$, $p \geq 375000$, and*

$$(16) \quad \sum_{x=1}^t \llbracket g^{dx+y} \rrbracket_p^2 \geq p^{48/25} t^{1/25} \quad (1 \leq y \leq d).$$

Then $G_d(p) \leq p^{1-1/n}$.

Proof. Taking $r := 25$ in the statement of Proposition 1, we observe that

$$\gamma_{24} = 4, \quad C_{25} = (5 \cdot 2^{24})^{-2/25}, \quad K_{25} = \frac{112}{29} C_{25}.$$

We put $\Theta := C_{25}^{-1}$ so that (12) and (16) are equivalent, and then we verify that the inequality (13) holds under the conditions of the corollary. \square

Similarly, with the choice $\Theta := 2C_{25}^{-1}$ we obtain the following statement.

Corollary 2. *Suppose that $n \geq 2000$, $\varphi(t) \geq 25$, $p \geq 6500$, and*

$$(17) \quad \sum_{x=1}^t \llbracket g^{dx+y} \rrbracket_p^2 \geq 2p^{48/25} t^{1/25} \quad (1 \leq y \leq d).$$

Then $G_d(p) \leq p^{1-1/n}$.

Corollary 3. *Suppose that $n \geq 2000$, $\varphi(t) \geq 10$, $p \geq 8000$, and*

$$(18) \quad \sum_{x=1}^t \llbracket g^{dx+y} \rrbracket_p^2 \geq 13p^{16/9} t^{1/9} \quad (1 \leq y \leq d).$$

Then $G_d(p) \leq p^{1-1/n}$.

Proof. Taking $r := 9$ in the statement of Proposition 1, we observe that

$$\gamma_8 = 2, \quad C_9 = 48^{-2/9}, \quad K_9 = \frac{40}{11} C_9.$$

We put $\Theta := 13C_9^{-1}$ so that (12) and (18) are equivalent, and then we verify that the inequality (13) holds under the conditions of the corollary. \square

When $\Theta := 1$ the bound (12) holds for $\varphi(t) \geq r \geq 2$ as is demonstrated in the proof of [7, Lemma 4.2]. Moreover, in this case we have the following variant of Proposition 1.

Proposition 2. *Fix n and p . Suppose that $\varphi(t) \geq r \geq 2$ and that the inequalities*

$$(19) \quad p^{2/r} t^{1-1/r} > 32rC_r$$

and

$$(20) \quad p^{1-1/n} \geq 1 + \lambda \left(\frac{p^5 \log p}{2K_r(p-1)^{1/r}} \right)^{3r/(16r-8)}$$

hold. Then $G_d(p) \leq p^{1-1/n}$.

Proof. Fix y in the range $1 \leq y \leq d$. For every set \mathcal{I} containing precisely r consecutive integers, the proof of [7, Theorem 4.2] shows that

$$\sum_{x \in \mathcal{I}} \llbracket g^{dx+y} \rrbracket_p^2 \geq \frac{rF_r(t, p)}{t},$$

where $F_r(t, p)$ is as in Proposition 1. If it is the case that

$$\sum_{x \in \mathcal{I}} \llbracket g^{dx+y} \rrbracket_p^2 \geq \frac{2rF_r(t, p)}{t},$$

then Lemma 1 gives

$$(21) \quad \Re \sum_{y \in \mathcal{I}} \mathbf{e}(b_y/p) \leq r - \frac{16rF_r(t, p)}{tp^2}.$$

On the other hand, suppose that

$$\sum_{x \in \mathcal{I}} \llbracket g^{dx+y} \rrbracket_p^2 < \frac{2rF_r(t,p)}{t}.$$

From (19) it follows that

$$\sum_{x \in \mathcal{I}} \llbracket g^{dx+y} \rrbracket_p^2 < \frac{p^2}{16};$$

hence $|\llbracket g^{dx+y} \rrbracket_p| < p/4$ for each $x \in \mathcal{I}$. By Lemma 1 we again obtain (21).

Since (21) holds for every set \mathcal{I} of r consecutive integers, it follows that

$$\Re \sum_{y=1}^{t-1} \mathbf{e}(b_y/p) \leq t - \frac{16F_r(t,p)}{p^2}.$$

Writing

$$G_d(p) = 1 + d \max_{1 \leq y \leq d} \left| \sum_{x=1}^t \mathbf{e}(g^{dx+y}/p) \right|$$

and proceeding as in the proof of [7, Theorem 4.2] we see that

$$(22) \quad G_d(p) \leq 1 + d(t - 8F_r(t,p)(1 - 1/t)p^{-2}).$$

We complete the proof of Proposition 2 by following that of Proposition 1, taking $\Theta := 1$ and applying (22) instead of (14). □

Corollary 4. *Suppose that $n \geq 2000$, $p \geq 8.5 \times 10^6$, and $t \geq 173$. Then $G_d(p) \leq p^{1-1/n}$.*

Proof. We put $r := 30$ in the statement of Proposition 2. For any $t \geq 173$, we have $\varphi(t) \geq r$, and the inequalities (19) and (20) are readily verified by taking into account that $2.08174 < \gamma_{29} < 3.90553$ (the lower bound on γ_{29} follows from

$$\gamma_k \geq \frac{1}{\pi} (2\zeta(k)\Gamma(1 + k/2))^{2/k},$$

which was first stated by Minkowski and proved by Hlawka [6]; the upper bound on γ_{29} follows from Cohn and Elkies [3, Table 3]). □

2.2. Numerical methods.

Computation. *For all $n \geq 2000$, $p \leq 8.5 \times 10^6$, and $t \geq 173$, the inequality $G_d(p) \leq p^{1-1/n}$ holds.*

Description. For all $t \geq 637$ one sees that $B(d,p) \leq p^{1-1/2000}$ for all primes $p \leq 8.5 \times 10^6$; hence by (7) $G_d(p) \leq p^{1-1/n}$ holds in this case.

For $375000 \leq p \leq 8.5 \times 10^6$ and $173 \leq t \leq 636$ we apply Corollary 1. Since the inequality $\varphi(t) \geq 25$ is easily satisfied, it suffices to verify that (16) holds for all such p and t , which we have done.

Similarly, for $6500 \leq p \leq 375000$ and $173 \leq t \leq 636$ we apply Corollary 2, checking that (17) holds for all such p and t .

For the remaining primes $p \leq 6500$ we have verified on a case-by-case basis that $G_d(p) \leq p^{1-1/2000}$ holds whenever $t \geq 173$. □

Taking into account Corollary 4 and the above computation along with the trivial bounds $G_1(p) = 0$, $G_2(p) = p^{1/2}$ and $G_d(p) \leq p$ when $d \geq 3$, for every $n \geq 2000$ we deduce from (9) that

$$(23) \quad A(n) \leq n^{3/n} \prod_{\substack{d|n \\ d \geq 3}} \prod_{\substack{p \equiv 1 \pmod{d} \\ (p-1)/d \leq 172}} p^{1/n} = n^{3/n} \prod_{\substack{d|n \\ d \geq 3}} \prod_{\substack{t \leq 172 \\ dt+1 \text{ is prime}}} (dt+1)^{1/n}.$$

This yields a useful but somewhat less precise bound:

$$(24) \quad A(n) \leq n^{3/n} (172n + 1)^{172\tau(n)/n}.$$

Combining (24) with the explicit bound of Nicolas and Robin [9],

$$\frac{\log \tau(n)}{\log 2} \leq 1.54 \frac{\log n}{\log \log n} \quad (n \geq 3),$$

one sees that $A(n) < 4.7$ for all $n \geq 456000$.

For smaller values of n , we have used the bound (23) to check that the inequality $A(n) < A(6)$ holds for all n in the range $2000 < n < 456000$ apart from 677 “exceptional” numbers, which we collect together into a set

$$\mathcal{E} := \{2002, 2004, 2010, \dots, 25200, 27720, 30240\}.$$

We take \mathcal{D} to be the set of integers $d \geq 3$ such that either $d \leq 2000$ or else d divides some number $n \in \mathcal{E}$; the set \mathcal{D} has 2710 elements.

For each $d \in \mathcal{D}$ and prime p satisfying the conditions $p \equiv 1 \pmod{d}$, $(p-1)/d \leq 172$, and $B(d, p) > p^{1-1/d}$, we have computed the value of $G_d(p)$ numerically to high precision; this has been done for precisely 85112 pairs (p, d) altogether, and of these, all but 3618 pairs have been subsequently eliminated as the condition $G_d(p) \leq p^{1-1/d}$ is met; for the surviving pairs, the value $G_d(p)$ has been retained. Having these values at our disposal, we have been able to accurately estimate the quantity $A_2(n)$ for all $n \leq 2000$ and for all $n \in \mathcal{E}$. In view of (9) we have found that $A(n) < 4.7$ for all $n > 6$.

It is well known that $A(2) = \sqrt{2}$, and using (8) we are able to determine $A(n)$ precisely for $n = 3, 4, 5, 6$ (see Table 1 in §3.1). We find that $A(n) < 4.7$ for $2 \leq n \leq 5$, whereas $A(6) > 4.7$, and the proof of Theorem 1 is complete.

3. FURTHER RESULTS AND CONJECTURES

3.1. Extreme and average behavior of $A(n)$. In Table 1, we list numerical upper bounds for $A(n)$ in the range $3 \leq n \leq 40$; each bound agrees with the exact value of $A(n)$ to within 10^{-8} .

We observe that $A(19) = A(31) = 1$. On the basis of this and other numerical data gathered for this project, we make the following

Conjecture 1. *We have $A(n) = 1$ for infinitely many natural numbers n .*

On the other hand, the average value of $A(n)$ is not too close to one in the following sense.

Proposition 3. *Put*

$$E(N) := \sum_{n=2}^N (A(n) - 1) \quad (N \geq 2).$$

Then $E(N) \geq (2 + o(1)) \log N$ as $N \rightarrow \infty$.

TABLE 1. Values $A(n)$ with $3 \leq n \leq 40$

n	$A(n)$	n	$A(n)$
3	3.92853006	22	1.46567511
4	4.26259099	23	1.31902122
5	2.59880326	24	1.77609946
6	4.70923686	25	1.42781090
7	2.11936480	26	1.60401011
8	2.21026135	27	1.54156739
9	2.28069995	28	1.35754104
10	3.25099720	29	1.14455967
11	1.53359821	30	1.69652491
12	2.65269611	31	1.00000000
13	1.39611207	32	1.51129998
14	1.56950385	33	1.31715766
15	1.44795316	34	1.18744155
16	1.78417788	35	1.23094084
17	1.15247718	36	1.78968236
18	2.53272793	37	1.19086823
19	1.00000000	38	1.08865451
20	1.94022813	39	1.31104883
21	1.60324184	40	1.47364476

Proof. Let $p \geq 5$ be an odd prime, and set $n := (p - 1)/2$. It is easy to see that $S_n(a, p) = 1 + (p - 1) \cos(2\pi a/p)$ if $p \nmid a$, hence

$$G_n(p) \geq 1 + (p - 1) \cos(2\pi/p) = p - 2\pi^2 p^{-1} + O(p^{-2}).$$

Using this bound together with the estimate

$$p^{1/n} = \exp\left(\frac{2 \log p}{p - 1}\right) = 1 + \frac{2 \log p}{p} + O\left(\frac{\log^2 p}{p^2}\right)$$

it follows that

$$A(n) \geq \frac{G_n(p)}{p^{1-1/n}} \geq 1 + \frac{2 \log p}{p} + O\left(\frac{\log^2 p}{p^2}\right);$$

therefore

$$\begin{aligned} E(N) &\geq \sum_{\substack{2 \leq n \leq N \\ 2n+1 \text{ is prime}}} (A(n) - 1) = \sum_{5 \leq p \leq 2N+1} (A((p - 1)/2) - 1) \\ &\geq \sum_{5 \leq p \leq 2N+1} \left(\frac{2 \log p}{p} + O\left(\frac{\log^2 p}{p^2}\right) \right) = (2 + o(1)) \log N, \end{aligned}$$

and the proposition is proved. □

Combining Proposition 3 with the upper bound $E(N) \ll (\log N)^3$, which follows immediately from (4), we see that

$$\log E(N) \asymp \log \log N,$$

and it seems reasonable to make the following:

Conjecture 2. *For some constant $c \in (1, 3)$ we have*

$$E(N) = (\log N)^{c+o(1)} \quad (N \rightarrow \infty).$$

Although we have only computed $E(N)$ precisely in the limited range $2 \leq N \leq 40$, for large N the value $E(N)$ is closely approximated by the quantity

$$E_2(N) := \sum_{n=2}^N (A_2(n) - 1),$$

which therefore provides a reasonably tight lower bound for $E(N)$. Using the data we collected for the proof of Theorem 1 we have computed $E_2(N)$ in the wider range $2 \leq N \leq 2000$. In Figures 1, 2, 3 below we have plotted the values $E_2(N)/(\log N)^c$ in the same range with the choices $c = 1.74, 1.762$ and 1.78 , respectively (note that the scales are different along the vertical axes). These data suggest that $(\log E_2(N))/\log \log N$ might tend to a constant $c \in (1.74, 1.78)$ as $N \rightarrow \infty$.

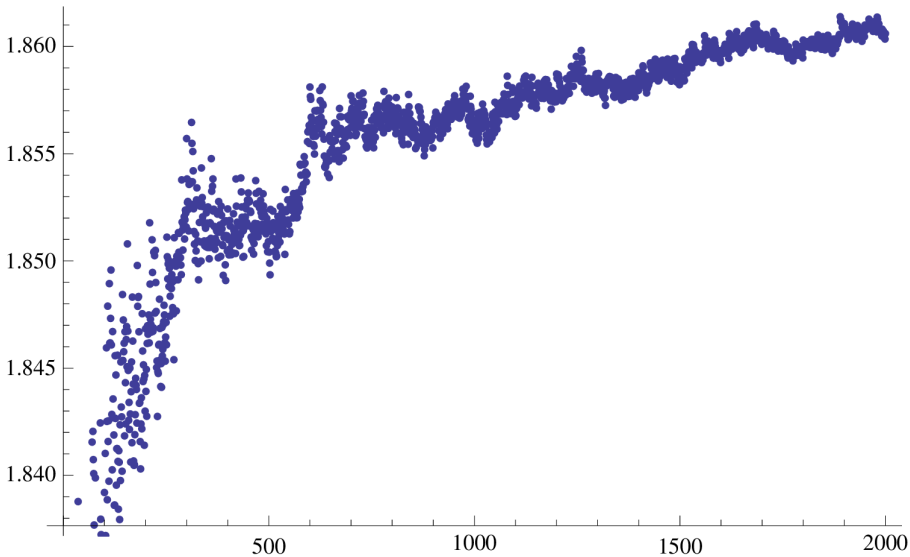


FIGURE 1. Values $E_2(N)/(\log N)^{1.74}$ with $2 \leq N \leq 2000$

To conclude this subsection, we provide Table 2, which, for any n in the range $3 \leq n \leq 40$, gives the modulus q for which $A(n) = G_n(q)/q^{1-1/n}$.

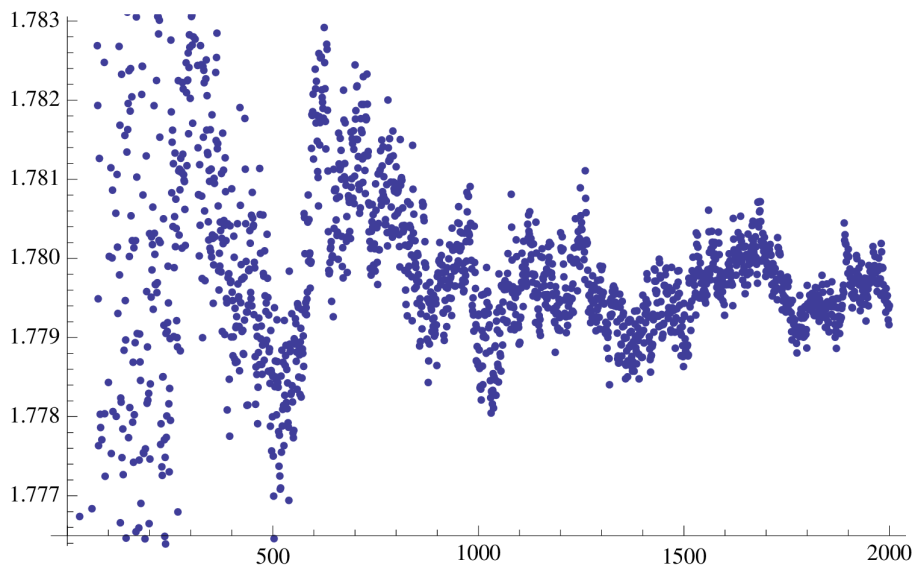
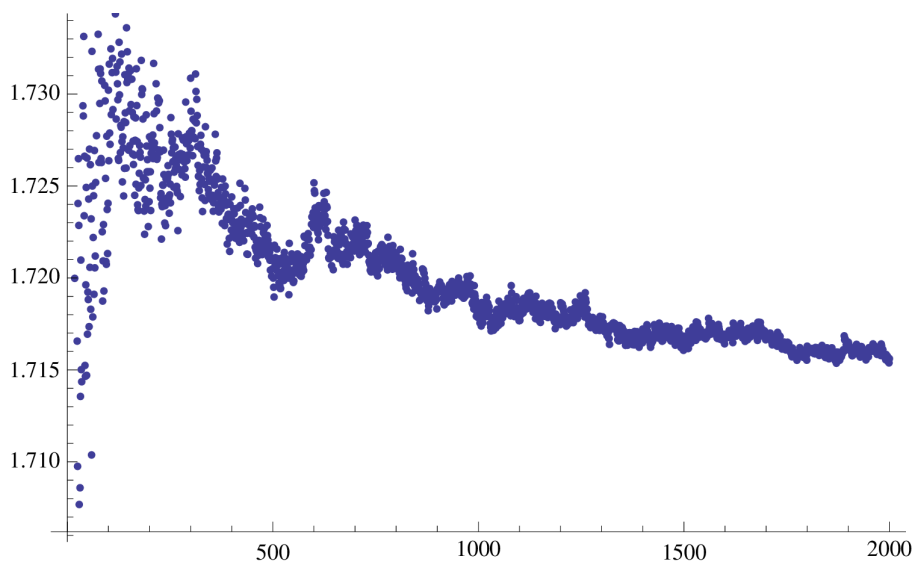
We remark that since $A(19) = A(31) = 1$ we have $A(19) = G_{19}(p^{18})$ for any prime $p \neq 19$ and $A(31) = G_{31}(p^{30})$ for any prime $p \neq 31$; see the justification of (6).

3.2. A useful bound on $G_n(p)$. It is interesting to explore conditions under which the bound

$$G_n(p) \leq p^{1-1/n}$$

holds. Recalling the notation $d := \gcd(n, p - 1)$ and $t := (p - 1)/d$, we have the following result.

Proposition 4. *The bound $G_n(p) \leq p^{1-1/n}$ holds for all $t \geq 246$ and $n \geq 3$.*

FIGURE 2. Values $E_2(N)/(\log N)^{1.762}$ with $2 \leq N \leq 2000$ FIGURE 3. Values $E_2(N)/(\log N)^{1.78}$ with $2 \leq N \leq 2000$

Proof. Taking into account that $p \geq t + 1 \geq 247$ (and thus $p \geq 251$), using the first estimate in (7) we have

$$G_3(p) \leq 2p^{1/2} \leq p^{2/3} \quad \text{and} \quad G_4(p) \leq 3p^{1/2} \leq p^{3/4}.$$

TABLE 2. Extreme moduli for $3 \leq n \leq 40$

n	q	n	q
3	767484081	22	1097192
4	724880	23	6533
5	24816275	24	11089264062240
6	4606056	25	1892365050125
7	61103	26	888749368
8	35360	27	122723007004143
9	2302452243	28	102143565680
10	170568200	29	59
11	1541	30	2221907019757425
12	2343607353360	31
13	4187	32	2647898240
14	488824	33	26150655643931
15	166568008135529	34	14111
16	6859840	35	261183353167
17	103	36	766359604548720
18	109951162776	37	33227
19	38	229
20	75391144400	39	728740376003003
21	2198500788029	40	36338531600800

Hence we can assume that $n \geq 5$ in what follows. Moreover, by Corollary 4 with the results of the numerical computation described in §2.2, for $t \geq 173$ and $n \geq 2000$ the bound $G_n(p) \leq p^{1-1/n}$ holds, so we can assume $n < 2000$.

The third estimate in (7) yields the bound $G_n(p) \leq p^{1-1/n}$ provided that

$$(25) \quad \lambda d^{3/8} p^{3/4} + 1 \leq p^{1-1/n}.$$

Since $p \geq 251$ one verifies that

$$(26) \quad \frac{p^{1-1/n}}{p^{1-1/n} - 1} \leq \eta$$

holds with $\eta := 1.0126$; therefore, (25) follows from the inequality

$$\lambda \eta d^{3/8} \leq p^{1/4-1/n}.$$

As $n \geq 5$ one can replace p here with $p - 1 = dt$; hence it suffices that

$$\lambda \eta d^{3/8} \leq d^{1/4-1/n} t^{1/4-1/n}.$$

Collecting powers of d on the left hand side and replacing d with the larger integer n , it follows that the inequality

$$\lambda \eta n^{1/8+1/n} \leq t^{1/4-1/n}$$

guarantees the desired estimate; that is, it is enough that

$$(27) \quad t \geq (\lambda \eta)^{4n/(n-4)} n^{(n+8)/(2n-8)}.$$

Simple calculations show that for $n \leq 1700$ the right hand side of (27) does not exceed 240, so we are done for such n .

For $n \geq 1700$ we also have $p \geq 1709$; hence, in this range of n we can take $\eta := 1.0006$ in (26). Using this new value of η , the right hand side of (27) does not exceed 246 for all $3 \leq n < 2000$, and this concludes the proof. \square

With further numerical computation one can, in principle, lower the threshold $t \geq 246$ in Proposition 4, perhaps to the bound $t \geq 173$ implied by Corollary 4 and the numerical work described in §2.2. In view of (7) (or (25)) the determination of the optimal threshold for t is a finite (but rather extensive) computational task.

ACKNOWLEDGEMENTS

The authors thank the referee for a careful reading of the manuscript and for the question that is addressed in §3.2.

This work was finished during a very enjoyable stay of the second author at the Max Planck Institute for Mathematics, Bonn. The second author was also supported in part by ARC grants DP130100237 and DP140100118.

REFERENCES

- [1] T. Cochrane and C. Pinner, *Explicit bounds on monomial and binomial exponential sums*, Q. J. Math. **62** (2011), no. 2, 323–349, DOI 10.1093/qmath/hap041. MR2805207 (2012d:11171)
- [2] T. Cochrane and Z. Zheng, *Pure and mixed exponential sums*, Acta Arith. **91** (1999), no. 3, 249–278. MR1735676 (2000k:11093)
- [3] H. Cohn and N. Elkies, *New upper bounds on sphere packings. I*, Ann. of Math. (2) **157** (2003), no. 2, 689–714, DOI 10.4007/annals.2003.157.689. MR1973059 (2004b:11096)
- [4] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., with additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, Springer-Verlag, New York, 1999. MR1662447 (2000b:11077)
- [5] D. R. Heath-Brown and S. Konyagin, *New bounds for Gauss sums derived from k th powers, and for Heilbronn's exponential sum*, Q. J. Math. **51** (2000), no. 2, 221–235, DOI 10.1093/qjmath/51.2.221. MR1765792 (2001h:11106)
- [6] E. Hlawka, *Zur Geometrie der Zahlen* (German), Math. Z. **49** (1943), 285–312. MR0009782 (5,201c)
- [7] S. V. Konyagin and I. E. Shparlinski, *Character Sums with Exponential Functions and Their Applications*, Cambridge Tracts in Mathematics, vol. 136, Cambridge University Press, Cambridge, 1999. MR1725241 (2000h:11089)
- [8] R. Lidl and H. Niederreiter, *Finite Fields*, with a foreword by P. M. Cohn, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983. MR746963 (86c:11106)
- [9] J.-L. Nicolas and G. Robin, *Majorations explicites pour le nombre de diviseurs de N* (French, with English summary), Canad. Math. Bull. **26** (1983), no. 4, 485–492, DOI 10.4153/CMB-1983-078-5. MR716590 (85e:11006)
- [10] I. E. Shparlinskiĭ, *Estimates for Gauss sums* (Russian), Mat. Zametki **50** (1991), no. 1, 122–130, DOI 10.1007/BF01156612; English transl., Math. Notes **50** (1991), no. 1-2, 740–746 (1992). MR1140360 (92m:11082)
- [11] S. B. Stečkin, *An estimate for Gaussian sums* (Russian), Mat. Zametki **17** (1975), no. 4, 579–588. MR0396430 (53 #295)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MISSOURI, COLUMBIA, MISSOURI 65211
E-mail address: bankswd@missouri.edu

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF NEW SOUTH WALES, SYDNEY, NSW
 2052, AUSTRALIA
E-mail address: igor.shparlinski@unsw.edu.au