On Gauss sums and the evaluation of Stechkin's constant

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

Igor E. Shparlinski
Department of Pure Mathematics
University of New South Wales
Sydney, NSW 2052, Australia
igor.shparlinski@unsw.edu.au

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

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

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

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

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

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

for all $n,q \geqslant 2$ 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 optimize the running time of our primary computational algorithm.

1 Introduction

In this paper we study the Gauss sums defined by

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

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

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

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 [10]) that for some constant $C(n)$ that depends only on n one has a bound of the form

$$G_n(q) \leqslant C(n)\, q^{1-1/n} \qquad (q \geqslant 2),$$

and therefore the number

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

is well-defined and finite for each $n \geqslant 2$. Stechkin [10] showed that the bound

$$A(n) \leqslant \exp\bigl(O(\log\log 3n)^2\bigr) \qquad (n \geqslant 2), \tag{1}$$

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

$$A(n) \leqslant C \qquad (n \geqslant 2). \tag{2}$$

Shparlinski [9] proved Stechkin's conjecture in the stronger form

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

We remark that the estimate (3) has been subsequently strengthened by Konyagin and Shparlinski (see [6, Theorem 6.7]) to

$$A(n) = 1 + O\left(n^{-1}\tau(n)\log n\right) \qquad (n \geqslant 2), \tag{4}$$

where $\tau(\cdot)$ is the divisor function. In the opposite direction, it has been shown in [6, Theorem 6.7] that for infinitely many integers n one has the lower bound

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

We also note that the lower bound

$$A(n) \geqslant 1 \tag{6}$$

holds for all $n \geqslant 2$ as one sees by applying [6, Lemma 6.4] with $m := n$ and $q := p$ for some prime $p \nmid n$.

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

$$A := \max_{n \geqslant 2} A(n),$$

and it is this problem that is the focus of the present paper.

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

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

one has

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

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

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 $G_n(p) \leqslant np^{1/2}$ holds (see, e.g., Lidl and Niederreiter [7, Theorem 5.32]), a result that plays the key role in Stechkin's proof of (1) in [10]. Stechkin [10] observed that in order to prove the conjecture (2) one simply needs a bound on $G_n(p)$ which remains nontrivial for all $n \leqslant p^{\vartheta}$ with some fixed $\vartheta > 1/2$. The first bound of this type, valid for any fixed $\vartheta < 4/7$, is given in [9]; taken together with the argument of Stechkin [10] this leads to (3). An improvement by Heath-Brown and Konyagin (see [4, Theorem 1]) of the principal result of [9], along with some additional arguments, leads to the stronger estimate (4); see [6, 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 [4, 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 [9]. 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 [6, Chapter 6] to obtain an effective version of [6, 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 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 $n \geqslant 2000$, $p \geqslant 8.5 \times 10^6$, and $(p-1)/\gcd(n,p-1) \geqslant 173$, essentially relies on effective lower bounds for the center density in the sphere packing problem due to Cohn and Elkies [2]. 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 [6, Lemma 6.6]. Our main technical tool for proving Theorem 1 is the bound

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

where

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

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 [6, Chapter 6] we have

$$A(n) = A_1(n) A_2(n), \tag{8}$$

where

$$A_1(n) := \prod_{p \mid n} \max_{1 \leqslant m \leqslant v_p(n)+2} \big\{G_n(p)/p^{m(1-1/n)}, 1\big\},$$

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

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

$$A(n) \leqslant n^{3/n} A_2(n) \tag{9}$$

holds; see [6, p. 42].

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

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

Then

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

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

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

Proof. The first bound (10) is [6, Lemma 4.1]; the proof is based on the inequality $\cos(2\pi u) \leqslant 1 - 8u^2$ for $u \in [-\frac{1}{2}, \frac{1}{2}]$. The second bound (11) is proved similarly using the inequality $\cos(2\pi u) \leqslant 1 - 16u^2$ for $u \in [-\frac{1}{4}, \frac{1}{4}]$. □

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 $[\![b]\!]_p$ the unique integer such that $b \equiv [\![b]\!]_p \pmod{p}$ and $-p/2 < [\![b]\!]_p < p/2$. 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 $r \geqslant 2$ let

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

where γ_k denotes the k-th Hermite constant (see Conway and Sloane [3]), and f_r is the least natural number such that $\varphi(f_r) \geqslant r$.

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

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

$$\sum_{x=1}^{t} [\![g^{dx+y}]\!]_p^2 \geqslant \Theta F_r(t,p) \qquad (1 \leqslant y \leqslant d) \tag{12}$$

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

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

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

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

Write

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

Replacing $F_r(t,p)$ with $\Theta F_r(t,p)$ in the proof of [6, Theorem 4.2], taking into account (12) and our hypothesis that $\varphi(t) \geqslant r \geqslant 2$, we see that

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

Since $t \geqslant f_r$ it follows that

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

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

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

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

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

which in turn yields the inequality

$$\Theta K_r d^{24/25} p^{-2/25} (p-1)^{1/25} \geqslant d^{-1} p \log p.$$

In view of (15) we deduce that

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

as required. □

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

$$\sum_{x=1}^{t} [\![g^{dx+y}]\!]_p^2 \geqslant p^{48/25} t^{1/25} \qquad (1 \leqslant y \leqslant d). \tag{16}$$

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

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

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

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. □

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

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

$$\sum_{x=1}^{t} [\![g^{dx+y}]\!]_p^2 \geqslant 2\, p^{48/25} t^{1/25} \qquad (1 \leqslant y \leqslant d). \tag{17}$$

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

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

$$\sum_{x=1}^{t} [\![g^{dx+y}]\!]_p^2 \geqslant 13\, p^{16/9} t^{1/9} \qquad (1 \leqslant y \leqslant d). \tag{18}$$

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

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

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

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

When $\Theta := 1$ the bound (12) holds for $\varphi(t) \geqslant r \geqslant 2$ as is demonstrated in the proof of [6, Lemma 4.2]. Moreover, in this case we have the following variant of Proposition 1.

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

$$p^{2/r} t^{1-1/r} > 32 r C_r \tag{19}$$

and

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

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

Proof. Fix y in the range $1 \leqslant y \leqslant d$. For every set $\mathcal{I}$ containing precisely r consecutive integers, the proof of [6, Theorem 4.2] shows that

$$\sum_{x \in \mathcal{I}} [\![g^{dx+y}]\!]_p^2 \geqslant \frac{r F_r(t,p)}{t}.$$

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

$$\sum_{x \in \mathcal{I}} [\![g^{dx+y}]\!]_p^2 \geqslant \frac{2r F_r(t,p)}{t},$$

then Lemma 1 gives

$$\Re \sum_{y \in \mathcal{I}} \mathbf{e}(b_y/p) \leqslant r - \frac{16 r F_r(t,p)}{t p^2}. \tag{21}$$

On the other hand, suppose that

$$\sum_{x \in \mathcal{I}} [\![g^{dx+y}]\!]_p^2 < \frac{2r F_r(t,p)}{t}.$$

From (19) it follows that

$$\sum_{x \in \mathcal{I}} [\![g^{dx+y}]\!]_p^2 < \frac{p^2}{16},$$

hence $\left| [\![g^{dx+y}]\!]_p \right| < p/4$ 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

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

Writing

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

and proceeding as in the proof of [6, Theorem 4.2] we see that

$$G_d(p)\leqslant 1+d\bigl(t-8F_r(t,p)(1-1/t)p^{-2}\bigr). \tag{22}$$

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 $n\geqslant 2000$, $p\geqslant 8.5\times 10^6$, and $t\geqslant 173$. Then $G_d(p)\leqslant p^{1-1/n}$.*

Proof. We put $r:=30$ in the statement of Proposition 2. For any $t\geqslant 173$, we have $\varphi(t)\geqslant r$, 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

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

which was first stated by Minkowski and proved by Hlawka [5]; the upper bound on γ_{29} follows from Cohn and Elkies [2, Table 3]). □

2.2 Numerical methods

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

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

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

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

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

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 $G_d(p) \leqslant p$ when $d \geqslant 3$, for every $n \geqslant 2000$ we deduce from (9) that

$$A(n) \leqslant n^{3/n} \prod_{\substack{d\,|\,n \\ d\geqslant 3}} \prod_{\substack{p\equiv 1 \,(\mathrm{mod}\ d) \\ (p-1)/d\leqslant 172}} p^{1/n} = n^{3/n} \prod_{\substack{d\,|\,n \\ d\geqslant 3 \\ dt+1 \text{ is prime}}} \prod_{t\leqslant 172} (dt+1)^{1/n}. \tag{23}$$

This yields a useful but somewhat less precise bound

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

Combining (24) with the explicit bound of Nicolas and Robin [8]

$$\frac{\log \tau(n)}{\log 2} \leqslant 1.54\,\frac{\log n}{\log\log n} \qquad (n \geqslant 3),$$

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

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

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

We take $\mathcal{D}$ to be the set of integers $d \geqslant 3$ such that either $d \leqslant 2000$ 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 $p \equiv 1 \pmod d$, $(p-1)/d \leqslant 172$, 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 $G_d(p) \leqslant p^{1-1/d}$ 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 $n \leqslant 2000$ 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). We find that $A(n) < 4.7$ for $2 \leqslant n \leqslant 5$, whereas $A(6) > 4.7$, and the proof of Theorem 1 is complete.

3 Further results and conjectures

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

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

Table 1: Values $A(n)$ with $3 \leqslant n \leqslant 40$

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*

$$E(N) := \sum_{n=2}^{N} \bigl(A(n) - 1\bigr) \qquad (N \geqslant 2).$$

Then $E(N) \geqslant (2+o(1))\log N$ *as* $N \to \infty$.

Proof. Let $p \geqslant 5$ 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

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

Using this bound together with the estimate

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

it follows that

$$A(n) \geqslant \frac{G_n(p)}{p^{1-1/n}} \geqslant 1 + \frac{2\log p}{p} + O\biggl(\frac{\log^2 p}{p^2}\biggr);$$

therefore

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

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*

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

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

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

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 $2 \leqslant N \leqslant 2000$. 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 $N \to \infty$.

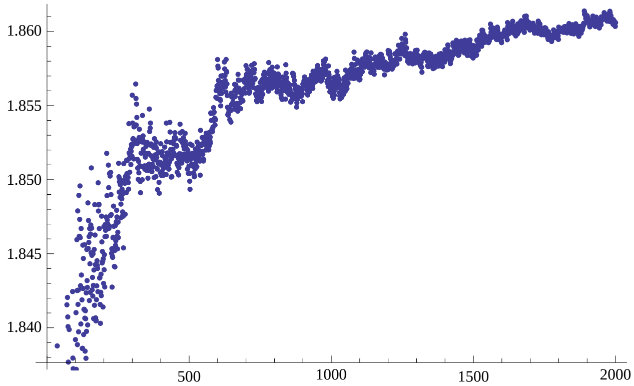

Figure 1: Values $E_2(N)/(\log N)^{1.74}$ with $2 \leqslant N \leqslant 2000$

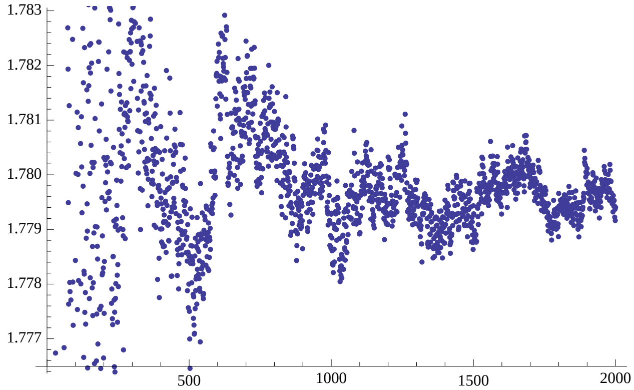

Figure 2: Values $E_2(N)/(\log N)^{1.762}$ with $2 \leqslant N \leqslant 2000$

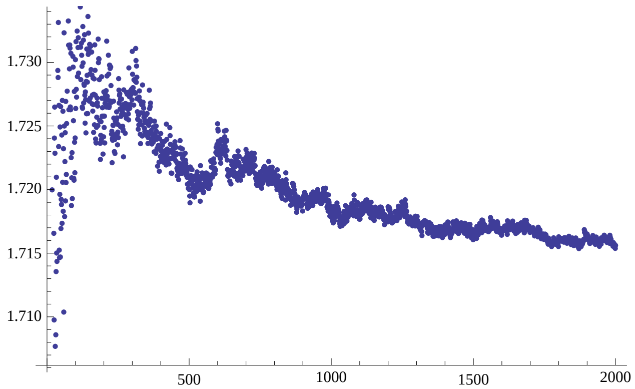

Figure 3: Values $E_2(N)/(\log N)^{1.78}$ with $2 \leqslant N \leqslant 2000$

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

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	$\cdots \quad \cdots$
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	$\cdots \quad \cdots$	38	229
20	75391144400	39	728740376003003
21	2198500788029	40	36338531600800

Table 2: Extreme moduli for $3 \leqslant n \leqslant 40$

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).

References

[1] T. Cochrane and C. Pinner, 'Explicit bounds on monomial and binomial exponential sums,' *Quart. J. Math.* **62** (2011), 323–349.

[2] H. Cohn and N. Elkies, 'New upper bounds on sphere packings I,' *Ann. of Math. (2)* **157** (2003), no. 2, 689–714.

[3] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups.* Third edition. Grundlehren der Mathematischen Wissenschaften, **290**. Springer-Verlag, New York, 1999.

[4] D. R. Heath-Brown and S. V. Konyagin, 'New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum,' *Quart. J. Math.* **51** (2000), 221–235.

[5] E. Hlawka, 'Zur Geometrie der Zahlen,' *Math. Z.* **49** (1943), 285–312 (in German).

[6] 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.

[7] R. Lidl and H. Niederreiter, *Finite fields.* Encyclopedia of Mathematics and its Applications, **20**. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983.

[8] J.-L. Nicolas and G. Robin, 'Majorations explicites pour le nombre de diviseurs de N,' *Canad. Math. Bull.* **26** (1983), no. 4, 485–492 (in French).

[9] I. E. Shparlinski, 'On bounds of Gaussian sums,' *Matem. Zametki* **50** (1991), 122–130 (in Russian).

[10] S. B. Stechkin, 'An estimate for Gaussian sums', *Matem. Zametki* **17** (1975), 342–349 (in Russian).