An Exponential Sum Over Primes

D. A. GOLDSTON
San Jose State University, San Jose, California

1. INTRODUCTION

In additive prime number theory the starting point of many investigations is the generating function

\[ S(\alpha) = \sum_{p \leq N} (\log p) e(p\alpha), \]  

where the sum is over primes \( p \) and \( e(u) = e^{2\pi i u} \). Our goal is to examine \( S(\alpha) \) as \( N \to \infty \). Using the prime number theorem for arithmetic progressions it is easy to find an approximation for \( S(\alpha) \) when \( \alpha \) is close to the fraction \( a/q \), where \( (a,q) = 1 \). Letting \( \alpha = a/q + \beta \), the approximation is given by

\[ J(\beta; q) = \frac{\mu(q)}{\phi(q)} I(\beta), \quad \text{where} \quad I(\beta) = \sum_{1 \leq n \leq N} e(n\beta). \]  

This approximation often provides the main term in additive problems such as the twin prime conjecture or the Goldbach conjecture, although the resulting error terms can not be handled at present. As a first step in analyzing these error terms, it is important to have estimates for the error in the approximation, which we measure with

\[ S_1(\beta; q, a) = S(\frac{a}{q} + \beta) - J(\beta; q). \]  

For small \( q \) we may estimate \( S_1(\beta; q, a) \) with the Siegel-Walfisz theorem, which gives \([1, p. 147]\) for \( 1 \leq q \leq (\log N)^A \), and any \( A > 0 \),

\[ S_1(\beta; q, a) \ll (1 + |\beta| N)^{1/2} N \exp(-c\sqrt{\log N}). \]  

---

Research supported in part by NSF Grant DMS9003329
For larger $q$ Vinogradov proved that $S(\alpha)$ is small if $\alpha$ is sufficiently close to a fraction $a/q$ with large denominator $q$. This type of result together with equation (4) allowed him to prove that every sufficiently large odd number is the sum of three primes. Such estimates can now be found much more simply by Vaughan's elementary method[1],[4]; the current best result is, for $(a,q) = 1$ and $|\beta| \leq 1/q^2$,

\[ S\left( \frac{a}{q} + \beta \right) \ll (q^{1/2}N^{1/2} + N^{4/5} + q^{-1/2}N)(\log N)^4. \]  

(5)

Equation (5) also holds with $S(\alpha/q + \beta)$ replaced by $S_1(\beta; q, a)$, since $J(\beta; q) \ll \frac{N}{q} \log N$ which may be absorbed into the last error term in (5). Assuming the Generalized Riemann Hypothesis (GRH), we have the result [2]

\[ S_1(\beta; q, a) \ll q^{1/2}(N^{1/2} \log^2(qN) + \beta^{1/2}N \log(qN)), \]  

(6)

which improves on (5) when $\beta$ and $q$ are not too large.

If we examine the proofs of (5) and (6) it appears difficult to substantially improve either result. However, by examining a type of fourth moment of $S_1(\beta; q, a)$, I made a conjecture [2] on what shape such an improvement should take. Let

\[ S_1^*(Q) = \max_{1 \leq \theta \leq Q} \max_{(a,q) = 1} \max_{\beta \in \theta \mathbb{Q}(q,a)} |S_1(\beta; q, a)|, \]  

(7)

where $\theta \mathbb{Q}(q,a)$ is the Farey arc of level $Q$ around $a/q$ and recentered at the origin, which will be defined precisely in the next section.

**Conjecture.** For $Q = N^{\theta}$, $0 < \theta < 1$, and any $\epsilon > 0$, we have

\[ S_1^*(Q) \ll N^{\max(\theta, 1-\theta)} = N^{1/2 + |\theta - 1/2| + \epsilon}. \]  

(8)

We see that (5) implies $S_1^*(Q) \ll N^{\max(1-\theta/2, 1/2 + \theta/2, 4/5) + \epsilon}$, while on GRH (6) implies $S_1^*(Q) \ll N^{3/4 + 1/2|\theta - 1/2| + \epsilon}$.

We prove in this paper that the conjecture is close to the best possible result.

**Theorem.** We have, for any $\epsilon > 0$,

\[ \max_{Q \leq P \leq 3Q} S_1^*(P) \geq \begin{cases} \frac{N}{Q \sqrt{\log N}}, & \text{for } N^\epsilon \leq Q \leq N^{1/2}/\log^{2+\epsilon} N; \\ \frac{Q}{\sqrt{\log N}}, & \text{for } N^{1/2}/\log^{2+\epsilon} N \leq Q \leq N^{1-\epsilon}; \end{cases} \]  

(7)

while for all $1 \leq Q \leq N$,

\[ S_1^*(Q) \geq \sqrt{N \log N}. \]  

(8)

Thus in particular, for $Q = N^\theta$, $0 < \theta < 1$, we have

\[ \max_{Q \leq P \leq 3Q} S_1^*(P) \geq \frac{N^{\max(\theta, 1-\theta)}}{\log^2 N}. \]  

(9)
AN EXponential SUM OVER PRIMES

We actually prove that at least one of \( S_1^*(Q) \) or \( S_1^*(3Q) \) is larger than the lower bound in (7) and (9). While one would not expect the level \( Q \) of the decomposition to matter, in applications we are free to choose any \( Q \) we want in a given range, such as \([Q,3Q]\). Thus we might weakened the conjecture by replacing \( S_1^*(Q) \) with \( \min_{P \leq Q} S_1^*(P) \) without any loss of usefulness. An application of the conjecture is to the Goldbach problem. Let \( E(N) \) denote the number of even numbers bigger than 2 and less than \( N \), which are not the sum of two primes. The conjecture implies \( E(N) \ll N^\epsilon \), while on GRH one obtains only \( E(N) \ll N^{1+\epsilon/2} \).

2. NOTATION

The proof of the theorem requires a number of definitions from [2]. The Farey fractions of order \( Q \) are given by

\[
\mathcal{F}_Q = \{ \frac{a}{q} : 1 \leq q \leq Q, 0 \leq a \leq q, (a,q) = 1 \}.
\]

We define the Farey arcs around each of these fractions, except 0/1 which we exclude, as follows. Let \( \frac{a'}{q'} < \frac{a}{q} < \frac{a''}{q''} \) be consecutive fractions in the Farey decomposition of order \( Q \), and let

\[
\mathcal{M}(q,a) = \mathcal{M}_Q(q,a) = \left( \frac{a + a'}{q + q'}, \frac{a + a''}{q + q''} \right)
\]

\[
= \left( \frac{a}{q} - \frac{1}{q(q + q')}, \frac{1}{q(q + q'')} \right) \quad \text{for } \frac{a}{q} \neq \frac{1}{1}, a \neq 0;
\]

\[
\mathcal{M}(1,1) = \mathcal{M}_Q(1,1) = \left( 1 - \frac{1}{Q + 1}, 1 + \frac{1}{Q + 1} \right).
\]

These intervals are disjoint and their union is \( \left( \frac{1}{Q+1}, 1 + \frac{1}{Q+1} \right) \). We denote the Farey arcs when recentered at the origin by

\[
\theta_Q(q,a) = \left( -\frac{1}{q(q + q')}, \frac{1}{q(q + q'')} \right);
\]

these are the intervals used in (7). Since \( Q < q + q' < 2Q \) and similarly for \( q + q'' \), we see

\[
\theta_Q(q,a) = \left( -\frac{1}{q(Q + \mu)}, \frac{1}{q(Q + 
u)} \right),
\]

for integers \( 0 < \mu, \nu < Q \) which depend on \( a, q, \) and \( Q \).

Throughout this paper we will use the notation

\[
\sum_Q = \sum_{1 \leq q \leq Q} \sum_{\substack{1 \leq a \leq q \\ (a,q) = 1}} \sum_Q,
\]

and

\[
Q_1 = \min(Q, \frac{N}{Q}).
\]
The letters $p$, $p'$ will always denote primes. The letter $\epsilon$ will denote a small positive constant which may vary from equation to equation.

We will be concerned with three exponential sums, the first two of which are the square of the sums in equations (1) and (2):

$$S^2(\alpha) = \sum_{1 \leq n \leq 2N} R(n, N) e(n\alpha), \quad R(n, N) = \sum_{\substack{p, p' \leq N \\ n = p + p'}} (\log p)(\log p');$$

$$J^2(\beta; q) = \frac{\mu^2(q)}{\phi(q)} I^2(\alpha) = \frac{\mu^2(q)}{\phi(q)} \sum_{1 \leq n \leq 2N} \nu(n, N) e(n\alpha), \quad \nu(n, N) = \sum_{\substack{1 \leq n', n'' \leq N \\ n = n' + n''}} 1.$$  \hspace{1cm} (16)

For $1 \leq n \leq 2N$ we have $\nu(n, N) = \min(n - 1, 2N - n + 1)$. Finally, let

$$V(\alpha) = \sum_{1 \leq n \leq 2N} \mathfrak{S}(n) \nu(n, N) e(n\alpha),$$

where $\mathfrak{S}(k)$ is defined for all integers $k \neq 0$ by

$$\mathfrak{S}(k) = \begin{cases} 0, & \text{if } k \text{ is odd;} \\ 2C \prod_{p \mid k} \left(1 - \frac{1}{p - 1} \right), & \text{if } k \text{ is even, } k \neq 0; \end{cases} \hspace{1cm} (18)$$

and

$$C = \prod_{p > 2} \left(1 - \frac{1}{(p - 1)^2} \right).$$

By Parseval's theorem

$$\mathcal{R} = \int_0^1 |S^2(\alpha) - V(\alpha)|^2 \, d\alpha = \sum_{1 \leq n \leq 2N} (R(n, N) - \mathfrak{S}(n) \nu(n, N))^2,$$

which we relate to the mean values

$$S(Q) = \sum_Q \int_{\theta_Q(q, a)} \left| S^2\left(\frac{a}{q} + \beta \right) - J^2(\beta; q) \right|^2 \, d\beta,$$

and

$$V(Q) = \sum_Q \int_{\theta_Q(q, a)} \left| V\left(\frac{a}{q} + \beta \right) - J^2(\beta; q) \right|^2 \, d\beta.$$  \hspace{1cm} (21)
3. PROOF OF THE THEOREM

Using the inequality \(|a + b|^2 \leq 2|a|^2 + 2|b|^2\), we have

\[
R = \sum_Q \int_{\theta_Q(q,a)} \left| S^2(\frac{a}{q} + \beta) - V(\frac{a}{q} + \beta) \right|^2 d\beta
\]

\[
= \sum_Q \int_{\theta_Q(q,a)} \left| (S^2(\frac{a}{q} + \beta) - J^2(\beta; q)) + (J^2(\beta; q) - V(\frac{a}{q} + \beta)) \right|^2 d\beta
\]

\[
\leq 2S(Q) + 2V(Q).
\]  
(23)

Similarly we obtain

\[
S(Q) \leq 2R + 2V(Q), \quad V(Q) \leq 2R + 2S(Q).
\]  
(24)

We now bound \(S(Q)\) in terms of \(S_1^*(Q)\). First,

\[
S(Q) = \sum_Q \int_{\theta_Q(q,a)} \left| S_1(\beta; q, a) \right|^2 \left| S(\frac{a}{q} + \beta) + J(\beta; q) \right|^2 d\beta
\]

\[
\leq 2(S^*(Q))^2 \left\{ \int_0^1 |S(\alpha)|^2 d\alpha + \sum_Q \int_{\theta_Q(q,a)} |J(\beta; q)|^2 d\beta \right\}.
\]

Now

\[
\int_0^1 |S(\alpha)|^2 d\alpha = \sum_{p \leq N} \log^2 p = N \log N + O(N)
\]

by the prime number theorem, and

\[
\sum_Q \int_{\theta_Q(q,a)} |J(\beta; q)|^2 d\beta \leq \sum_{1 \leq r \leq Q} \frac{\mu^2(q)}{\phi(q)} \int_0^1 |I(\beta)|^2 d\beta
\]

\[
= N(\log Q + O(1)),
\]

by [2, Lemma 2] or [3]. We conclude that for \(Q = N^\theta, 0 < \theta < 1\), and \(N\) sufficiently large,

\[
S(Q) \leq 4N \log N(S^*(Q))^2.
\]  
(25)

For \(V(Q)\) we use the main results proved in [2]:

\[
V(Q) \leq \frac{N^3}{Q^2} \log N, \text{ for } 1 \leq Q \leq N,
\]  
(26)

and for any \(\epsilon > 0\),

\[
V(Q) \sim \begin{cases} \frac{A N^2 \log Q}{3g^2}, & \text{for } N^\epsilon \leq Q \leq N^{1/2}/\log^{2+\epsilon} N; \\ \frac{A N Q^2}{4\pi^2}, & \text{for } N^{1/2} \log^{2+\epsilon} N \leq Q \leq N^{1-\epsilon}, \end{cases}
\]  
(27)
where $\mathcal{A}$ is the constant
\[ \prod_p \left( 1 + \frac{2-1/p}{(p-1)^2} \right) = 4.432 \ldots \]

We now prove that the conjecture implies $E(N) \ll N^\epsilon$. From equation (26) we obtain on choosing $Q = N^{1/2}$ that $\mathcal{V}(Q) \ll N^2 \log N$, and by the conjecture and (25) we have $S(Q) \ll N^{2+\epsilon}$. Hence by (23) $R \ll N^{2+\epsilon}$. Since $\Theta(n) \gg 1$ for $n$ even, we see $R \gg N^2(E(N) - E(N/2))$, and therefore $E(N) - E(N/2) \ll N^\epsilon$. Replacing $N$ by $N/2, N/4, \ldots$, and adding we obtain $E(N) \ll N^\epsilon$.

To prove the theorem, we start with the second part of (24): $\mathcal{V}(Q) \leq 2R + 2S(Q)$, and eliminate $R$ in this formula by applying (23) with $Q = P$: $R \leq 2S(P) + 2\mathcal{V}(P)$. Thus
\[ \mathcal{V}(Q) \leq 4S(P) + 4\mathcal{V}(P) + 2S(Q), \]
and hence by (25)
\[ \mathcal{V}(Q) - 4\mathcal{V}(P) \leq 4S(P) + 2S(Q) \leq 4(S(P) + S(Q)) \ll N \log N \left( (S^*(Q))^2 + (S^*(P))^2 \right). \]

If $N^\epsilon \leq Q \leq N^{1/2}/\log^{2+\epsilon} N$, we take $P = 3Q$ and obtain by (27) that
\[ \mathcal{V}(Q) - 4\mathcal{V}(3Q) \sim \frac{5A}{27} \frac{AN^3}{Q^2}, \]
and the first part of (7) follows from the last two equations. If $N^{1/2} \log^{2+\epsilon} N \leq Q \leq N^{1-\epsilon}$, we take $P = Q/3$ and obtain
\[ \mathcal{V}(Q) - 4\mathcal{V}(Q/3) \sim \frac{5A}{36\pi} NQ^2, \]
from which the second part of (7) follows.

To prove (8) we use the easily proven result [2, Lemma 6] that for $1 \leq Q \leq N$,
\[ \sum_Q \int_{\Theta_Q} |S_1(\beta; q, a)|^2 \, d\beta \gg N \log(N/Q_1) \gg N \log N. \quad (28) \]
The left hand side is majorized by $(S^*(Q))^2$, and (8) follows. The estimate in equation (9) follows from (7) except in the range $N^{1/2}/\log^{2+\epsilon} N \leq Q \leq N^{1/2} \log^{2+\epsilon} N$, where the lower bound follows from the lower bound in (8).

REFERENCES