Bull. Aust. Math. Soc. **100** (2019), 225–229
doi:10.1017/S0004972719000224

A LOWER BOUND FOR THE LARGE SIEVE WITH SQUARE MODULI

STEPHAN BAIER, SEAN B. LYNCH[✉] and LIANGYI ZHAO

(Received 20 December 2018; accepted 13 January 2019; first published online 27 February 2019)

Abstract

We prove a lower bound for the large sieve with square moduli.

2010 *Mathematics subject classification*: primary 11N35; secondary 11B57, 11J25, 11J71, 11L03, 11L07, 11L40.

Keywords and phrases: large sieve, Farey fractions in short intervals, estimates on exponential sums.

1. Introduction

The classical large sieve inequality states that for $Q, N \in \mathbb{N}$, $M \in \mathbb{Z}$ and any sequence of complex numbers $\{a_n\}$,

$$\sum_{q=1}^{Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{an}{q}\right) \right|^2 \leq (Q^2 + N - 1) \sum_{n=M+1}^{M+N} |a_n|^2.$$

In [8], the third author studied the large sieve inequality for square moduli and conjectured that for any $\varepsilon > 0$,

$$\sum_{q=1}^{Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q^2} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{an}{q^2}\right) \right|^2 \ll Q^{\varepsilon}(Q^3 + N) \sum_{n=M+1}^{M+N} |a_n|^2, \tag{1.1}$$

where the implied constant depends only on ε. In his undergraduate thesis, the second author investigated the validity of (1.1) numerically. A natural question is whether (1.1) can hold with the factor Q^{ε} removed. In this note, we answer this question in the negative. More precisely, we prove the following result.

The third author was supported by the FRG grant PS43707 and the Faculty Silverstar Fund PS49334 at UNSW during this work.

THEOREM 1.1. *For every $\varepsilon > 0$, there are infinitely many natural numbers Q such that for suitable $M \in \mathbb{Z}$, $N \in \mathbb{N}$ and sequences $\{a_n\}$ of complex numbers,*

$$\sum_{q=1}^{Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q^2} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{an}{q^2}\right) \right|^2 \geq D Q^{\log 2/(1+\varepsilon) \log\log Q} (Q^3 + N) \sum_{n=M+1}^{M+N} |a_n|^2 \tag{1.2}$$

for some absolute positive constant D.

The theorem shows that the Q^ε factor in (1.1) cannot be discarded or even replaced by a power of logarithm. We note that the best-known upper bound for the left-hand side of (1.1) is

$$\ll (QN)^\varepsilon (Q^3 + N + \min\{\sqrt{Q}N, \sqrt{N}Q^2\}) \sum_{n=M+1}^{M+N} |a_n|^2$$

due to the first and third authors [2].

The large sieve inequality for square (and quadratic) moduli has many applications. For example, it is used in the study of the Bombieri–Vinogradov theorem for square moduli [1], elliptic curves over finite fields [3, 7], Fermat quotients [4] and the representation of primes [1, 6].

In [8], the third author also studied the large sieve inequality for k-power moduli, where $k > 2$. The best-known result for these k-power moduli with $k > 2$ is due to Halupczok [5], who gave a large sieve inequality for k-power moduli which is uniform in k.

2. Proof of Theorem 1.1

We first establish a lower bound for the number of Farey fractions with square denominators near certain rational points.

LEMMA 2.1. *Let $\varepsilon > 0$ and $p_1, \ldots, p_m$ be the first m odd primes. Set $Q := p_1 \cdots p_m$ and*

$$\mathcal{S}(Q) := \left\{ (a,q) \in \mathbb{N} \times \mathbb{N} : Q < q \leq 2Q, 1 \leq a \leq q^2, (a,q) = 1, \left| \frac{a}{q^2} - \frac{1}{Q} \right| \leq \frac{1}{Q^3} \right\}. \tag{2.1}$$

Then

$$\sharp\mathcal{S}(Q) \geq Q^{\log 2/(1+\varepsilon) \log\log Q}, \tag{2.2}$$

provided m is sufficiently large.

Here we note that the expected number of Farey fractions of the form a/q^2 with $Q < q \leq 2Q$, $1 \leq a \leq q^2$ and $(a,q) = 1$ in an interval of length Δ is, heuristically, of order of magnitude $Q^3\Delta$. Lemma 2.1 shows that under certain circumstances, the true number can exceed the expectation significantly.

PROOF OF LEMMA 2.1. Using the Chinese remainder theorem, the number of solutions to the congruence

$$q^2 \equiv 1 \pmod{Q}$$

https://doi.org/10.1017/S0004972719000224 Published online by Cambridge University Press

with $Q < q \leq 2Q$ is exactly 2^m. If q solves the above congruence, then

$$q^2 = 1 + aQ$$

for some a with $1 \leq a \leq q^2$ and $(a, q) = 1$, and it follows that

$$\left|\frac{a}{q^2} - \frac{1}{Q}\right| = \frac{1}{q^2 Q} \leq \frac{1}{Q^3}.$$

Hence,

$$\sharp\mathcal{S}(Q) \geq 2^m.$$

Moreover, using the prime number theorem, for any given $\varepsilon > 0$,

$$\log Q = \sum_{i=1}^{m} \log p_i \leq (1+\varepsilon)p_m \leq (1+2\varepsilon)m \log m,$$

if m is sufficiently large. Consequently, for any given $\varepsilon > 0$,

$$m \geq \frac{\log Q}{(1+\varepsilon)\log\log Q},$$

if m is sufficiently large. Now the desired inequality (2.2) follows. □

Proof of Theorem 1.1. It suffices to prove (1.2) with the summation range $1 \leq q \leq Q$ replaced by $Q < q \leq 2Q$. Set $Q = p_1 \cdots p_m$ as in Lemma 2.1. Further, set

$$M := 0, \quad N := \frac{Q^3}{9}, \quad a_n := e\left(-\frac{n}{Q}\right).$$

Then

$$\sum_{n=M+1}^{M+N} a_n e\left(\frac{an}{q^2}\right) = \sum_{n=1}^{N} e(\alpha_n)$$

with

$$\alpha_n := n\left(\frac{a}{q^2} - \frac{1}{Q}\right).$$

If

$$\left|\frac{a}{q^2} - \frac{1}{Q}\right| \leq \frac{1}{Q^3},$$

then $|\alpha_n| \leq 1/9$ for $n = 1, \ldots, N$ and

$$\left|\sum_{n=1}^{N} e(\alpha_n)\right| \geq CN \tag{2.3}$$

for some absolute positive constant C.

https://doi.org/10.1017/S0004972719000224 Published online by Cambridge University Press

Define $\mathcal{S}(Q)$ as in (2.1). Then

$$\begin{aligned}
\sum_{q=Q+1}^{2Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q^2} \bigg| \sum_{n=M+1}^{M+N} a_n e\Big(\frac{an}{q^2}\Big) \bigg|^2 &\geq \sum_{(a,q)\in\mathcal{S}(Q)} \bigg| \sum_{n=M+1}^{M+N} a_n e\Big(\frac{an}{q^2}\Big) \bigg|^2 \\
&\geq \sharp\mathcal{S}(Q) \cdot (CN)^2 \\
&= C^2 \cdot \sharp\mathcal{S}(Q) \cdot N \sum_{n=M+1}^{M+N} |a_n|^2 \\
&= \frac{C^2}{10} \cdot \sharp\mathcal{S}(Q) \cdot (Q^3+N) \sum_{n=M+1}^{M+N} |a_n|^2 \\
&\geq \frac{C^2}{10} \cdot Q^{\log 2/(1+\varepsilon)\log\log Q} \cdot (Q^3+N) \sum_{n=M+1}^{M+N} |a_n|^2,
\end{aligned}$$

where the third line follows from (2.3), and the last line follows from Lemma 2.1. This completes the proof. □

Acknowledgements

The first author would like to thank the University of New South Wales (UNSW) for its financial support and hospitality during his pleasant stay at the School of Mathematics and Statistics. The second author thanks the following organisations for his Research Training Program scholarship: the Department of Education and Training, Australian Government and the School of Mathematics and Statistics, UNSW.

References

[1] S. Baier and L. Zhao, 'Bombieri–Vinogradov theorem for sparse sets of moduli', *Acta Arith.* **125**(2) (2006), 187–201.

[2] S. Baier and L. Zhao, 'An improvement for the large sieve for square moduli', *J. Number Theory* **128**(1) (2008), 154–174.

[3] W. D. Banks, F. Pappalardi and I. E. Shparlinski, 'On group structures realized by elliptic curves over arbitrary finite fields', *Exp. Math.* **21**(1) (2012), 11–25.

[4] J. Bourgain, K. Ford, S. V. Konyagin and I. E. Shparlinski, 'On the divisibility of Fermat quotients', *Michigan Math. J.* **59** (2010), 313–328.

[5] K. Halupczok, 'A new bound for the large sieve inequality with power moduli', *Int. J. Number Theory* **8**(3) (2012), 689–695.

[6] K. Matomäki, 'A note on primes of the form $p = aq^2 + 1$', *Acta Arith.* **137** (2009), 133–137.

[7] I. E. Shparlinski and L. Zhao, 'Elliptic curves in isogeny classes', *J. Number Theory* **191** (2018), 194–212.

[8] L. Zhao, 'Large sieve inequality for characters to square moduli', *Acta Arith.* **112**(3) (2004), 297–308.

STEPHAN BAIER, Department of Mathematics,
RKMVERI, G.T. Road, Belur Math, Howrah,
West Bengal 711202, India
e-mail: stephanbaier2017@gmail.com

SEAN B. LYNCH, School of Mathematics and Statistics,
University of New South Wales, UNSW-Sydney,
NSW 2052, Australia
e-mail: s.b.lynch@unsw.edu.au

LIANGYI ZHAO, School of Mathematics and Statistics,
University of New South Wales, UNSW-Sydney,
NSW 2052, Australia
e-mail: l.zhao@unsw.edu.au

https://doi.org/10.1017/S0004972719000224 Published online by Cambridge University Press