Density of non-residues in Burgess-type intervals and applications

W. D. Banks
Department of Mathematics
University of Missouri
Columbia, MO 65211 USA
bbanks@math.missouri.edu

M. Z. Garaev
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
garaev@matmor.unam.mx

D. R. Heath-Brown
Mathematical Institute
24–29, St. Giles’
Oxford, OX1 3LB
rhb@maths.ox.ac.uk

I. E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au
Abstract

We show that for any fixed $\varepsilon > 0$, there are numbers $\delta > 0$ and $p_0 \geq 2$ with the following property: for every prime $p \geq p_0$ and every integer $N$ such that $p^{1/(4\sqrt{e}) + \varepsilon} \leq N \leq p$, the sequence $1, 2, \ldots, N$ contains at least $\delta N$ quadratic non-residues modulo $p$. We use this result to obtain strong upper bounds on the sizes of the least quadratic non-residues in Beatty and Piatetski-Shapiro sequences.

2000 Mathematics Subject Classification: 11A15, 11L40, 11N37

1 Introduction

In 1994 Heath-Brown conjectured the existence of an absolute constant $c > 0$ such that, for all positive integers $N$ and all prime numbers $p$, the interval $[1, N]$ contains at least $cN$ quadratic residues modulo $p$. This conjecture has been established by Hall [12]. In the seminal work of Granville and Soundararajan [11] it has been shown that if $N$ is sufficiently large, then for every prime $p$ more than 17.15% of the integers in $[1, N]$ are quadratic residues modulo $p$. On the other hand, for any fixed positive integer $N$ there exist infinitely many primes $p$ such that the interval $[1, N]$ is free of quadratic non-residues modulo $p$; see [10] for a more precise statement. In particular, complete analogues of the results of Hall [12] and of Granville and Soundararajan [11] are not possible in the case of quadratic non-residues.

In the present paper we show that for any given $\varepsilon > 0$ there exists a constant $c(\varepsilon) > 0$ with the following property: for every sufficiently large prime $p$ and every integer $N$ in the range $p^{1/(4\sqrt{e}) + \varepsilon} \leq N \leq p$, the interval $[1, N]$ contains at least $c(\varepsilon)N$ quadratic non-residues modulo $p$. This is the partial analogue of Hall’s result for quadratic non-residues in Burgess-type intervals. We recall that the celebrated result of Burgess [6] states that the least positive quadratic non-residue modulo $p$ is of size $O(p^{1/(4\sqrt{e}) + \varepsilon})$ for any given $\varepsilon > 0$, and the constant $1/(4\sqrt{e})$ has never been improved.

We apply our result on the density of non-residues to obtain strong upper bounds on the sizes of the least quadratic non-residues in Beatty and Piatetski-Shapiro sequences, which substantially improve all previously known results for these questions.
2 Statement of results

For an odd prime $p$, we use $(\cdot | p)$ to denote the Legendre symbol modulo $p$, and we put

$$S_p(x) = \sum_{n \leq x} (n|p) \quad (x \geq 1).$$

**Theorem 2.1.** For every $\varepsilon > 0$ there exists $\delta > 0$ such that, for all sufficiently large primes $p$, the bound

$$|S_p(N)| \leq (1 - \delta)N$$

holds for all integers $N$ in the range $p^{1/(4\sqrt{e})} + \varepsilon \leq N \leq p$.

For two fixed real numbers $\alpha$ and $\beta$, the corresponding non-homogeneous Beatty sequence is the sequence of integers defined by

$$B_{\alpha,\beta} = (\lfloor \alpha n + \beta \rfloor)_{n=1}^\infty.$$

Beatty sequences appear in a variety of apparently unrelated mathematical settings, and because of their versatility, the arithmetic properties of these sequences have been extensively explored in the literature; see, for example, [1, 5, 17, 18, 21, 28] and the references contained therein.

For each prime $p$, let $N_{\alpha,\beta}(p)$ denote the least positive integer $n$ such that $\lfloor \alpha n + \beta \rfloor$ is a quadratic non-residue modulo $p$ (we formally put $N_{\alpha,\beta}(p) = \infty$ if no such integer exists). Below, we show that Theorem 2.1 can be applied to establish the following Burgess-type bound, which substantially improves earlier results in [3, 4, 7, 22, 23, 24]:

**Theorem 2.2.** Let $\alpha, \beta$ be fixed real numbers with $\alpha$ irrational. Then, for every $\varepsilon > 0$ the bound

$$N_{\alpha,\beta}(p) \leq p^{1/(4\sqrt{e})+\varepsilon}$$

holds for all sufficiently large primes $p$.

We remark that the irrationality of $\alpha$ is essential to our argument. Even in the “simple” case $\alpha = 3, \beta = 1$, we have not been able to improve upon the inequality

$$N_{3,1}(p) \leq p^{1/4+o(1)}$$

which follows from the Burgess bound on the relevant character sum.
Next, let $N_c(p)$ be the least positive integer $n$ such that $\lfloor n^c \rfloor$ is a quadratic non-residue modulo $p$. It is easy to show that $N_c(p)$ exists for any non-integer $c > 1$. For values of $c$ close to 1, good upper bounds for $N_c(p)$ have been obtained in [7, 20]. Here, we establish a much stronger bound by appealing to Theorem 2.1. It is formulated in terms of exponent pairs, we refer to [9, 15, 16, 25, 26, 27] for their exact definition and properties.

**Theorem 2.3.** Let $(\kappa, \lambda)$ be an exponent pair, and suppose that

$$1 < c < 1 + \frac{1 - \lambda}{2\kappa - \lambda + 3}.$$  

Then, for every $\varepsilon > 0$ the bound

$$N_c(p) \leq p^{1/(4(2-c)\sqrt{e})+\varepsilon}$$

holds for all sufficiently large primes $p$.

The classical exponent pair $(\kappa, \lambda) = (1/2, 1/2)$ implies that Theorem 2.3 is valid for $c$ in the range $1 < c < 8/7$. Graham’s optimization algorithm (see [8, 9]) extends this range to

$$1 < c < 1 + \frac{1 - R}{2 - R} = 1.14601346\ldots,$$

where $R = 0.8290213568\ldots$ is Rankin’s constant. Note that as $c \to 1^+$ our upper bound for $N_c(p)$ tends to the Burgess bound, which illustrates the strength of our estimate.

3 Proofs

3.1 Proof of Theorem 2.1

We can assume that $0 < \varepsilon \leq 0.01$. In view of the identities

$$\#\{n \leq x : (n|p) = \pm 1\} = \sum_{n \leq x} \frac{1}{2} (1 \pm (n|p)) = \frac{1}{2} ([x] \pm S_p(x)) \quad (x \geq 1),$$

and taking into account the result of Hall [12] mentioned earlier, it suffices to establish only the lower bound

$$\#\{n \leq N : (n|p) = -1\} \geq \frac{1}{2} \delta N$$
with $N$ in the stated range.

By the character sum estimate of Hildebrand [14] (which extends the range of validity of the Burgess bound [6]) it follows that $S_p(p^{1/4}) = o(p^{1/4})$ as $p \to \infty$; therefore,

$$\#\{n \leq p^{1/4} : (n|p) = -1\} = (0.5 + o(1))p^{1/4}.$$ 

Since every non-residue $n$ is divisible by a prime non-residue $q$, we have

$$(0.5 + o(1))p^{1/4} \leq \sum_{n \leq p^{1/4}} \sum_{q|n} 1 \leq \sum_{q \leq p^{1/4}} \frac{p^{1/4}}{q},$$

and thus

$$0.5 + o(1) \leq \sum_{j=1}^{s} \frac{1}{q_j} + \sum_{p^{1/4}/(4\sqrt{e})+0.5\varepsilon < q \leq p^{1/4}} \frac{1}{q},$$

where $q_1 < \cdots < q_s$ are the prime quadratic non-residues modulo $p$ that do not exceed $p^{1/4}/(4\sqrt{e})+0.5\varepsilon$. Using Mertens’ formula (see [13, Theorem 427]), we bound the latter sum by

$$\sum_{p^{1/4}/(4\sqrt{e})+0.5\varepsilon < q \leq p^{1/4}} \frac{1}{q} = \log \left( \frac{\log p^{1/4}}{\log p^{1/4}/(4\sqrt{e})+0.5\varepsilon} \right) + O \left( \frac{1}{\log p} \right) \leq 0.5 - 2\varepsilon,$$

where the inequality holds for all sufficiently large $p$. Consequently,

$$\sum_{j=1}^{s} \frac{1}{q_j} \geq \varepsilon$$

if the prime $p$ is large enough.

For each $j = 1, \ldots, k$, let $\mathcal{N}_j$ denote the set of positive quadratic residues modulo $p$ which do not exceed $N/q_j$. From the result of Granville and Soundararajan [11] we have

$$\#\mathcal{N}_j \geq \frac{0.1N}{q_j} \quad (j = 1, \ldots, s).$$

In particular, if $q_1 \leq \varepsilon^{-1}$, then the numbers

$$\{q_1n : n \in \mathcal{N}_1\}$$
are all positive non-residues of size at most $N$, and the theorem follows from the lower bound $\# \mathcal{N}_1 \geq 0.1 \varepsilon N$.

Now suppose that $q_1 > \varepsilon^{-1}$. In this case, we can choose $k$ such that

$$\varepsilon \leq \frac{1}{\sum_{\ell=1}^{k} \frac{1}{q_\ell}} \leq 2 \varepsilon.$$ 

For each $j = 1, \ldots, s$, let $\mathcal{M}_j$ be the set of numbers in $\mathcal{N}_j$ that are not divisible by any of the primes $q_1, \ldots, q_k$; then

$$\# \mathcal{M}_j \geq \# \mathcal{N}_j - \sum_{\ell=1}^{k} \frac{N}{q_j q_\ell} \geq \frac{(0.1 - 2 \varepsilon)N}{q_j} \geq \frac{0.09N}{q_j},$$

where we have used the fact that $\varepsilon \leq 0.01$ for the last inequality. It is easy to see that the numbers of the form $q_j n$ with $j \in \{1, \ldots, k\}$ and $n \in \mathcal{M}_j$ are distinct non-residues of size at most $N$, and the number of such integers is

$$\sum_{j=1}^{k} \# \mathcal{M}_j \geq \sum_{j=1}^{k} \frac{0.09N}{q_j} \geq 0.09 \varepsilon N.$$

This completes the proof of Theorem 2.1.

### 3.2 Proof of Theorem 2.2

Using Theorem 2.1, we immediately obtain the following result, which is needed in our proof of Theorem 2.2 below:

**Lemma 3.1.** Let $\sigma \in \{\pm 1\}$ be fixed. For every $\varepsilon > 0$ there exists a constant $\eta > 0$ such that, for all sufficiently large primes $p$, the lower bound

$$\# \left\{ (n,m) : 1 \leq n \leq N, 1 \leq m \leq M, \ (nm|p) = \sigma \right\} \geq \eta NM$$

holds with $N = \left\lfloor p^{1/(4\sqrt{\pi}) + \varepsilon} \right\rfloor$ and an arbitrary positive integer $M$.

The next elementary result characterizes the set of values taken by the Beatty sequence $B_{\alpha,\beta}$ in the case that $\alpha > 1$:

**Lemma 3.2.** Let $\alpha > 1$. A positive integer $m > \beta$ belongs to the Beatty sequence $B_{\alpha,\beta}$ if and only if

$$0 < \{\alpha^{-1}(m - \beta + 1)\} \leq \alpha^{-1},$$

and in this case $m = \lfloor \alpha n + \beta \rfloor$ if and only if $n = \lfloor \alpha^{-1}(m - \beta) \rfloor$.
The following estimate is a particular case of a series of similar estimates dating back to the early works of Vinogradov (see, for example, [29]):

**Lemma 3.3.** Let $\lambda$ be a real number and suppose that the inequality

$$\left| \lambda - \frac{r}{q} \right| \leq \frac{1}{q^2}$$

holds for some integers $r$ and $q \geq 1$ with $\gcd(r, q) = 1$. Then, for any complex numbers $a_n, b_m$ such that

$$\max_{n \leq N} \{|a_n|\} \leq 1 \quad \text{and} \quad \max_{m \leq M} \{|b_m|\} \leq 1,$$

the following bound holds:

$$\sum_{n \leq N} \sum_{m \leq M} a_n b_m e(\lambda nm) \ll XY \sqrt{\frac{1}{X} + \frac{1}{Y} + \frac{1}{q} + \frac{q}{XY}},$$

where $e(z) = \exp(2\pi iz)$ for all $z \in \mathbb{R}$.

Considering for every integer $h \geq 1$ the sequence of convergents in the continued fraction expansion of $\lambda h$, from Lemma 3.3 we derive the following statement:

**Corollary 3.4.** For every irrational $\lambda$, there are functions $H_\lambda(K) \to \infty$ and $\rho_\lambda(K) \to 0$ as $K \to \infty$ such that for any complex numbers $a_n, b_m$ such that

$$\max_{n \leq N} \{|a_n|\} \leq 1 \quad \text{and} \quad \max_{m \leq M} \{|b_m|\} \leq 1,$$

the bound

$$\left| \sum_{n \leq N} \sum_{m \leq M} a_n b_m e(\lambda hnm) \right| \leq \rho_\lambda(K) NM$$

for all integers $h$ in the range $1 \leq |h| \leq H_\lambda(K)$, where $K = \min\{N, M\}$.

In particular, if $\lambda$ is irrational and $h \neq 0$ is fixed, then

$$\sum_{n \leq N} \sum_{m \leq M} a_n b_m e(\lambda hnm) = o(NM)$$

whenever $\min\{N, M\} \to \infty$. 

7
We now turn to the proof of Theorem 2.2.

Case 1: \( \alpha > 1 \). Put \( \lambda = \alpha^{-1} \), and let \( \sigma \in \{ \pm 1 \} \) be fixed. For all integers \( N, M \geq 1 \) and primes \( p \), we consider the set of ordered pairs

\[
W_\sigma(N, M) = \left\{ (n, m) : 1 \leq n \leq N, 1 \leq m \leq M, \ (nm|p) = \sigma \right\}.
\]

For every \( \varepsilon > 0 \), Lemma 3.1 shows that there is a constant \( \eta > 0 \) such that, for all sufficiently large primes \( p \), the inequality

\[
\#W_\sigma(N, M) \geq \eta NM
\]

holds with \( N = \left\lceil p^{1/(4\sqrt{e}) + \varepsilon/2} \right\rceil \) and an arbitrary positive integer \( M \). For every large prime \( p \), let \( N \) be such an integer, and put \( M = \left\lfloor p^{\varepsilon/2} \right\rfloor \). To prove Theorem 2.2 when \( \alpha > 1 \), by Lemma 3.2 it suffices to show that the set

\[
V_\sigma(N, M) = \left\{ (n, m) \in W_\sigma(N, M) : 0 < \{\lambda nm - \lambda \beta + \lambda\} \leq \lambda \right\}
\]

is nonempty for \( \sigma = -1 \) when \( p \) is sufficiently large. In fact, we shall prove this result for either choice of \( \sigma \in \{ \pm 1 \} \).

To simplify the notation, write \( W_\sigma = W_\sigma(N, M) \) and \( V_\sigma = V_\sigma(N, M) \). To estimate \( \#V_\sigma \), we use the well known Erdős–Turán inequality between the discrepancy of a sequence and its associated exponential sums; for example, see [19, Theorem 2.5, Chapter 2]. For any integer \( H > 1 \), we have

\[
\left| \#V_\sigma - \lambda \#W_\sigma \right| \ll \frac{\#W_\sigma}{H} + \sum_{h=1}^{H} \frac{1}{h} \left| \sum_{(n, m) \in W_\sigma} e(\lambda hnm) \right|.
\]

Applying Corollary 3.4 with the choice

\[
H = \min \left\{ H_{\lambda}(K), \exp \left( \rho_{\lambda}(K)^{-1/2} \right) \right\}
\]

where \( K = \min\{N, M\} \) as before, we see that

\[
\left| \#V_\sigma - \lambda \#W_\sigma \right| \ll \frac{\#W_\sigma}{H} + \rho_{\lambda}(K) NM \log H \ll \frac{NM}{\log H}.
\]

Since \( H \to \infty \) as \( p \to \infty \), and the lower bound

\[
\#W_\sigma \geq \eta NM
\]

holds with \( N = \left\lceil p^{1/(4\sqrt{e}) + \varepsilon/2} \right\rceil \) and an arbitrary positive integer \( M \). For every large prime \( p \), let \( N \) be such an integer, and put \( M = \left\lfloor p^{\varepsilon/2} \right\rfloor \). To prove Theorem 2.2 when \( \alpha > 1 \), by Lemma 3.2 it suffices to show that the set

\[
V_\sigma(N, M) = \left\{ (n, m) \in W_\sigma(N, M) : 0 < \{\lambda nm - \lambda \beta + \lambda\} \leq \lambda \right\}
\]

is nonempty for \( \sigma = -1 \) when \( p \) is sufficiently large. In fact, we shall prove this result for either choice of \( \sigma \in \{ \pm 1 \} \).

To simplify the notation, write \( W_\sigma = W_\sigma(N, M) \) and \( V_\sigma = V_\sigma(N, M) \). To estimate \( \#V_\sigma \), we use the well known Erdős–Turán inequality between the discrepancy of a sequence and its associated exponential sums; for example, see [19, Theorem 2.5, Chapter 2]. For any integer \( H > 1 \), we have

\[
\left| \#V_\sigma - \lambda \#W_\sigma \right| \ll \frac{\#W_\sigma}{H} + \sum_{h=1}^{H} \frac{1}{h} \left| \sum_{(n, m) \in W_\sigma} e(\lambda hnm) \right|.
\]

Applying Corollary 3.4 with the choice

\[
H = \min \left\{ H_{\lambda}(K), \exp \left( \rho_{\lambda}(K)^{-1/2} \right) \right\}
\]

where \( K = \min\{N, M\} \) as before, we see that

\[
\left| \#V_\sigma - \lambda \#W_\sigma \right| \ll \frac{\#W_\sigma}{H} + \rho_{\lambda}(K) NM \log H \ll \frac{NM}{\log H}.
\]

Since \( H \to \infty \) as \( p \to \infty \), and the lower bound

\[
\#W_\sigma \geq \eta NM
\]
holds by Lemma 3.1, it follows that
\[ \#V^\sigma \geq (\lambda \eta + o(1)) NM \quad (p \to \infty). \]

In particular, \( V^\sigma \neq \emptyset \) for either choice of \( \sigma \in \{\pm 1\} \) once \( p \) is sufficiently large.

**Case 2:** \( 0 < \alpha < 1 \). In this case, Theorem 2.2 follows easily from the classical Burgess bound for the least quadratic non-residue modulo \( p \) since the sequence \( B_{\alpha,\beta} \) contains all integers exceeding \( \lfloor \alpha + \beta \rfloor \).

**Case 3:** \( \alpha < 0 \). We note that the identity
\[ \lfloor \alpha n + \beta \rfloor = -\lfloor -\alpha n - \beta + 1 \rfloor \]
holds for all \( n \geq 1 \) with at most \( O(1) \) exceptions (since \( \alpha \) is irrational), hence the sequences \( B_{\alpha,\beta} \) and \( -B_{-\alpha,-\beta+1} \) are essentially the same.

If \( \alpha < -1 \), we argue as in Case 1 with \( \alpha \) replaced by \(-\alpha > 1 \) and \( \beta \) replaced by \(-\beta + 1 \). Choosing \( \sigma = -(1|p) \), Theorem 2.2 then follows from the fact that \( V^\sigma \neq \emptyset \) once \( p \) is sufficiently large.

Finally, if \(-1 < \alpha < 0 \), we note that the sequence \( B_{\alpha,\beta} \) contains all integers up to \( \lfloor \alpha + \beta \rfloor \). Hence, the result follows from the Burgess bound in the case that \((1|p) = +1 \) and from the ubiquity of quadratic residues modulo \( p \) in the case that \((1|p) = -1 \).

### 3.3 Proof of Theorem 2.3

The following statement is a variant of [9, Lemma 4.3] (we omit the proof, which follows the same lines):

**Lemma 3.5.** Let \( L \) and \( M \) be large positive parameters, and let \((\kappa, \lambda)\) be an exponent pair. Then for any complex numbers \( a_\ell, b_m \) such that
\[ \max_{L/2 < \ell \leq L} \{|a_\ell|\} \leq 1 \quad \text{and} \quad \max_{M/2 < m \leq M} \{|b_m|\} \leq 1, \]
the bound
\[ \left| \sum_{L/2 < \ell \leq L} \sum_{M/2 < m \leq M} a_\ell b_m e(h^{1/c}m^{1/c}) \right| \ll \left( h^{\kappa_\alpha} L^{\kappa_\alpha/c + \lambda_0} M^{1-\kappa_\alpha + \kappa_\alpha/c} + h^{-1/2} (LM)^{1-1/(2c)} + LM^{1/2} \right) \log L \]
holds for any \( h \geq 1 \), where

\[
\kappa_0 = \frac{\kappa}{2\kappa + 2} \quad \text{and} \quad \lambda_0 = \frac{\kappa + \lambda + 1}{2\kappa + 2}.
\]

Turning to the proof of Theorem 2.3, let us fix \( c \) in the range

\[
1 < c < 1 + \frac{1 - \lambda}{2\kappa - \lambda + 3}.
\]

If \( L \) and \( M \) are sufficiently large, and \( \ell \in (L/2, L] \), \( m \in (M/2, M] \) are integers such that

\[
1 - \frac{1}{2(\ell\ell m^{1/c})} \leq \{\ell^{1/c} m^{1/c}\},
\]

then \( [n^c] = \ell m \) for some integer \( n \). Indeed, with \( n = \lceil \ell^{1/c} m^{1/c} \rceil + 1 \) we see that \( n^c \geq \ell m \), and also

\[
n^c = (\ell^{1/c} m^{1/c} + 1 - \{\ell^{1/c} m^{1/c}\})^c \\
\leq \ell m \left(1 + \frac{1}{2\ell^{1/c} m^{1/c} (LM)^{1-1/c}}\right)^c \\
\leq \ell m \left(1 + \frac{1}{2\ell m}\right)^c < \ell m + 1,
\]

where the last inequality holds if \( L \) and \( M \) are large enough. Below, we work with integers \( L, M \) that tend to infinity with the prime \( p \).

Let

\[
J = \left\lceil \frac{\log(2/\delta)}{\log 2} \right\rceil \quad \text{and} \quad \delta_1 = \frac{\delta}{2(J + 1)},
\]

where \( \delta \) is as in Theorem 2.1. Since \( 2^{-J-1} < \delta/2 \), by considering the intervals \((2^{-j-1} p^{1/4\sqrt{\varepsilon} + \varepsilon}, 2^{-j} p^{1/4\sqrt{\varepsilon} + \varepsilon}]\) for \( j = 0, \ldots, J \) we see that there is an integer \( L \) with \( 2^{-j} p^{1/4\sqrt{\varepsilon} + \varepsilon} < L \leq p^{1/4\sqrt{\varepsilon} + \varepsilon} \) such that the interval \((L/2, L]\) contains a set \( \mathcal{L} \) with \#\( \mathcal{L} \geq \delta_1 L \) quadratic non-residues modulo \( p \). Let \( A \) be a large positive constant. From the aforementioned result of Hall [12] we see that there exists an integer \( M \) with

\[
L^{2(c-1)/(2-c)} (\log L)^A \ll M \ll L^{2(c-1)/(2-c)} (\log L)^A
\]

such that the interval \((M/2, M]\) contains a set \( \mathcal{M} \) with \#\( \mathcal{M} \geq \delta_2 M \) quadratic residues modulo \( p \), where \( \delta_2 > 0 \) is an absolute constant. It suffices to show that for some integers \( \ell \in \mathcal{L}, m \in \mathcal{M} \) the inequality

\[
1 - \frac{1}{2(\ell\ell m^{1/c})} \leq \{\ell^{1/c} m^{1/c}\}
\]

10
holds. As in the proof of Theorem 2.2 from the Erdős–Turán inequality we see that for any \( H \geq 1 \) the number of solutions \( T \) of this inequality is

\[
T = \frac{\#L \#M}{2(LM)^{1-1/c}} + O \left( \frac{LM}{H} + \sum_{h=1}^{H} \frac{1}{h} \sum_{L/2 < \ell \leq L} \sum_{M/2 < m \leq M} e\left( h \ell^{1/c} m^{1/c} \right) \right)
\]

\[
\geq 0.5\delta_1 \delta_2 (LM)^{1/c} - \frac{c_0 LM}{H} - c_0 \sum_{h=1}^{H} \frac{1}{h} \left| \sum_{L/2 < \ell \leq L} \sum_{M/2 < m \leq M} e\left( h \ell^{1/c} m^{1/c} \right) \right|,
\]

where \( c_0 \) is an absolute constant. Take \( H = \lceil 4c_0(LM)^{1-1/c}/(\delta_1 \delta_2) \rceil \). With this choice it suffices to prove that

\[
c_0 \sum_{h=1}^{H} \frac{1}{h} \left| \sum_{L/2 < \ell \leq L} \sum_{M/2 < m \leq M} e\left( h \ell^{1/c} m^{1/c} \right) \right| < 0.1\delta_1 \delta_2 (LM)^{1/c}.
\]

If \( A \) is large enough, this inequality follows from Lemma 3.5 which in turn implies that \( T > 0 \) and concludes the proof.

## 4 Remarks

We are grateful to the referee who has pointed that some recent work of Granville and Soundararajan (unpublished) contains the following result, which yields a stronger form of our Theorem 2.1.

**Theorem 4.1.** Let \( x \) be large, and let \( f \) be a completely multiplicative function with \( -1 \leq f(n) \leq 1 \) for all \( n \). Suppose that

\[
\sum_{n \leq x} f(n) = o(x).
\]

Then for \( 1/\sqrt{e} \leq \alpha \leq 1 \) we have

\[
\left| \sum_{n \leq x^\alpha} f(n) \right| \leq \left( \max\{|\xi|, 1/2 + 2(\log \alpha)^2\} + o(1) \right) x^\alpha
\]

where

\[
\xi = 1 - 2 \log(1 + \sqrt{e}) + 4 \int_1^{\sqrt{e}} \frac{\log t}{t+1} dt = -0.656999 \cdots.
\]
We note that $\xi$ is the same constant that appears in [11, Theorem 1] (where it is called $\delta_1$, which has a different meaning in our paper).

The referee has suggested that the following conjecture seems natural:

**Conjecture 4.2.** Let $x$ be large, let $f$ be a completely multiplicative function with $-1 \leq f(n) \leq 1$ for all $n$. and suppose that

$$\sum_{n \leq x} f(n) = o(x).$$

Then for $1/\sqrt{e} \leq \alpha \leq 1$ we have

$$\left| \sum_{n \leq x^\alpha} f(n) \right| \leq (-2 \log \alpha + o(1))x^\alpha.$$

Finally, the referee also observes that Theorem 2.2 holds also for rational $\alpha \neq 0$. The proof uses recent work of Balog, Granville and Soundararajan [2].

**References**

[1] A. G. Abercrombie, ‘Beatty sequences and multiplicative number theory’, *Acta Arith.* 70 (1995), 195–207.

[2] A. Balog, A. Granville and K. Soundararajan, ‘Multiplicative functions in arithmetic progressions’, *Preprint*, 2007 (available from [http://arxiv.org/abs/math/0702389](http://arxiv.org/abs/math/0702389)).

[3] W. Banks and I. E. Shparlinski, ‘Non-residues and primitive roots in Beatty sequences’, *Bull. Austral. Math. Soc.* 73 (2006), 433–443.

[4] W. Banks and I. E. Shparlinski, ‘Short character sums with Beatty sequences’, *Math. Res. Lett.* 13 (2006), 539–547.

[5] A. V. Begunts, ‘An analogue of the Dirichlet divisor problem’, *Moscow Univ. Math. Bull.* 59 (2004), no. 6, 37–41.

[6] D. A. Burgess, ‘The distribution of quadratic residues and non-residues’, *Mathematika* 4 (1957), 106–112.

[7] M. Z. Garaev, ‘A note on the least quadratic non-residue of the integer-sequences’, *Bull. Austral. Math. Soc.* 68 (2003), 1–11.
[8] S. W. Graham, ‘An algorithm for computing optimal exponent pairs’, *J. London Math. Soc. (2)* **33** (1986), 203–218.

[9] S. W. Graham and G. Kolesnik, *Van der Corput’s Method of Exponential Sums*, Cambridge Univ. Press, 1991.

[10] S. W. Graham and C. J. Ringrose, ‘Lower bounds for least quadratic nonresidues’, *Analytic number theory (Allerton Park, IL, 1989)*, Birkhäuser, Boston, MA, 1990, 269–309.

[11] A. Granville and K. Soundararajan, ‘The spectrum of multiplicative functions’, *Ann. Math.* **153** (2001), 407–470.

[12] R. R. Hall, ‘Proof of a conjecture of Heath-Brown concerning quadratic residues’, *Proc. Edinburgh Math. Soc. (2)* **39** (1996), 581–588.

[13] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford, 1979.

[14] A. Hildebrand, ‘A note on Burgess’ character sum estimate’, *C. R. Math. Rep. Acad. Sci. Canada* **8** (1986), no. 1, 35–37.

[15] M. N. Huxley, *Area, lattice points and exponential sums*, Oxford Univ. Press, 1996.

[16] I. A. Ivić, *The Riemann zeta-function*, John Willey, 1985.

[17] T. Komatsu, ‘A certain power series associated with a Beatty sequence’, *Acta Arith.* **76** (1996), 109–129.

[18] T. Komatsu, ‘The fractional part of $nd + \varphi$ and Beatty sequences’, *J. Théor. Nombres Bordeaux* **7** (1995), 387–406.

[19] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience, New York-London-Sydney, 1974.

[20] Y. K. Lau and J. Wu, ‘On the least quadratic non-residue’, *Preprint*, 2006, [http://hal.archives-ouvertes.fr/hal-00097136/en/](http://hal.archives-ouvertes.fr/hal-00097136/en/).

[21] K. O’Bryant, ‘A generating function technique for Beatty sequences and other step sequences’, *J. Number Theory* **94** (2002), 299–319.
[22] S. N. Preobrazhenskii, ‘On the least quadratic non-residue in an arithmetic sequence’, *Moscow Univ. Math. Bull.* **56** (2001), no. 1, 44–46.

[23] S. N. Preobrazhenskii, ‘On power non-residues modulo a prime number in a special integer sequence’, *Moscow Univ. Math. Bull.* **56** (2001), no. 4, 41–42.

[24] S. N. Preobrazhenskii, ‘On the least power non-residue in an integer sequence’, *Moscow Univ. Math. Bull.* **59** (2004), no. 1, 33–35.

[25] O. Robert and P. Sargos, ‘A fourth derivative test for exponential sums’, *Compositio Math.* **130** (2002), no. 3, 275–292.

[26] O. Robert and P. Sargos, ‘A third derivative test for mean values of exponential sums with application to lattice point problems’, *Acta Arith.* **106** (2003), no. 1, 27–39.

[27] P. Sargos, ‘An analog of van der Corput’s $A^4$-process for exponential sums’, *Acta Arith.* **110** (2003), no. 3, 219–231.

[28] R. Tijdeman, ‘Exact covers of balanced sequences and Fraenkel’s conjecture’, *Algebraic number theory and Diophantine analysis (Graz, 1998)*, 467–483, de Gruyter, Berlin, 2000.

[29] I. M. Vinogradov, ‘An improvement of the estimation of sums with primes’, *Izvestia Akad. Nauk SSSR* **17** (1943), 17–34 (in Russian).