NON-RESIDUES AND PRIMITIVE ROOTS
IN BEATTY SEQUENCES

WILLIAM D. BANKS AND IGOR E. SHPARLINSKI

We study multiplicative character sums taken on the values of a non-homogeneous Beatty sequence

$$\mathcal{B}_{\alpha,\beta} = \left\{ \lfloor \alpha n + \beta \rfloor \ : \ n = 1, 2, 3, \dots \right\},$$

where $\alpha, \beta \in \mathbb{R}$, and α is irrational. In particular, our bounds imply that for every fixed $\varepsilon > 0$, if p is sufficiently large and $p^{1/2+\varepsilon} \leqslant N \leqslant p$, then among the first N elements of $\mathcal{B}_{\alpha,\beta}$, there are $N/2 + o(N)$ quadratic non-residues modulo p. When more information is available about the Diophantine properties of α, then the error term $o(N)$ admits a sharper estimate.

1. INTRODUCTION

For two fixed real numbers α and β, the corresponding *non-homogeneous Beatty sequence* is the sequence of integers defined by

$$\mathcal{B}_{\alpha,\beta} = \left\{ \lfloor \alpha n + \beta \rfloor \ : \ n = 1, 2, 3, \dots \right\}.$$

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, 3, 7, 12, 13, 18, 25] and the references contained therein.

In this paper, we study sums of the form

$$S_p(\alpha, \beta, \chi; N) = \sum_{n \leqslant N} \chi(\lfloor \alpha n + \beta \rfloor),$$

where α is *irrational*, and χ is a *nontrivial multiplicative character* modulo a prime number p. Our main result is Theorem 4.1 in Section 4 below. In particular, our bounds imply that for every fixed $\varepsilon > 0$, if p is sufficiently large and $p^{1/2+\varepsilon} \leqslant N \leqslant p$, then among the first N elements of the Beatty sequence $\mathcal{B}_{\alpha,\beta}$, there are $N/2 + o(N)$ *quadratic*

non-residues modulo p. In the case that α is not *Liouville* (which includes all algebraic irrationals and almost all real numbers), our results yield explicit bounds on the error term.

For non-Liouville numbers α, we also obtain results about the uniform distribution of *primitive roots* in Beatty sequences.

Various bounds on the size of the least quadratic non-residue modulo p in the sequence $\{\lfloor \alpha n \rfloor \ : \ n = 1, 2, 3, \dots\}$ have been given by Garaev [8] and by Preobrazhen-skiĭ [19, 20, 21]. For example, it has been shown in [8] that for any real number $\alpha > 0$ and any prime p, there is a positive integer $n \leqslant p^{(1+e^{-1/2})/4+o(1)}$ such that $\lfloor \alpha n \rfloor$ is a quadratic non-residue modulo p. The bounds of [19, 20, 21] are stronger than those of [8], but they require certain restrictions on the number α. These results have recently been improved in [2] where it is shown that for any irrational α, $\lfloor \alpha n + \beta \rfloor$ is a quadratic nonresidue modulo p for $N/2 + o(N)$ positive integers $n \leqslant N$, provided that $N \geqslant p^{1/3+\delta}$ for some fixed $\delta > 0$.

We also remark that, by the result of Hildebrand [10], for any prime p there is a positive integer $a \leqslant p^{1/(4e^{1/2})+o(1)}$ such that both a and $a+1$ are quadratic nonresidues modulo p. Thus, in the case that $\alpha \leqslant 2$, one can choose $n = \lceil \alpha^{-1}(a - \beta) \rceil$ to guarantee that $\lfloor \alpha n + \beta \rfloor$ is either a or $a+1$ and is thus a quadratic non-residue modulo p. In particular, this observation eliminates the dependency on α in the bound of [8].

We remark that the methods of [8, 19, 20, 21] are much different from ours and cannot be applied to bound the character sums that we consider. The method of [2] applies to short character sums and gives stronger bounds on the size of the least quadratic non-residue and on higher degree non-residues. For longer sums, however, the bounds of the present paper are stronger and more explicit. The method we use can also be applied to several other sums with Beatty sequences.

2. NOTATION

Throughout the paper, the implied constants in the symbols O, $\ll$ and $\gg$ may depend on the real number α but are absolute otherwise. We recall that the notations $U = O(V)$, $U \ll V$, and $V \gg U$ are all equivalent to the assertion that the inequality $|U| \leqslant cV$ holds for some constant $c > 0$. We also use the symbol $o(1)$ to denote a function which tends to 0 and depends only on α. It is important to note that our bounds are uniform with respect to all of the other parameters, in particular, with respect to β.

In what follows, the letters k, m, and n (with or without subscripts) always denote non-negative integers.

The notation $\|x\|$ denotes the distance from the real number x to the nearest integer; in other words,

$$\|x\| = \min_{n \in \mathbf{Z}} |x - n|.$$

We also use $\{x\} = x - \lfloor x \rfloor$ to denote the fractional part of x, as usual.

3. Preliminaries

To describe the class of real numbers α for which our results apply, we need to recall some familiar notions from the theory of *Diophantine approximations*.

For an irrational number α, we define its *type* τ by the relation

$$\tau = \sup \left\{ \vartheta \in \mathbb{R} \ : \ \liminf_{q \to \infty, \ q \in \mathbb{Z}^+} q^{\vartheta} \, \|\alpha q\| = 0 \right\}.$$

Using *Dirichlet's approximation theorem*, it is easy to see that $\tau \geqslant 1$ for every irrational α. The celebrated theorems of Khinchin [11] and of Roth [22, 23] assert that $\tau = 1$ for almost all real (in the sense of the Lebesgue measure) and all irrational algebraic numbers α, respectively; see also [6, 24]. We remark that the number $\mu = \tau + 1$ is called the *irrationality measure* of α, or the *Liouville–Roth constant*.

The *discrepancy* D of a sequence of M (not necessarily distinct) real numbers $\gamma_1, \ldots, \gamma_M \in [0, 1)$ is defined by the relation

$$D = \sup_{\mathcal{I} \subseteq [0,1)} \left| \frac{V(\mathcal{I}, M)}{M} - |\mathcal{I}| \right|, \tag{1}$$

where the supremum is taken all subintervals $\mathcal{I} = (a, b)$ of the interval $[0, 1)$, $V(\mathcal{I}, M)$ is the cardinality of the set $\{1 \leqslant m \leqslant M \ : \ \gamma_m \in \mathcal{I}\}$, and $|\mathcal{I}|$ is the length of $\mathcal{I}$.

It is well known (see [16, Example 2.1, Chapter 1]) that for every irrational α, the sequence of fractional parts $\{\{\alpha m + \beta\} \ : \ m = 1, 2, \ldots\}$ is uniformly distributed modulo 1:

Lemma 3.1. *Let α be a fixed irrational number. Then, for all real numbers β and positive integers M, the discrepancy $D_{\alpha,\beta}(M)$ of the sequence of fractional parts*

$$\{\{\alpha m + \beta\} \ : \ m = 1, \ldots, M\}$$

satisfies the bound

$$D_{\alpha,\beta}(M) = o(1).$$

The following result is taken from [16, Theorem 3.2, Chapter 2]:

Lemma 3.2. *Let α be a fixed irrational number of type $\tau < \infty$. Then, for all real numbers β and positive integers M, the discrepancy $D_{\alpha,\beta}(M)$ of the sequence of fractional parts*

$$\{\{\alpha m + \beta\} \ : \ m = 1, \ldots, M\}$$

satisfies the bound

$$D_{\alpha,\beta}(M) \leqslant M^{-1/\tau + o(1)}.$$

We also need the following elementary statement:

LEMMA 3.3. *Let α be a fixed irrational number. Then, for every positive integer M and real number $\delta \in (0,1]$, there exists a real number γ such that*

$$\#\{m \leqslant M \ : \ \{\alpha m + \gamma\} < \delta\} \geqslant 0.5\, M\delta.$$

PROOF: Let $e(x) = \exp(2\pi i x)$ for all $x \in \mathbb{R}$, and note that $e(x) = e(y)$ if and only if $\{x\} = \{y\}$. Since α is irrational, the numbers $e(\alpha m)$ have distinct arguments for $m = 1, \dots, M$. Put $L = \lceil \delta^{-1} \rceil$, and let

$$\mathcal{S}_j = \left\{m \leqslant M \ : \ \frac{2\pi j}{L} \leqslant \arg\big(e(\alpha m)\big) < \frac{2\pi(j+1)}{L}\right\} \qquad (0 \leqslant j \leqslant L-1).$$

Since $\{1, \dots, M\}$ is the disjoint union of the sets $\mathcal{S}_j$, $j = 0, \dots, L-1$, by the *pigeonhole principle* there exists an index j for which

$$\#\mathcal{S}_j \geqslant \frac{M}{L} = \frac{M}{\lceil \delta^{-1} \rceil} \geqslant 0.5\, M\delta.$$

Defining $\gamma = -j/L$, we have for each $m \in \mathcal{S}_j$:

$$\{\alpha m + \gamma\} = \frac{1}{2\pi} \arg\big(e(\alpha m + \gamma)\big) = \frac{1}{2\pi}\left(\arg\big(e(\alpha m)\big) - \frac{2\pi j}{L}\right) < \frac{1}{L} \leqslant \delta,$$

which finishes the proof. $\qquad\qquad\square$

Finally, we assume the reader is familiar with the basic properties of *multiplicative characters* (see, for example, [17]).

4. MAIN RESULT

As in Section 3, we use $D_{\alpha,\beta}(N)$ to denote the discrepancy of the sequence of fractional parts

$$\big\{\{\alpha n + \beta\} \ : \ n = 1, \dots, N\big\}.$$

THEOREM 4.1. *Let α be a fixed irrational number. Then, for all real numbers β, primes p, nontrivial multiplicative characters $\chi \pmod{p}$, and positive integers $N \leqslant p$, the following bound holds:*

$$S_p(\alpha, \beta, \chi; N) \ll p^{1/4} N^{1/2} + N D_{\alpha,\beta}(N).$$

PROOF: Let $K \leqslant N$ be a positive integer, and let Δ be a real number in the interval $(0,1]$. For every real number γ, let

$$
\begin{aligned}
\mathcal{N}_\gamma &= \big\{1 \leqslant n \leqslant N \ : \ \{\alpha n + \beta - \gamma\} < 1 - \Delta\big\}, \\
\mathcal{K}_\gamma &= \big\{1 \leqslant k \leqslant K \ : \ \{\alpha k + \gamma\} < \Delta\big\},
\end{aligned}
$$

and put
$$\mathcal{N}_\gamma^c = \{1, 2, \ldots, N\} \setminus \mathcal{N}_\gamma.$$

From the definition (1), we immediately conclude that
$$\#\mathcal{N}_\gamma^c = N\Delta + O\big(ND_{\alpha,\beta}(N)\big). \tag{2}$$

By Lemma 3.3, we also have
$$\#\mathcal{K}_\gamma \geqslant 0.5\,K\Delta. \tag{3}$$

for *some* choice of $\gamma \in \mathbb{R}$. Fix γ with this property, and put $\mathcal{N} = \mathcal{N}_\gamma$, $\mathcal{N}^c = \mathcal{N}_\gamma^c$ and $\mathcal{K} = \mathcal{K}_\gamma$.

We have for every $k \in \mathcal{K}$:
$$\begin{aligned}
S_p(\alpha, \beta, \chi; N) &= \sum_{n \leqslant N} \chi(\lfloor \alpha(n+k) + \beta \rfloor) + O(k) \\
&= \sum_{n \leqslant N} \chi(\lfloor \alpha(n+k) + \beta \rfloor) + O(K) \\
&= \sum_{n \in \mathcal{N}} \chi(\lfloor \alpha(n+k) + \beta \rfloor) + O(K + \#\mathcal{N}^c).
\end{aligned}$$

Therefore,
$$S_p(\alpha, \beta, \chi; N) = \frac{W}{\#\mathcal{K}} + O(K + \#\mathcal{N}^c), \tag{4}$$

where
$$W = \sum_{n \in \mathcal{N}} \sum_{k \in \mathcal{K}} \chi(\lfloor \alpha(n+k) + \beta \rfloor).$$

For any $n \in \mathcal{N}$ and $k \in \mathcal{K}$, we have
$$\begin{aligned}
\lfloor \alpha(n+k) + \beta \rfloor &= \alpha(n+k) + \beta - \{\alpha(n+k) + \beta\} \\
&= (\alpha n + \beta - \gamma) + (\alpha k + \gamma) - \{\alpha n + \beta - \gamma\} - \{\alpha k + \gamma\} \\
&= \lfloor \alpha n + \beta - \gamma \rfloor + \lfloor \alpha k + \gamma \rfloor.
\end{aligned}$$

We also remark that, since $N \leqslant p$, we have
$$\#\big\{n \in \mathcal{N} \ : \ \lfloor \alpha n + \beta - \gamma \rfloor \equiv s \pmod{p}\big\} = O(1)$$

uniformly for all $s \in \mathbb{Z}$. Therefore, applying the Cauchy inequality, we derive that
$$\begin{aligned}
|W|^2 &\leqslant N \sum_{n \in \mathcal{N}} \left| \sum_{k \in \mathcal{K}} \chi(\lfloor \alpha n + \beta - \gamma \rfloor + \lfloor \alpha k + \gamma \rfloor) \right|^2 \\
&\ll N \sum_{s=1}^{p} \left| \sum_{k \in \mathcal{K}} \chi(s + \lfloor \alpha k + \gamma \rfloor) \right|^2 \\
&= N \sum_{k, \ell \in \mathcal{K}} \sum_{s=1}^{p} \chi(s + \lfloor \alpha k + \gamma \rfloor) \overline{\chi}(s + \lfloor \alpha \ell + \gamma \rfloor)).
\end{aligned}$$

The inner sum takes only two possible values (see [**17**, Exercise 5.54]):

$$\sum_{s=1}^{p} \chi\big(s + \lfloor \alpha k + \gamma \rfloor\big)\overline{\chi}\big(s + \lfloor \alpha \ell + \gamma \rfloor\big)\big)$$

$$= \begin{pmatrix} p - 1 & \text{if } \lfloor \alpha k + \gamma \rfloor \equiv \lfloor \alpha \ell + \gamma \rfloor \pmod{p}; \\ -1 & \text{otherwise.} \end{pmatrix}$$

Since $K \leqslant p$, the congruence $\lfloor \alpha k + \gamma \rfloor \equiv \lfloor \alpha \ell + \gamma \rfloor \pmod{p}$ occurs for at most $O(\#\mathcal{K})$ pairs $k, \ell \in \mathcal{K}$; therefore, it follows that

$$|W|^2 \ll N\big((\#\mathcal{K})^2 + p \cdot \#\mathcal{K}\big) \ll pN \cdot \#\mathcal{K}.$$

Substituting this bound in (4), and using (2) and (3), we obtain

$$S_p(\alpha, \beta, \chi; N) \ll \sqrt{\frac{pN}{K\Delta}} + K + N\Delta + ND_{\alpha,\beta}(N), \tag{5}$$

We now choose

$$K = \lceil p^{1/4} N^{1/2} \rceil \quad \text{and} \quad \Delta = \frac{p^{1/4}}{N^{1/2}},$$

and the theorem follows.   □

Combining Theorem 4.1 with Lemma 3.1, we immediately obtain:

COROLLARY 4.2. *Let α be a fixed irrational number. Then, for all real numbers β, primes p, nontrivial multiplicative characters χ (mod p), and positive integers $N \leqslant p$ with $Np^{-1/2} \to \infty$, the following bound holds:*

$$S_p(\alpha, \beta, \chi; N) = o(N).$$

Similarly, combining Theorem 4.1 with Lemma 3.2, we obtain:

COROLLARY 4.3. *Let α be a fixed irrational number of type $\tau < \infty$. Then, for all real numbers β, primes p, nontrivial multiplicative characters χ (mod p), and positive integers $N \leqslant p$, the following bound holds:*

$$S_p(\alpha, \beta, \chi; N) \ll p^{1/4} N^{1/2} + N^{1-1/\tau+o(1)}.$$

In the preceding statement, if $\tau < 4$, then the term $N^{1-1/\tau+o(1)}$ is smaller than $p^{1/4} N^{1/2}$; therefore:

COROLLARY 4.4. *Let α be a fixed irrational number of type $\tau < 4$. Then, for all real numbers β, primes p, nontrivial multiplicative characters χ (mod p), and positive integers $N \leqslant p$, the following bound holds:*

$$S_p(\alpha, \beta, \chi; N) \ll p^{1/4} N^{1/2}.$$

Clearly, since the bounds of Theorem 4.1 and of Corollaries 4.2, 4.3 and 4.4 are uniform with respect to β, one can extend them to the values of $N > p$ simply by splitting the entire range into intervals of length at most p.

5. Non-residues and primitive roots

Here, we record some applications of the results of Section 4.

Let $Q_{\alpha,\beta}(N,p)$ denote the number of quadratic non-residues modulo p among the first N elements of the Beatty sequence $\mathcal{B}_{\alpha,\beta}$. Using Corollaries 4.2, 4.3 and 4.4, respectively, with the *Legendre symbol*, we immediately obtain:

COROLLARY 5.1. *Let α be a fixed irrational number. Then, for all real numbers β, primes p, and positive integers $N \leqslant p$, such that $Np^{-1/2} \to \infty$, the following estimate holds:*

$$Q_{\alpha,\beta}(N,p) = \frac{N}{2} + o(N).$$

COROLLARY 5.2. *Let α be a fixed irrational number of type $\tau < \infty$. Then, for all real numbers β, primes p, and positive integers $N \leqslant p$, the following estimate holds:*

$$Q_{\alpha,\beta}(N,p) = \frac{N}{2} + O(p^{1/4}N^{1/2} + N^{1-1/\tau+o(1)}).$$

COROLLARY 5.3. *Let α be a fixed irrational number of type $\tau < 4$. Then, for all real numbers β, primes p, and positive integers $N \leqslant p$, the following estimate holds:*

$$Q_{\alpha,\beta}(N,p) = \frac{N}{2} + O(p^{1/4}N^{1/2}).$$

It is well known that the characteristic function of the set of primitive roots modulo p can be expressed via multiplicative characters modulo p (see, for example, [17, Exercise 5.14]). Let $T_{\alpha,\beta}(N,p)$ denote the number of primitive roots modulo p in the first N elements of the Beatty sequence $\mathcal{B}_{\alpha,\beta}$. We also denote by $\varphi(k)$ the Euler function of integer $k \geqslant 1$. From Corollaries 4.3 and 4.4, respectively, using standard arguments, we immediately obtain:

COROLLARY 5.4. *Let α be a fixed irrational number of type $\tau < \infty$. Then, for all real numbers β, primes p, and positive integers $N \leqslant p$, the following estimate holds:*

$$T_{\alpha,\beta}(N,p) = \frac{N\varphi(p-1)}{p} + O(p^{1/4}N^{1/2+o(1)} + N^{1-1/\tau+o(1)}).$$

COROLLARY 5.5. *Let α be a fixed irrational number of type $\tau < 4$. Then, for all real numbers β, primes p, and positive integers $N \leqslant p$, the following estimate holds:*

$$T_{\alpha,\beta}(N,p) = \frac{N\varphi(p-1)}{p} + O(p^{1/4}N^{1/2+o(1)}).$$

6. Other sums

The methods of Section 4 can also be used to estimate character and exponential sums such as

$$\sum_{n \leqslant N} \chi\big(f(\lfloor \alpha n + \beta \rfloor)\big), \qquad \sum_{n \leqslant N} e\big(F(\lfloor \alpha n + \beta \rfloor)\big),$$

where $f(X)$ is a polynomial with integer coefficients, and $F(X)$ is a polynomial with real coefficients (and known Diophantine properties).

Here, we focus on estimates for slightly different sums of the form:

$$\sigma_m(\alpha, \beta, a, g; N) = \sum_{n \leqslant N} \mathbf{e}(ag^{\lfloor \alpha n + \beta \rfloor}/m),$$

where $\gcd(ag, m) = 1$. If the multiplicative order of g modulo m exceeds $m^{1/2}$, these sums can be estimated nontrivially as follows:

THEOREM 6.1. *Let α be a fixed irrational number. Then, for all real numbers β, integers a, g, m with $\gcd(ag, m) = 1$, and positive integers $N \leqslant t$, where t is the multiplicative order of g modulo m, the following bound holds:*

$$\sigma_m(\alpha, \beta, \chi; N) \ll m^{1/4} N^{1/2} + N D_{\alpha, \beta}(N).$$

PROOF: Choosing γ and the sets $\mathcal{N}_\gamma$, $\mathcal{N}_\gamma^c$, $\mathcal{K}_\gamma$ as in the proof of Theorem 4.1, we obtain in the same way the estimate:

$$\sigma_m(\alpha, \beta, \chi; N) = \frac{W}{\#\mathcal{K}} + O\big(K + \#\mathcal{N}^c\big),$$

where

$$W = \sum_{n \in \mathcal{N}} \sum_{k \in \mathcal{K}} \mathbf{e}\big(ag^{\lfloor \alpha(n+k)+\beta \rfloor}/m\big)$$
$$= \sum_{n \in \mathcal{N}} \sum_{k \in \mathcal{K}} \mathbf{e}\big(ag^{\lfloor \alpha n + \beta - \gamma \rfloor + \lfloor \alpha k + \gamma \rfloor}/m\big).$$

As in the proof of Theorem 4.1, since $N \leqslant t$ (and $\gcd(a, m) = 1$), we have

$$\#\{n \in \mathcal{N} \; : \; ag^{\lfloor \alpha n + \beta - \gamma \rfloor} \equiv s \pmod{m}\} = O(1)$$

uniformly for all $s \in \mathbb{Z}$. Therefore, using the Cauchy inequality, we derive that

$$|W|^2 \ll N \sum_{s=1}^{m} \left| \sum_{k \in \mathcal{K}} \mathbf{e}\big(sg^{\lfloor \alpha k + \gamma \rfloor}/m\big) \right|^2$$
$$= N \sum_{k, \ell \in \mathcal{K}} \sum_{s=1}^{m} \mathbf{e}\big(s(g^{\lfloor \alpha k + \gamma \rfloor} - g^{\lfloor \alpha \ell + \gamma \rfloor})/m\big).$$

The inner sum vanishes unless

$$g^{\lfloor \alpha k + \gamma \rfloor} \equiv g^{\lfloor \alpha \ell + \gamma \rfloor} \pmod{m}, \tag{6}$$

in which case it is equal to m. Since $K \leqslant t$, the congruence (6) is equivalent to

$$\lfloor \alpha k + \gamma \rfloor \equiv \lfloor \alpha \ell + \gamma \rfloor \pmod{t},$$

which occurs for at most $O(\#\mathcal{K})$ pairs $k, \ell \in \mathcal{K}$; thus, it follows that

$$|W|^2 \ll mN \cdot \#\mathcal{K}.$$

Continuing our calculations as in the proof of Theorem 4.1, we obtain the stated result. □

The bound of Theorem 6.1 is nontrivial only if $t \geqslant N \geqslant m^{1/2}$. However, in the case that $m = p$ is prime, our methods can be combined with recent results of Bourgain, Glibichuk and Konyagin [4] (see also [5]) to obtain a nontrivial estimate for any integer g whose multiplicative order t modulo p satisfies the inequality $t > p^\delta$ for some fixed $\delta > 0$.

THEOREM 6.2. *Let α be a fixed irrational number. For any fixed $\delta > 0$, there exists a constant $\eta > 0$ such that for all real numbers β, integers a, g and a prime p with $\gcd(ag, p) = 1$, and positive integers $p^\delta < N \leqslant t$, where t is the multiplicative order of g modulo p, the following bound holds:*

$$\sigma_p(\alpha, \beta, \chi; N) \ll Np^{-\eta} + ND_{\alpha,\beta}(N).$$

PROOF: The proof is identical to that of Theorem 6.1, except that we now write

$$|W|^2 \ll N \sum_{1 \leqslant u \leqslant [\alpha N + \beta]} \left| \sum_{k \in \mathcal{K}} \mathbf{e}\big(ag^{u + \lfloor \alpha k + \gamma \rfloor}/p\big) \right|^2$$
$$= N \sum_{k,\ell \in \mathcal{K}} \sum_{1 \leqslant u \leqslant [\alpha N + \beta]} \mathbf{e}\Big(a\big(g^{\lfloor \alpha k + \gamma \rfloor} - g^{\lfloor \alpha \ell + \gamma \rfloor}\big)g^u/m\Big).$$

By a result of [4], the inner sum is $O(Np^{-\kappa})$ for some constant $\kappa > 0$ that depends only on δ, unless (6) holds (with $m = p$), in which case it is equal $O(N)$. Since $K \leqslant t$, the congruence (6) is equivalent to $\lfloor \alpha k + \gamma \rfloor \equiv \lfloor \alpha \ell + \gamma \rfloor \pmod{t}$, which occurs for at most $O(\#\mathcal{K})$ pairs $k, \ell \in \mathcal{K}$; thus, it follows that

$$|W|^2 \ll N\big((\#\mathcal{K})^2 Np^{-\kappa} + N\#\mathcal{K}\big).$$

After optimising the choice of K and Δ, we obtain the announced result. □

Since the bounds of Theorems 6.1 and 6.2 are uniform with respect to β, one can extend these results to numbers $N > t$ simply by splitting the entire range into intervals of length at most t. If $m = p$ is prime and the multiplicative order of t modulo p is large enough (starting with $t > p^{1/4+\delta}$), one can also use results from [9, 14, 15] to derive more explicit bounds on the sums $\sigma_m(\alpha, \beta, a, g; N)$. Finally, it is clear that Theorems 6.1 and 6.2 can be used to derive analogues of Corollaries 4.2, 4.3 and 4.4.

7. REMARKS

Unfortunately, we cannot get an analogue of Corollary 5.1 for primitive roots as the additional term of size $N^{o(1)}$ prevents a direct application of Corollary 4.2; one requires

a sharper bound than simply $o(N)$. It would be interesting to see whether Corollary 4.2 can be sharpened sufficiently to provide such a result, or else a proof that a stronger bound is not possible over the entire class of Liouville numbers; we pose this question as an open problem to the reader.

Finally, we remark that, using our method, one can obtain asymptotic formulas for the average values of various arithmetic functions taken on a Beatty sequence.

References

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

[2] W. Banks and I.E. Shparlinski, 'Short character sums with Beatty sequences', *Math. Res. Lett.* (to appear).

[3] A.V. Begunts, 'An analogue of the Dirichlet divisor problem', *Moscow Univ. Math. Bull.* **59** (2004), 37–41.

[4] J. Bourgain, A.A. Glibichuk and S.V. Konyagin, 'Estimates for the number of sums and products and for exponential sums in fields of prime order', *J. Lond. Math. Soc.* (to appear).

[5] J. Bourgain and S.V. Konyagin, 'Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order', *C. R. Math. Acad. Sci. Paris* **337** (2003), 75–80.

[6] Y. Bugeaud, *Approximation by algebraic numbers* (Cambridge University Press, Cambridge, 2004).

[7] A.S. Fraenkel and R. Holzman, 'Gap problems for integer part and fractional part sequences', *J. Number Theory* **50** (1995), 66–86.

[8] M.Z. Garaev, 'A note on the least quadratic non-residue of the integer-sequences', *Bull. Austral. Math. Soc.* **68** (2003), 1–11.

[9] 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.

[10] A. Hildebrand, 'On the least pair of consecutive quadratic non-residues', *Mich. Math. J.* **34** (1987), 57–62.

[11] A.Y. Khinchin, 'Zur metrischen Theorie der diophantischen Approximationen', *Math. Z.* **24** (1926), 706–714.

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

[13] T. Komatsu, 'The fractional part of $n\vartheta + \varphi$ and Beatty sequences', *J. Théor. Nombres Bordeaux* **7** (1995), 387–406.

[14] S.V. Konyagin, 'Bounds of exponential sums over subgroups and Gauss sums', (in Russian), in *Proc. 4th Intern. Conf. Modern Problems of Number Theory and Its Applications* (Moscow Lomonosov State Univ., Moscow, 2002), pp. 86–114.

[15] S.V. Konyagin and I.E. Shparlinski, *Character sums with exponential functions and their applications* (Cambridge Univ. Press, Cambridge, 1999).

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

[17]   R. Lidl and H. Niederreiter, *Finite fields* (Cambridge University Press, Cambridge, 1997).

[18]   K. O'Bryant, 'A generating function technique for Beatty sequences and other step sequences', *J. Number Theory* **94** (2002), 299–319.

[19]   S.N. Preobrazhenskiĭ, 'On the least quadratic non-residue in an arithmetic sequence', *Moscow Univ. Math. Bull.* **56** (2001), 44–46.

[20]   S.N. Preobrazhenskiĭ, 'On power non-residues modulo a prime number in a special integer sequence', *Moscow Univ. Math. Bull.* **56** (2001), 41–42.

[21]   S.N. Preobrazhenskiĭ, 'On the least power non-residue in an integer sequence', *Moscow Univ. Math. Bull.* **59** (2004), 33–35.

[22]   K.F. Roth, 'Rational approximations to algebraic numbers', *Mathematika* **2** (1955), 1–20.

[23]   K.F. Roth, 'Corrigendum to "Rational approximations to algebraic numbers"', *Mathematika* **2** (1955), 168.

[24]   W.M. Schmidt, *Diophantine approximation* (Springer–Verlag, Berlin, 1980).

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

Department of Mathematics   Department of Computing
University of Missouri   Macquarie University
Columbia, MO 65211   Sydney, NSW 2109
United States of america   Australia
e-mail: bbanks@math.missouri.edu   e-mail: igor@ics.mq.edu.au