Journal of Number Theory 260 (2024) 198–211

Contents lists available at ScienceDirect

Journal of Number Theory

journal homepage: www.elsevier.com/locate/jnt

General Section

A zero-sum problem related to the max gap of the unit group of the residue class ring ☆

Xiao Jiang *, Wenkai Yang

Center for Applied Mathematics, Tianjin University, Tianjin 300072, PR China

A R T I C L E   I N F O

Article history:
Received 29 November 2023
Received in revised form 23 February 2024
Accepted 25 February 2024
Available online 20 March 2024
Communicated by S.J. Miller

MSC:
11A07
11B05
11B30
20K01

Keywords:
Cyclic groups
Zero-sum subsequence
Max gap
Reduced residue systems

A B S T R A C T

Let S be a sequence over a finite abelian group G and $\mathsf{v}_g(S)$ be the times that $g \in G$ occurs in S. A sequence S over G is called weak-regular if $\mathsf{v}_g(S) \le \mathrm{ord}(g)$ for every $g \in G$. Denote by $N(G)$ the smallest integer t such that every weak-regular sequence S over G of length $|S| \ge t$ has a nonempty zero-sum subsequence T of S satisfying $\mathsf{v}_g(T) = \mathsf{v}_g(S)$ for some $g \mid S$. $N(G)$ has been formulated by Gao et al. very recently to study zero-sum problems in a unify way and determined only for cyclic groups of prime-power order and some other very special groups. As for general cyclic groups $G = C_n$, they gave that

$$2n - \lceil 3\sqrt{n} \rceil + 1 \le \mathsf{N}(G) \le 2n - \lceil 2\sqrt{n+1} \rceil + 1.$$

In this paper, we first study the max gap of the unit group of the residue class ring and give an upper bound of it. Then we prove that there is always an integer $a \in [n^{\frac{1}{2}}, n^{\frac{1}{2}} + n^{\frac{1}{4}}]$ such that $\gcd(a, n) = 1$ for $n \ge 2227$. Finally, we improve the result of Gao et al. by showing that

$$2n - \lceil 2\sqrt{n+1} \rceil \le \mathsf{N}(G) \le 2n - \lceil 2\sqrt{n+1} \rceil + 1$$

for any cyclic group $G = C_n$ with $n \ge 3$, in which for each equality, there are infinitely many n making it hold.

☆ This work was supported by National Natural Science Foundation of China (Grant No. 12071344).

* Corresponding author.
E-mail addresses: jiangxiao2022@tju.edu.cn (X. Jiang), 3016210052@tju.edu.cn (W. Yang).

https://doi.org/10.1016/j.jnt.2024.02.005
0022-314X/

And a computing result prefigures that $\mathsf{N}(G)$ has not been determined only for very few cyclic groups G.

1. Introduction

The zero-sum theory on abelian groups can be traced back to 1960's and has been developed rapidly in recent several decades. Many invariants have been formulated in the zero-sum theory, such as the Erdős-Ginzburg-Ziv constant $\mathsf{s}(G)$, the Davenport constant $\mathsf{D}(G)$, the Olson constant $\mathsf{Ol}(G)$ and so on. For more information on the development of the zero-sum theory we refer to [1,5,6].

In order to describe zero-sum invariants uniformly, in 2021 [2], Gao et al. provided a unified way to formulate zero-sum invariants, which is more general than the definition in 2018 [4]. To understand zero-sum invariants better, they introduced the concepts of the weak-regular sequence over G and the constant $\mathsf{N}(G)$ of G. A sequence S over G is called weak-regular if $\mathsf{v}_g(S) \le \mathrm{ord}(g)$ for every $g \in G$. $\mathsf{N}(G)$ is the smallest integer t such that every weak-regular sequence S over G of length $|S| \ge t$ has a nonempty zero-sum subsequence T of S satisfying $\mathsf{v}_g(T) = \mathsf{v}_g(S)$ for some $g \mid S$ or, equivalently, $\mathrm{supp}(ST^{-1}) \ne \mathrm{supp}(S)$. They also pointed it out that $\mathsf{N}(G) \le 1 + \mathsf{ol}(G)(\exp(G) - 1)$.

One year later, Gao et al. [3] made some further study on $\mathsf{N}(G)$ for the cyclic groups and the elementary abelian groups. They proved that $2n - B_{n+1} + 1 \le \mathsf{N}(G) \le 2n - A_{n+1} + 1$ for a cyclic group $G = C_n$ with $n \ge 3$, where $\lceil 2\sqrt{n} \rceil = A_n \le B_n \le \lceil 3\sqrt{n} \rceil$. More detail of A_n and B_n will be introduced and discussed in Section 4. Obviously, if $A_{n+1} = B_{n+1}$, then $\mathsf{N}(C_n) = 2n - \lceil 2\sqrt{n+1} \rceil + 1$.

In this paper, we start with an elementary question in Elementary Number Theory. Some usual notations in Number Theory will be explained at the end of this section intensively.

In Section 2, we introduce a combinatorics constant $\mathsf{MG}(n)$, which we call the max gap of the unit group of the residue class ring modulo n, and find it no greater than $2^{\omega(n)-1} p_{\omega(n)}$ for any integer $n \ge 2$. In plain language, for an integer $n \ge 2$ and any $2^{\omega(n)-1} p_{\omega(n)}$ consecutive integers, there is always one of them relatively prime to n. The method is also elementary and the successive sweep principle plays an important role. Although this upper bound is too large for n with a large $\omega(n)$ and is reached only if n is a power of a prime number, it is enough for what we need next.

In Section 3, we focus on the interval $[n^{\frac{1}{2}}, n^{\frac{1}{2}} + n^{\frac{1}{4}}]$. With the help of a personal computer and the explicit estimate of p_k and $\vartheta(p_k)$ (see Lemma 3.1) obtained by Massias and Robin, we compare $\mathsf{MG}(n)$ with $\lfloor n^{\frac{1}{4}} \rfloor$ for n with a large $\omega(n)$. Together with more careful analysis for n with a small $\omega(n)$, we prove that for any integer $n \ge 2227$, there is always an integer $a \in [n^{\frac{1}{2}}, n^{\frac{1}{2}} + n^{\frac{1}{4}}]$ such that $\gcd(a, n) = 1$.

In Section 4, we turn back to the zero-sum theory mentioned above. Using the above result, we prove that $A_n \le B_n \le A_n + 1$ for $n \ge 2$. Moreover, for each equality, there are infinitely many n making it hold. Therefore, we give a very sharp bound of the constant $\mathsf{N}(G)$ and state it as below.

Theorem 1.1. *For any cyclic group $G = C_n$ with $n \ge 3$,*

$$2n - \lceil 2\sqrt{n+1} \rceil \le \mathsf{N}(G) \le 2n - \lceil 2\sqrt{n+1} \rceil + 1.$$

Moreover, for each equality, there are infinitely many n making it hold.

In the final section, as a concluding remark, we give the computing result of $B_{n+1} - A_{n+1}$ for $2 \le n \le 10^8$ and four more classes of n such that $B_{n+1} > A_{n+1}$. This result tells us that $B_{n+1} = A_{n+1}$ for the overwhelming majority of positive integers n. Thus, $\mathsf{N}(C_n) = 2n - \lceil 2\sqrt{n+1} \rceil + 1$ for these n. The remaining n that $\mathsf{N}(C_n)$ have not been determined should be of density 0.

At the end of this section, we list some notations used in this paper.

Let $\mathbb{Z}$ denote the set of integers and $\mathbb{N} := \mathbb{Z}_{\ge 1}$ denote the set of positive integers.

Let p_n be the n-th prime number. That is, $p_1 = 2$, $p_2 = 3$ and so on. We set $p_0 := 1$ in this paper.

For a real number x, we set $\lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \le x\}$ and $\lceil x \rceil := \min\{n \in \mathbb{Z} \mid n \ge x\}$.

In the symbol $\sum$ or $\prod$, the variable is limited to positive integers. If the variable is p, then it is limited to prime numbers.

Let $\omega(n) := \sum_{p|n} 1$ be the number of different prime divisors of n and $\omega(1) := 0$.

Let $\varphi(n)$ be the Euler phi function.

Let $\mathsf{rad}(n) := \prod_{p|n} p$ be the product of all different prime divisors of n and $\mathsf{rad}(1) := 1$.

Let $\vartheta(x) := \sum_{p \le x} \ln p$ be the well-known Chebyshev function.

For a positive integer n and a set X of integers, let $X_{(n)} := \{x \in X \mid n \text{ divides } x\}$ and $X^{[n]} := \{x \in X \mid \gcd(x, n) = 1\}$.

For any prime p and any integer n, let $\mathsf{v}_p(n)$ stand for the p-adic valuation of n, i.e., $\mathsf{v}_p(n)$ is the biggest nonnegative integer r with p^r dividing n.

2. The gap of the unit group of the residue class ring

In this and the next section, we use the notations

$$X_{(n)} := \{x \in X \mid n \text{ divides } x\}$$

and

$$X^{[n]} := \{x \in X \mid \gcd(x, n) = 1\}$$

for a positive integer n and a set X of integers.

For an integer $n \geq 2$, let $\mathbb{Z}/n\mathbb{Z}$ be the residue class ring modulo n and let $\eta : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the canonical epimorphism. Then $(\mathbb{Z}/n\mathbb{Z})^\times$ is the unit group of $\mathbb{Z}/n\mathbb{Z}$ and $\eta^{-1}((\mathbb{Z}/n\mathbb{Z})^\times) = \{x \in \mathbb{Z} \mid \gcd(x, n) = 1\} = \mathbb{Z}^{[n]} \subset \mathbb{Z}$.

The set $\mathbb{Z}^{[n]}$ has the same order "$<$" of $\mathbb{Z}$. Two different integers $x, y \in \mathbb{Z}^{[n]}$ are called adjacent in $\mathbb{Z}^{[n]}$ if there is no element of $\mathbb{Z}^{[n]}$ between x and y. And the gap of adjacent x, y in $\mathbb{Z}^{[n]}$ is defined by $|x - y|$. The concepts of "adjacent" and "gap" here can be kept by the function η. That is, two residue classes $x + n\mathbb{Z}$ and $y + n\mathbb{Z}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ are adjacent if and only if there are $a \in x + n\mathbb{Z}$ and $b \in y + n\mathbb{Z}$ such that a, b are adjacent in $\mathbb{Z}^{[n]}$. And the gap of adjacent $x + n\mathbb{Z}$ and $y + n\mathbb{Z}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ can be taken by $|a - b|$ except for $n = 3$ or 6. It is easy to check that the concepts of "adjacent" and "gap" are well defined here, if we accept that $1 + 6\mathbb{Z}$ and $5 + 6\mathbb{Z}$ have two gaps 2 and 4, and $1 + 3\mathbb{Z}$ and $2 + 3\mathbb{Z}$ have two gaps 1 and 2.

Let $\mathsf{GAP}(\mathbb{Z}^{[n]}) := \{|x-y| \mid x, y \text{ are adjacent in } \mathbb{Z}^{[n]}\}$ be the set of all the gaps over $\mathbb{Z}^{[n]}$ and $\mathsf{GAP}((\mathbb{Z}/n\mathbb{Z})^\times) := \{|x-y| \mid x, y$ are adjacent in $\mathbb{Z}^{[n]}$ and respectively in two adjacent reduced residue classes modulo $n\}$ be the set of all the gaps over $(\mathbb{Z}/n\mathbb{Z})^\times$. Obviously, $\mathsf{GAP}(\mathbb{Z}^{[n]}) = \mathsf{GAP}((\mathbb{Z}/n\mathbb{Z})^\times)$ for $n \geq 2$ and so we do not distinguish $\mathsf{GAP}(\mathbb{Z}^{[n]})$ and $\mathsf{GAP}((\mathbb{Z}/n\mathbb{Z})^\times)$ for convenience. Since $\mathbb{Z}^{[n]}$ is of period n, $\mathsf{GAP}(\mathbb{Z}^{[n]})$ is a finite set of positive integers.

The minimum of $\mathsf{GAP}(\mathbb{Z}^{[n]})$ is trivial. It is 1 for odd n since $\mathsf{rad}(n)+1, \mathsf{rad}(n)+2 \in \mathbb{Z}^{[n]}$. And it is 2 for even n since $\mathbb{Z}^{[n]}$ only contains odd integers and $n - 1, n + 1 \in \mathbb{Z}^{[n]}$.

The maximum of $\mathsf{GAP}(\mathbb{Z}^{[n]})$ is an interesting and valuable research object, which will be discussed in this and the next section. Here we give an equivalent definition of it in a simple description.

Definition 2.1. Let $\mathsf{MG}(n)$ be the smallest integer l such that, for any l consecutive integers, there is always one of them relatively prime to n.

In the next part of this section, we give a unified upper bound of $\mathsf{MG}(n)$, which is stated as below.

Theorem 2.2. *For any integer $n \geq 2$,*

$$\mathsf{MG}(n) \leq 2^{\omega(n)-1} p_{\omega(n)}.$$

To prove it, we need some auxiliary lemmas.

Lemma 2.3. *Let $X = \{a + kb\}_{k=1}^{l}$ be a finite arithmetic progression with integers a, b. If an integer $n \geq 2$ and $\gcd(n, b) = 1$, then $|X^{[n]}| > \frac{\varphi(n)}{n} l - 2^{\omega(n)} + 1$.*

Proof. If an integer $d \geq 2$ and $\gcd(d, b) = 1$, then any d consecutive terms in X constitute a complete set of residues modulo d. Therefore,

$$\frac{|X|}{d} - 1 < \left\lfloor \frac{|X|}{d} \right\rfloor \le |X_{(d)}| \le \left\lceil \frac{|X|}{d} \right\rceil < \frac{|X|}{d} + 1$$

and so

$$(-1)^{\omega(d)} \frac{|X|}{d} - 1 < (-1)^{\omega(d)} |X_{(d)}| < (-1)^{\omega(d)} \frac{|X|}{d} + 1.$$

By the successive sweep principle,

$$\begin{aligned} \left|X^{[n]}\right| &= \Big|X \setminus \bigcup_{p|\mathsf{rad}(n)} X_{(p)}\Big| \\ &= \sum_{d|\mathsf{rad}(n)} (-1)^{\omega(d)} |X_{(d)}| \\ &> |X| + \sum_{\substack{d|\mathsf{rad}(n) \\ d>1}} \Big((-1)^{\omega(d)} \frac{|X|}{d} - 1\Big) \\ &= |X| \prod_{p|\mathsf{rad}(n)} (1 - \frac{1}{p}) - \sum_{\substack{d|\mathsf{rad}(n) \\ d>1}} 1 \\ &= |X| \frac{\varphi(n)}{n} - 2^{\omega(n)} + 1. \end{aligned}$$

Lemma 2.3 is proved. □

Lemma 2.4. *Let* $\mathsf{rad}(n) = \prod_{k=1}^{\omega(n)} q_k$ *with prime numbers* $q_1 < ... < q_{\omega(n)}$ *and* $1 \le \omega(n) \le 4$.

(1). *If* $\omega(n) = 1$, *then* $\mathsf{MG}(n) = 2$.
(2). *If* $\omega(n) = 2$, *then* $\mathsf{MG}(n) \le \mathsf{MG}(6) = 4 = 2p_1$.
(3). *If* $\omega(n) = 3$, *then* $\mathsf{MG}(n) \le \mathsf{MG}(30) = 6 = 2p_2$.
(4). *If* $\omega(n) = 4$, *then* $\mathsf{MG}(n) \le \mathsf{MG}(210) = 10 = 2p_3$.

Proof. (1). If $\omega(n) = 1$, then n is a power of a prime number. It is easy to see $\mathsf{MG}(n) = 2$ by the Definition 2.1.

(2). If $\omega(n) = 2$, then $\mathsf{rad}(n) = q_1 q_2$ and let X be a set of 4 consecutive integers.

If $q_1 \ge 3$, then

$$\left|X^{[n]}\right| \ge |X| - |X_{(q_1)}| - |X_{(q_2)}| \ge |X| - \left\lceil \frac{|X|}{q_1} \right\rceil - \left\lceil \frac{|X|}{q_2} \right\rceil \ge |X| - \left\lceil \frac{|X|}{3} \right\rceil - \left\lceil \frac{|X|}{5} \right\rceil = 1.$$

If $q_1 = 2$, then let $Y \subset X$ be the set of the $\frac{|X|}{2} = 2$ consecutive odd integers in X. Since $q_2 \ge 3$, we have

$$\left|X^{[n]}\right| \ge \left|Y^{[n]}\right| = \left|Y^{[q_2]}\right| \ge |Y| - |Y_{(q_2)}| \ge |Y| - \left\lceil \frac{|Y|}{q_2} \right\rceil \ge |Y| - \left\lceil \frac{|Y|}{3} \right\rceil = 1.$$

In both cases, we get $\left|X^{[n]}\right| > 0$ and so $\mathsf{MG}(n) \le 4$ for $\omega(n) = 2$.

Moreover, $\gcd(x, 6) \ne 1$ for $x \in \{2, 3, 4\}$. So $\mathsf{MG}(6) = 4$.

(3). If $\omega(n) = 3$, then $\mathsf{rad}(n) = q_1q_2q_3$ and let X be a set of 6 consecutive integers. If $q_1 \ge 3$, then

$$\left|X^{[n]}\right| \ge |X| - \left\lceil \frac{|X|}{q_1} \right\rceil - \left\lceil \frac{|X|}{q_2} \right\rceil - \left\lceil \frac{|X|}{q_3} \right\rceil \ge |X| - \left\lceil \frac{|X|}{3} \right\rceil - \left\lceil \frac{|X|}{5} \right\rceil - \left\lceil \frac{|X|}{7} \right\rceil = 1.$$

If $q_1 = 2$, then let $Y \subset X$ be the set of the $\frac{|X|}{2} = 3$ consecutive odd integers in X. Since $q_2 \ge 3$ and $q_3 \ge 5$, we have

$$\left|X^{[n]}\right| \ge \left|Y^{[q_2q_3]}\right| \ge |Y| - \left\lceil \frac{|Y|}{q_2} \right\rceil - \left\lceil \frac{|Y|}{q_3} \right\rceil \ge |Y| - \left\lceil \frac{|Y|}{3} \right\rceil - \left\lceil \frac{|Y|}{5} \right\rceil = 1.$$

In both cases, we get $\left|X^{[n]}\right| > 0$ and so $\mathsf{MG}(n) \le 6$ for $\omega(n) = 3$.

Moreover, $\gcd(x, 30) \ne 1$ for $x \in \{2, 3, 4, 5, 6\}$. So $\mathsf{MG}(30) = 6$.

(4). If $\omega(n) = 4$, then $\mathsf{rad}(n) = q_1q_2q_3q_4$ and let X be a set of 10 consecutive integers. If $q_1 \ge 3$, then

$$\left|X^{[n]}\right| \ge |X| - \left\lceil \frac{|X|}{q_1} \right\rceil - \left\lceil \frac{|X|}{q_2} \right\rceil - \left\lceil \frac{|X|}{q_3} \right\rceil - \left\lceil \frac{|X|}{q_4} \right\rceil \ge |X| - \left\lceil \frac{|X|}{3} \right\rceil - \left\lceil \frac{|X|}{5} \right\rceil - \left\lceil \frac{|X|}{7} \right\rceil - \left\lceil \frac{|X|}{11} \right\rceil = 1.$$

If $q_1 = 2$, then let $Y \subset X$ be the set of the $\frac{|X|}{2} = 5$ consecutive odd integers in X. Since $q_2 \ge 3$, $q_3 \ge 5$ and $q_4 \ge 7$, we have

$$\left|X^{[n]}\right| \ge \left|Y^{[q_2q_3q_4]}\right| \ge |Y| - \left\lceil \frac{|Y|}{q_2} \right\rceil - \left\lceil \frac{|Y|}{q_3} \right\rceil - \left\lceil \frac{|Y|}{q_4} \right\rceil \ge |Y| - \left\lceil \frac{|Y|}{3} \right\rceil - \left\lceil \frac{|Y|}{5} \right\rceil - \left\lceil \frac{|Y|}{7} \right\rceil = 1.$$

In both cases, we get $\left|X^{[n]}\right| > 0$ and so $\mathsf{MG}(n) \le 10$ for $\omega(n) = 4$.

Moreover, $\gcd(x, 210) \ne 1$ for $x \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$. So $\mathsf{MG}(210) = 10$.

Hence Lemma 2.4 is proved completely. □

Set $p_0 := 1$. Lemma 2.4 seems to tell us that for a certain $\omega(n)$, $\mathsf{MG}(n)$ is no greater than $2p_{\omega(n)-1}$ and reaches the maximum when $\mathsf{rad}(n) = \prod_{k=1}^{\omega(n)} p_k$. Unfortunately, we are unable to prove or disprove these two conjectures. Here, we just give a unified upper bound of $\mathsf{MG}(n)$ as an auxiliary tool and prove it now.

Proof of Theorem 2.2. When $1 \le \omega(n) \le 4$, we have $\mathsf{MG}(n) \le 2^{\omega(n)-1}p_{\omega(n)}$ by Lemma 2.4.

When $\omega(n) \ge 5$, let X be a set of $2^{\omega(n)-1}p_{\omega(n)}$ consecutive integers. From Lemma 2.3, one derives that

$$\left|X^{[n]}\right| > |X|\frac{\varphi(n)}{n} - 2^{\omega(n)} + 1$$

$$
\begin{aligned}
&= 2^{\omega(n)-1}p_{\omega(n)}\prod_{p|n}(1-\frac{1}{p}) - 2^{\omega(n)} + 1 \\
&> 2^{\omega(n)}\Big(\frac{p_{\omega(n)}}{2}\prod_{p|n}(1-\frac{1}{p}) - 1\Big) \\
&\geq 2^{\omega(n)}\Big(\frac{p_{\omega(n)}}{2}\prod_{k=1}^{\omega(n)}(1-\frac{1}{p_k}) - 1\Big) \\
&= 2^{\omega(n)}\Big(\frac{1}{2}\prod_{k=2}^{\omega(n)}\frac{p_k-1}{p_{k-1}} - 1\Big) \\
&\geq 2^{\omega(n)}\Big(\frac{1}{2}\prod_{k=2}^{5}\frac{p_k-1}{p_{k-1}} - 1\Big) \\
&= 2^{\omega(n)}\Big(\frac{1}{2}\cdot\frac{16}{7} - 1\Big) > 0
\end{aligned}
$$

as desired since $p_k - 1 \geq p_{k-1}$ for $k \geq 2$.

This completes the proof of Theorem 2.2. □

3. The reduced residue system modulo n and the interval $[n^{\frac{1}{2}}, n^{\frac{1}{2}} + n^{\frac{1}{4}}]$

In this section, we focus on the interval $[n^{\frac{1}{2}}, n^{\frac{1}{2}} + n^{\frac{1}{4}}]$ and search whether $\mathbb{Z}^{[n]} \cap [n^{\frac{1}{2}}, n^{\frac{1}{2}} + n^{\frac{1}{4}}] \neq \emptyset$. To begin with, we introduce a remarkable result of the distribution of primes and compare the upper bound of $\mathsf{MG}(n)$ in Theorem 2.2 with the length of this interval.

Lemma 3.1.

(1). *[7] If $k \geq 6$, then $p_k \leq k(\ln k + \ln\ln k) < 2k\ln k$.*
(2). *[8] If $k \geq 13$, then $\vartheta(p_k) \geq k\ln k$.*

Lemma 3.2. *If $\omega(n) \geq 26$, then $n^{\frac{1}{4}} \geq 2^{\omega(n)-1}p_{\omega(n)}$.*

Proof. When $\ln\omega(n) > 8$ or, equivalently, $\omega(n) \geq 2981$, Lemma 3.1 infers that

$$
n^{\frac{1}{4}} \geq \Big(\prod_{k=1}^{\omega(n)} p_k\Big)^{\frac{1}{4}} = e^{\frac{1}{4}\vartheta(p_{\omega(n)})} \geq e^{\frac{1}{4}\omega(n)\ln\omega(n)} > e^{2\omega(n)}
$$

and

$$
2^{\omega(n)-1}p_{\omega(n)} < 2^{\omega(n)-1}\cdot 2\omega(n)\ln\omega(n) < 2^{\omega(n)}\cdot 2^{\omega(n)}.
$$

Therefore, $n^{\frac{1}{4}} > 2^{\omega(n)-1}p_{\omega(n)}$ in this situation.

When $26 \leq \omega(n) \leq 2980$, we still have $n^{\frac{1}{4}} \geq \left(\prod_{k=1}^{\omega(n)} p_k\right)^{\frac{1}{4}}$ and just need to check

$$\frac{1}{4}\sum_{k=1}^{\omega(n)} \ln p_k \geq (\omega(n)-1)\ln 2 + \ln p_{\omega(n)}.$$

With the help of a personal computer, we check them all in a fraction of a second.

So Lemma 3.2 is proved. □

Theorem 2.2 tells us that $\mathsf{MG}(n) \leq 2^{\omega(n)-1} p_{\omega(n)}$. Together with Lemma 3.2, it implies that $\mathsf{MG}(n) \leq \lfloor n^{\frac{1}{4}} \rfloor$ if $\omega(n) \geq 26$. On the other hand, Lemma 2.4 gives a sharp upper bound of $\mathsf{MG}(n)$ for $1 \leq \omega(n) \leq 4$. So next, we continue the work of Lemma 2.4 to find an upper bound of $\mathsf{MG}(n)$ for $5 \leq \omega(n) \leq 25$ but not necessarily sharp. And here, we point out that the method below in the proof of Lemma 3.3 (1) and (3) also gives a better upper bound of $\mathsf{MG}(n)$ than Lemma 2.4 when $1 \leq \omega(n) \leq 4$. We make a table to give a convenient view. It will take some time to check every equation by taking the corresponding value.

Lemma 3.3. *Let* $\mathsf{rad}(n) = \prod_{k=1}^{\omega(n)} q_k$ *with prime numbers* $q_1 < ... < q_{\omega(n)}$ *and* $5 \leq \omega(n) \leq 25$.

(1). *If* $q_1 \geq 5$, *then* $\mathsf{MG}(n)$ *has an upper bound given in the second line of Table 1 for each corresponding* $\omega(n)$.

(2). *If* $q_1 = 3$, *then* $\mathsf{MG}(n)$ *has an upper bound given in the third line of Table 1 for each corresponding* $\omega(n)$.

(3). *If* $q_1 = 2$ *and* $q_2 \geq 5$, *then* $\mathsf{MG}(n)$ *has an upper bound given in the fourth line of Table 1 for each corresponding* $\omega(n)$.

(4). *If* $q_1 = 2$ *and* $q_2 = 3$, *then* $\mathsf{MG}(n)$ *has an upper bound given in the fifth line of Table 1 for each corresponding* $\omega(n)$.

Proof. Let X be a set of consecutive integers of number $|X|$.

(1). If $q_1 \geq 5$, then

$$\left|X^{[n]}\right| \geq |X| - \sum_{p|n} \left\lceil \frac{|X|}{p} \right\rceil \geq |X| - \sum_{k=1}^{\omega(n)} \left\lceil \frac{|X|}{p_{k+2}} \right\rceil.$$

The right part is only depended on $|X|$ and $\omega(n)$. By $|X|$ taking the value in the second line of Table 1 for the corresponding $\omega(n)$, the right part above is greater than 0.

(2). If $q_1 = 3$, then let $n = 3^{\mathsf{v}_3(n)} n_3$ with $\mathsf{rad}(n_3) = \prod_{k=2}^{\omega(n)} q_k$ and $Y_3 \subset X$ be the longer one of the sets $\{x \in X \mid x \equiv i \pmod 3\}$ for $i = 1$ or 2. So

$$|Y_3| = \left\lceil \frac{|X|-1}{3} \right\rceil$$

Table 1
An upper bound of $\mathsf{MG}(n)$ under the different conditions.

$\omega(n)$	1	2	3	4	5	6	7	8	9	10	11	12	13
$q_1 \geq 5$	2	3	4	5	7	9	10	13	17	19	25	28	33
$q_1 = 3$	2	4	6	10	14	20	26	29	38	50	56	74	83
$q_1 = 2, q_2 \geq 5$		4	6	8	10	14	18	20	26	34	38	50	56
$q_1 = 2, q_2 = 3$		4	6	10	23	29	41	53	59	77	101	113	149
$\lfloor n^{\frac{1}{4}} \rfloor$	1	1	2	3	6	13	26	55	122	283	669	1650	4176

$\omega(n)$	14	15	16	17	18	19	20
$q_1 \geq 5$	49	55	73	82	102	109	140
$q_1 = 3$	98	146	164	218	245	305	326
$q_1 = 2, q_2 \geq 5$	66	98	110	146	164	204	218
$q_1 = 2, q_2 = 3$	167	197	293	329	437	491	611
$\lfloor n^{\frac{1}{4}} \rfloor$	10694	28002	75555	209402	585212	1674296	4860120

$\omega(n)$	21	22	23	24	25
$q_1 \geq 5$	182	230	340	468	979
$q_1 = 3$	419	545	689	1019	1403
$q_1 = 2, q_2 \geq 5$	280	364	460	680	936
$q_1 = 2, q_2 = 3$	653	839	1091	1379	2039
$\lfloor n^{\frac{1}{4}} \rfloor$	14206194	42353033	127836257	392646335	1232237672

and

$$\left|X^{[n]}\right| \geq \left|Y_3^{[n_3]}\right| \geq |Y_3| - \sum_{p|n_3} \left\lceil \frac{|Y_3|}{p} \right\rceil \geq |Y_3| - \sum_{k=2}^{\omega(n)} \left\lceil \frac{|Y_3|}{p_{k+1}} \right\rceil.$$

By $|X|$ taking the value in the third line of Table 1 for the corresponding $\omega(n)$, the right part above is greater than 0.

(3). If $q_1 = 2$ and $q_2 \geq 5$, then let $n = 2^{\mathsf{v}_2(n)} n_2$ with $\mathsf{rad}(n_2) = \prod_{k=2}^{\omega(n)} q_k$ and $Y_2 \subset X$ be the set of all the odd integers in X. So

$$|Y_2| = \left\lceil \frac{|X| - 1}{2} \right\rceil$$

and

$$\left|X^{[n]}\right| \geq \left|Y_2^{[n_2]}\right| \geq |Y_2| - \sum_{p|n_2} \left\lceil \frac{|Y_2|}{p} \right\rceil \geq |Y_2| - \sum_{k=2}^{\omega(n)} \left\lceil \frac{|Y_2|}{p_{k+1}} \right\rceil.$$

By $|X|$ taking the value in the fourth line of Table 1 for the corresponding $\omega(n)$, the right part above is greater than 0.

(4). If $q_1 = 2$ and $q_2 = 3$, then let $n = 2^{\mathsf{v}_2(n)} 3^{\mathsf{v}_3(n)} n_6$ with $\mathsf{rad}(n_6) = \prod_{k=3}^{\omega(n)} q_k$ and $Y_6 \subset X$ be the longer one of the sets $\{x \in X \mid x \equiv i \pmod 6\}$ for $i = 1$ or 5. So

$$|Y_6| = \left\lceil \frac{|X| - 4}{6} \right\rceil$$

and

$$\left|X^{[n]}\right| \geq \left|Y_6^{[n_6]}\right| \geq |Y_6| - \sum_{p|n_6} \left\lceil \frac{|Y_6|}{p} \right\rceil \geq |Y_6| - \sum_{k=3}^{\omega(n)} \left\lceil \frac{|Y_6|}{p_k} \right\rceil.$$

By $|X|$ taking the value in the fifth line of Table 1 for the corresponding $\omega(n)$, the right part above is greater than 0.

We complete the proof of Lemma 3.3. □

In the last line of Table 1, we add the lower bound of $\lfloor n^{\frac{1}{4}} \rfloor$, which is from $n^{\frac{1}{4}} \geq \left(\prod_{k=1}^{\omega(n)} p_k\right)^{\frac{1}{4}}$ for a given $\omega(n)$. From Table 1, Lemma 3.2 and Theorem 2.2, we can immediately get the below result.

Lemma 3.4.

(1). *If* $\omega(n) \geq 8$, *then* $\mathsf{MG}(n) \leq \lfloor n^{\frac{1}{4}} \rfloor$.
(2). *If* $\omega(n) \leq 7$, *then* $\mathsf{MG}(n) \leq 41$.

Now, we can confirm the question mentioned at the beginning of this section.

Theorem 3.5. *For any integer* $n \geq 2227$, *there is always an integer* $a \in [n^{\frac{1}{2}}, n^{\frac{1}{2}} + n^{\frac{1}{4}}]$ *such that* $\gcd(a, n) = 1$.

Proof. If $n \geq 41^4 = 2825761$, then $\lfloor n^{\frac{1}{4}} \rfloor \geq 41$. By Lemma 3.4, whatever $\omega(n) \geq 8$ or $\omega(n) \leq 7$, it holds that $\mathsf{MG}(n) \leq \lfloor n^{\frac{1}{4}} \rfloor$. Note that the interval $[n^{\frac{1}{2}}, n^{\frac{1}{2}} + n^{\frac{1}{4}}]$ contains at least $\lfloor n^{\frac{1}{4}} \rfloor$ consecutive integers. By the definition of $\mathsf{MG}(n)$, we know that there is always an integer $a \in [n^{\frac{1}{2}}, n^{\frac{1}{2}} + n^{\frac{1}{4}}]$ such that $\gcd(a, n) = 1$.

If $2227 \leq n \leq 2825760$, then with the help of a personal computer and within 2300 seconds, we check that there is always an integer $a \in [n^{\frac{1}{2}}, n^{\frac{1}{2}} + n^{\frac{1}{4}}]$ such that $\gcd(a, n) = 1$.

Actually, all the integers $n \geq 6$ for which the result does not hold make up the set $\{6, 10, 20, 28, 42, 54, 60, 66, 88, 130, 156, 170, 174, 204, 342, 414, 460, 540, 570, 930, 966, 1110, 1974, 2226\}$. It is of 24 integers and the maximum one is 2226.

This completes the proof of Theorem 3.5. □

4. The sharp bound of the zero-sum constant $\mathsf{N}(G)$

Let's turn back to the zero-sum theory mentioned in the introduction.

For $n \geq 2$, let

$$A_n := \min\{a + b \mid ab \geq n \text{ and } a, b \in \mathbb{N}\}$$

and

$$B_n := \min\{a+b \mid ab \geq n,\ \gcd(a,n-1)=1 \text{ and } a,b \in \mathbb{N}\}.$$

In [2] and [3], Gao et al. proved that $\lceil 2\sqrt{n}\rceil = A_n \leq B_n \leq \lceil 3\sqrt{n}\rceil$ for $n \geq 2$. And they found infinitely many n such that $B_n = A_n + 1$.

Lemma 4.1. *[3] Let $n = (3m)^2 - 3$ with m being a positive odd integer. Then $B_{n+1} = \lceil 2\sqrt{n+1}\rceil + 1$ and $\mathsf{N}(C_n) = 2n - B_{n+1} + 1 = 2n - \lceil 2\sqrt{n+1}\rceil$.*

Here, with the help of Theorem 3.5, we can give a very sharp bound of B_n.

Lemma 4.2. *For $n \geq 2$,*

$$\lceil 2\sqrt{n}\rceil \leq B_n \leq \lceil 2\sqrt{n}\rceil + 1.$$

Moreover, for each equality, there are infinitely many n making it hold.

Proof. In [3], Gao et al. has checked this result for $2 \leq n \leq 3001$. And Lemma 4.1 implies that there are infinitely many n such that $B_n = \lceil 2\sqrt{n}\rceil + 1$.

If $n-1$ is a square number, then let $n-1 = m^2$ with a positive integer m. Since

$$2m < 2\sqrt{n} = 2\sqrt{m^2+1} < 2m+1$$

for $m \geq 1$, it is easy to see that $B_n = 2m+1 = \lceil 2\sqrt{n}\rceil$. So there are infinitely many n such that $B_n = \lceil 2\sqrt{n}\rceil$.

Next, we assume that $n > 3001$ and $n-1$ is not a square number. We are just going to prove $B_n \leq \lceil 2\sqrt{n}\rceil + 1$.

Since $n-1 > 3000 > 2227$, Theorem 3.5 tells us that there is an integer $t \in [(n-1)^{\frac{1}{2}}, (n-1)^{\frac{1}{2}} + (n-1)^{\frac{1}{4}}]$ such that $\gcd(t, n-1) = 1$. On the other hand, since $n-1$ is not a square number by the assumption, there is no integer in the interval $[(n-1)^{\frac{1}{2}}, n^{\frac{1}{2}})$. It follows that

$$n^{\frac{1}{2}} \leq t < n^{\frac{1}{2}} + n^{\frac{1}{4}}.$$

Now we can give an upper bound of B_n.

$$\begin{aligned} B_n &= \min\{a+b \mid b \geq \frac{n}{a},\ \gcd(a,n-1)=1 \text{ and } a,b \in \mathbb{N}\} \\ &= \min\{a + \left\lceil \frac{n}{a} \right\rceil \mid 1 \leq a \leq n-1,\ \gcd(a,n-1)=1 \text{ and } a \in \mathbb{N}\} \\ &\leq \left\lceil t + \frac{n}{t} \right\rceil \\ &\leq \left\lceil n^{\frac{1}{2}} + n^{\frac{1}{4}} + \frac{n}{n^{\frac{1}{2}} + n^{\frac{1}{4}}} \right\rceil \end{aligned}$$

$$= \left\lceil n^{\frac{1}{2}}\left(1+n^{-\frac{1}{4}}+\frac{1}{1+n^{-\frac{1}{4}}}\right)\right\rceil$$
$$\leq \left\lceil n^{\frac{1}{2}}\left(1+n^{-\frac{1}{4}}+1-n^{-\frac{1}{4}}+n^{-\frac{1}{2}}\right)\right\rceil$$
$$= \left\lceil 2n^{\frac{1}{2}}+1\right\rceil,$$

where the fourth inequality is due to the fact that the function $x+\frac{n}{x}$ increases as x increases in the interval $[\sqrt{n}, +\infty)$ and the last second inequality holds since $(1+x)(1-x+x^2) = 1+x^3 > 1$ for $x > 0$.

Lemma 4.2 is proved. □

Lemma 4.3. *[3] For any cyclic group $G = C_n$ with $n \geq 3$,*

$$2n - B_{n+1} + 1 \leq \mathsf{N}(G) \leq 2n - A_{n+1} + 1.$$

Theorem 1.1 immediately follows from Lemma 4.1, Lemma 4.2 and Lemma 4.3.

5. A concluding remark

Lemma 4.1 gives an infinite class of n such that $B_{n+1} - A_{n+1} = 1$, which is the integer sequence $\{6(6t^2-6t+1)\}_{t=1}^{+\infty}$. Gao et al. in [3] checked that all the integers $2 \leq n \leq 3000$ such that $B_{n+1} > A_{n+1}$ are of the form $6(6t^2-6t+1)$.

Now, by the monotonicity of the function $x + \frac{n+1}{x}$ and setting $\sqrt{n+1}$ as the starting point, we can search faster than them with a personal computer. Within 50786 seconds (about 14 hours), we have checked it for $2 \leq n \leq 10^8$ and find more n such that $B_{n+1} > A_{n+1}$.

Lemma 5.1. *For integer $2 \leq n \leq 10^8$,*

$$B_{n+1} - A_{n+1} = \begin{cases} 1, & \text{if } n \in \{6(6t^2-6t+1)\}_{t=1}^{+\infty} \cup M; \\ 0, & \text{others,} \end{cases}$$

where M=\{1722630,2009280,4804800,16341780,17201730,45866730,47299980,90297480, 92304030\}. *Clearly,* $\{6(6t^2-6t+1)\}_{t=1}^{+\infty} \cap M = \emptyset$.

From the set M, we find four more classes of n such that $B_{n+1} = A_{n+1} + 1$. Here we summarize all the classes that we have got up to now.

Lemma 5.2. $B_{n+1} - A_{n+1} = 1$ *if n belongs to one of the below sets.*

(1). $T_1 := \{6(6t^2-6t+1)\}_{t=1}^{+\infty}$.
(2). $T_2 := \{2730(2730t^2-2835t+736)\}_{t=1}^{+\infty}$.
(3). $T_3 := \{2730(2730t^2-2625t+631)\}_{t=1}^{+\infty}$.

(4). $T_4 := \{30030(30030t^2 + 4384t + 160)\}_{t=0}^{+\infty}$.
(5). $T_5 := \{30030(30030t^2 - 4384t + 160)\}_{t=1}^{+\infty}$.

Proof. Let

$$\begin{aligned}\mathcal{A}_{n+1} :=&\{(a,b) \mid ab \geq n+1, a+b = \lceil 2\sqrt{n+1}\rceil, a,b \in \mathbb{N}, a \geq b\}\\ =&\{(a, \left\lceil \frac{n+1}{a}\right\rceil) \mid a + \left\lceil \frac{n+1}{a}\right\rceil = \lceil 2\sqrt{n+1}\rceil, a \in \mathbb{N}, a \geq \sqrt{n+1}\}.\end{aligned}$$

(1). See Proposition 5.2 in [3].

(2). If $n = 2730(2730t^2 - 2835t + 736)$ for $t \geq 1$, then let $n = d(d-1) - 26$ with $d = 1365(2t-1) - 52$ and so

$$(d-1)^2 < n+1 < d(d-1),$$

which implies $\lceil\sqrt{n+1}\rceil = d$ and $A_{n+1} = \lceil 2\sqrt{n+1}\rceil = 2d-1 = 2730(2t-1)-105$. Since $(d+5) + \lceil\frac{n+1}{d+5}\rceil = 2d > 2d-1$, we have

$$\mathcal{A}_{n+1} = \{(d,d-1),(d+1,d-2),(d+2,d-3),(d+3,d-4),(d+4,d-5)\}.$$

It is easy to check that every integer in the interval $[d-5, d+4] = [1365(2t-1) - 57, 1365(2t-1) - 48]$ is not relatively prime to n since $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$. It follows from the definition of B_n that $B_{n+1} > A_{n+1}$. Then by Lemma 4.2, $B_{n+1} = A_{n+1} + 1$.

(3). If $n = 2730(2730t^2 - 2625t + 631)$ for $t \geq 1$, then let $n = d(d-1) - 26$ with $d = 1365(2t-1) + 53$. By a similar proof as the previous one, $B_{n+1} = A_{n+1} + 1$.

(4). If $n = 30030(30030t^2 + 4384t + 160)$ for $t \geq 0$, then let $n = d^2 - 64$ with $d = 30030t + 2192$ and so

$$(d-1)^2 < n+1 < d^2,$$

which implies $\lceil\sqrt{n+1}\rceil = d$ and $A_{n+1} = \lceil 2\sqrt{n+1}\rceil = 2d = 60060t + 4384$. Since $(d+8) + \lceil\frac{n+1}{d+8}\rceil = 2d+1 > 2d$, we have

$$\begin{aligned}\mathcal{A}_{n+1} = \{&(d,d),(d+1,d-1),(d+2,d-2),(d+3,d-3),\\ &(d+4,d-4),(d+5,d-5),(d+6,d-6),(d+7,d-7)\}.\end{aligned}$$

It is easy to check that every integer in the interval $[d-7, d+7] = [30030t+2185, 30030t+2199]$ is not relatively prime to n since $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$. It follows from the definition of B_n that $B_{n+1} > A_{n+1}$. Then by Lemma 4.2, $B_{n+1} = A_{n+1} + 1$.

(5). If $n = 30030(30030t^2 - 4384t + 160)$ for $t \geq 1$, then let $n = d^2 - 64$ with $d = 30030t - 2192$. Similarly, $B_{n+1} = A_{n+1} + 1$.

This completes the proof. □

Clearly, $1722630, 16341780, 45866730, 90297480 \in T_2$, $2009280, 17201730, 47299980, 92304030 \in T_3$, $4804800 \in T_4$ and $\min T_5 = 774954180 > 10^8$. T_1 can be written as $\{(6t-3)^2-3\}_{t=1}^{+\infty}$. T_2 and T_3 can be combined into $\{2730(1+105(2t-1)(13t-\frac{13\pm1}{2}))\}_{t=1}^{+\infty}$. And T_4 and T_5 can be combined into $\{(30030t \pm 2192)^2 - 64\}_{t=0}^{+\infty}$ too.

We conjecture that there are more classes of n such that $B_{n+1} = A_{n+1} + 1$. But to find them is beyond our computing power at present. To determine the explicit value of B_n for all integer n is still an open problem with an elementary description and very important for the zero-sum constant $\mathsf{N}(G)$.

Data availability

No data was used for the research described in the article.

Acknowledgment

The authors wish to thank W. Gao for his kind guidance and useful suggestions, and the anonymous referee for careful reading of the manuscript and helpful comments. This work is supported in part by National Natural Science Foundation of China with Grant No. 12071344.

References

[1] W. Gao, A. Geroldinger, Zero-sum problems in finite abelian groups: a survey, Expo. Math. 24 (2006) 337–369.
[2] W. Gao, S. Hong, W. Hui, X. Li, Q. Yin, P. Zhao, Representation of zero-sum invariants by sets of zero-sum sequences over a finite abelian group, Period. Math. Hung. 85 (2022) 52–71.
[3] W. Gao, S. Hong, W. Hui, X. Li, Q. Yin, P. Zhao, Representation of zero-sum invariants by sets of zero-sum sequences over a finite abelian group II, J. Number Theory 241 (2022) 738–760.
[4] W. Gao, Y. Li, J. Peng, G. Wang, A unifying look at zero-sum invariants, Int. J. Number Theory 14 (2018) 705–711.
[5] A. Geroldinger, Additive group theory and non-unique factorizations, in: A. Geroldinger, I. Ruzsa (Eds.), Combinatorial Number Theory and Additive Group Theory, in: Advanced Courses in Mathematics, CRM Barcelona, Birkhäuser, 2009, pp. 1–86.
[6] A. Geroldinger, F. Halter-Koch, Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory, Pure Appl. Math., vol. 278, Chapman & Hall/CRC, Boca Raton, 2006.
[7] J.B. Rosser, L. Schoenfeld, Approximate formulas for some functions of prime numbers, Ill. J. Math. 6 (1962) 64–94.
[8] J.B. Rosser, L. Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$, Math. Comput. 29 (1975) 243–269.