LENGTH OF THE LONGEST ARITHMETIC PROGRESSIONS IN A CERTAIN REDUCED RESIDUE SYSTEM

Chaninat Phothila
Department of Mathematics, Khon Kaen University, Khon Kaen, Thailand
chaninat.p@kkumail.com

Natthakan Thoket
Department of Mathematics, Khon Kaen University, Khon Kaen, Thailand
natthakan.tho@kkumail.com

Narakorn Rompurk Kanasri[1]
Department of Mathematics, Khon Kaen University, Khon Kaen, Thailand
naraka@kku.ac.th

Received: 2/19/25, Revised: 8/19/25, Accepted: 11/27/25, Published: 1/5/26

Abstract

For any integers m and n with $n > 1$, let

$$R_m(n) := \{a \in \mathbb{Z} \mid m+1 \le a \le m+n, \gcd(a,n) = 1\}$$

be a reduced residue system modulo n. Denote by $f_m(n)$ the length of the longest arithmetic progressions contained in $R_m(n)$. In this paper, we establish an explicit formula for $f_{-\lceil n/2 \rceil}(n)$, where $\lceil x \rceil$ is the smallest integer larger than or equal to x. Moreover, explicit formulas for $\max\limits_{m\in\mathbb{Z}} f_m(n)$ and $\min\limits_{m\in\mathbb{Z}} f_m(n)$ are also verified.

1. Introduction

Given integers $m, n \in \mathbb{Z}$ with $n > 1$, let

$$R_m(n) := \{a \in \mathbb{Z} \mid m+1 \le a \le m+n, \gcd(a,n) = 1\}$$

be a reduced residue system modulo n. Denote by $f_m(n)$ the length of the longest arithmetic progressions contained in $R_m(n)$. It is noted that $R_0(n)$ is the least positive reduced residue system modulo n, namely,

$$R_0(n) = \{a \in \mathbb{Z} \mid 1 \le a \le n, \gcd(a,n) = 1\}.$$

DOI: 10.5281/zenodo.18154061
[1]Corresponding author.

In [2], Recamán asked if $f_0(n) \to \infty$ as $n \to \infty$, that is, if, for each positive integer k, there exists a constant n_k such that $R_0(n)$ contains an arithmetic progression of length k for all $n \geq n_k$. Throughout this article, let $\mathrm{gpf}(n)$ be the largest prime factor of n and $\mathrm{rad}(n)$ be the product of all distinct prime factors of n. In 2017, Stumpf [5] answered this problem affirmatively and also gave the bounds as

$$\max\left\{\frac{\mathrm{gpf}(n)-1}{2}, \frac{n}{\mathrm{rad}(n)}\right\} \leq f_0(n) \leq \max\left\{\mathrm{gpf}(n)-1, \frac{n}{\mathrm{rad}(n)}\right\}.$$

For any real number x, let $\lfloor x \rfloor$ denote the largest integer less than or equal to x and $\lceil x \rceil$ denote the smallest integer larger than or equal to x. In 2018, Pongsriiam [4] established an explicit formula for $f_0(n)$ as follows.

(i) If $n > 1$ is squarefree, then

$$f_0(n) = \begin{cases} p-1 & \text{if } n = p \text{ is a prime,} \\ \frac{p+1}{2} & \text{if } n = 2p, p \text{ is an odd prime, } p \equiv 3 \pmod 4, \\ \mathrm{gpf}(n) - \left\lfloor \frac{\mathrm{gpf}(n)^2}{n} \right\rfloor - 1 & \text{otherwise.} \end{cases}$$

(ii) If $n = p^r$, where p is a prime and $r > 1$, then $f_0(n) = p^{r-1}$.

(iii) If $n > 1$ is not a prime power and is not squarefree, then

$$f_0(n) = \max\left\{\frac{n}{\mathrm{rad}(n)}, \mathrm{gpf}(n)-1\right\}.$$

In addition, let

$$F(n) = \max\{f_B(n) \mid B(n) \text{ is a reduced residue system modulo } n\},$$

where $f_B(n)$ is the length of the longest arithmetic progressions contained in $B(n)$. Note that $f_{R_0(n)}(n) = f_0(n)$. He also gave an explicit formula for $F(n)$ [4] as

$$F(n) = \max\left\{\frac{n}{\mathrm{rad}(n)}, \mathrm{gpf}(n)-1\right\}. \tag{1}$$

In the same year, Chen and Lei [1] gave an asymptotic formula for $\sum_{n \leq x} f_0(n)$, thereby solving a problem posed by Pongsriiam in [4].

It thus seems natural to study the same problem for another reduced residue system. In this article, we are interested in the reduced residue system modulo n, $R(n) := R_{-\lceil n/2 \rceil}(n)$. We note from [3] that

$$R(n) = \begin{cases} \left\{a \in \mathbb{Z} \mid -\frac{n-1}{2} \leq a \leq \frac{n-1}{2}, \gcd(a,n) = 1\right\} & \text{if } n \text{ is odd,} \\ \left\{a \in \mathbb{Z} \mid -\frac{n-2}{2} \leq a \leq \frac{n}{2}, \gcd(a,n) = 1\right\} & \text{if } n \text{ is even.} \end{cases} \tag{2}$$

It should be noted that the above choice of $R(n)$, the set of absolute least residues modulo n that are relatively prime to n, is crucial to our work, for it provides the most convenient way to choose the representatives closest to 0 within each residue class. This yields a system containing the smallest possible absolute residues, which in turn considerably simplifies our calculation. For convenience, we let $g(n) := f_{-\lceil n/2 \rceil}(n)$, the length of the longest arithmetic progressions contained in $R(n)$. This work aims to establish an explicit formula for $g(n)$ for all positive integers $n > 1$. We found that the case of squarefree integers is more complicated than the other. However, we successfully obtain an explicit formula for $g(n)$ for all positive integers n except for the case n being an even squarefree integer having at least three prime factors. In such a case, we obtain bounds for $g(n)$ and an explicit formula for $g(n)$ under a certain condition. In addition, we establish an explicit formula for $\max_{m \in \mathbb{Z}} f_m(n)$ for all positive integers $n > 1$. An explicit formula for $\min_{m \in \mathbb{Z}} f_m(n)$ is also verified, where n is a prime power. When n is neither a prime power nor a squarefree integer, we obtain bounds for $\min_{m \in \mathbb{Z}} f_m(n)$ and an explicit formula for $\min_{m \in \mathbb{Z}} f_m(n)$ under a certain condition.

2. Main Results

In this section, we define $f_m(d, n)$ as the length of the longest arithmetic progressions contained in $R_m(n)$ with common difference d. We begin with the following auxiliary lemma, which will be used to establish an explicit formula for $g(n)$. Its proof is similar to the proof of Lemma 2.1 in [4].

Lemma 1. *For any integers $m, n, d \in \mathbb{Z}$ with $n > 1$ and $d > 0$, the following statements hold.*

(i) If p is a prime such that $p \mid n$ and $p \nmid d$, then $f_m(d, n) \leq p - 1$.

(ii) If n is squarefree, then $f_m(d, n) \leq \operatorname{gpf}(n) - 1$.

Proof. (i) Let $b, b+d, b+2d, \ldots, b+(s-1)d$ be an arithmetic progression contained in the complete residue system modulo n defined by $\{m+1, m+2, \ldots, m+n\}$, where b is an integer. By the division algorithm, there exist integers q and r such that $s = pq + r$, where $0 \leq r < p$. Let

$$\begin{aligned}
A_0 &= \{b, b+d, \ldots, b+(p-1)d\}, \\
A_1 &= \{b+pd, b+(p+1)d, \ldots, b+(2p-1)d\}, \\
&\vdots \\
A_{q-1} &= \{b+(q-1)pd, b+((q-1)p+1)d, \ldots, b+(qp-1)d\}.
\end{aligned}$$

Then,

$$\{b, b+d, \ldots, b+(s-1)d\} = A_0 \cup A_1 \cup \ldots \cup A_{q-1} \cup \\ \{b+qpd, b+(qp+1)d, \ldots, b+(qp+r-1)d\}.$$

One can see that A_i is a complete residue system modulo p for all $i \in \{0, 1, \ldots, q-1\}$. Consequently, there exists a unique integer $k \in \{0, 1, \ldots, p-1\}$ such that

$$b + (ip+k)d \in A_i \text{ and } p \mid (b + (ip+k)d)$$

for each $i \in \{0, 1, \ldots, q-1\}$. This implies $f_m(d, n) \leq p - 1$.
(ii) Assume that n is squarefree. If $d \geq n$, then $f_m(d, n) = 1 \leq \operatorname{gpf}(n) - 1$ because $a + d \geq m + 1 + n$ for all $a \in R_m(n)$. Assume that $d < n$. Since n is squarefree, there must exist a prime factor q of n such that $q \nmid d$. From (i), it follows that $f_m(d, n) \leq q - 1 \leq \operatorname{gpf}(n) - 1$ as desired. □

For the case $m = -\lceil n/2 \rceil$, we let $g(d, n) := f_{-\lceil n/2 \rceil}(d, n)$ and we are now ready to establish an explicit formula for $g(n)$ as in the following theorem.

Theorem 1. *For any positive integer $n > 1$, let $d = n/\operatorname{gpf}(n)$.*
If n is odd, then

$$g(n) = \begin{cases} \frac{p-1}{2} & \text{if } n = p \text{ is a prime and } p \equiv 1 \pmod 4, \\ \frac{p+1}{2} & \text{if } n = p \text{ is a prime and } p \equiv 3 \pmod 4, \\ p^{r-1} & \text{if } n = p^r, p \text{ is a prime and } r > 1, \\ \left\lfloor \operatorname{gpf}(n) - \frac{\operatorname{gpf}(n)+1}{2d} \right\rfloor & \text{if } n \text{ is squarefree but is not a prime}, \\ \max\left\{ \frac{n}{\operatorname{rad}(n)}, \operatorname{gpf}(n) - 1 \right\} & \text{if } n \text{ is not a prime power and is not squarefree.} \end{cases}$$

If n is even, then

$$g(n) = \begin{cases} 2^{r-1} & \text{if } n = 2^r \text{ and } r \geq 1, \\ p - 1 & \text{if } n = 2p \text{ and } p \text{ is an odd prime}, \\ \max\left\{ \frac{n}{\operatorname{rad}(n)}, \operatorname{gpf}(n) - 1 \right\} & \text{if } n \text{ is not a prime power and is not squarefree.} \end{cases}$$

Moreover, if n is an even squarefree integer having at least three prime factors, then

$$\left\lfloor \operatorname{gpf}(n) - \frac{2\operatorname{gpf}(n)}{d} \right\rfloor \leq g(n) \leq \operatorname{gpf}(n) - 1. \tag{3}$$

In particular, if $d \geq 2\operatorname{gpf}(n)$, then $g(n) = \operatorname{gpf}(n) - 1$.

Proof of Theorem 1 for n odd. Let $n > 1$ be an odd positive integer. By Equation (2), we have

$$R(n) = \left\{ a \in \mathbb{Z} \mid -\frac{n-1}{2} \leq a \leq \frac{n-1}{2}, \gcd(a,n) = 1 \right\}.$$

We divide the proof into four cases as follows.

`Case 1:` $n = p$, where p is a prime. Then,

$$R(p) = \left\{ -\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 1, \ldots, \frac{p-3}{2}, \frac{p-1}{2} \right\}.$$

It can be seen that $-(p-1)/2, -(p-3)/2, \ldots, -1$ and $1, \ldots, (p-3)/2, (p-1)/2$ are the longest arithmetic progressions contained in $R(p)$ with common difference $d = 1$ and have length $(p-1)/2$. For $d \geq 2$, we consider the following two subcases.

`Subcase (i)` $p \equiv 1 \pmod 4$. Then, $(p-1)/2$ is even, and thus

$$-\frac{p-3}{2}, \ldots, -1, 1, \ldots, \frac{p-3}{2}$$

is the longest arithmetic progression contained in $R(p)$ with common difference $d = 2$ and has length $(p-1)/2$. Clearly, any arithmetic progression contained in $R(p)$ with common difference $d > 2$ always has length less than $(p-1)/2$. This shows that $g(n) = (p-1)/2$.

`Subcase (ii)` $p \equiv 3 \pmod 4$. Then, $(p-1)/2$ is odd, and thus

$$-\frac{p-1}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2}$$

is the longest arithmetic progression contained in $R(p)$ with common difference $d = 2$ and has length $(p+1)/2$. Clearly, any arithmetic progression contained in $R(p)$ with common difference $d > 2$ always has length less than $(p+1)/2$. This means that $g(n) = (p+1)/2$ as desired.

`Case 2:` $n = p^r$, where p is a prime and $r > 1$. Then,

$$R(p^r) = \left\{ a \in \mathbb{Z} \mid -\frac{p^r-1}{2} \leq a \leq \frac{p^r-1}{2}, \gcd(a,p^r) = 1 \right\}.$$

We first show that the arithmetic progression of length p^{r-1} defined by

$$-\frac{p^r-1}{2}, -\frac{p^r-1}{2} + p, -\frac{p^r-1}{2} + 2p, \ldots, -\frac{p^r-1}{2} + \left(p^{r-1} - 1\right) p$$

is contained in $R(p^r)$.

For any $i \in \{0, 1, \dots, p^{r-1}-1\}$, we have

$$-\frac{p^r-1}{2} \le -\frac{p^r-1}{2} + ip \le -\frac{p^r-1}{2} + \left(p^{r-1}-1\right)p = \frac{p^r-(2p-1)}{2} < \frac{p^r-1}{2}.$$

If $p \mid (-(p^r-1)/2 + ip)$, then $p \mid (p^r-1)/2$ and thus $p \mid (p^r-1)$, a contradiction. It follows that $\gcd\left(-(p^r-1)/2 + ip, p^r\right) = 1$. This shows that $-(p^r-1)/2+ip \in R(p^r)$ for all $i \in \{0, 1, \dots, p^{r-1}-1\}$, which implies that $g(n) \ge p^{r-1}$.

Let $a_1, a_2, \dots, a_s$ be any arithmetic progression contained in $R(p^r)$ with common difference d_0. We will show that $s \le p^{r-1}$. Consider the following two subcases.

`Subcase (i)` $p \mid d_0$. Then, $p \le d_0$. Suppose to the contrary that $s > p^{r-1}$. Then,

$$\frac{p^r-1}{2} \ge a_s = a_1 + (s-1)d_0 \ge -\frac{p^r-1}{2} + p^{r-1}p = \frac{p^r+1}{2},$$

which is a contradiction.

`Subcase (ii)` $p \nmid d_0$. By Lemma 1(i), we obtain $s \le g(d_0, n) \le p-1 < p^{r-1}$.
From both subcases, we deduce that $s \le p^{r-1}$ and hence $g(n) \le p^{r-1}$.

Since $g(n) \ge p^{r-1}$ and $g(n) \le p^{r-1}$, we obtain $g(n) = p^{r-1}$ as required.

`Case 3:` $n = p_1 p_2 \cdots p_m$, where p_i's are odd primes such that $p_1 < p_2 < \ldots < p_m$ with $m \ge 2$. Let $d = n/p_m$ and $k = \lfloor p_m - (p_m+1)/2d \rfloor$. We first show that the arithmetic progression of length k defined by

$$-\frac{n-1}{2} + \frac{p_m-1}{2} + d, -\frac{n-1}{2} + \frac{p_m-1}{2} + 2d, \dots, -\frac{n-1}{2} + \frac{p_m-1}{2} + kd$$

is contained in $R(n)$. Note that $k \le p_m - 1$ and let $y = -(n-1)/2 + (p_m-1)/2$.

For any $i \in \{1, 2, \dots, k\}$, we have

$$-\frac{n-1}{2} < y + id \le y + kd \le y + \left(p_m - \frac{p_m+1}{2d}\right)d = y + n - \frac{p_m+1}{2} = \frac{n-1}{2}.$$

For each $j \in \{1, 2, \dots, m-1\}$, if $p_j \mid y$, then $p_j \mid 2y$ and hence $p_j \mid (p_m - n)$, which is impossible. Thus, $\gcd(y, p_j) = 1$, implying that $\gcd(y + id, d) = \gcd(y, d) = 1$. One can see that $p_m \mid 2y$, and thus $p_m \mid y$ because p_m is odd. Consequently, $\gcd(y + id, p_m) = \gcd(id, p_m) = 1$ and thus $\gcd(y + id, n) = 1$. This shows that $y + id \in R(n)$ for all $i \in \{1, 2, \dots, k\}$, yielding $g(n) \ge k$.

Let $a_1, a_2, \dots, a_s$ be any arithmetic progression contained in $R(n)$ with common difference d_0. We will show that $s \le k$. If $d \ge (p_m+1)/2$, then $k = p_m - 1$. By Lemma 1(ii), we obtain $s \le g(d_0, n) \le p_m - 1 = k$. Now we assume that $d < (p_m+1)/2$ and consider the following two subcases.

`Subcase (i)` $d \nmid d_0$. Then, there exists $j \in \{1, \dots, m-1\}$ such that $p_j \nmid d_0$. By Lemma 1(i), we obtain

$$s \le g(d_0, n) \le p_j - 1 \le d - 1. \tag{4}$$

Note that $p_m - \lfloor (p_m+1)/2d \rfloor - 1 \le k$. Since $d < (p_m+1)/2$, we have

$$2dp_m - p_m - 1 = (2d-1)p_m - 1 > (2d-1)^2 - 1 = 4d(d-1) > 2d^2$$

because $d = n/p_m \ge 3$. It follows that

$$d < \frac{2dp_m - p_m - 1}{2d} = p_m - \frac{p_m+1}{2d} \le p_m - \left\lfloor \frac{p_m+1}{2d} \right\rfloor. \tag{5}$$

Using Equations (4) and (5), we consequently have

$$s < p_m - \left\lfloor \frac{p_m+1}{2d} \right\rfloor - 1 \le k.$$

`Subcase (ii)` $d \mid d_0$. Then, there exists a positive integer c such that $d_0 = dc$. Suppose to the contrary that $s > k$. If $c \ge 2$, then

$$\begin{aligned}
\frac{n-1}{2} &\ge a_s = a_1 + (s-1)d_0 \\
&\ge -\frac{n-1}{2} + 2kd \\
&> -\frac{n-1}{2} + \left(p_m - \frac{p_m+1}{2d} - 1\right)2d \\
&= -\frac{n-1}{2} + 2n - p_m - 1 - 2d \\
&> -\frac{n-1}{2} + 2n - p_m - 1 - p_m - 1 \\
&= \frac{n + 2n - 4p_m - 3}{2} \\
&> \frac{n+1}{2}
\end{aligned}$$

because $2n - 4p_m - 3 \ge 2 \cdot 3p_m - 4p_m - 3 = 2p_m - 3 > 1$. However, this is impossible, so $c = 1$ and thus $d_0 = d$. Now we have

$$p_m - \frac{p_m+1}{2d} - 1 < k \le p_m - \frac{p_m+1}{2d} < p_m - 1.$$

It follows that

$$kd \le n - \frac{p_m+1}{2} < (k+1)d \tag{6}$$

and thus

$$n - \frac{p_m+1}{2} - d < kd. \tag{7}$$

Since $s - 1 \ge k$ and $d_0 = d$, the sequence $a_1, a_1+d, a_1+2d, \ldots, a_1+kd$ belongs to $R(n)$. One can see that $\{a_1, a_1+d, a_1+2d, \ldots, a_1+(p_m-1)d\}$ is a complete residue system modulo p_m. Since $k < p_m - 1$, there exists $l \in \{k+1, \ldots, p_m-1\}$

such that $p_m \mid (a_1 + ld)$, so $a_1 + ld = p_m r$ for some integer r. By Equation (6), we obtain

$$p_m r = a_1 + ld \geq -\frac{n-1}{2} + (k+1)d > -\frac{n-1}{2} + n - \frac{p_m+1}{2} = \frac{n-p_m}{2} > 0,$$

so $r \geq 1$ and $(2r+1)p_m > n$. We have $a_1 + kd \leq (n-1)/2$, and using Equation (7), we obtain

$$a_1 \leq \frac{n-1}{2} - kd < \frac{n-1}{2} - \left(n - \frac{p_m+1}{2} - d\right) = \frac{-n+p_m+2d}{2},$$

yielding $p_m r - ld < (-n + p_m + 2d)/2$. It follows that

$$(2r-1)p_m + n < 2ld + 2d \leq 2(p_m-1)d + 2d = 2n$$

and thus $(2r-1)p_m < n$. Hence, $(2r-1)p_m < n < (2r+1)p_m$, which implies that $d = n/p_m = 2r$, a contradiction because d is odd. This shows that $s \leq k$ and thus $g(n) \leq k$. Therefore, $g(n) = k$ as desired.

Case 4: $n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$, where r_i's are positive integers, p_i's are odd primes such that $p_1 < p_2 < \ldots < p_m$ with $m \geq 2$, and n is not squarefree. We first show that $g(n) \geq n/\operatorname{rad}(n)$ by showing that the arithmetic progression of length n/d defined by

$$-\frac{n-1}{2}, -\frac{n-1}{2} + d, -\frac{n-1}{2} + 2d, \ldots, -\frac{n-1}{2} + \left(\frac{n}{d} - 1\right) d$$

is contained in $R(n)$, where $d = \operatorname{rad}(n)$.

For any $i \in \{0, 1, 2, \ldots, n/d - 1\}$, we have

$$-\frac{n-1}{2} \leq -\frac{n-1}{2} + id \leq -\frac{n-1}{2} + \left(\frac{n}{d} - 1\right) d = \frac{n-2d+1}{2} < \frac{n-1}{2}.$$

For each $j \in \{1, 2, \ldots, m\}$, if $p_j \mid -(n-1)/2$, then $p_j \mid (n-1)$, which is impossible. Thus, $\gcd(-(n-1)/2, p_j) = 1$. It follows that $\gcd(-(n-1)/2 + id, d) = 1$ and hence $\gcd(-(n-1)/2 + id, n) = 1$. This shows that $-(n-1)/2 + id \in R(n)$ for all $i \in \{0, 1, 2, \ldots, n/d - 1\}$.

Next, we show that $g(n) \geq p_m - 1$ by showing that the arithmetic progression of length $p_m - 1$ defined by

$$-p_m + d, -p_m + 2d, -p_m + (p_m - 1)d$$

is contained in $R(n)$, where $d = \operatorname{rad}(n)/p_m$.

For any $i \in \{1, 2, \ldots, p_m - 1\}$, we have

$$\begin{aligned} -\frac{n-1}{2} &= -\left(\frac{p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m - 1}}{2}\right) p_m + \frac{1}{2} \\ &< -p_m + \frac{1}{2} \\ &< -p_m + id \\ &\leq -p_m + (p_m - 1)\frac{\operatorname{rad}(n)}{p_m} \\ &= p_1 p_2 \cdots p_m - (p_1 p_2 \cdots p_{m-1} + p_m) \\ &< p_1 p_2 \cdots p_m - \frac{1}{2} \\ &= \frac{2p_1 p_2 \cdots p_m - 1}{2} \\ &< \frac{p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} - 1}{2} \\ &= \frac{n-1}{2} \end{aligned}$$

since n is not squarefree. Moreover, $\gcd(-p_m + id, p_m) = \gcd(id, p_m) = 1$ and $\gcd(-p_m + id, d) = \gcd(-p_m, d) = 1$. It follows that $\gcd(-p_m + id, \operatorname{rad}(n)) = 1$ and thus $\gcd(-p_m + id, n) = 1$. This shows that $-p_m + id \in R(n)$ for all $i \in \{1, 2, \ldots, p_m - 1\}$. Now, we have $g(n) \geq n/\operatorname{rad}(n)$ and $g(n) \geq p_m - 1$, yielding

$$g(n) \geq \max\left\{\frac{n}{\operatorname{rad}(n)}, p_m - 1\right\}. \tag{8}$$

Let $a_1, a_2, \ldots, a_s$ be any arithmetic progression contained in $R(n)$ with common difference d_0. We treat the following two subcases.

`Subcase (i)` $\operatorname{rad}(n) \nmid d_0$. Then, there exists $j \in \{1, 2, \ldots, m\}$ such that $p_j \nmid d_0$. By Lemma 1(i), we obtain

$$s \leq g(d_0, n) \leq p_j - 1 \leq p_m - 1 \leq \max\left\{\frac{n}{\operatorname{rad}(n)}, p_m - 1\right\}.$$

`Subcase (ii)` $\operatorname{rad}(n) \mid d_0$. Then, $d_0 \geq \operatorname{rad}(n)$. If $s > n/\operatorname{rad}(n)$, then

$$\frac{n-1}{2} \geq a_s = a_1 + (s-1)d_0 \geq -\frac{n-1}{2} + \frac{n}{\operatorname{rad}(n)} \cdot \operatorname{rad}(n) = \frac{n+1}{2},$$

which is a contradiction. Thus, $s \leq n/\operatorname{rad}(n) \leq \max\{n/\operatorname{rad}(n), p_m - 1\}$. From both subcases, we deduce that

$$g(n) \leq \max\left\{\frac{n}{\operatorname{rad}(n)}, p_m - 1\right\}. \tag{9}$$

The desired result then follows from Equations (8) and (9). □

Proof of Theorem 1 for n even. Let n be an even positive integer. By Equation (2), we have

$$R(n) = \left\{ a \in \mathbb{Z} \mid -\frac{n-2}{2} \le a \le \frac{n}{2}, \gcd(a,n) = 1 \right\}.$$

We divide the proof of Theorem 1 into three cases as follows.

`Case 1:` $n = 2^r$, where $r \ge 1$. If $r = 1$, then $R(2) = \{1\}$ and thus $g(2) = 1 = 2^{1-1}$. Assuming that $r \ge 2$, we have

$$R(2^r) = \left\{ -2^{r-1}+1, \ldots, -1, 1, \ldots, 2^{r-1}-1 \right\}.$$

It is clear that $-2^{r-1}+1, \ldots, -1, 1, \ldots, 2^{r-1}-1$ is an arithmetic progression of length 2^{r-1}, so $g(2^r) = 2^{r-1}$.

`Case 2:` $n > 2$ is an even squarefree integer. If $n = 2p$, where p is an odd prime number, then

$$R(n) = \{-(p-2), -(p-4), \ldots, -1, 1, \ldots, p-4, p-2\}.$$

It is clear that $-(p-2), -(p-4), \ldots, -1, 1, \ldots, p-4, p-2$ is an arithmetic progression of length $p-1$, which implies that $g(n) = p-1$.

Assume now that $n = 2p_1p_2\cdots p_m$, where p_i's are odd primes such that $p_1 < p_2 < \ldots < p_m$ with $m \ge 2$. Let $d = n/p_m$ and $k = \lfloor p_m - 2p_m/d \rfloor$. We first show that the arithmetic progression of length k defined by

$$-\frac{n-2}{2} + (2p_m - 1) + d, -\frac{n-2}{2} + (2p_m - 1) + 2d, \ldots, -\frac{n-2}{2} + (2p_m - 1) + kd$$

is contained in $R(n)$. Note that $k \le p_m - 1$ and let $y = -(n-2)/2 + (2p_m - 1)$.

For any $i \in \{1, 2, \ldots, k\}$, we have

$$-\frac{n-2}{2} < y + id \le y + kd \le y + \left(p_m - \frac{2p_m}{d} \right) d = y + n - 2p_m = \frac{n}{2}.$$

It is clear that y is odd. For each $j \in \{1, 2, \ldots, m-1\}$, if $p_j \mid y$, then $p_j \mid 2y$ and hence $p_j \mid (4p_m - n)$, which is impossible. Thus, $\gcd(y, p_j) = 1$, so $\gcd(y+id, d) = 1$. One can see that $p_m \nmid 2y$, so $p_m \nmid y$ because p_m is odd. Consequently, $\gcd(y+id, p_m) = 1$ and thus $\gcd(y+id, n) = 1$. This shows that $y + id \in R(n)$ for all $i \in \{1, 2, \ldots, k\}$, yielding $g(n) \ge k$. By Lemma 1(ii), we obtain $g(n) \le p_m - 1$. This proves Equation (3).

In particular, if $d \ge 2p_m$, then $k = p_m - 1$ and hence $g(n) = p_m - 1$ as desired.

`Case 3:` $n = 2^{r_0}p_1^{r_1}\cdots p_m^{r_m}$, where r_i's are positive integers, p_i's are odd primes such that $p_1 < \ldots < p_m$, and n is not squarefree. We first show that $g(n) \ge n/\operatorname{rad}(n)$ by considering the following two subcases.

`Subcase (i)` $r_0 = 1$. Then, $(n-4)/2$ is odd. We show that the arithmetic progression of length n/d defined by

$$-\frac{n-4}{2}, -\frac{n-4}{2}+d, -\frac{n-4}{2}+2d, \ldots, -\frac{n-4}{2}+\left(\frac{n}{d}-1\right)d$$

is contained in $R(n)$, where $d = \operatorname{rad}(n)$.

For any $i \in \{0, 1, 2, \ldots, n/d - 1\}$, we have

$$-\frac{n-2}{2} \leq -\frac{n-4}{2} + id \leq -\frac{n-4}{2} + \left(\frac{n}{d}-1\right)d = \frac{n-2d+4}{2} < \frac{n}{2}.$$

If $2 \mid (n-4)/2$, then $2 \mid n/2$, which is impossible. Thus, $\gcd(-(n-4)/2+id, 2) = 1$. For each $j \in \{1, 2, \ldots, m\}$, if $p_j \mid (n-4)/2$, then $p_j \mid (n-4)$, which is impossible. Thus, $\gcd(-(n-4)/2+id, p_j) = 1$. It follows that $\gcd(-(n-4)/2+id, n) = 1$. This shows that $-(n-4)/2 + id \in R(n)$ for all $i \in \{0, 1, 2, \ldots, n/d - 1\}$.

`Subcase (ii)` $r_0 > 1$. Then, $(n-2)/2$ is odd. We show that the arithmetic progression of length n/d defined by

$$-\frac{n-2}{2}, -\frac{n-2}{2}+d, -\frac{n-2}{2}+2d, \ldots, -\frac{n-2}{2}+\left(\frac{n}{d}-1\right)d$$

is contained in $R(n)$, where $d = \operatorname{rad}(n)$.

For any $i \in \{0, 1, 2, \ldots, n/d - 1\}$, we have

$$-\frac{n-2}{2} \leq -\frac{n-2}{2} + id \leq -\frac{n-2}{2} + \left(\frac{n}{d}-1\right)d = \frac{n-2d+2}{2} < \frac{n}{2}.$$

If $2 \mid (n-2)/2$, then $2 \mid 1$, which is impossible. Thus, $\gcd(-(n-2)/2+id, 2) = 1$. For each $j \in \{1, 2, \ldots, m\}$, if $p_j \mid (n-2)/2$, then $p_j \mid (n-2)$, which is impossible. Thus, $\gcd(-(n-2)/2+id, p_j) = \gcd(-(n-2)/2, p_j) = 1$. It follows that $\gcd(-(n-2)/2+id, 2p_1 \cdots p_m) = 1$ and hence $\gcd(-(n-2)/2+id, n) = 1$. This shows that $-(n-2)/2 + id \in R(n)$ for all $i \in \{0, 1, 2, \ldots, n/d - 1\}$.

From both subcases, we obtain $g(n) \geq n/d = n/\operatorname{rad}(n)$. Next, we show that $g(n) \geq p_m - 1$ by showing that the arithmetic progression of length $p_m - 1$ defined by

$$-p_m + d, -p_m + 2d, -p_m + (p_m - 1)d$$

is contained in $R(n)$, where $d = \operatorname{rad}(n)/p_m$.

For any $i \in \{1, 2, \ldots, p_m - 1\}$, we have

$$\begin{aligned}
-\frac{n-2}{2} &= -\left(\frac{2^{r_0} p_1^{r_1} \cdots p_m^{r_m - 1}}{2}\right) p_m + 1 \\
&< -p_m + 1 \\
&< -p_m + id \\
&\le -p_m + (p_m - 1)\frac{\operatorname{rad}(n)}{p_m} \\
&= 2p_1 \cdots p_m - (2p_1 \cdots p_{m-1} + p_m) \\
&< 2^{r_0 - 1} p_1^{r_1} \cdots p_m^{r_m} - \frac{1}{2} \\
&= \frac{2^{r_0} p_1^{r_1} \cdots p_m^{r_m} - 1}{2} \\
&= \frac{n-1}{2} < \frac{n}{2}
\end{aligned}$$

since n is not squarefree. Moreover, $\gcd(-p_m + id, p_m) = \gcd(id, p_m) = 1$ and $\gcd(-p_m + id, d) = \gcd(-p_m, d) = 1$. It follows that $\gcd(-p_m + id, \operatorname{rad}(n)) = 1$ and thus $\gcd(-p_m + id, n) = 1$. This shows that $-p_m + id \in R(n)$ for all $i \in \{1, 2, \ldots, p_m - 1\}$.

Now, we obtain $g(n) \ge n/\operatorname{rad}(n)$ and $g(n) \ge p_m - 1$, yielding

$$g(n) \ge \max\left\{\frac{n}{\operatorname{rad}(n)}, p_m - 1\right\}. \tag{10}$$

Let $a_1, a_2, \ldots, a_s$ be any arithmetic progression contained in $R(n)$ with common difference d_0. If $\operatorname{rad}(n) \nmid d_0$, then there exists a prime q such that $q \mid n$ but $q \nmid d_0$. By Lemma 1(i), we obtain

$$s \le g(d_0, n) \le q - 1 \le p_m - 1 \le \max\left\{\frac{n}{\operatorname{rad}(n)}, p_m - 1\right\}.$$

Assume that $\operatorname{rad}(n) \mid d_0$. Then, $d_0 \ge \operatorname{rad}(n)$. If $s > n/\operatorname{rad}(n)$, then

$$\frac{n}{2} \ge a_s = a_1 + (s-1)d_0 \ge -\frac{n-2}{2} + \frac{n}{\operatorname{rad}(n)} \cdot \operatorname{rad}(n) = \frac{n+2}{2},$$

which is a contradiction. Thus, $s \le n/\operatorname{rad}(n) \le \max\{n/\operatorname{rad}(n), p_m - 1\}$. Hence, we deduce that

$$g(n) \le \max\left\{\frac{n}{\operatorname{rad}(n)}, p_m - 1\right\}. \tag{11}$$

The desired result then follows from Equations (10) and (11). $\square$

The following examples provide the longest arithmetic progressions contained in $R(n)$ along with their lengths for odd and even positive integers n.

Example 1. (i) Since $-2, -1; 1, 2;$ and $-1, 1$ are the longest arithmetic progressions contained in

$$R(5) = \{-2, -1, 1, 2\},$$

we have $g(5) = 2 = (5-1)/2$. One can see that $-3, -1, 1, 3$ is the longest arithmetic progression contained in

$$R(7) = \{-3, -2, -1, 1, 2, 3\},$$

we obtain $g(7) = 4 = (7+1)/2$.
(ii) Since $-12, -7, -2, 3, 8$ is the longest arithmetic progression contained in

$$R(25) = \{-12, -11, -9, -8, -7, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 7, 8, 9, 11, 12\},$$

we have $g(25) = 5 = 5^{2-1}$.
(iii) Since $-8, -5, -2, 1, 4$ and $-4, -1, 2, 5, 8$ are the longest arithmetic progressions contained in

$$R(21) = \{-10, -8, -5, -4, -2, -1, 1, 2, 4, 5, 8, 10\},$$

we obtain $g(21) = 5 = \lfloor 7 - (7+1)/2 \cdot 3 \rfloor$, where $\mathrm{gpf}(21) = 7$ and $d = 3$.
(iv) Since $-22, -19, -16, -13$ and $-2, 1, 4, 7$ are the longest arithmetic progressions contained in

$$R(45) = \{-22, -19, -17, -16, -14, \dots, -1, 1, \dots, 14, 16, 17, 19, 22\},$$

we have $g(45) = 4 = \max\{45/15, 5-1\}$, where $\mathrm{rad}(45) = 15$ and $\mathrm{gpf}(45) = 5$.

Example 2. (i) Since $-7, -5, -3, -1, 1, 3, 5, 7$ is the longest arithmetic progression contained in

$$R(16) = \{-7, -5, -3, -1, 1, 3, 5, 7\},$$

we have $g(16) = 8 = 2^{4-1}$.
(ii) Since $-3, -1, 1, 3$ is the longest arithmetic progression contained in

$$R(10) = \{-3, -1, 1, 3\},$$

it follows that $g(10) = 4 = 5 - 1$. One can see that $-13, -7, -1$ and $1, 7, 13$ are the longest arithmetic progressions contained in

$$R(30) = \{-13, -11, -7, -1, 1, 7, 11, 13\},$$

we have $g(30) = 3 = \lfloor 5 - 2 \cdot 5/6 \rfloor$, where $\mathrm{gpf}(30) = 5$ and $d = 6$.
(iii) Since $-1, 5, 11, 17, 23, 29$ is the longest arithmetic progression contained in

$$R(84) = \{-41, -37, -31, -29, -25, \dots, -1, 1, \dots, 25, 29, 31, 37, 41\},$$

we obtain $g(84) = 6 = \max\{84/42, 7-1\}$, where $\mathrm{rad}(84) = 42$ and $\mathrm{gpf}(84) = 7$.

Note that Equations (9) and (11) can be proved in another way by using Equation (1) because

$$g(n) \le F(n) = \max\left\{\frac{n}{\operatorname{rad}(n)}, p_m - 1\right\}.$$

From the case of n being an even squarefree integer and having at least three prime factors (Case 2), we conjecture that if $d < 2\operatorname{gpf}(n)$, then $g(n) = \lfloor \operatorname{gpf}(n) - 2\operatorname{gpf}(n)/d \rfloor$, which is supported by Example 2(ii). Although we are currently unable to prove this, the reader is welcome to solve this problem.

3. Further Results

Given integers $m, n \in \mathbb{Z}$ with $n > 1$, recall that

$$R_m(n) := \{a \in \mathbb{Z} \mid m+1 \le a \le m+n, \gcd(a,n) = 1\}$$

is a reduced residue system modulo n and $f_m(n)$ denotes the length of the longest arithmetic progressions contained in $R_m(n)$. One can show that if $a_1, a_2, \ldots, a_s$ is an arithmetic progression contained in $R_m(n)$, then $a_1 + n, a_2 + n, \ldots, a_s + n$ is an arithmetic progression contained in $R_{m+n}(n)$. On the other hand, if $b_1, b_2, \ldots, b_s$ is an arithmetic progression contained in $R_{m+n}(n)$, then $b_1 - n, b_2 - n, \ldots, b_s - n$ is an arithmetic progression contained in $R_m(n)$. This implies that $f_m(n) = f_{m+n}(n)$ for all m, n. Therefore,

$$\{f_m(n) \mid m \in \mathbb{Z}\} = \{f_0(n), f_1(n), \ldots, f_{n-1}(n)\}. \tag{12}$$

The following theorem gives an explicit formula for $\max\limits_{m\in\mathbb{Z}} f_m(n)$.

Theorem 2. *For any integer $n > 1$, we have*

$$\max_{m\in\mathbb{Z}} f_m(n) = \max\left\{\frac{n}{\operatorname{rad}(n)}, \operatorname{gpf}(n) - 1\right\}.$$

Proof. It is clear from Equation (1) that

$$\max_{m\in\mathbb{Z}} f_m(n) \le F(n) = \max\left\{\frac{n}{\operatorname{rad}(n)}, \operatorname{gpf}(n) - 1\right\}. \tag{13}$$

On the other hand, consider three possible cases.
`Case 1:` n is squarefree. We first show that $f_{\operatorname{gpf}(n)+d-1}(n) \ge \operatorname{gpf}(n) - 1$ by showing that the arithmetic progression of length $\operatorname{gpf}(n) - 1$ defined by

$$\operatorname{gpf}(n) + d, \operatorname{gpf}(n) + 2d, \ldots, \operatorname{gpf}(n) + (\operatorname{gpf}(n) - 1)d$$

is contained in $R_{\operatorname{gpf}(n)+d-1}(n)$, where $d = n/\operatorname{gpf}(n)$.

For any $i \in \{1, 2, \ldots, \mathrm{gpf}(n) - 1\}$, we have

$$\mathrm{gpf}(n)+d \le \mathrm{gpf}(n)+id \le \mathrm{gpf}(n)+(\mathrm{gpf}(n)-1)d = \mathrm{gpf}(n)+n-d < \mathrm{gpf}(n)+d+n-1.$$

Moreover, $\gcd(\mathrm{gpf}(n)+id, \mathrm{gpf}(n)) = 1$ and $\gcd(\mathrm{gpf}(n)+id, d) = \gcd(\mathrm{gpf}(n), d) = 1$, which implies $\gcd(\mathrm{gpf}(n)+id, n) = 1$. This shows that $\mathrm{gpf}(n)+id \in R_{\mathrm{gpf}(n)+d-1}(n)$ for all $i \in \{1, 2, \ldots, \mathrm{gpf}(n) - 1\}$. Since $n/\operatorname{rad}(n) = 1$, we have

$$\max_{m\in\mathbb{Z}} f_m(n) \ge f_{\mathrm{gpf}(n)+d-1}(n) \ge \mathrm{gpf}(n) - 1 = \max\left\{\frac{n}{\operatorname{rad}(n)}, \mathrm{gpf}(n) - 1\right\}.$$

`Case 2:` $n = p^r$, where p is a prime and $r > 1$. Then, $\operatorname{rad}(n) = p = \mathrm{gpf}(n)$. By Theorem 1 and since $n/\operatorname{rad}(n) = p^{r-1}$, we have

$$\max_{m\in\mathbb{Z}} f_m(n) \ge f_{-\lceil n/2\rceil}(n) = g(n) = p^{r-1} = \max\left\{\frac{n}{\operatorname{rad}(n)}, \mathrm{gpf}(n) - 1\right\}.$$

`Case 3:` n is not squarefree and is not a prime power. By Theorem 1, we obtain

$$\max_{m\in\mathbb{Z}} f_m(n) \ge f_{-\lceil n/2\rceil}(n) = g(n) = \max\left\{\frac{n}{\operatorname{rad}(n)}, \mathrm{gpf}(n) - 1\right\}.$$

From every case, we deduce that

$$\max_{m\in\mathbb{Z}} f_m(n) \ge \max\left\{\frac{n}{\operatorname{rad}(n)}, \mathrm{gpf}(n) - 1\right\}. \tag{14}$$

The desired result then follows from Equations (13) and (14). □

We note from Theorem 2 that

$$\max_{m\in\mathbb{Z}} f_m(n) = \begin{cases} \mathrm{gpf}(n) - 1 & \text{if } n \text{ is squarefree,} \\ p^{r-1} & \text{if } n = p^r, p \text{ is a prime and } r > 1, \\ \max\left\{\frac{n}{\operatorname{rad}(n)}, \mathrm{gpf}(n) - 1\right\} & \text{otherwise.} \end{cases}$$

Next, we verify an explicit formula for $\min_{m\in\mathbb{Z}} f_m(n)$, where n is a prime power. Furthermore, if n is not squarefree and is not a prime power, then we obtain bounds for $\min_{m\in\mathbb{Z}} f_m(n)$. We note that $f_m(2) = 1$ for all $m \in \mathbb{Z}$.

Theorem 3. *For any integer $n > 2$, we have*

$$\min_{m\in\mathbb{Z}} f_m(n) = \begin{cases} \frac{p-1}{2} & \text{if } n = p \text{ is a prime and } p \equiv 1 \pmod 4, \\ \frac{p+1}{2} & \text{if } n = p \text{ is a prime and } p \equiv 3 \pmod 4, \\ p^{r-1} & \text{if } n = p^r,\ p \text{ is a prime, and } r > 1. \end{cases}$$

In addition, if n is not squarefree and is not a prime power, then

$$\frac{n}{\operatorname{rad}(n)} \le \min_{m\in\mathbb{Z}} f_m(n) \le \max\left\{\frac{n}{\operatorname{rad}(n)}, \mathrm{gpf}(n) - 1\right\}.$$

In particular, if $n/\operatorname{rad}(n) \ge \mathrm{gpf}(n) - 1$, then $\min_{m\in\mathbb{Z}} f_m(n) = n/\operatorname{rad}(n)$.

Proof. We divide the proof into three cases as follows.

Case 1: $n = p$, where p is an odd prime. We have that

$$\begin{aligned}
R_0(p) &= \{1, 2, \ldots, p-1\}\\
R_1(p) &= \{2, 3, \ldots, p-1, p+1\}\\
&\vdots\\
R_{\frac{p-3}{2}}(p) &= \left\{\frac{p-1}{2}, \frac{p+1}{2}, \ldots, p-1, p+1, \ldots, \frac{3p-3}{2}\right\}\\
R_{\frac{p-1}{2}}(p) &= \left\{\frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1, p+1, \ldots, \frac{3p-1}{2}\right\}\\
R_{\frac{p+1}{2}}(p) &= \left\{\frac{p+3}{2}, \frac{p+5}{2}, \ldots, p-1, p+1, \ldots, \frac{3p+1}{2}\right\}\\
&\vdots\\
R_{p-1}(p) &= \{p+1, p+2, \ldots, 2p-1\}.
\end{aligned}$$

For each $i \in \{0, 1, \ldots, (p-3)/2\}$, we can see that $i+1, i+2, \ldots, p-1$ is the longest arithmetic progression contained in $R_i(p)$ and $p+1, p+2, \ldots, 2p-i-1$ is the longest arithmetic progression contained in $R_{(p-1)-i}(p)$. Thus,

$$f_i(p) = f_{(p-1)-i}(p) = p - i - 1 \geq \frac{p+1}{2}$$

for all $i \in \{0, 1, \ldots, (p-3)/2\}$. Moreover, if $p \equiv 1 \pmod 4$, then $(p+1)/2$ is odd. Thus,

$$\frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1$$

and

$$\frac{p+3}{2}, \frac{p+7}{2}, \ldots, p-1, p+1, \ldots, \frac{3p-3}{2}$$

are the longest arithmetic progressions contained in $R_{(p-1)/2}(p)$. It follows that $f_{(p-1)/2}(p) = (p-1)/2$. If $p \equiv 3 \pmod 4$, then $(p+1)/2$ is even, so

$$\frac{p+1}{2}, \frac{p+5}{2}, \ldots, p-1, p+1, \ldots, \frac{3p-1}{2}$$

is the longest arithmetic progression contained in $R_{(p-1)/2}(p)$. Thus, $f_{(p-1)/2}(p) = (p+1)/2$ and the desired result follows by Equation (12).

Case 2: $n = p^r$, where p is a prime and $r > 1$. For any $i \in \{0, 1, \ldots, p^r - 1\}$, we have

$$R_i(p^r) = \{a \in \mathbb{Z} \mid i + 1 \leq a \leq i + p^r, p \nmid a\}.$$

If $p \nmid (i+1)$, then

$$i+1, i+1+p, \ldots, i+1+(p^{r-1}-1)p$$

is an arithmetic progression contained in $R_i(p^r)$ because

$$i+1 \leq i+1+jp \leq i+1+(p^{r-1}-1)p = i+p^r+1-p < i+p^r$$

and $\gcd(i+1+jp, p) = \gcd(i+1, p) = 1$ for all $j \in \{0, 1, \ldots, p^{r-1}-1\}$. If $p \mid (i+1)$, then $p \nmid (i+2)$ so that

$$i+2, i+2+p, \ldots, i+2+(p^{r-1}-1)p$$

is an arithmetic progression contained in $R_i(p^r)$ because

$$i+1 < i+2+jp \leq i+2+(p^{r-1}-1)p = i+p^r+2-p \leq i+p^r$$

and $\gcd(i+2+jp, p) = \gcd(i+2, p) = 1$ for all $j \in \{0, 1, \ldots, p^{r-1}-1\}$. This shows that $f_i(p^r) \geq p^{r-1}$ for all $i \in \{0, 1, \ldots, p^r-1\}$.

Let $a_1, a_2, \ldots, a_s$ be any arithmetic progression contained in $R_i(p^r)$ with common difference d_0. We will show that $s \leq p^{r-1}$. Consider the following two subcases.

`Subcase (i)` $p \mid d_0$. Then, $p \leq d_0$. Suppose, in contrast, that $s > p^{r-1}$. Then,

$$i+p^r \geq a_s = a_1 + (s-1)d_0 \geq i+1+p^{r-1}p = i+1+p^r,$$

which is a contradiction.

`Subcase (ii)` $p \nmid d_0$. By Lemma 1(i), we obtain $s \leq f_i(d_0, p^r) \leq p-1 < p^{r-1}$.

From both subcases, we deduce that $s \leq p^{r-1}$, implying $f_i(p^r) \leq p^{r-1}$ for all $i \in \{0, 1, \ldots, p^r-1\}$. This shows that $f_i(p^r) = p^{r-1}$ for all $i \in \{0, 1, \ldots, p^r-1\}$ and the desired result follows by Equation (12).

`Case 3:` n is not squarefree and is not a prime power. For any $i \in \{0, 1, \ldots, n-1\}$, we have

$$R_i(n) = \{a \in \mathbb{Z} \mid i+1 \leq a \leq i+n, \gcd(a, n) = 1\}.$$

We first prove the following claim: for any divisor d of n, there exists $l \in \{1, 2, \ldots, d\}$ such that $\gcd(i+l, d) = 1$.

If $i = 0$, then $\gcd(i+1, d) = \gcd(1, d) = 1$, so $l = 1$. Assume that $i \geq 1$ then $(j-1)d < i \leq jd$ for some $j \in \{1, 2, \ldots, n/d\}$. Let $l = jd - i + 1 \geq 1$. Then, $l = (j-1)d + 1 + d - i \leq i + d - i = d$ and $\gcd(i+l, d) = \gcd(jd+1, d) = 1$.

We now show that $f_i(n) \geq n/\operatorname{rad}(n)$ by showing that the arithmetic progression of length n/d defined by

$$i+l, i+l+d, i+l+2d, \ldots, i+l+\left(\frac{n}{d}-1\right)d$$

is contained in $R_i(n)$, where $d = \mathrm{rad}(n)$ and $1 \le l \le d$ such that $\gcd(i+l, d) = 1$ by the earlier claim.

For any $j \in \{0, 1, \ldots, n/d - 1\}$, we have

$$i + 1 \le i + l + jd \le i + l + \left(\frac{n}{d} - 1\right) d = i + n + l - d \le i + n.$$

Moreover, $\gcd(i+l+jd, d) = \gcd(i+l, d) = 1$, so $\gcd(i+l+jd, n) = 1$. This shows that $i + l + jd \in R_i(n)$ for all $j \in \{0, 1, \ldots, n/d - 1\}$. Consequently, we have

$$\min_{m \in \mathbb{Z}} f_m(n) \ge n/\,\mathrm{rad}(n).$$

From Equation (1), we obtain

$$\min_{m \in \mathbb{Z}} f_m(n) \le F(n) = \max\{n/\mathrm{rad}(n), \mathrm{gpf}(n) - 1\},$$

which completes the proof. □

We end this article with an explicit formula for the average length of $f_m(n)$ for a broad class of non-squarefree integers n.

Let n be a non-squarefree integer. For convenience, we define

$$A(n) := \frac{1}{n} \sum_{m=0}^{n-1} f_m(n), \ L(n) := \min_{m \in \mathbb{Z}} f_m(n), \text{ and } U(n) := \max_{m \in \mathbb{Z}} f_m(n).$$

Corollary 1. *For any non-squarefree integer n with $n/\,\mathrm{rad}(n) \ge \mathrm{gpf}(n) - 1$, we have*

$$\frac{1}{n} \sum_{m=0}^{n-1} f_m(n) = \frac{n}{\mathrm{rad}(n)}.$$

Proof. For any $m \in \{0, 1, \ldots, n-1\}$, we have $L(n) \le f_m(n) \le U(n)$. Summing from $m = 0$ to $n - 1$ and dividing by n yields

$$L(n) \le A(n) \le U(n).$$

We consider two possible cases.

`Case 1:` $n = p^r$, p is a prime and $r > 1$. By Theorem 2 and Theorem 3, we have $L(n) = p^{r-1} = U(n)$ and so $A(n) = p^{r-1} = n/\,\mathrm{rad}(n)$, where $\mathrm{rad}(n) = p$.

`Case 2:` n is not a prime power. By Theorem 2, Theorem 3, and the condition $n/\,\mathrm{rad}(n) \ge \mathrm{gpf}(n) - 1$, we obtain $L(n) = n/\,\mathrm{rad}(n) = U(n)$ so that $A(n) = n/\,\mathrm{rad}(n)$. □

Note that the condition $n/\operatorname{rad}(n) \geq \operatorname{gpf}(n) - 1$ in Corollary 1 holds for infinitely many integers n. For any odd prime $n = p$, we can only verify bounds for $A(n)$ as follows:

$$\frac{p-1}{2} \leq A(n) \leq p - 1.$$

The case where n is a squarefree integer but not a prime seems more complicated than the others. One reason is that an explicit formula for $f_{-\lceil n/2 \rceil}(n)$ cannot be established in general. In this case, we currently do not have an explicit formula or a bound for $L(n)$ and $A(n)$. This will hopefully be the subject of future work.

Acknowledgement. The authors thank the anonymous referees for their valuable comments and suggestions.

References

[1] Y. G. Chen and C. H. Lei, Arithmetic progressions in the least positive reduced residue systems, *J. Number Theory* **190** (2018), 303–310.

[2] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, New York, 2004.

[3] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley & Sons, New York, 1991.

[4] P. Pongsriiam, Longest arithmetic progressions in reduced residue systems, *J. Number Theory* **183** (2018), 309–325.

[5] P. Stumpf, A short note on reduced residues, *Integers* **17** (2017), #A4.