Original Research Article

Gaps Between Integers Having a Common Divisor with an Odd Semiprime

Abstract

This paper elucidates the distribution law of integers that share a common divisor with an odd semiprime $N = pq$, where p and q are odd primes satisfying $\lambda p < q < (\lambda + 1)p$, and λ is a positive integer. It demonstrates that within the interval $[1, N-1]$, the gaps between integers having p or q as a divisor exhibit symmetric behavior ranging from 0 to $p-1$. Specifically, each gap value from 0 to $p-2$ appears exactly twice, while the gap value $p-1$ occurs precisely $q-p-1$ times across p distinct subintervals. Among these p subintervals, $q-\lambda p-1$ subintervals each contain λ gaps of value $p-1$, while the remaining subintervals each contain $\lambda-1$ gaps of value $p-1$. These findings are valuable and referable for developing methods to identify divisors of odd semiprimes.

Keywords: Integer Distribution; Gap; Congruence classes; Common Divisor; Semiprime.

2010 Mathematics Subject Classification:11B05, 11N25, 11A51.

1 Introduction

This section introduces an open problem and briefly overviews the pertinent literature.

1.1 Problems From Observation

Given a semiprime $N = 15$, which consists of two divisors, 3 and 5; an examination of each integer from 3 to 14 reveals that the integers 3, 6, 9, and 12 are multiples of 3, whereas the integers 5 and 10 are multiples of 5. Using the terminology defined in [1] and [2], the multiples of 3 are hosts of the divisor 3, the multiples of 5 are hosts of the divisor 5, and each of these multiples is a host of N's divisors. Arranging all of these hosts in order results in a sequence.

$$3, \underline{5}, \underline{6}, |, \underline{9}, \underline{10}, 12,$$

where the symbol | means the 'middle' of the sequence.

Apparently, the hosts of 3, namely, 3, 6, 9, and 12, as well as those of 5, namely, 5 and 10, are symmetrically distributed with respect to |. Employing the term 'gap' to quantify the number of integers between two specified integers reveals that pairs (5, 6) and (10, 9) exhibit a gap of 0, pairs (3, 5) and (12, 10) demonstrate a gap of 1, while pair (6, 9) presents a gap of 2. Notably, since the pair (6, 9) is symmetric with respect to itself, it is easily found that the pairs having the same gap are symmetrically distributed with respect to |. If N is changed to 119, which has divisors of 7 and 17, the following host sequence is obtained

$$7, 14, 17, 21, 28, 34, 35, 42, 49, 51, 56, |, 63, 68, 70, 77, 84, 85, 91, 98, 102, 105, 112$$

It is clear that pairs (34, 35) and (85, 84) contribute to gap 0, (49, 51) and (70, 68) to gap 1, (14, 17) and (105, 102) to gap 2, (17, 21) and (102, 98) to gap 3, (56,51) and (63,68) to gap 4, (28,34) and (91,85) to gap 5, while each of the pairs (7,14), (21,28), (35,42), (42,49), (56,63), (70,77), (84 ,77), (98 ,91), and (112 ,105) produces gap 6. Furthermore, those pairs having same gap exhibit symmetry with respect to |.

The phenomena mentioned above were first observed in [3] and then examined in papers [3] and [4]. Paper [3] shows that there is a symmetric gap distribution between two hosts that have different divisors of the odd semiprime $N = pq$ and that there exists a gap 0. However, it did not address whether non-zero gaps, such as 1, 2, and so on, could occur, but left it as an open problem. Paper [4] extends the investigation started in paper [3], focusing on the maximum gaps. It proves that the maximum gap is $p-1$. By constructing a gap sequence under the condition $p < q < 2p$ and within the interval $[1, N-1]$, it also demonstrates that the gap $p-1$ occurs symmetrically with high frequency in an almost periodic manner, determined by the quotient of p divided by $q-p$. Clearly, paper [4] addressed part of the question posed in [3]. Furthermore, it can be seen that the gap sequence constructed in [4] occasionally misses some gaps of value $p-1$. For example, taking $N = 493$ obtains $p = 17$, $q = 29$, and all the hosts of p and q are listed as follows.

17, 29, 34, 51, 58, 68, 85, 87, 102, 116, 119, 136, 145, 153, 170, 174, 187, 203, 204, 221, 232, 238, |, 255, 261, 272, 289, 290, 306, 319, 323, 340, 348, 357, 374, 377, 391, 406, 408, 425, 435, 442, 459, 464, 476.

It is evident that the gap sequence generated by [4] excludes 119, 136, as well as 357 and 374. Therefore, paper [4] provides a preliminary assessment of the distribution of the maximum gaps, indicating that further refinement is necessary.

A comprehensive understanding of the distribution of gaps among the divisors of N is essential for designing effective algorithms aimed at identifying a host that encompasses these divisors, thereby facilitating the discovery of a divisor of N and addressing the hard problem of integer factorization, as highlighted in references [3] and [4]. Paper [5] has made significant headway to develop such a search algorithm by integrating Lévy flight (LF) with local search (LS) techniques. As elaborated in Section 4.5.2 of [5], both the initial point and the step length are critical for optimizing the search efficiency. Those two factors that influence the search efficiency are intrinsically connected to the distribution of gaps. Therefore, an in-depth understanding of the distribution is crucial for improving search

algorithms. This paper thus builds upon the investigations conducted in references [3] and [4] to achieve more thorough outcomes.

The paper is structured into four sections. Section 1 provides an introductory overview that articulates the problem at hand and includes a brief review of relevant literature to demonstrate that this issue is indeed novel. Section 2 delineates the symbols, notations, and previously established lemmas essential for subsequent sections; Section 3 presents the main results along with their proofs and computational validations; finally, Section 4 offers concluding remarks.

1.2 Brief Review of Relevant Literatures

The subject of this paper pertains to two significant issues in number theory: the exploration of gaps between integers and the distribution of divisors of composite integers [6] [7]. The former has a historical lineage that spans several centuries, primarily focusing on the investigation of gaps between prime numbers, within arithmetic progressions, and across specific sets of integers. Early research on this topic is documented in references [8] [9] [10], while more recent studies are presented in [11], [12], and [13]. In reference [8], D. R. Beath-Brown and H. Iwaniec analyzed the differences between consecutive primes; J. Galambos and I. Katai, as noted in references [9] and [10], examined gaps within particular sequences of integers characterized by positive density; Y. Brandon Wang and X. Wang, referenced in study [11], established a symmetrical distribution concerning primes along with their associated gaps; B. Melvyn Nathanson's work cited as reference [12] focused on arithmetic progressions contained within sequences defined by bounded gaps; finally, Y. Liu's study mentioned as reference [13] provided estimates for bounded gaps among products formed from distinct primes.

The second issue primarily concerns the distribution of an integer's divisors within a specified interval or sequence. The introductory section of reference [1] summarizes more recent studies, while early research can be found in references [14] and [15]. In reference [14], Jean-Marie De Koninck looked at how far away certain divisors of an integer are, while D. Berend and J. E. Harmse discussed how far away certain divisors of factorials are in reference [15]. As noted in the literature list provided in reference [1], relevant research has continued due to its close relationship with the study of integer factorization.

The issue addressed in this paper pertains to the gaps between integers that share a common divisor with a specified composite integer. This matter is distinct from the two previously discussed topics, thus categorizing it as an entirely separate area for exploration.

2 Preliminaries

This section delineates the essential symbols, notations, and previously established lemmas that are referenced in subsequent analyses.

2.1 Terminologies, Symbols and Notations

Except for the symbols and notations introduced in [1], [2], [3], and [4], this paper uses symbol $\veebar X$ to mean that quantity X occurs or appears, symbol $x \triangleq S$ to mean that x is the least positive element of a specified integer set S, and symbol $even_b(x)$ to mean a function of integer x defined by

$$even_b(x) = \begin{cases} x, x \bmod 2 = 0 \\ x+1, x \bmod 2 \neq 0 \end{cases}.$$

Symbols $[a]_m$, Z_m, Z_p^*, and $(mZ_p)^*$ are also additionally employed to convey the following meanings.

$$[a]_m = \{x \in Z | x \equiv a (\bmod m)\},$$

$$Z_m = \{[0]_m, [1]_m, [2]_m, ..., [m-1]_m\},$$

$$Z_p^* = \{[1]_p, [2]_p, ..., [p-1]_p\},$$

and

$$(mZ_p)^* = \{[m]_p, [2m]_p ..., [(p-1)m]_p\},$$

where $m > 1$ is an integer, $p > 2$ is a prime, and $(mZ_p)^*$ is *ordered*.

For example, taking $p = 11$ and $m = 3$ results in

$$Z_{11}^* = \{[1]_{11}, [2]_{11}, [3]_{11}, [4]_{11}, [5]_{11}, [6]_{11}, [7]_{11}, [8]_{11}, [9]_{11}, [10]_{11}\},$$

and

$$(3Z_{11})^* = \{[3]_{11}, [6]_{11}, [9]_{11}, [12]_{11}, [15]_{11}, [18]_{11}, [21]_{11}, [24]_{11}, [27]_{11}, [30]_{11}\}.$$

2.2 Previously Proven Lemmas

The following two lemmas are established in references [3] and [4], respectively. They are directly cited in the forthcoming sectons.

Lemma 1. *(see in [3]). Let $N = pq$ be an odd integer and $I_N = [1, N-1]$ be an integer interval, where p and q are odd integers with $1 < p < q$ and $(p, q) = 1$; then for each pair of h^p and h^q in I_N satisfying $1 < h^p, h^q < \frac{N-1}{2}$, it holds*

$$g_{h^p}^{h^q} = g_{N-h^p}^{N-h^q}$$

Lemma 2. *(see in [4]). Let $N = pq$ be an odd integer and $I_N = [1, N-1]$ be an integer interval, where p and q are odd integers with $1 < p < q$ and $(p, q) = 1$; Assume $h^p \in I_N$ and $h^q \in I_N$ are hosts of p and q, respectively; then*

$$0 \le g_{h^p}^{h^q} \le p - 2.$$

3 Main Results

This section introduces novel findings with rigorous proofs and comprehensive computational validations. It includes six new lemmas, five corollaries, two theorems, and a series of computational tests. Specifically, Subsection 3.1 focuses on the presentation of the new lemmas; Subsection 3.2 details the corollaries and theorems; Subsection 3.3 provides the results of the computational tests; and Subsection 3.4 highlights the intriguing phenomena observed from these tests. For ease of reference, Table 1 provides a comprehensive and intuitive summary of the relationships among the theorems, corollaries, and lemmas, including Lemmas 1 and 2 previously list in Subsection 2.2.

Table 1: *Theorems, corollaries, lemmas, and their logical relationships*

Theorem 1	←	Corollary 1	←	Lemmas 1, 2, 4, and 6
		Corollary 3	←	
		Lemma 5	←	
Theorem 2	←	Corollary 2	←	Lemmas 3 and 4
		Corollary 3	←	
		Corollary 4	←	Lemma 7
		Corollary 5	←	Lemmas 5, 7, and 8

3.1 New Lemmas

Lemma 3. *Let p and r be positive integers with $p > 1$ and $0 < r < p$. Then there is not an integer α with $1 < \alpha < p$ such that $\alpha r \geq p$ if $r = 1$; otherwise, $\alpha = \lceil \frac{p}{r} \rceil$ is the unique integer that enables $\alpha r \geq p$ and $(\alpha - 1)r < p$.*

Proof. Lemma 3.1 in [4] has proven that $\alpha = \lceil \frac{p}{r} \rceil$ is the smallest one that enables $\alpha r \geq p$ and $(\alpha - 1)r < p$. Now assume there is a β that enables $\beta r \geq p$ and $(\beta - 1)r < p$. Then

$$\begin{cases} \alpha r \geq p \\ (\beta - 1)r < p \end{cases} \Leftrightarrow \begin{cases} \alpha r \geq p \\ -(\beta - 1)r > -p \end{cases} \Rightarrow \alpha r - (\beta - 1)r > 0 \Leftrightarrow \alpha > \beta + 1,$$

which is contradictory to that α is the smallest one. □

Lemma 4. *Let p and q be two odd integers such that $(p, q) = 1$ and $q = \lambda p + r$ with integers r and λ satisfying $1 < r < p$ and $\lambda \geq 1$; then integer $\alpha = \lceil \frac{p}{r} \rceil$ enables $(\alpha - 1)r < p$, $\alpha r > p$,*

$$(\alpha - 1)\lambda p < (\alpha - 1)q < (\alpha - 1)\lambda p + p \tag{3.1}$$

and

$$\alpha\lambda p + p < \alpha q < \alpha\lambda p + 2p. \tag{3.2}$$

Proof. By Lemma 3, $r \geq 2$ ensures $\alpha = \lceil \frac{p}{r} \rceil$ satisfying $1 < \alpha < p - 1$, $(\alpha - 1)r < p$, and $\alpha r \geq p$. The condition $(p, q) = 1$ yields $\alpha r = \lceil \frac{p}{r} \rceil r > p$ because $(p, q) = 1 \Rightarrow (p, r) = 1$. Now prove α also satisfies (3.1) and (3.2). By $\alpha r > p$, let $\alpha r = sp + t$, where integers s and t satisfy $s \geq 1$ and $0 < t < p$; then

$$(\alpha - 1)q = (\alpha - 1)\lambda p + (\alpha - 1)r, 0 < (\alpha - 1)r < p \tag{3.3}$$

and

$$\alpha q = \alpha\lambda p + \alpha r = (\alpha\lambda + s)p + t, 0 < t < p. \tag{3.4}$$

From (3.3), (3.1) surely holds. Next prove $s = 1$. In fact $\alpha r = sp + t$ yields

$$(\alpha - 1)r = sp + t - r \tag{3.5}$$

Since $0 < t < p$ and $1 < r < p$, it follows

$$-(p - 2) \leq t - r \leq p - 3 < p - 2,$$

indicating by (3.5)

$$(\alpha - 1)r \geq sp - p + 2$$

If $s > 1 \Leftrightarrow s \geq 2$, it deduces $(\alpha - 1)r \geq p + 2$, which is contradictory to $0 < (\alpha - 1)r < p$. Accordingly, (3.4) becomes $\alpha q = (\alpha\lambda + 1)p + t$ with $0 < t < p$, identical to (3.2). □

Lemma 5. *Let p and q be odd integers such that $(p, q) = 1$ and $\lambda p < q < (\lambda + 1)p$ with $\lambda \geq 1$ being an integer. Then there are $even_b(\lambda)$ hosts of p that are symmetrically distributed between $(\frac{p-1}{2})q$ and $(\frac{p+1}{2})q$; among all these $even_b(\lambda)$ hosts of p, there is not a host of q. Particularly, $(\frac{q-1}{2})p$ and $(\frac{q+1}{2})p$ are exact two hosts of p between $(\frac{p-1}{2})q$ and $(\frac{p+1}{2})q$ if $\lambda = 1$.*

Proof. The condition $\lambda p < q < (\lambda + 1)p$ leads to $\lambda = \left\lfloor \frac{q}{p} \right\rfloor$ because

$$\lambda p < q < (\lambda + 1)p \Leftrightarrow q = \lambda p + r, 0 < r < p \Leftrightarrow \lambda = \left\lfloor \frac{q}{p} \right\rfloor.$$

To prove the first conclusion, consider an integer α that satisfies the following (3.6) given by

$$(\frac{p-1}{2})q < \alpha p < (\frac{p+1}{2})q. \tag{3.6}$$

Then it follows

$$q-\frac{q}{p}<2\alpha<q+\frac{q}{p}$$

Note that, $q-\lambda, q-\lambda+1, ..., q, ..., q+\lambda-1$, and $q+\lambda$, totally $2\lambda+1$ ones, are integers between $q-\frac{q}{p}$ and $q+\frac{q}{p}$, distributed symmetrically with respect to q. Obviously, there are $even_b(\lambda)$ even integers between $q-\lambda$ and $q+\lambda$, among which each one can contribute a solution to α. Hence the first conclusion holds.

To prove the second conclusion, use proof by contradiction. Let h_i^p be the host of p, where integer i satisfies $1\le i\le even_b(\lambda)$; then

$$(\frac{p-1}{2})q<h_i^p<(\frac{p+1}{2})q.$$

A host of q must be of the form αq with $\alpha\ge 1$ being an integer. If there is an αq among the $even_b(\lambda)$ hosts of p, then $(\frac{p-1}{2})q<\alpha q<(\frac{p+1}{2})q$, yielding

$$\frac{p-1}{2}<\alpha<\frac{p+1}{2}\Leftrightarrow p-1<2\alpha<p+1\Rightarrow p=2\alpha,$$

leading to a contradiction to that p is odd.

In the particular case, $\lambda=1\Rightarrow 1<\frac{q}{p}<2\Leftrightarrow\left\lfloor\frac{q}{p}\right\rfloor=1$; hence $q-1, q$, and $q+1$ are three integers to hold (3.6), meaning $\alpha=\frac{q-1}{2}$ and $\alpha=\frac{q+1}{2}$ are the only two integers satisfying (3.6). □

Lemma 6. *Let $a>1$ and $b>1$ be two positive integers such that $a>b$ and $(a,b)=1$; then for an arbitrary positive integer c satisfying $1\le c\le b$, the Diophantine equation $ax-by=c$ has a unique integer solution $(x,y)\in Z\times Z$ that satisfies $0<x\le b$ and $0<y<a$. Particularly, $x=b$ if and only if $c=b$.*

Proof. The proof is composed of the following five parts.

(P1). $x>0\Leftrightarrow y>0$. Otherwise, it is contradictory to $ax-by=c$ under the condition $a>b\ge c\ge 1$.

(P2). $x\le b\Leftrightarrow y<a$. Use proof by contradiction. For an $x\le b$, assume $y\ge a$; then it follows $y\ge a\Rightarrow by=ax-c\ge ab\Rightarrow x\ge b+\frac{c}{a}>b$, contradictory to $x\le b$. Similarly, for a $y\le a-1$ assuming $x>b$ results in $x>b\Rightarrow ax=by+c>ab\Rightarrow y>a-\frac{c}{b}$, a contradiction.

(P3). Existence of $0<x\le b$ and $0<y<a$. Referring to Section 2.4 of book [16], the condition $(a,b)=1$ results in the general solution of $ax-by=c$ given by

$$\begin{cases} x=cx_0+bt \\ y=cy_0+at \end{cases},t=0,\pm1,\pm2,\cdots. \tag{3.7}$$

where $(x_0,y_0)\in Z\times Z$ is a solution of $ax-by=1$.

Since $(a,b)=1$, such (x_0,y_0) can always be found. Furthermore, by Lemma 3.3 of paper [3], a solution satisfying $0<x_0<b, 0<y_0<a$ can also be found. Note that, taking $-\frac{cx_0}{b}<t\le 1-\frac{cx_0}{b}$ in (3.7) yields $0<x\le b$ and $-\frac{c}{b}<y=\frac{ax-c}{b}<\frac{ab-c}{b}=a-\frac{c}{b}$. By $1\le c\le b$, it follows $0<x\le b$ and $0<y<a$, taking into account the previously established (P1) and (P2).

(P4). Uniqueness. Assume $(x_1,y_1)\in Z\times Z$ and $(x_2,y_2)\in Z\times Z$ are two solutions with $0<x_1,x_2\le b$ and $0<y_1,y_2<a$; then by (3.7)

$$x_1=cx_0+bt_1, x_2=cx_0+bt_2\Rightarrow x_1-x_2=b(t_1-t_2).$$

Since

$$0<x_1,x_2\le b\Rightarrow -(b-1)\le x_2-x_1\le b-1$$

it follows

$$-\frac{(b-1)}{b}\le t_2-t_1\le\frac{b-1}{b}\Rightarrow t_2-t_1=0.$$

(P5). The particular case. If $c=b$, direct calculations yield that $x=b$ and $y=a-1$ contribute a solution. Now assume $x=b$ but $c<b$. Then $ax-by=c\Leftrightarrow ab-by=c<b\Rightarrow y>a-1$, contradictory to what is proved in (P2). □

Lemma 7. *Given an odd prime p; let m be an integer with $1 < m < p$; then*

(C1). The least positive representatives of $(mZ_p)^*$ are calculated by

$$e_i = im - \left\lfloor \frac{im}{p} \right\rfloor p, i = 1,2,...,p-1. \tag{3.8}$$

(C2). The $p-1$ representatives, $e_1, e_2, ...,$ and e_{p-1}, can be classified into m subsets; the k-th subset contains $n_k = \left\lceil \frac{(k+1)p}{m} \right\rceil - \left\lfloor \frac{kp}{m} \right\rfloor - 1$ representatives calculated by

$$e_k^j = (j + \left\lfloor \frac{kp}{m} \right\rfloor)m - kp, k = 0,2,...,m-1. \tag{3.9}$$

where $1 \le j \le n_k$.

Thus it holds in the k-th subset

$$e_k^{j+1} - e_k^j = m, j = 1,2,...,n_k - 1. \tag{3.10}$$

Furthermore, it holds for $1 \le j \le n_k$

$$e_k^j = e_{j+n_0+n_1+n_2+...+n_{k-1}}. \tag{3.11}$$

(C3). The difference between the last element and the first element in the k-th subset is given by

$$e_k^{n_k} - e_k^1 = (\left\lceil \frac{(k+1)p}{m} \right\rceil - \left\lfloor \frac{kp}{m} \right\rfloor - 2)m, k = 0,1,...,m-1. \tag{3.12}$$

or equivalently

$$e_k^{n_k} - e_k^1 = \begin{cases} (\left\lfloor \frac{(k+1)p}{m} \right\rfloor - \left\lfloor \frac{kp}{m} \right\rfloor - 1)m, k = 0,1,...,m-2 \\ (\left\lfloor \frac{p}{m} \right\rfloor - 1)m, k = m-1 \end{cases}. \tag{3.13}$$

And thus

$$p - 2m < e_k^{n_k} - e_k^1 < \begin{cases} p, k = 0,1,...,m-2 \\ p-m, k = m-1 \end{cases} \tag{3.14}$$

(C4) The difference between the first element in the (k+1)-th subset and the last element in the k-th subset is given by

$$e_k^{n_k} - e_{k+1}^1 = p - m, k = 0,1,...,m-2. \tag{3.15}$$

(C5). In the case $1 < m < p$ and regardless of the order, $e_0^1, e_1^1, e_2^1, ...,$ and e_{m-1}^1 form the least positive complete residue system modulo m, namely,

$$Z_m = \{e_0^1, e_1^1, ..., e_{m-1}^1\} \tag{3.16}$$

Proof. Assume $im = k_i p + r_i$ with integers k_i and r_i satisfying $k_i \ge 0$ and $0 < r_i < p$; then

$$[im] = [r_i].$$

Because $k_i = \left\lfloor \frac{im}{p} \right\rfloor$, it is known

$$r_i = im - k_i p = im - \left\lfloor \frac{im}{p} \right\rfloor p > 0,$$

which validates (3.8) and finishes proving the conclusion (C1).

Note that under the condition $0 < i, m < p$, specifying an m leads to

$$0 = \left\lfloor \frac{m}{p} \right\rfloor \le \left\lfloor \frac{im}{p} \right\rfloor \le \left\lfloor \frac{(p-1)m}{p} \right\rfloor = \left\lfloor m - \frac{m}{p} \right\rfloor = m - 1,$$

saying $0 \le k_i \le m-1$, namely, the $p-1$ values of $\left\lfloor \frac{im}{p} \right\rfloor$ for $1 \le i \le p-1$ generate m values of k_i. Consequently, the $p-1$ elements of $(mZ_p)^*$ can surely be classified into m subsets by $k_i = 0,1,2,$ ..., and $m-1$, resulting in that each subset corresponds to one value of $k_i = 0,1,2,$ ..., and $m-1$.

Now take an arbitrary integer k with $0 \le k \le m-1$ to see which of the $p-1$ elements belongs to the k-th subset. This merely needs to check which i satisfies $\left\lfloor \frac{im}{p} \right\rfloor = k$. Since

$$\left\lfloor \frac{im}{p} \right\rfloor = k \Leftrightarrow k \le \frac{im}{p} < k+1 \Leftrightarrow kp \le im < (k+1)p \Leftrightarrow \frac{kp}{m} \le i < \frac{(k+1)p}{m}$$

it immediately follows

$$\left\lfloor \frac{kp}{m} \right\rfloor + 1 \le i \le \left\lceil \frac{(k+1)p}{m} \right\rceil - 1.$$

In fact, $k=0$ yields $\left\lfloor \frac{kp}{m} \right\rfloor + 1 = 1$ and $k = m-1$ yields $\left\lceil \frac{(k+1)p}{m} \right\rceil - 1 = p-1$, which is consistent with $0 < i < p$. When $0 < k < m-1$, $\{\frac{kp}{m}\} > 0$ and $\{\frac{(k+1)p}{m}\} > 0$, leading to

$$\frac{kp}{m} \le i < \frac{(k+1)p}{m} \Leftrightarrow \left\lfloor \frac{kp}{m} \right\rfloor + \{\frac{kp}{m}\} \le i < \left\lfloor \frac{(k+1)p}{m} \right\rfloor + \{\frac{(k+1)p}{m}\}$$

indicating

$$\left\lfloor \frac{kp}{m} \right\rfloor + 1 \le i < \left\lceil \frac{(k+1)p}{m} \right\rceil$$

because $\left\lceil \frac{(k+1)p}{m} \right\rceil$ is the smallest integer bigger than $\left\lfloor \frac{(k+1)p}{m} \right\rfloor + \{\frac{(k+1)p}{m}\}$.

Counted from $\left\lfloor \frac{kp}{m} \right\rfloor + 1$ to $\left\lceil \frac{(k+1)p}{m} \right\rceil - 1$, the total number of the representatives corresponding to k is given by

$$n_k = \left\lceil \frac{(k+1)p}{m} \right\rceil - \left\lfloor \frac{kp}{m} \right\rfloor - 1.$$

Letting $j = i - \left\lfloor \frac{kp}{m} \right\rfloor$knows that j changes from 1 to n_k as i changes from $\left\lfloor \frac{kp}{m} \right\rfloor + 1$ to $\left\lceil \frac{(k+1)p}{m} \right\rceil - 1$. Hence (3.9) holds. The formula (3.10) can be directly obtained by (3.9). The proof of (3.11) simply comes from the following reasoning.

$$\begin{aligned}
&k = 0 : e_0^j = e_j, 1 \le j \le n_0 \\
&k = 1 : e_1^j = e_{j+n_0}, 1 \le j \le n_1 \\
&k = 2 : e_2^j = e_{j+n_0+n_1}, 1 \le j \le n_2 \\
&k = 3 : e_3^j = e_{j+n_0+n_1+n_2}, 1 \le j \le n_3 \\
&\ldots\ldots \\
&k = s : e_s^j = e_{j+n_0+n_1+n_2+\ldots+n_{s-1}}, 1 \le j \le n_s
\end{aligned}$$

Therefore, the conclusion (C2) has been established.

Now calculating directly by (3.9) shows

$$e_k^{n_k} - e_k^1 = (\left\lceil \frac{(k+1)p}{m} \right\rceil - \left\lfloor \frac{kp}{m} \right\rfloor - 2)m = \begin{cases} (\left\lfloor \frac{(k+1)p}{m} \right\rfloor - \left\lfloor \frac{kp}{m} \right\rfloor - 1)m, k = 0, 1, \ldots, m-2 \\ (p - \left\lfloor \frac{kp}{m} \right\rfloor - 2)m, k = m-1 \end{cases}$$

because $k = m-1 \Rightarrow \left\lceil \frac{(k+1)p}{m} \right\rceil = p$ otherwise $\left\lceil \frac{(k+1)p}{m} \right\rceil = \left\lfloor \frac{(k+1)p}{m} \right\rfloor + 1$.

Note that, $p - \left\lfloor \frac{(m-1)p}{m} \right\rfloor - 2 = p - \lfloor p - \frac{p}{m} \rfloor - 2 = -\lfloor -\frac{p}{m} \rfloor - 2$; by (P16) in [17], it yields $-\lfloor -\frac{p}{m} \rfloor - 2 = \lfloor \frac{p}{m} \rfloor - 1$, which verifies (3.13), namely,

$$e_k^{n_k} - e_k^1 = \begin{cases} (\left\lfloor \frac{(k+1)p}{m} \right\rfloor - \left\lfloor \frac{kp}{m} \right\rfloor - 1)m, k = 0, 1, \ldots, m-2 \\ (\lfloor \frac{p}{m} \rfloor - 1)m, k = m-1 \end{cases}.$$

According to (P2) in [17], (3.12) yields for $0 \le k \le m-2$

$$(\left\lfloor \frac{p}{m} \right\rfloor - 1)m \le e_k^{n_k} - e_k^1 \le \left\lfloor \frac{p}{m} \right\rfloor m$$

which derives

$$p - 2m < e_k^{n_k} - e_k^1 < p \tag{3.17}$$

In fact, write $p = km + r$ with integers $k \geq 1$ and $1 \leq r \leq m-1$ because p is prime and $0 < m < p$; then it follows

$$\{\frac{p}{m}\} = \frac{r}{m} \geq \frac{1}{m}$$

By (P8) and (P9) in [17], it is known

$$p - 2m + 1 \leq \left\lfloor \frac{p}{m} \right\rfloor m < p$$

which validates (3.17).

For the case $k = m-1$, direct calculations by (P32) in [17] lead to

$$p - 2m \leq e_k^{n_k} - e_k^1 = (\left\lfloor \frac{p}{m} \right\rfloor - 1)m < p - m.$$

Therefore, the conclusion (C3) has been substantiated up to this point.

To prove the conclusion (C4), calculating directly $e_k^{n_k}$ and e_{k+1}^1 yields

$$e_k^{n_k} = (\left\lceil \frac{(k+1)p}{m} \right\rceil - 1)m - kp$$

and

$$e_{k+1}^1 = (1 + \left\lfloor \frac{(k+1)p}{m} \right\rfloor)m - (k+1)p.$$

As a result,

$$e_k^{n_k} - e_{k+1}^1 = (\left\lceil \frac{(k+1)p}{m} \right\rceil - \left\lfloor \frac{(k+1)p}{m} \right\rfloor - 2)m + p = p - m, k = 0, 1, ..., m-2,$$

validating (3.15).

To prove the conclusion (C5), choosing an arbitrary $s \in \{0, 1, 2, ..., m-1\}$ and $t \in \{0, 1, 2, ..., m-1\}$ leads to by (3.9)

$$e_s^1 - e_t^1 = (\left\lfloor \frac{sp}{m} \right\rfloor - \left\lfloor \frac{tp}{m} \right\rfloor)m + (t-s)p,$$

which says

$$e_s^1 - e_t^1 \equiv (t-s)p (\mathrm{mod}\, m).$$

Since p is prime, $1 < m < p \Rightarrow (m, p) = 1$. Hence $s \neq t \Leftrightarrow e_s^1 \not\equiv e_t^1 (\mathrm{mod}\, m)$, indicating $e_0^1, e_1^1, e_2^1, ...$, and e_{m-1}^1 form the least positive complete residue system modulo m. □

Remark 1. By (3.11), it follows

$$e_k^{n_k} = e_{n_0 + n_1 + n_2 + ... + n_k} \tag{3.18}$$

and

$$e_{k+1}^1 = e_{n_0 + n_1 + n_2 + ... + n_k + 1} \tag{3.19}$$

Since $0 \leq k \leq m-2 \Rightarrow \left\lceil \frac{(k+1)p}{m} \right\rceil = \left\lfloor \frac{(k+1)p}{m} \right\rfloor + 1$ and $k = m-1 \Rightarrow \left\lceil \frac{(k+1)p}{m} \right\rceil = p$, it follows

$$n_k = \left\lceil \frac{(k+1)p}{m} \right\rceil - \left\lfloor \frac{kp}{m} \right\rfloor - 1 = \begin{cases} \left\lfloor \frac{p}{m} \right\rfloor, k = 0 \\ \left\lfloor \frac{(k+1)p}{m} \right\rfloor - \left\lfloor \frac{kp}{m} \right\rfloor, k = 1, 2, ..., m-2 \\ \left\lfloor \frac{p}{m} \right\rfloor, k = m-1 \end{cases}.$$

Hence

$$\begin{cases} n_0 = \left\lfloor \frac{p}{m} \right\rfloor \\ \left\lfloor \frac{p}{m} \right\rfloor \leq n_k \leq \left\lfloor \frac{p}{m} \right\rfloor + 1, k = 1, 2, ..., m-2 \\ n_{m-1} = \left\lfloor \frac{p}{m} \right\rfloor \end{cases}, \tag{3.20}$$

$$\sum_{j=0}^{k} n_j = \sum_{j=0}^{k} (\left\lfloor \frac{(j+1)p}{m} \right\rfloor - \left\lfloor \frac{jp}{m} \right\rfloor) = \left\lfloor \frac{(k+1)p}{m} \right\rfloor, 0 \leq k \leq m-2, \tag{3.21}$$

and

$$\sum_{j=0}^{m-1} n_j = \left\lfloor \frac{p}{m} \right\rfloor + \sum_{j=0}^{m-2} \left(\left\lfloor \frac{(j+1)p}{m} \right\rfloor - \left\lfloor \frac{jp}{m} \right\rfloor \right) = \left\lfloor \frac{(m-1)p}{m} \right\rfloor + \left\lfloor \frac{p}{m} \right\rfloor = p-1.$$

As a result, for $0 \le k \le m-2$, it holds

$$e_k^{n_k} = e_{n_0+n_1+n_2+\ldots+n_k} \triangleq [\left\lfloor \frac{(k+1)p}{m} \right\rfloor m]_p \tag{3.22}$$

and

$$e_{k+1}^{1} = e_{n_0+n_1+n_2+\ldots+n_k+1} \triangleq [(\left\lfloor \frac{(k+1)p}{m} \right\rfloor + 1)m]_p. \tag{3.23}$$

Because $0 \le k \le m-2$, it follows by (P32) in [17]

$$\left\lfloor \frac{(k+1)p}{m} \right\rfloor m < (k+1)p \tag{3.24}$$

and

$$(k+1)p < (\left\lfloor \frac{(k+1)p}{m} \right\rfloor + 1)m < (k+1)p + m. \tag{3.25}$$

Lemma 8. *Given an odd prime p; let $q = \lambda p + r$ with q, r, and λ being integers such that $(p,q) = 1$, $1 < r < p$, and $\lambda \ge 1$; assume $e_j \triangleq [jm]_p \in (mZ_p)^*$ for integer j with $0 < j < p$. Then an α satisfying $e_\alpha - e_{\alpha+1} = p - r$ must enable*

$$\begin{cases} \alpha q < h^p \\ h^p + \lambda p < (\alpha+1)q < h^p + \lambda p + p \end{cases}, \tag{3.26}$$

where $h^p = (\lambda\alpha + 1)p + \left\lfloor \frac{\alpha r}{p} \right\rfloor p$.

Proof. Let $E = \{e_1, e_2, \ldots, e_{p-1}\}$. By Lemma 7, E can be grouped into r subsets. Without loss of generality, assume G_k and G_{k+1} are two adjacent subsets with $0 \le k \le r-2$. Let e_α represent the last element of G_k and $e_{\alpha+1}$ represent the first element of G_{k+1}. Consequently, the conclusions (C2) and (C4) of Lemma 7 guarantee e_α and $e_{\alpha+1}$ are the sole qualified elements in G_k and G_{k+1} that satisfy $e_\alpha - e_{\alpha+1} = p - r$. By (C1) of Lemma 7,

$$e_\alpha = \alpha r - \left\lfloor \frac{\alpha r}{p} \right\rfloor p$$

and

$$e_{\alpha+1} = (\alpha+1)r - \left\lfloor \frac{(\alpha+1)r}{p} \right\rfloor p$$

Hence

$$e_\alpha - e_{\alpha+1} = (\left\lfloor \frac{(\alpha+1)r}{p} \right\rfloor - \left\lfloor \frac{\alpha r}{p} \right\rfloor)p - r.$$

The condition $e_\alpha - e_{\alpha+1} = p - r$ results in

$$\left\lfloor \frac{(\alpha+1)r}{p} \right\rfloor - \left\lfloor \frac{\alpha r}{p} \right\rfloor = 1.$$

Now direct calculations show

$$\begin{aligned} \alpha q &= \lambda\alpha p + \alpha r \\ &= \lambda\alpha p + \left\lfloor \frac{\alpha r}{p} \right\rfloor p + e_\alpha \\ &= \lambda\alpha p + \left\lfloor \frac{\alpha r}{p} \right\rfloor p + e_{\alpha+1} + p - r \\ &= (\lambda\alpha + 1)p + e_{\alpha+1} + \left\lfloor \frac{\alpha r}{p} \right\rfloor p - r \end{aligned}$$

and

$$\begin{aligned} (\alpha+1)q &= \lambda(\alpha+1)p + (\alpha+1)r \\ &= \lambda(\alpha+1)p + \left\lfloor \frac{(\alpha+1)r}{p} \right\rfloor p + e_{\alpha+1} \\ &= (\lambda\alpha+1)p + e_{\alpha+1} + (\left\lfloor \frac{\alpha r}{p} \right\rfloor + 1)p + (\lambda-1)p \\ &= (\lambda\alpha+1)p + e_{\alpha+1} + \left\lfloor \frac{\alpha r}{p} \right\rfloor p + \lambda p \end{aligned}.$$

Letting $h^p = (\lambda\alpha+1)p + \left\lfloor \frac{\alpha r}{p} \right\rfloor p$ yields

$$\begin{cases} \alpha q = h^p + e_{\alpha+1} - r \\ (\alpha+1)q = h^p + e_{\alpha+1} + \lambda p \end{cases}$$

By the conclusion (C5) of Lemma 7, $e_{\alpha+1} > 0$ and $e_{\alpha+1} - r < 0$; hence

$$\begin{cases} \alpha q < h^p \\ h^p + \lambda p < (\alpha+1)q < h^p + \lambda p + r < h^p + \lambda p + p \end{cases}$$

which is just (3.26). □

Remark 2. By Lemma 8, $h^p, h^p + p, h^p + 2p, ...$, and $h^p + \lambda p$ are $\lambda + 1$ hosts of p between αq and $(\alpha+1)q$.

3.2 Corollaries and Theorems

Corollary 3.1. *[From Lemmas 1, 4, and 6] Let $N = pq$ be an odd integer and $I_N = [1, N-1]$ be an integer interval, where p and q are odd integers with $1 < p < q$ and $(p,q) = 1$; then for each integer α satisfying $0 \le \alpha \le p-2$, there exist uniquely $h^p \in I_N$ and $h^q \in I_N$ such that*

$$g_{h^p}^{h^q} = g_{N-h^p}^{N-h^q} = \alpha$$

Proof. Referring to the proof of Theorem 4.2 in [3], the gap set $G^{p,q}$, which represents the gaps between the hosts of p and those of q, can be calculated by

$$G^{p,q} = \{xq - yp - 1 | 1 \le x \le p-1, 1 \le y \le q-1, (x,y) \in Z \times Z\}$$

By Lemma 6, for an integer g satisfying $1 \le g \le p-1$, the Diophantine equation $xq - yp - 1 = g - 1$ always has a unique solution $(x,y) \in Z \times Z$ with $0 < x \le p-1$ and $0 < y \le q-1$. That is equivalent to stating that for any integer α satisfying $0 \le \alpha < p-2$, the Diophantine equation $xq - yp - 1 = \alpha$ can always has a unique solution $(x,y) \in Z \times Z$ with respect to $0 < x \le p-1$ and $0 < y \le q-1$. Since $0 \le g_{h^p}^{h^q} = xq - yp - 1 \le p-2$ exactly matches to $0 \le \alpha \le p-2$, by Lemma 4 there exist uniquely $h^p \in I_N$ and $h^q \in I_N$ such that $g_{h^p}^{h^q} = \alpha$. In the end, the symmetric property (Lemma 1) validates the proof. □

Corollary 3.2. *[From Lemmas 3 and 4] Given two odd integers p and q such that $(p,q) = 1$, $q = \lambda p + r$ with integers r and λ satisfying $1 < r < p$ and $\lambda \ge 1$; let $\alpha = \left\lceil \frac{p}{r} \right\rceil$ and β be an integer with $1 < \beta < \alpha$. Then there are λ hosts of p between $(\beta-1)q$ and βq, whereas there are $\lambda+1$ hosts of p between $(\alpha-1)q$ and αq.*

Proof. Calculating directly by $q = \lambda p + r$ and $1 < r < p$ yields

$$\begin{cases} (\beta-1)q = \lambda(\beta-1)p + (\beta-1)r \\ \beta q = \lambda\beta p + \beta r \end{cases} \Rightarrow \begin{cases} \lambda(\beta-1)p < (\beta-1)q < \lambda(\beta-1)p + p \\ \lambda\beta p < \beta q < \lambda\beta p + p \end{cases},$$

indicating $(\beta-1)q$ is between $\lambda(\beta-1)p$ and $\lambda(\beta-1)p + p$ while βq is between $\lambda\beta p$ and $\lambda\beta p + p$, as illustrated with Figure 1.

Figure 1: *$(\beta-1)q$, βq and their related hosts of p*

Hence $\lambda(\beta-1)p + p, \lambda(\beta-1)p + 2p, ...$, and $\lambda\beta p$ are λ hosts of p between $(\beta-1)q$ and βq.

By Lemma 4, $\alpha = \left\lceil \frac{p}{r} \right\rceil$ yields (3.1) and (3.2). The positions of $(\alpha-1)q$ and αq along with their related hosts of p can be illustrated with Figure 2.

This time, $\lambda(\alpha-1)p + p, \lambda(\alpha-1)p + 2p, ...$, and $\lambda\alpha p + p$ are $\lambda + 1$ hosts of p between $(\alpha-1)q$ and αq. And this concludes the proof of the corollary. □

Figure 2: *$(\alpha-1)q$, αq and their related hosts of p*

Corollary 3.3. *Given an odd integer $N = pq$, where p and q are odd integers such that $(p,q)=1$ and $q=\lambda p+1$with $\lambda \geq 1$ being an integer; let $I_N=[1,N-1]$ be an integer interval; Then*

(i). G^0 occurs symmetrically twice in I_N; one occurrence is situated between λp and q, while the other is positioned between $\lambda(p-1)p$ and $(p-1)q$.

(ii). G^{p-1} occurs $\lambda-1$ times in each of the p integer intervals $[p,\lambda p]$, $[jq,(j+1)q]$, and $[((p-1)\lambda+1)p,(q-1)p]$, where integer j satisfies $1\leq j\leq p-2$. Hence it totally occurs $q-p-1$ times symmetrically in I_N.

Proof. Consider an arbitrary positive integer $0<\alpha<p$ and

$$\alpha q=\alpha\lambda p+\alpha r. \tag{3.27}$$

If $r=1$, then $\alpha q=\alpha\lambda p+\alpha$ lies between $\alpha\lambda p$ and $(\alpha\lambda+1)p$, resulting in $G^{\alpha-1}$ occurring from $\alpha\lambda p$ to αq and $G^{p-\alpha-1}$ appearing from αq to $(\alpha\lambda+1)p$, as illustrated with Figure 3.

Figure 3: *$\alpha q=\alpha\lambda p+\alpha$ lies between $\alpha\lambda p$ and $(\alpha\lambda+1)p$*

Accordingly, this time $\alpha=1$ or $\alpha=p-1$ yields G^0 to appear between $\alpha\lambda p$ and $(\alpha\lambda+1)p$, finishing proving the conclusion (i).

Since p, $2p$, ..., and λp are λ hosts of p in $[p,\lambda p]$, G^{p-1} surely occurs $\lambda-1$ times in the interval. Note that, $(p-1)q$ and $(q-1)p$ are respectively the biggest hosts of q and p in I_N. Since

$$(q-1)p-(p-1)q=q-p=(\lambda-1)p+1>0,$$

it is known there exist hosts of p following $(p-1)q$.

Because $(p-1)\lambda p<(p-1)q=(p-1)\lambda p+p-1<((p-1)\lambda+1)p$, integer $((p-1)\lambda+1)p$ is the smallest host of p bigger than $(p-1)q$. Hence $((p-1)\lambda+1)p,((p-1)\lambda+2)p,...,$ and $((p-1)\lambda+\lambda)p$ are all the hosts of p following $(p-1)q$. Since $((p-1)\lambda+\lambda)p=(\lambda p)p=(q-1)p$, interval $[((p-1)\lambda+1)p,(q-1)p]$ surely contains λ hosts of p and thus G^{p-1} occurs $\lambda-1$ times in it. Referring to the proof of Corollary 3.2 for the β-case, there always exist λ hosts of p between arbitrary two adjacent hosts of q. The total number of the intervals is p and the total number of the occurrences is $(\lambda-1)p=q-p-1$. □

Remark 3. Seen in the proof, $((p-1)\lambda+1)p,((p-1)\lambda+2)p,...,$ and $((p-1)\lambda+\lambda)p$ are all the hosts of p in interval $[(p-1)q,(q-1)p]$ owning to

$$[(p-1)\lambda+1)p,(q-1)p]\subseteq[(p-1)q,(q-1)p]. \tag{3.28}$$

Theorem 3.4. *Let $N=pq$ be an odd integer and $I_N=[1,N-1]$ be an integer interval, where p and q are odd integers with $1<p<q$ and $(p,q)=1$; then the gaps between two hosts of N's divisors in I_N range symmetrically from 0 to $p-1$.*

Proof. By Lemma 5, G^{p-1} occurs symmetrically between $(\frac{p-1}{2})q$ and $(\frac{p+1}{2})q$. By Corollary 3.1, the gaps between hosts of p and hosts of q range symmetrically from 0 to $p-2$. By Corollary 3.3, G^{p-1} totally occurs $q-p-1$ times symmetrically in I_N. Consequently, all the gaps range symmetrically from 0 to $p-1$. □

Corollary 3.5. *[From Lemmas 3 and 7]. Given an odd integer $N = pq$, where p and q are odd integers such that $(p,q) = 1$ and $\lambda p < q < (\lambda+1)p$ with $\lambda \geq 1$ being an integer; let $r = q - \lambda p > 1$ and $I_N = [1, N-1]$ be an integer interval; assume Ξ is a set defined by*

$$\Xi = \{r, (\left\lfloor \frac{p}{r} \right\rfloor + 1)r - p, ..., (\left\lfloor \frac{jp}{r} \right\rfloor + 1)r - jp, ..., (\left\lfloor \frac{(r-1)p}{r} \right\rfloor + 1)r - (r-1)p\} \tag{3.29}$$

Then Ξ contains two elements to identify where G^0 appears and the two elements are symmetrically distributed with respect to the middle | of I_N.

Proof. Write q by $q = \lambda p + r$ with $1 < r < p$; then $(p,r) = 1$ owning to $(p,q) = 1$, and thus an arbitrary integer $0 < \alpha < p$ yields $\alpha q = \alpha\lambda p + \alpha r$. By Lemma 3 $\alpha = \lceil \frac{p}{r} \rceil$ enables $(\alpha - 1)r < p$ and $\alpha r > p$. Let $\alpha r = \lambda_1 p + r_1$ with $\lambda_1 \geq 1$ and $0 < r_1 < p$ being integers turns αq to be

$$\alpha q = (\alpha\lambda + \lambda_1)p + r_1 \tag{3.30}$$

meaning αq to lie between $(\alpha\lambda + \lambda_1)p$ and $(\alpha\lambda + \lambda_1 + 1)p$, as illustrated with Figure 4.

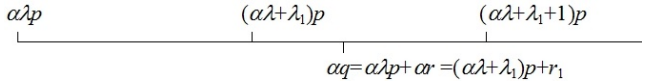


Figure 4: *αq lies between $(\alpha\lambda + \lambda_1)p$ and $(\alpha\lambda + \lambda_1 + 1)p$*

This time, $G^{r_1 - 1}$ occurs between $(\alpha\lambda + \lambda_1)p$ and αq, whereas $G^{p - r_1 - 1}$ occurs between αq and $(\alpha\lambda + \lambda_1 + 1)p$. Continuing such process finally obtains

$$\veebar G^{g-1} \Leftrightarrow \alpha r \equiv g (\bmod p), 0 < g < p \tag{3.31}$$

Since any time G^{g-1} occurs, G^{p-g-1} must simultaneously appears; it follows

$$\veebar G^{g-1} \Leftrightarrow \begin{cases} \alpha r \equiv g (\bmod p) \\ \alpha r \equiv p - g (\bmod p) \end{cases}, 0 < g < p \tag{3.32}$$

Now let α take $1, 2, ...,$ and $p-1$ in (3.27); then a set Λ is obtained by

$$\Lambda = \{1r, 2r, ..., (p-1)r\}. \tag{3.33}$$

As indicated in (3.31), knowing when G^0 occurs is equivalent to knowing what α makes $\alpha r \equiv 1 (\bmod p)$ or $\alpha r \equiv p - 1 (\bmod p)$. Consequently, the problem is turned to ascertain the existence of the residue classes $[1]_p$ and $[p-1]_p$ within $(rZ_p)^* = \{[r]_p, [2r]_p, ..., [(p-1)r]_p\}$. By the conclusion (C2) of Lemma 7, $(rZ_p)^*$ can be divided into r subsets, say,

$$(rZ_p)^* = \Lambda_0 \cup \Lambda_1 \cup \cdots \cup \Lambda_{r-1}, \tag{3.34}$$

where the k-th subset Λ_k contains $n_k = \left\lceil \frac{(k+1)p}{r} \right\rceil - \left\lfloor \frac{kp}{r} \right\rfloor - 1$ elements calculated by

$$\Lambda_k = \{(\left\lfloor \frac{kp}{r} \right\rfloor + 1)r - kp, (\left\lfloor \frac{kp}{r} \right\rfloor + 2)r - kp, \cdots, (\left\lceil \frac{(k+1)p}{r} \right\rceil - 1)r - kp\}, \tag{3.35}$$

in which the j-th element is calculated by

$$e_k^j = (j + \left\lfloor \frac{kp}{r} \right\rfloor)r - kp, k = 0, 2, ..., r-1,$$

where $1 \leq j \leq n_k$.

It is seen that the set Ξ is actually formed by taking the first element from each of $\Lambda_0, \Lambda_1,$ ..., and Λ_{r-1}, namely,

$$\Xi = \{r, (\left\lfloor \frac{p}{r} \right\rfloor + 1)r - p, ..., (\left\lfloor \frac{jp}{r} \right\rfloor + 1)r - jp, ..., (\left\lfloor \frac{(r-1)p}{r} \right\rfloor + 1)r - (r-1)p\} \tag{3.36}$$

According to the conclusion (C5) of Lemma 7, Ξ constitutes the least positive complete residue system modulo r. Consequently, two elements, $1 \in \Xi$ and $r - 1 \in \Xi$, can determine the locations where G^0 occurs. By virtue of symmetry, the occurrences G^0 is symmetrically distributed in I_N. □

Remark 4. By (3.32),

$$\veebar G^0 \Leftrightarrow \alpha r \equiv \pm 1 (\mathrm{mod}\, p) \tag{3.37}$$

which is equivalent to

$$\veebar G^0 \Leftrightarrow \alpha(q-\lambda p) \equiv \pm 1 (\mathrm{mod}\, p) \Leftrightarrow \alpha q \equiv \pm 1 (\mathrm{mod}\, p)$$

indicating α is a solution of x in the Diophantine equation $xq - yp = \pm 1$. This perfectly matches to the assertions made in Lemma 6.

Corollary 3.6. *[From Lemmas 5, 7, and 8]. Given an odd integer $N = pq$, where p and q are odd integers such that $(p,q) = 1$ and $\lambda p < q < (\lambda+1)p$ with $\lambda \geq 1$ being an integer; let $r = q - \lambda p > 1$ and $I_N = [1, N-1]$ be an integer interval; assume Θ is a set defined by*

$$\Theta = \{(\left\lceil \frac{p}{r} \right\rceil - 1)r, (\left\lceil \frac{2p}{r} \right\rceil - 1)r - p, \ldots, (\left\lceil \frac{(j+1)p}{r} \right\rceil - 1)r - jp, \ldots, (p - \left\lceil \frac{p}{r} \right\rceil)r - (r-2)p\}. \tag{3.38}$$

Then G^{p-1} occurs $q-p-1$ times symmetrically in I_N and all the $q-p-1$ occurrences are distributed in p integer intervals $[p, \lambda p]$, $[jq, (j+1)q]$, and $[(p-1)\lambda + 1)p, (q-1)p]$, where integer j satisfies $1 \leq j \leq p-2$. Among all the p intervals, there exist $r-1$ ones, each of which is associated with a distinct element of Θ and in which G^{p-1} occurs λ times, whereas in the other ones G^{p-1} occurs $\lambda - 1$ times.

Proof. First prove that G^{p-1}occurs $\lambda - 1$ times in each of $[p, \lambda p]$ and $[((p-1)\lambda + 1)p, (q-1)p]$. In fact, write $q = \lambda p + r$ with $1 < r < p$; then q lies between λp and $(\lambda+1)p$, resulting in G^{p-1} occurring $\lambda - 1$ times from p to λp, as illustrated with Figure 5. The symmetric property ensures that the same situation occurs from $((p-1)\lambda + 1)p$ to $(q-1)p$.

Figure 5: *$q = \lambda p + r$ lies between λp and $(\lambda+1)p$*

By Corollary 3.2, there are λ or $\lambda + 1$ hosts of p between two adjacent hosts of q. To know when they occur $\lambda + 1$ times, still use the sets Λ and $(rZ_p)^*$ defined in (3.33) and (3.34). Consider the k-th subset Λ_k given by

$$\Lambda_k = \{e_k^1, e_k^2, \ldots, e_k^{n_k}\},$$

where the last element $e_k^{n_k}$ is calculated by $e_k^{n_k} = (\left\lceil \frac{(k+1)p}{r} \right\rceil - 1)r - kp$.

For convenience, let e_k^{last} represent $e_k^{n_k}$. By the conclusion (C4) of Lemma 7,

$$e_k^{last} - e_{k+1}^1 = p - r, 0 \leq k \leq r-2.$$

Referring to (3.22), let $\alpha_k = \left\lceil \frac{(k+1)p}{r} \right\rceil - 1 = \left\lfloor \frac{(k+1)p}{r} \right\rfloor$ for $k = 0, 1, \ldots, r-2$ so as to obtain $r-1$ integer interval $[\alpha_k q, (\alpha_k + 1)q]$. Since $\Theta = \{e_0^{last}, e_1^{last}, \ldots, e_{r-2}^{last}\}$, each of its elements is uniquely associated with such an interval, whose total number is $r-1$. By Lemma 8, G^{p-1} occurs λ times in each of these intervals. Meanwhile, for $0 \leq k \leq r-1$ each element but for e_k^{last} in Λ_k accomplishes an interval in which G^{p-1} occurs $\lambda - 1$ times. The number of all these intervals is

$$n_I^{\lambda-1} = \sum_{i=0}^{r-1} (n_k - 1).$$

By (3.21), $\sum_{j=0}^{r-1} n_j = p - 1$, resulting in

$$n_I^{\lambda-1} = \sum_{i=0}^{r-1} (n_k - 1) = p - r - 1.$$

Hence including $[p,\lambda p]$ and $[(p-1)\lambda+1)p,(q-1)p]$, there are $p-r+1$ intervals in each of which G^{p-1} occurs $\lambda-1$ times. As a result, including the $r-1$ ones where G^{p-1} occurs λ times, the total number of the intervals where G^{p-1} occurs is p and the total number of the times that G^{p-1} occurs is calculated by

$$n_{G^{p-1}} = (r-1)\lambda + (p-r+1)(\lambda-1) = p\lambda + r - p - 1 = q - p - 1.$$

Finally, the symmetric property ensures that Corollary 3.6 holds.

□

Theorem 3.7. *Given an odd integer $N = pq$, where p and q are odd integers such that $(p,q) = 1$ and $\lambda p < q < (\lambda+1)p$ with λ being a positive integer; let $I_N = [1, N-1]$ be an integer interval. Then in I_N, each of $G^0, G^1, \ldots,$ and G^{p-2} occurs symmetrically twice, while G^{p-1} symmetrically occurs $q-p-1$ times in p distinct subintervals. Furthermore, among the p subintervals, there are $r-1$ ones in each of which G^{p-1} occurs λ times, whereas it occurs $\lambda-1$ times in each of the rest $p-r+1$ ones, where $r = q-\lambda p$.*

Proof. Corollaries 3.3, 3.5, and 3.6 directly induce this theorem. □

3.3 Computational Tests

The outcomes of the lemmas, corollaries, and theorems were evaluated using Maple software. The corresponding Maple script programs are available in reference [18]. Here present several examples of these evaluations.

Example 1. Take $N = 115$; then $p = 5$, $q = 23$, $\lambda = 4$, $r = 3$, and $q-p-1 = 17$. The computed results are as follows.

1). Hosts of p and q are as follows:

5, 10, 15, 20, 23, 25, 30, 35, 40, 45, 46, 50, 55, | ,60, 65, 69, 70, 75, 80, 85, 90, 92, 95, 100, 105, 110.

2). There are 5 hosts of p following 23 and 69, respectively.

3). In $[1,114]$, there are 5 subintervals each of which contains 3 or 4 gaps of values 4; among the 5 subintervals, 2 ones contain 4 gaps of value 4 each. All the gaps are symmetrically distributed in $[1,114]$.

4). The distribution of all the gaps is illustrated with Figure 6, which is exactly consistent with Theorem 3.7.

Example 2. Take $N = 923$; then $p = 13$, $q = 71$, $\lambda = 5$, $r = 6$, and $q-p-1 = 57$. Computed results are as follows.

1). Hosts of p and q are as follows:

13, 26, 39, 52, 65, 71, 78, 91, 104, 117, 130, 142, 143, 156, 169, 182, 195, 208, 213, 221, 234, 247, 260, 273, 284, 286, 299, 312, 325, 338, 351, 355, 364, 377, 390, 403, 416, 426, 429, 442, 455, |, 468, 481, 494, 497, 507, 520, 533, 546, 559, 568, 572, 585, 598, 611, 624, 637, 639, 650, 663, 676, 689, 702, 710, 715, 728, 741, 754, 767, 780, 781, 793, 806, 819, 832, 845, 852, 858, 871, 884, 897, 910.

2). There 6 hosts of p following 142,284,436,568, and 710, respectively.

3). In $[1,922]$, there are 13 subintervals each of which contains 4 or 5 gaps of value 12; among the 13 subintervals, 5 ones contain 5 gaps of value 12 each. All the gaps are symmetrically distributed in $[1,922]$.

4). The distribution of all the gaps is depicted with Figure 7, which is exactly consistent with Theorem 3.7.

Example 3. Take $N = 495$; then $p = 11$, $q = 45$, $\lambda = 4$, $r = 1$, and $q-p-1 = 33$. Computed results are as follows.

1). Hosts of p and q are as follows:

11, 22, 33, 44, 45, 55, 66, 77, 88, 90, 99, 110, 121, 132, 135, 143, 154, 165, 176, 180, 187, 198, 209, 220, 225, 231, 242, |,253, 264, 270, 275, 286, 297, 308, 315, 319, 330, 341, 352, 360, 363, 374, 385, 396, 405, 407, 418, 429, 440, 450, 451, 462, 473, 484.

2). In $[1,494]$, G^{10} occurs 33 times across 11 subintervals; each of the 11 subintervals contains 3 occurrences. All the gaps are symmetrically distributed in $[1,494]$.

3). The distribution of all the gaps is depicted with Figure 8, which is exactly consistent with Corollary 3 and Theorem 3.7.

Example 4. Take $N = 493$; then $p = 17$, $q = 29$, $\lambda = 1$, $r = 12$, and $q-p-1 = 11$. Computed results are as follows.

1). Hosts of p and q are as follows:

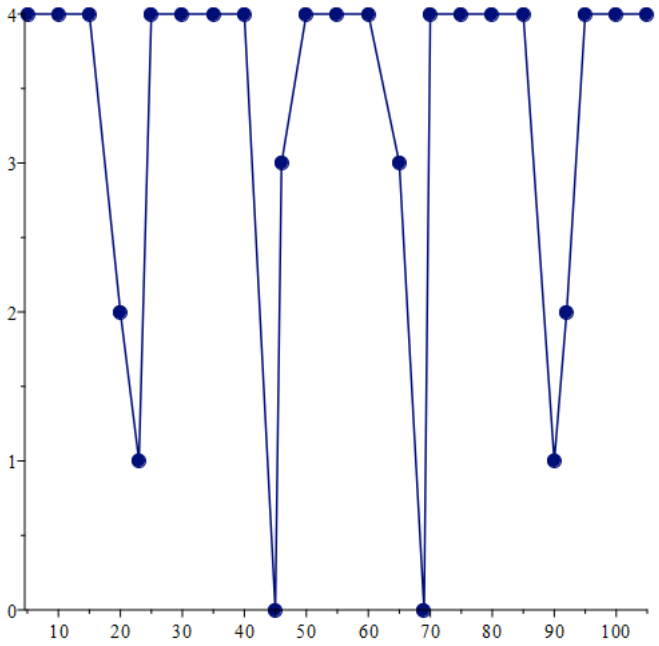


Figure 6: *Gap distribution of hosts hosting 5 and 23*

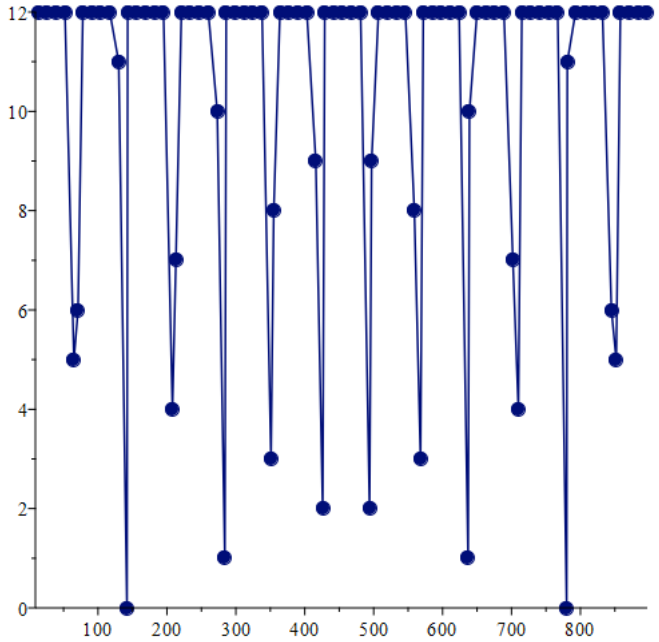


Figure 7: *Gap distribution of hosts hosting 13 and 71*

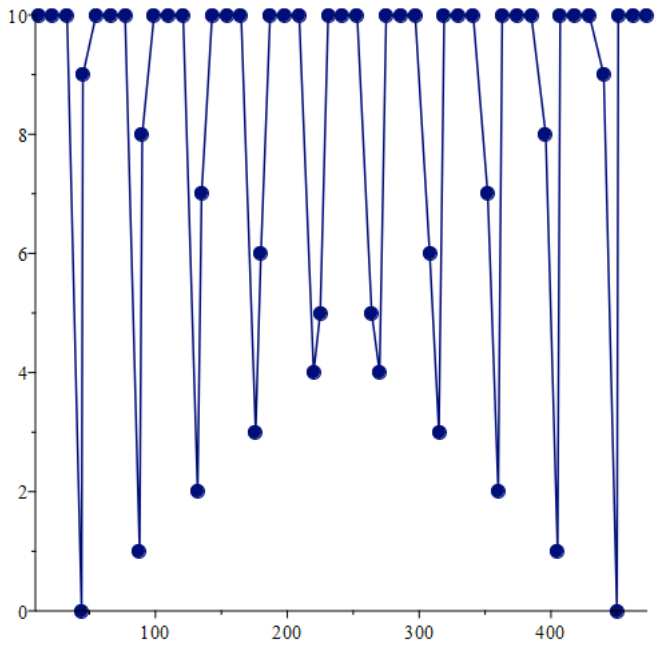


Figure 8: *Gap distribution of hosts hosting 11 and 45*

17, 29, 34, 51, 58, 68, 85, 87, 102, 116, 119, 136, 145, 153, 170, 174, 187, 203, 204, 221, 232, 238, ⋮,255, 261, 272, 289, 290, 306, 319, 323, 340, 348, 357, 374, 377, 391, 406, 408, 425, 435, 442, 459, 464, 476.

2). In $[1,492]$, G^{16} occurs 11 times and all the gaps are symmetrically distributed.

3). The distribution of all gaps is illustrated in Figure 9, which aligns precisely with Corollary 3 and Theorem 3.7.

3.4 An Intriguing Phenomenon For Further Exploration

An intriguing phenomenon has been observed in the computer tests, as illustrated in Figures 10, 11, and 12. These figures are derived from cases that $q = \lambda p \pm 1$ and $q = \alpha p \pm 3$, where $\lambda, \alpha > 1$. The case $q = 2p \pm 1$, including that depicted in Figure 8, exhibits a prominent X shape for the gaps smaller than $p - 1$. The case $q = \alpha p \pm 3$ emerges several Xs. In fact, tests shows that $q = \alpha p \pm 1$ also exhibits a big X. This phenomenon is surely worth to have an exploration, as another mathematical problem.

4 Conclusion and Future Work

Understanding the distribution of divisors of an odd integer within a specified interval is undoubtedly advantageous for developing effective algorithms to identify the divisors of an unfactorized odd integer. This paper completes the investigation to discover such distributions. The corollaries and theorems established herein unveil a novel symmetric and nearly periodic characteristic among hosts of semiprime's divisors, indicating that the distribution of the hosts hosting a semiprime's divisors exhibits local accumulation amidst global sparsity. When extended to general composite odd integers, this distribution proves beneficial in narrowing down ranges for identifying specific expected divisors of unfactorized composite integers.

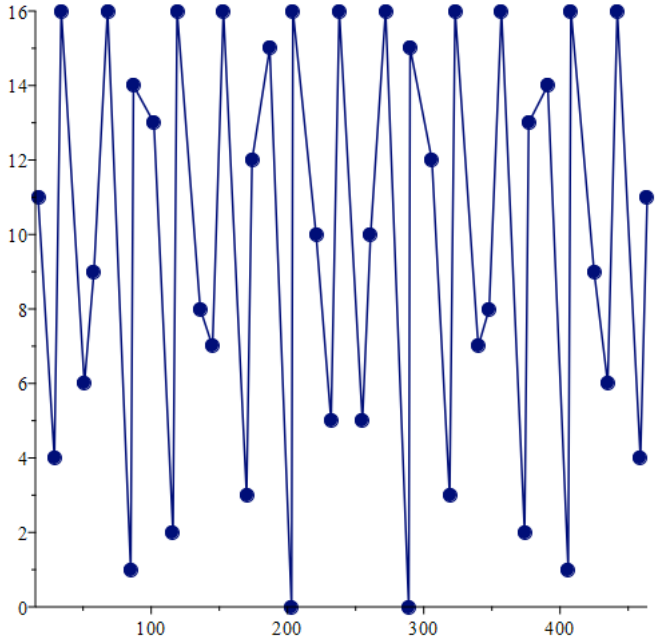
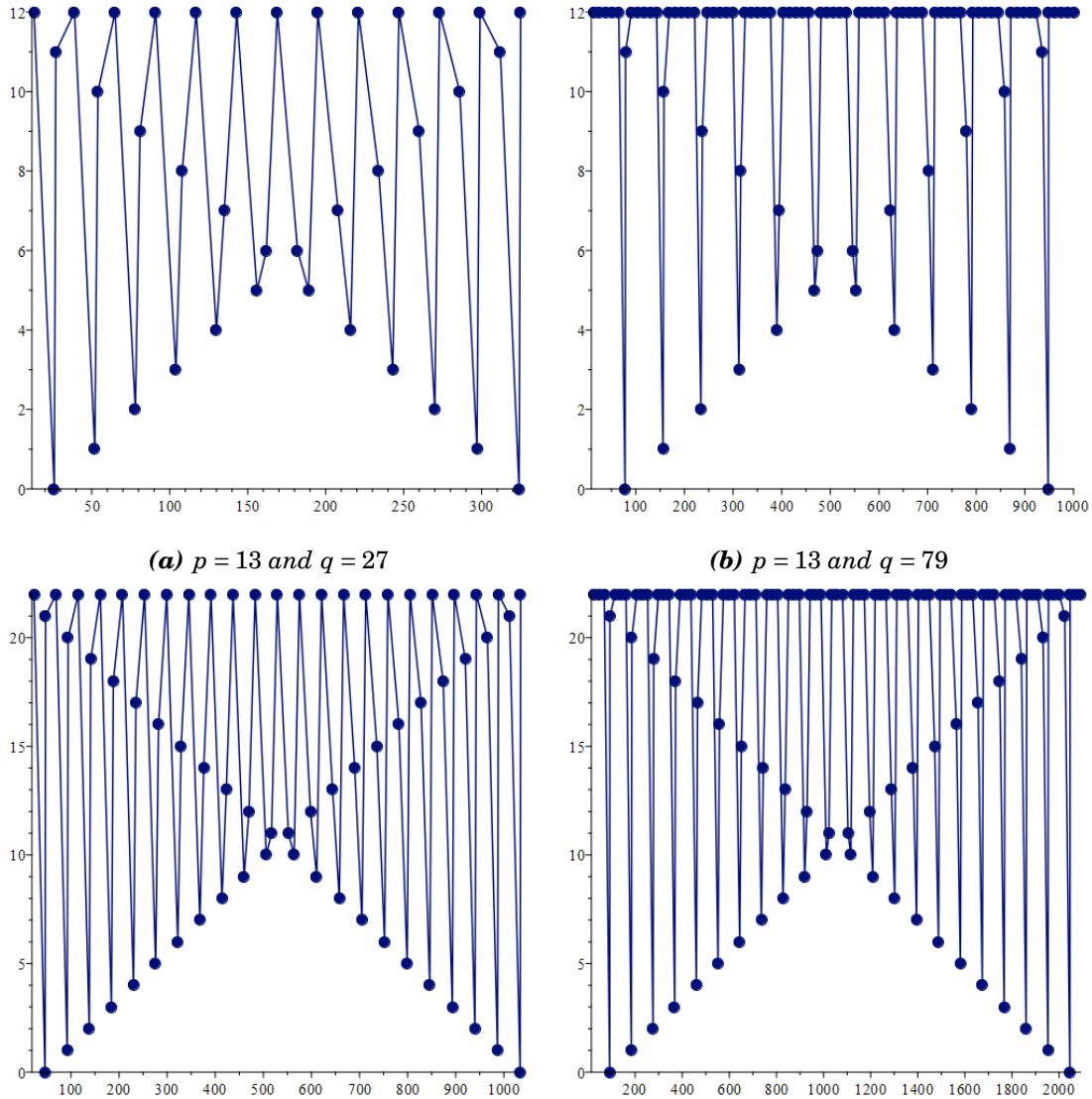


Figure 9: *Gap distribution of hosts hosting 17 and 29*

By the way, the phenomenon observed during computational tests presents an intriguing problem for future research endeavors of interest. It is hoped to be addressed by emerging researchers in due course.

Disclaimer (Artificial Intelligence)

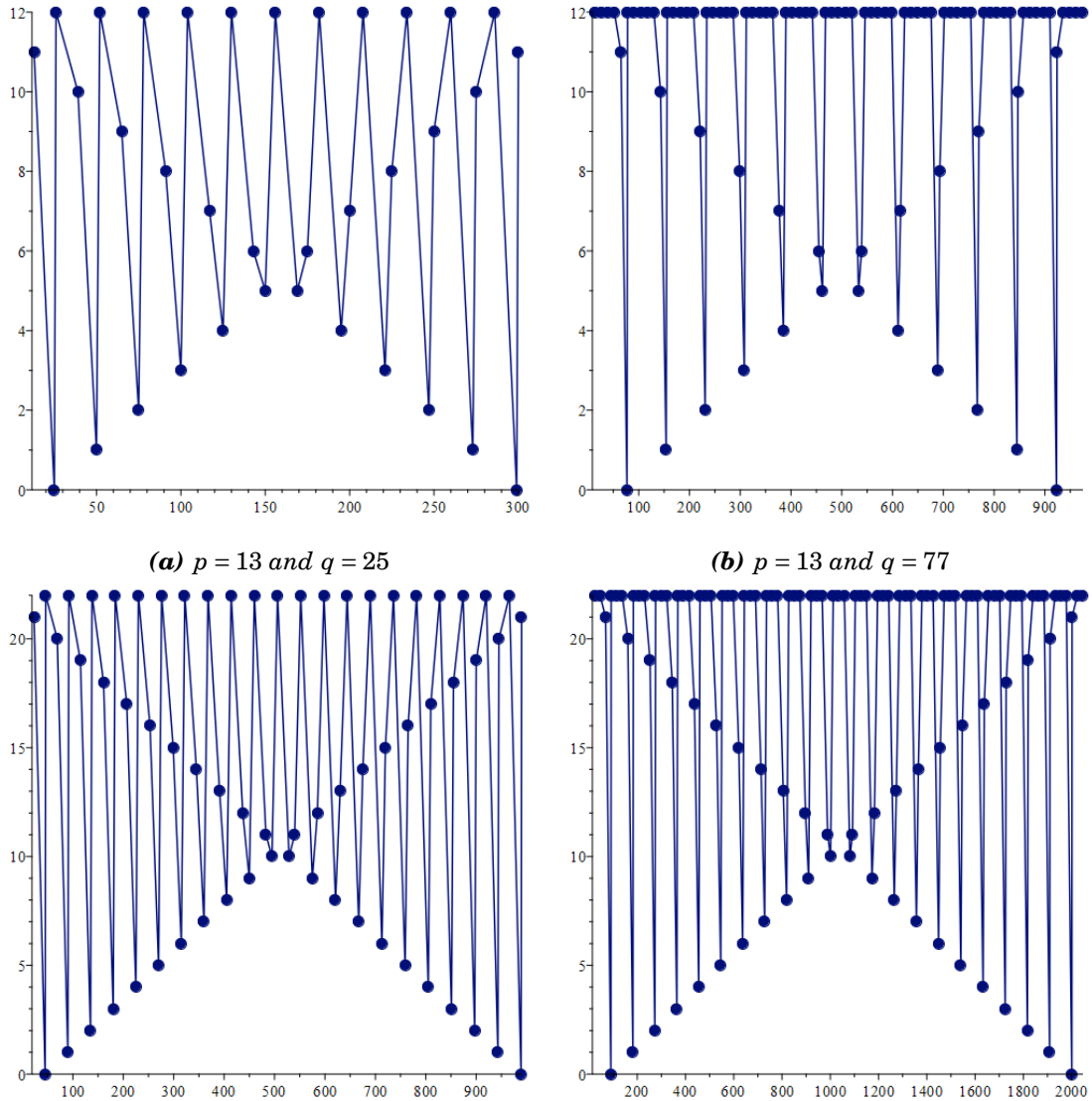
Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc) and text-to-image generators have been used during writing or editing of this manuscript.



(a) $p = 13$ *and* $q = 27$ ***(b)*** $p = 13$ *and* $q = 79$

(c) $p = 23$ *and* $q = 47$ ***(d)*** $p = 23$ *and* $q = 93$

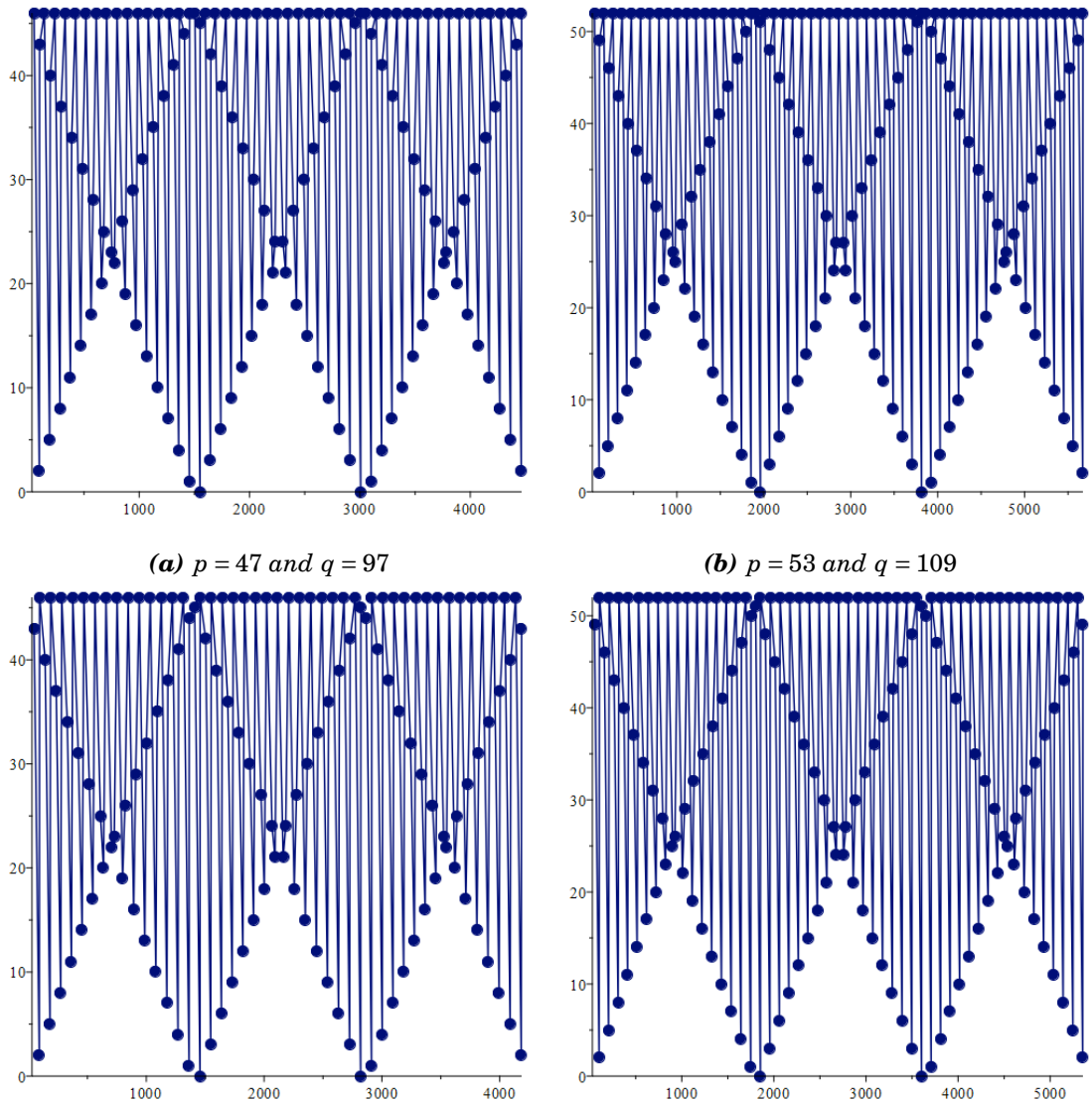
Figure 10: *Big X in the case of* $q = \lambda p + 1$



(a) $p = 13$ *and* $q = 25$ ***(b)*** $p = 13$ *and* $q = 77$

(c) $p = 23$ *and* $q = 45$ ***(d)*** $p = 23$ *and* $q = 91$

Figure 11: *Big X in the case of* $q = \lambda p - 1$



(a) $p = 47$ *and* $q = 97$ ***(b)*** $p = 53$ *and* $q = 109$

(c) $p = 47$ *and* $q = 91$ ***(d)*** $p = 53$ *and* $q = 103$

Figure 12: *Several Xs in the case of* $q = \lambda p \pm 3$

References

1 .X. Wang, Distribution of Divisors of an Integer in a Triangle Integer Sequence, JP Journal of Algebra, Number Theory and Applications 63(2) (2024) 185–208.
DOI:10.17654/0972555524011.

[2] X. Wang, *Densification of witnesses for randomized algorithm design*, Journal of Advances in Mathematics and Computer Science **38**(10) (2023) 44–69.
DOI:10.9734/JAMCS/2023/v38i101823.

[3] X. Wang, *Minimal Gap among Integers having a Common Divisor with an Odd Semi-prime*, Journal of Advances in Mathematics and Computer Science **39**(6) (2024) 1–7.
DOI:10.9734/jamcs/2024/v39i61896

[4] X. Wang, *Maximum Gap Among Integers Having a Common Divisor With an Odd Semi-Prime*,Journal of Advances in Mathematics and Computer Science, **39**(10) (2024) 51–61.
DOI:10.9734/jamcs/2024/ v39i101934.

[5] X. Wang, *Leveraging Lévy Flight for Efficient Divisor Identification in Odd Composite Integers*,Journal of Advances in Mathematics and Computer Science, **39** (11) 116–139.
DOI:10.9734/jamcs/2024/v39i111943.

[6] David M. Burton. *Elementary Number Theory(7th ed)*, McGraw-Hill,(2010).

[7] K. H. Rosen, *Elementary Number Theory and Its Applications(6th ed.)*, Addison-Wesley (2011).

[8] D. R. Beath-Brown and H. Iwaniec, *On the Difference Between Consecutive Primes*, Bulletin of the American Mathematical Society **1**(5) (1979) 758–759.

[9] J. Galambos, *On a conjecture of Katai concerning weakly composite numbers*, Proc. Amer.Math. Soc. **96** (1984) 215–216.

[10] J. Galambos and I. Katai, *The Gaps in a Particular Sequence of Integers of Positive Density*,Journal of the London Mathematical Society,**2**(36) (1987) 429–435.

[11] B. Y. Wang and X. Wang, *Symmetrical Distribution of Primes and Their Gaps*, Advances in Pure Mathematics **11**(05) (2021) 447–456.
DOI:10.4236/apm.2021.115031.

[12] B. Melvyn Nathanson, *Arithmetic Progressions Contained in Sequences with Bounded Gaps*, Canadian Mathematical Bulletin, **23**(04) (2018) 491–493.
DOI:10.4153/CMB-1980-074-x.

[13] Y. Liu, P. S. Park, and Z. Song, *Bounded gaps between products of distinct primes*, Res. number theory **3**(26) (2017) 1–28.
DOI:10.1007/s40993-017-0089-3.

[14] Jean-Marie De Koninck, *On the distance between consecutive divisors of an integer*, Canadian Mathematical Bulletin **29**(02) (1986) 208–217.

[15] D. Berend and J. E. Harmse, *Gaps between consecutive divisors of factorials*, Annales de l'institut Fourier **43**(3) (1993) 569–583.

[16] C. D. Olds, *Continued Fractions*, Mathematical Association of America (1992).
DOI:10.5948/UPO9780883859261.

[17] X. Wang, *Frequently-Used Properties of the Floor Function*,International Journal of Applied Physics and Mathematics **10**(4) (2020) 135–142.
DOI:10.17706/ijapm.2020.10.4.135-142.

[18] X. Wang, *Maple Source Codes, Mapleprimes*.Traced at:
https://www.mapleprimes.com/posts/227697-Source-Codes-For-Gaps-Among-Integers?sp=227697