Minimal Gap Among Integers Having a Common Divisor with an Odd Semi-prime

Abstract

For an odd semi-prime N = pq, this paper proves that the gaps are symmetrically distributed between two integers in interval [1;N 1] that have a common divisor with N and there exists a gap of zero between a multiple of p and a multiple of q. These results exhibit that the multiples of the divisors of a composite odd integer lie accumulatively here and there, although each of them lies sparsely in a whole interval. Such distribution of local accumulation in global sparsity is beneficial for designing randomized algorithms that can find a divisor of a composite odd integer. The paper also leaves a problem to find out the detail distribution of the non-zero gaps.

Keywords:Integer Distribution; Gap; Semi-prime; Common Divisor; Algorithm Design.

1 New Problems From Observation

Given a semiprime N = 15 that has two divisors, 3 and 5; Checking each integer from 3 to 14 knows that integers 3, 6, 9, and 12 are multiples of 3, while integers 5 and 10 are multiples of 5. Using the terminologies 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. By arranging all these hosts in order, a sequence can be achieved.

3, 5, 6, 9, 10, 12

Using a terminology 'gap' to describe the number of integers between two given integers, it is seen that two pairs of the hosts, 5 and 6, 9 and 10, have a gap of zero respectively and they are distributed symmetrically with respect to 'the intermediate spot' of the sequence. Changing N to 119, which has two divisors of 7 and 17, leads to the following host sequence

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

It can be seen that 34 and 35 are respectively symmetric to 85 and 84 with respect to the intermediate spot of the sequence, and each pair leaves a gap of zero.

Now comes a problem: is this a general property of the hosts of a semi-prime's divisors? This paper investigates the problem and proves that the answer is YES. The paper consists of six sections. Section 2 reviews the related literature to show that the problem is truly a new one that no previous study of it has been made. Section 3 introduces the symbols, notations, and the definitions of the researched integer sequence; section 4 presents main results as well as their proofs; section 5 shows a potential application of the results; section 6 is the conclusion.

2 Simple Review of Relevant Literatures

The topic of this paper is related with two issues in number theory: one is the study of the gaps between integers and the other is the distributions of the divisors of a composite integer. The first one can be traced hundreds of years ago, mainly involved in the exploring the gaps between primes, between integers in an arithmetic progression, and between integers in some particular set of integers. Typical recent literatures of the first kind are [3], [4],and [5]. Brandon Y Wang and his partner in [3] proved a symmetrical distribution of primes and their Gaps, Melvyn B Nathanson in [4] researched arithmetic progressions contained in sequences with bounded gaps, and Liu Y in [5] estimated bounded gaps between products of distinct primes. The second issue mainly concerns the distribution of an integer's divisors in an interval or a sequence. Seen in the introductory section of [1], the relevant researches have been continued because it is closely related with the study of integer factorization. The problem raised in this paper concerns the gaps between the integers having a common divisor with a third composite integer. It does not belong to either of the two mentioned issues. It is therefore a new type of problem.

3 Preliminaries

This section presents necessary symbols, notations, definitions, and fundamental knowledge

for later investigation.

3.1 Terminologies, Symbols and Notations

Symbol A) B means conclusion B can be derived from condition A. A , B means both A) B and B) A. Symbols bxc is the floor function taking integer part of real x such that x□1 < bxc _ x. The terminologies of integer interval, odd interval, host interval, host number of an integer, and the Cartesian subtraction are seen in [1] or [2]. Symbol **Z** denotes the set of integers, symbol Z_+ denotes the set of positive integers, and symbol (a; b) expresses the greatest common divisor (GCD) of integers a and b. Symbols $S_{m!n}$, $n_{p\ x}$, $n_{p;q\ x}$, and $n_{p\ m!x}$ are those described in [1]. Symbol h_x means h is a host of x. For positive integers a and b, integer g_{ba} = ja □ bj □ 1 is called the gap between a and b. For example, a = 5 and b = 3 result in $g_{5\ 3}$ = 1, saying there is one integer between 3 and 5.

3.2 Lemmas

Lemma 3.1. (Seen in [1]) Let N = pq be an odd composite integer with 2 < p < q being odd integers, and $S_{1!N□1}$ = f1; 2; :::; m; :::;N □ m; :::;N □ 1g, where 1 _ m _ N □ 1; then $n_{p\ 1!m}$ = $n_{p\ N□m!N□1}$ =

$$\frac{m}{p}$$

Lemma 3.2. (Seen in [6]) Let q be a positive odd number, S = f$a_i$ji 2 Z_+g be a set composed of consecutive odd numbers; if a_ 2 S is a host of q, then so it is with $a_{\_+q}$ 2 S.

Lemma 3.3. Let a > 1 and b > 1 be two positive integers such that (a; b) = 1; then there exists (x; y) 2 Z _ Z satisfying ax □ by = 1 with 0 < x < b and 0 < y < a.

Proof. The Theorem 2.1 in C D Olds's book [7] shows the Diophantine equation ax □ by = 1 has an infinite number of integer solutions (x; y) and a particular solution (x_0; y_0) 2 Z _Z can be found with the method of continued fraction (Seen at page 37 in [7]). Then x_0 6_ 0 (mod b)) and the general solution is given by

$$\begin{aligned} x &= x_0 + bt \\ y &= y_0 + at \end{aligned}$$

where t 2 Z.

Next is to prove the existence of 0 < x < b and 0 < y < a through proving the following facts.

(1). x > 0 , y > 0. Otherwise, it is contradictory to ax □ by = 1 under the condition a > 1 and b > 1.

(2). x < b , y < a. Use proof by contradiction. For given x < b, assume y _ a; then it follows y _ a) by = ax□1 _ ab) a(x□b) _ 1) x _ b. Similarly, for given y < a assuming x _ b results in x _ b) ax = by + 1 _ ab) 1 _ (a □ y)b) y _ a, a contradiction.

(3). Existence of 0 < x < b and 0 < y < a. Taking $\frac{□x_0}{b}$ < t < 1 □ $\frac{x_0}{b}$ yields 0 < x = x_0 + bt < b and □1

b < y = y0 + at < a □ 1
b .

4 Main results

Theorem 4.1. Let N = pq be an odd integer and IN = [3;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 hp and hq in IN satisfying 1 < hp; hq < N□1
2 , it holds

ghq
hp = gN□hq
N□hp

Proof. Take m = N□1
2 . Since N is odd, 2 is not a divisor of it. Without loss of generality, let
S1 = f1; 2; :::;mg and S2 = fN □ m;N □ m + 1; :::;N □ 1g. By Lemma 3.1 it yields

np
S1
=
_
N □ 1
2p
_
= np
S2

and

nq
S1
=
_
N □ 1
2q
_
= nq
S2

Since hp 2 S1 is a host of p, N □ hp 2 S2 is surely a host of p. Referring to Lemma 3.2, it knows that hp 2 S1 counted from 1 to m is symmetric to N □ hq 2 S2 counted from N □ 1 to N □m, respectively. Likewise, hq 2 S1 counted from 1 to m must be symmetric to N □hq 2 S2 counted from N □ 1 to N □ m, respectively. As a result, each pair of hp and hq must have a symmetric pair,N □ hp and N □ hq. Therefore it must hold

ghq
hp = gN□hq
N□hp

Example 3.1 Take N = 55; then p = 5, q = 11, m = (N □ 1)=2 = 27,
S1 = f1; 2; 3; 4; 5; 6; 7; 8; 9; 10; 11; 12; 13; 14; 15;
16; 17; 18; 19; 20; 21; 22; 23; 24; 25; 26; 27g
and
S2 = f28; 29; 30; 31; 32; 33; 34; 35; 36; 37; 38; 39; 40;
41; 42; 43; 44; 45; 46; 47; 48; 49; 50; 51; 52; 53; 54g
Let Hp
1 ,Hq
1 be respectively the sets of the hosts of p and q counted from 1 to 27, Hp
2 ,Hq
2 be
respectively the sets of the hosts of p and q counted from 54 to 28; then

$H_{p_1} = \{5, 10, 15, 20, 25\}; H_{p_2} = \{30, 35, 40, 45, 50\}$

$H_{q_1} = \{11, 22\}; H_{q_2} = \{33, 44\}$

Use the Cartesian products, $H_{p_1} \times H_{q_1}$ and $H_{p_2} \times H_{q_2}$, to produces all the pairs of $h_p \in S_1$, $h_q \in S_1$, $h_p \in S_2$ and $h_q \in S_2$ by

$H_{p_1} \times H_{q_1} = \{(5, 11), (5, 22), (10, 11), (10, 22), (15, 11), (15, 22), (20, 11), (20, 22), (25, 11), (25, 22)\}$

and

$H_{p_2} \times H_{q_2} = \{(30, 33), (30, 44), (35, 33), (35, 44), (40, 33), (40, 44), (45, 33), (45, 44), (50, 33), (50, 44)\}$

leading to the sets of gaps by

$G_{p,q_1} = \{5, 16, 0, 11, 3, 6, 8, 1, 13, 2\}$

and

$G_{p,q_2} = \{2, 13, 1, 8, 6, 3, 11, 0, 16, 5\}$

G_{p,q_1} and G_{p,q_2} are surely as stated in Theorem 1.

Theorem 4.2. Let $N = pq$ be an odd integer and $I_N = [3, N-1]$ be an integer interval, where p and q are odd integers with $1 < p < q$ and $(p, q) = 1$; then there exists in I_N a pair, h_p and h_q, satisfying $1 < h_p, h_q < N - 1$, and

$$g_{h_q} - h_p = g_{N-h_q} - h_p = 0$$

Proof. Let $S = \{1, 2, \ldots, N-1\}$. The S and I_N contain the same number of the hosts hosting p and q because N is odd. S contains $q - 1$ hosts of p and $p - 1$ hosts of q. Denote $s = q - 1$ and $t = p - 1$; assume H_p and H_q are the sets of the hosts of p and q in S, respectively; then

$H_p = \{p, 2p, 3p, \ldots, sp\}$

and

$H_q = \{q, 2q, 3q, \ldots, tq\}$

Because $1 < p < q$ and $(p, q) = 1$, assume $q = \_p + r$ with $0 < r < p$; then $\_ = \left\lfloor \frac{q}{p} \right\rfloor$

and

$H_q = \{\_p + r, 2\_p + 2r, 3\_p + 3r, \ldots, t\_p + tr\}$

Let $C_{p,q}$ be the set formed by the Cartesian subtraction $H_q - H_p$; then

$C_{p;q}$ = f(_ □ 1)p + r; (_ □ 2)p + r; (_ □ 3)p + r; :::; (_ □ s)p + r;
(2_ □ 1)p + 2r; (2_ □ 2)p + 2r; (2_ □ 3)p + 2r; :::; (2_ □ s)p + 2r;
(3_ □ 1)p + 3r; (3_ □ 2)p + 3r; (3_ □ 3)p + 3r; :::; (3_ □ s)p + 3r;
::::::
(t_ □ 1)p + tr; (t_ □ 2)p + tr; (t_ □ 3)p + tr; :::;
(t_ □ t)p + tr; :::; (t_ □ s)p + trg

and the gap set $G_{p;q}$ is obtained by
$G_{p;q}$ = fj(_ □ 1)p + rj □ 1; j(_ □ 2)p + rj □ 1; :::; j(_ □ s)p + rj □ 1;
j(2_ □ 1)p + 2rj □ 1; j(2_ □ 2)p + 2rj □ 1; :::; j(2_ □ s)p + 2rj □ 1;
::::::
j(t_ □ 1)p + trj □ 1; j(t_ □ 2)p + trj □ 1; :::;
j(t_ □ t)p + trj □ 1; :::; j(t_ □ s)p + trj □ 1g
Or
$G_{p;q}$ = fj(x_ □ y)p + xrj □ 1g
where 1 < x < t and 1 < y < s are integers.
Note that, q = _p + r) (x_ □ y)p + xr = x(_p + r) □ yp = xq □ yp. By Lemma 3.3, there exist an integer solution (x; y) 2 Z _ Z for xq □ yp = 1 with 0 < x < p and 0 < y < q, leading to j(x_ □ y)p + xrj □ 1 = 0 and saying there is a pair, h_p and h_q with 1 < h_p; h_q < N □ 1 and g_{h_q}
$_{h_p}$ = 0. By symmetric property stated in Theorem 4.1, Theorem 4.2 holds.
Remark 4.1. With Maple software, programs to test Theorems 4.1 and 4.2 can be easily programmed, as traced at:
https://www.mapleprimes.com/posts/224943-Distribution-Of-Integers-Having-A-Divisor?sp=224943
Remark 4.2. Observation shows that there exist h_p and h_q in I_N, satisfying 1 < h_p; h_q < N□1, and
g_{h_q}
$_{h_p}$ = $g_{N□h_q}$
$_{N□h_p}$ = _
where _ > 0 is an integer.
Unfortunately, no proof has been found for this statement yet, nor is it known what values _ takes.

5 Application Occasion

Given a composite odd integer N and an integer interval I_N = [3;N □ 1], let H_{dN} be the set of
all the hosts of N's divisors, say
H_{dN}
= fh1; h2; :::; $h_{d(N)}$g
where d(N) is the number of distinct divisors of N.
By Theorems 4.1 and 4.2, the elements of H_{dN} demonstrate a distribution of a certain
symmetry with respect to the intermediate of H_{dN} and there are pairs of elements having
a zero-gap if those elements are arranged in order. This property not only answers the question raised in the introductory part, but also reveals a distribution of global-sparse-withlocal-accumulation: all the hosts are distributed sparsely in a global scope while some are locally accumulated somewhere. Such distribution of global-sparse-with-local-accumulation provides a reference to design algorithm to find a divisor of a composite integer with globallocal blending searches.

6 Conclusion

The theorems proved in this paper reveal a new symmetric characteristic of the hosts of semiprime
divisors. The new symmetric characteristic shows that the distribution of the hosts of a semi-prime's divisors is normally of global-sparse-with-local-accumulation. Extended to a general composite odd integer, such a distribution can be a reference for designing certain algorithm to find a divisor of a composite integer, benefiting for solve the problem of integer factorization.

Nevertheless, this paper leaves behind a regret that is stated in Remark 4.2. Hope the problem can be solved by younger researchers soon in the future.

References

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

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

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

[4] Melvyn B. Nathanson. (2018). Arithmetic Progressions Contained in Sequences with Bounded Gaps. Canadian Mathematical Bulletin , 23(4), 491 - 493.
DOI: 10.4153/CMB-1980-074-x

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

[6] Wang X. (2016). Valuated Binary Tree: A New Approach in Study of Integers. International Journal of Scientific and Innovative Mathematical Research (IJSIMR), 4(3),63-67.
DOI: 10.20431/2347-3142.0403008

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