Original Research Article

Distribution of Integers Having a Divisor with an Odd Semi-prime

Abstract

This paper proves that the integers having a divisor with a given odd semi-prime $N = pq$ are symmetrically distributed in interval $[1, N-1]$ and there exists a multiple of p lying adjacent to 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 benefits in designing certain randomized algorithms to find a divisor of a composite odd integer.

Keywords:Integer Distribution; Semi-prime; Common Divisor; Algorithm Design.
2010 Mathematics Subject Classification:11N05, 65Y04

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 five sections. Section 2 introduces the symbols, notations, and the definitions of the researched integer sequence; section 3 presents main results as well as their proofs; section 4 shows a potential application of the results; section 5 is the conclusion.

2 Preliminaries

This section presents necessary symbols, notations, definitions, and fundamental knowledge for later investigation.

2.0.1 Terminologies, Symbols and Notations

Symbol $A \Rightarrow B$ means conclusion B can be derived from condition A. $A \Leftrightarrow B$ means both $A \Rightarrow B$ and $B \Rightarrow A$. Symbols $\lfloor x \rfloor$ is the floor function taking integer part of real x such that $x - 1 < \lfloor x \rfloor \leq x$. 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 $\mathbf{Z}$ denotes the set of integers, symbol $\mathbf{Z}^+$ denotes the set of positive integers, and symbol (a, b) expresses the greatest common divisor (GCD) of integers a and b. Symbols $S_{m\to n}$, n_X^p, $n_X^{p,q}$, and $n_{m\to x}^p$ are those described in [1]. Symbol h^x means h is a host of x. For positive integers a and b, integer $g_a^b = |a - b| - 1$ is called the gap between a and b. For example, $a = 5$ and $b = 3$ result in $g_3^5 = 1$, saying there is one integer between 3 and 5.

2.0.2 Lemmas

Lemma 2.1. *(Seen in [1]) Let $N = pq$ be an odd composite integer with $2 < p < q$ being odd integers, and $S_{1\to N-1} = \{1, 2, ..., m, ..., N-m, ..., N-1\}$, where $1 \le m \le N-1$; then*

$$n^p_{1\to m} = n^p_{N-m\to N-1} = \left\lfloor \frac{m}{p} \right\rfloor$$

Lemma 2.2. *(Seen in [3]) Let q be a positive odd number, $S = \{a_i | i \in Z^+\}$ be a set composed of consecutive odd numbers; if $a_\alpha \in S$ is a host of q, then so it is with $a_{\alpha+q} \in S$.*

Lemma 2.3. *Let $a > 1$ and $b > 1$ be two positive integers such that $(a, b) = 1$; then there exists $(x, y) \in Z \times Z$ satisfying $ax - by = 1$ with $0 < x < b$ and $0 < y < a$.*

Proof. The Theorem 2.1 in C D Olds's book [4] shows the Diophantine equation $ax - by = 1$ has an infinite number of integer solutions (x, y) and a particular solution $(x_0, y_0) \in Z \times Z$ can be found with the method of continued fraction (Seen at page 37 in [4]). Then $x_0 \not\equiv 0 \pmod b)$ and the general solution is given by

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

where $t \in Z$.

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

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

(2). $x < b \Leftrightarrow y < a$. Use proof by contradiction. For given $x < b$, assume $y \ge a$; then it follows $y \ge a \Rightarrow by = ax - 1 \ge ab \Rightarrow a(x - b) \ge 1 \Rightarrow x \ge b$. Similarly, for given $y < a$ assuming $x \ge b$ results in $x \ge b \Rightarrow ax = by + 1 \ge ab \Rightarrow 1 \ge (a - y)b \Rightarrow y \ge a$, 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 $-\frac{1}{b} < y = y_0 + at < a - \frac{1}{b}$. □

3 Main results

Theorem 3.1. *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 for each pair of h^p and h^q in I_N satisfying $1 < h^p, h^q < \frac{N-1}{2}$, it holds*

$$g^{h^q}_{h^p} = g^{N-h^q}_{N-h^p}$$

Proof. Take $m = \frac{N-1}{2}$. Since N is odd, 2 is not a divisor of it. Without loss of generality, let $S_1 = \{1, 2, ..., m\}$ and $S_2 = \{N - m, N - m + 1, ..., N - 1\}$. By Lemma 2.1 it yields

$$n^p_{S_1} = \left\lfloor \frac{N-1}{2p} \right\rfloor = n^p_{S_2}$$

and

$$n_{S_1}^q = \left\lfloor \frac{N-1}{2q} \right\rfloor = n_{S_2}^q$$

Since $h^p \in S_1$ is a host of p, $N - h^p \in S_2$ is surely a host of p. Referring to Lemma 2.2, it knows that $h^p \in S_1$ counted from 1 to m is symmetric to $N - h^q \in S_2$ counted from $N-1$ to $N-m$, respectively. Likewise, $h^q \in S_1$ counted from 1 to m must be symmetric to $N - h^q \in S_2$ counted from $N-1$ to $N-m$, respectively. As a result, each pair of h^p and h^q must have a symmetric pair,$N - h^p$ and $N - h^q$. Therefore it must hold

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

□

Example 3.1 Take $N = 55$; then $p = 5$, $q = 11$, $m = (N-1)/2 = 27$,

$$S_1 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, \\ 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27\}$$

and

$$S_2 = \{28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, \\ 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54\}$$

Let H_1^p,H_1^q be respectively the sets of the hosts of p and q counted from 1 to 27, H_2^p,H_2^q be respectively the sets of the hosts of p and q counted from 54 to 28; then

$$H_1^p = \{5, 10, 15, 20, 25\}, H_2^p = \{30, 35, 40, 45, 50\}$$

$$H_1^q = \{11, 22\}, H_2^q = \{33, 44\}$$

Use the Cartesian products, $H_1^p \otimes H_1^q$ and $H_2^p \otimes H_2^q$, 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

$$H_1^p \otimes H_1^q = \{(5, 11), (5, 22), (10, 11), (10, 22), (15, 11), \\ (15, 22), (20, 11), (20, 22), (25, 11), (25, 22)\}$$

and

$$H_2^p \otimes H_2^q = \{(30, 33), (30, 44), (35, 33), (35, 44), (40, 33), \\ (40, 44), (45, 33), (45, 44), (50, 33), (50, 44)\}$$

leading to the sets of gaps by

$$G_1^{p,q} = \{5, 16, 0, 11, 3, 6, 8, 1, 13, 2\}$$

and

$$G_2^{p,q} = \{2, 13, 1, 8, 6, 3, 11, 0, 16, 5\}$$

$G_1^{p,q}$ and $G_2^{p,q}$ are surely as stated in Theorem 1.

Theorem 3.2. *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*

$$g_{h^p}^{h^q} = g_{N-h^p}^{N-h^q} = 0$$

Proof. Let $S = \{1, 2, ..., N-1\}$. 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

$$H^p = \{p, 2p, 3p, ..., sp\}$$

and

$$H^q = \{q, 2q, 3q, ..., tq\}$$

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

$$H^q = \{\alpha p + r, 2\alpha p + 2r, 3\alpha p + 3r, ..., t\alpha p + tr\}$$

Let $C^{p,q}$ be the set formed by the Cartesian subtraction $H^q \ominus H^p$; then

$$\begin{aligned} C^{p,q} = \{&(\alpha-1)p + r, (\alpha-2)p + r, (\alpha-3)p + r, ..., (\alpha-s)p + r,\\ &(2\alpha-1)p + 2r, (2\alpha-2)p + 2r, (2\alpha-3)p + 2r, ..., (2\alpha-s)p + 2r,\\ &(3\alpha-1)p + 3r, (3\alpha-2)p + 3r, (3\alpha-3)p + 3r, ..., (3\alpha-s)p + 3r,\\ &.....\\ &(t\alpha-1)p + tr, (t\alpha-2)p + tr, (t\alpha-3)p + tr, ...,\\ &(t\alpha-t)p + tr, ..., (t\alpha-s)p + tr\} \end{aligned}$$

and the gap set $G^{p,q}$ is obtained by

$$\begin{aligned} G^{p,q} = \{&|(\alpha-1)p + r| - 1, |(\alpha-2)p + r| - 1, ..., |(\alpha-s)p + r| - 1,\\ &|(2\alpha-1)p + 2r| - 1, |(2\alpha-2)p + 2r| - 1, ..., |(2\alpha-s)p + 2r| - 1,\\ &.....\\ &|(t\alpha-1)p + tr| - 1, |(t\alpha-2)p + tr| - 1, ...,\\ &|(t\alpha-t)p + tr| - 1, ..., |(t\alpha-s)p + tr| - 1\} \end{aligned}$$

Or

$$G^{p,q} = \{|(x\alpha - y)p + xr| - 1\}$$

where $1 < x < t$ and $1 < y < s$ are integers.

Note that, $q = \alpha p + r \Rightarrow (x\alpha - y)p + xr = x(\alpha p + r) - yp = xq - yp$. By Lemma 2.3, there exist an integer solution $(x, y) \in Z \times Z$ for $xq - yp = 1$ with $0 < x < p$ and $0 < y < q$, leading to $|(x\alpha - y)p + xr| - 1 = 0$ and saying there is a pair, h^p and h^q with $1 < h^p, h^q < N - 1$ and $g_{h^p}^{h^q} = 0$. By symmetric property stated in Theorem 3.1, Theorem 3.2 holds. □

Remark 3.1. With Maple software, programs to test Theorems 3.1 and 3.2 can be easily programmed, as traced at:
https://www.mapleprimes.com/posts/224943-Distribution-Of-Integers-Having-A-Divisor?sp=224943

Remark 3.2. Observation shows there exists in I_N a pair, h^p and h^q, satisfying $1 < h^p, h^q < N-1$, and

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

where $\alpha > 0$ is an integer.

Unfortunately, no proof has been found for this statement yet, nor is it known what values α takes.

4 Application Occasion

Given a composite odd integer N and an integer interval $I_N = [3, N-1]$, let H_N^d be the set of all the hosts of N's divisors, say

$$H_N^d = \{h_1, h_2, ..., h_{d(N)}\}$$

where $d(N)$ is the number of distinct divisors of N.

By Theorems 3.1 and 3.2, the elements of H_N^d demonstrate a distribution of a certain symmetry with respect to the intermediate of H_N^d 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-with-local-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 global-local blending searches.

5 Conclusion

The theorems proved in this paper reveal a new symmetric characteristic of the hosts of semi-prime 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 3.2. Hope the problem can be solved by younger researchers soon in the future.

References

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

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

[4] Olds C D Continued Fractions. Mathematical Association of America, 1992. DOI: /10.5948/UPO9780883859261