



## Korselt numbers through computational algorithms

Abeer Eshtaya, Khalid Adarbeh\* and Hadi Hamad,

An-Najah National University, Nablus, Palestine

(Dated: November 7, 2023)

**Abstract:** In this article, many concepts such as Korselt numbers that are related to Carmichael numbers have been studied. It deserves to mention that the Korselt numbers and sets were discussed for the first time in 2007 by Echi.

Let  $N$  be a positive integer and  $\alpha$  a non-zero integer. If  $N \neq \alpha$  and  $p - \alpha$  divides  $N - \alpha$  for each prime divisor  $p$  of  $N$ , then  $N$  is called an  $\alpha$ -Korselt number ( $K_\alpha$ -number). Korselt numbers were determined by studying the converse of Fermat's Little Theorem. To validate the concerned theorems, illustrated examples are solved in order to support the correctness of these theories. In this article we addressed errors in the relevant literature, and we introduced proper corrections with proofs for them.

Finally, many notes have been taken and directed us to build and develop a number of algorithms in order to find Korselt sets for relatively large numbers in an effective way which may require a great time and need tedious effort if it is to be calculated manually. .

**Keywords:** Korselt numbers, Korselt sets, Carmichael numbers.

### I. INTRODUCTION

In 1640, Fermat proved his well known result (Fermat's Little Theorem [6, 9]) which states that: "If  $p$  is a prime number, then  $p$  divides  $a^p - a$  for every integer  $a$ ". On the other hand, Korselt studied the converse of Fermat's Little Theorem [10]: If  $N$  divides  $a^N - a$  for any integer  $a$ , does it follow that  $N$  is prime? Actually, he proved that a composite odd number  $N$  divides  $a^N - a$  for any integer  $a$  if and only if  $N$  is squarefree and  $p - 1$  divides  $N - 1$  for each prime divisor  $p$  of  $N$ , but he did not provide any numerical example of these numbers! In 1910, [5] Carmichael observed that the number 561 provides a counterexample that proves the converse of Fermat's little theorem helped him to make the conclusion that the theorem is not true in general, which motivated the appearance of the Carmichael numbers.

A composite number  $N$  is called a *pseudoprime to the base  $a$*  iff  $a^{N-1} \equiv 1 \pmod{N}$  where  $a \in \mathbb{Z} \setminus \{0\}$  and  $\gcd(a, N) = 1$  [11], it is called an absolute pseudoprime, or Carmichael number, if it is pseudoprime for all bases  $a$  with  $\gcd(a, N) = 1$  [8]. These numbers were first described by Robert D. Carmichael in 1910 [5], and the term Carmichael number was used by Beeger in 1950 [3]. In 1994, Alford, Granville and Pomerance showed that there are infinitely many Carmichael numbers [2].

In 2010, Echi, Bouallegue and Pinch introduced the notion of the Korselt number [4]. They defined that a natural number  $N > 1$  is called an  $\alpha$ -Korselt number with  $\alpha \in \mathbb{Z} \setminus \{0\}$  (denoted  $K_\alpha$ -number) iff  $p - \alpha$  divides  $N - \alpha$  for every prime factor  $p$  of  $N$ . The Korselt set of  $N$ , denoted by  $KS(N)$ , is the set of all  $\alpha \in \mathbb{Z} \setminus \{0, 1\}$  such that  $N$  is  $K_\alpha$ -number. The Korselt weight of  $N$ , denoted by  $K_w(N)$  is the cardinality of  $KS(N)$ . Notice that Carmichael numbers are exactly  $k_1$ -numbers [12].

In general, numerical calculations need a lot of effort, and difficult to check errors unless automated algorithms are used by computer. This motivated us to construct algorithms to convert suggested definitions and propositions into algorithms built through detailed instructions, consequently, helped us to check and compare results relevant to Korselt numbers under different conditions. Three algorithms were proposed by us in this work for verification, noting that other literature are lack of algorithms.

### II. KORSELT SET OF SQUAREFREE NUMBERS THAT HAVE 2, 3 AND 4 PRIME FACTORS

We start this section by introducing the following definitions of Korselt numbers and Korselt sets.

**Definition 1.** [1, 4] Let  $N \in \mathbb{N} \setminus \{0, 1\}$  and  $\alpha$  be a non zero integer. Then:

\*: Corresponding Author

1: An-Najah National University, Nablus, Palestine.

1.  $N$  is an  $\alpha$ -Korselt number iff  $N \neq \alpha$  and  $p - \alpha$  divides  $N - \alpha$  for every prime divisor  $p$  of  $N$ . If  $N$  is an  $\alpha$ -Korselt number, then we write  $N$  is a  $K_\alpha$ -number.
2. The set of all  $\alpha$  such that  $N$  is a  $K_\alpha$ -number is called the Korselt set of  $N$ , and denoted by  $KS(N)$ .
3. The cardinality of  $KS(N)$  is called the Korselt weight of  $N$ , and denoted by  $K_w(N)$ .

Below is an example illustrates the above definition

**Example 2.**

- 6 is a  $K_4$ -number. Indeed,  $6 = 2 * 3$  and  $2 - 4 = -2 \mid 6 - 4 = 2$  and  $3 - 4 = -1 \mid 6 - 4 = 2$ . Here,  $KS(6) = \{4\}$  and  $K_w(6) = 1$ .
- $N = 770 = 2 * 5 * 7 * 11$  is  $K_8$  and  $K_{14}$ -number. Hence,  $KS(770) = \{8, 14\}$  and  $K_w(770) = 2$ .

The following result helps in finding the Korselt set of a given squarefree integer  $N$ .

**Proposition 3.** [1] Let  $\alpha$  be a non zero integer and  $N$  be a composite number where largest prime factor is  $q$  and smallest prime factor is  $p$ . (eg.  $N = 30$ , here,  $p = 2$  and  $q = 5$ ). If  $N$  is a  $K_\alpha$ -number, then the following inequalities hold:

$$\frac{3q - N}{2} \leq \alpha \leq \frac{N + p}{2}$$

*Proof.* To prove that  $\frac{3q - N}{2} \leq \alpha$ , assume that  $\alpha \in KS(N)$ . By definition of the Korselt number,  $q - \alpha$  divides  $N - \alpha$ . Thus, there exists a natural number  $y$  such that  $N - \alpha = y(q - \alpha)$ . And as  $N > q$ , this implies that  $y \geq 2$ .

**Claim:**  $y \neq 2$ . By contradiction, suppose that  $y = 2$ . Hence,  $N - \alpha = 2q - 2\alpha$ , consequently  $\alpha = 2q - N$ .

**Claim:**  $\alpha \neq 2q - N$ . Here,  $N \neq q$  because  $N$  is a composite number and  $q$  is a prime number. Also,  $\alpha$  being a non-zero implies that  $N \neq 2q$ . Thus,  $N = mq$  where  $m \geq 3$ , and hence  $\alpha = 2q - mq = -(m - 2)q$ . Now, if  $s$  is a prime factor of  $m$ , then since  $N$  is a  $K_\alpha$ -number,  $s - \alpha = s + (m - 2)q$  divides  $N - \alpha = q(2m - 2)$ . But  $\gcd(s + (m - 2)q, q)$  equals 1 or  $q$ . If  $\gcd(s + (m - 2)q, q) = q$ , then this leads that  $q$  divides  $s$  which is not possible. Hence,  $\gcd(s + (m - 2)q, q) = \gcd(s, q) = 1$ , and this implies that  $s + (m - 2)q$  divides  $2m - 2$ . But  $2m - 2 = 2 + 2(m - 2) \leq s + (m - 2)q$  because  $s \geq 2$  and  $q \geq 2$ , this gives a contradiction. Therefore,  $y \geq 3$ . This leads that  $N - \alpha = y(q - \alpha) \geq 3(q - \alpha)$ . Hence,  $\alpha \geq \frac{3q - N}{2}$ .

Now, the case  $\alpha < 0$  is trivially as  $\frac{N + p}{2} > 0$ . If  $0 < \alpha \leq p$ , then  $\alpha \leq \frac{p + p}{2} < \frac{N + p}{2}$ . Also, when  $p < \alpha < N$ , then  $|p - \alpha| \leq |N - \alpha|$  and  $\alpha - p \leq N - \alpha$ , hence  $\alpha \leq \frac{N + p}{2}$ . Also, when  $\alpha \geq N$  and as  $q < N$ , then  $\alpha - q > \alpha - N \geq 0$ . But  $q - \alpha$  divides  $N - \alpha$  ( $N$

is a  $K_\alpha$ -number), which implies that  $\alpha - N = 0$ , and hence  $\alpha = N$ . But by definition of the Korselt number,  $N \neq \alpha$ , a contradiction. Thus  $\alpha < N$ .  $\square$

**Example 4.** Let  $N = 165 = 3 * 5 * 11$ . Here,  $q = 11$  and  $p = 3$ .

$$\bullet \alpha \geq \frac{3q - N}{2} = \frac{3 * 11 - 165}{2} = -66.$$

$$\bullet \alpha \leq \frac{N + p}{2} = \frac{165 + 3}{2} = 84.$$

One application of Proposition 3 is that it can be used to find the Korselt set of numbers with 2, 3 and 4 prime factors after a deep understanding and analysis to this Proposition and converting it into stages and steps, we managed to build algorithm through clear sequential steps and converting it into a powerful program using MATLAB software shown in the next figure (Figure 1) where the input is any integer and the output is the  $KS$  of this number.

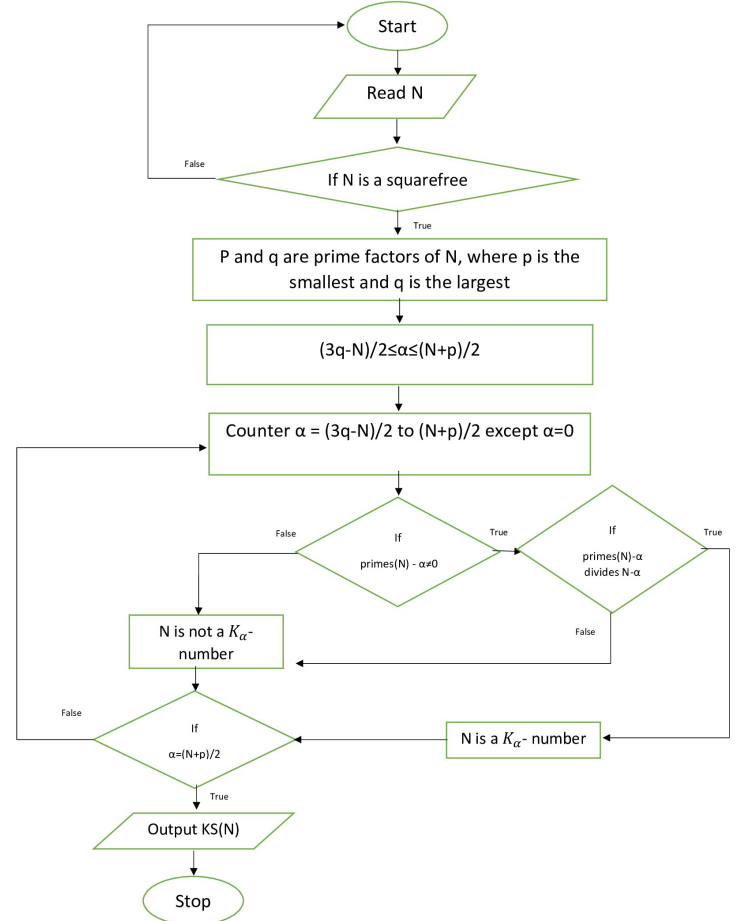


FIG. 1: Flowchart represents the way to calculate the  $KS(N)$ .

The next tables (Tables 1, 2, 3) contain some squarefree numbers  $N$  with their prime factorization (Pf) and  $KS(N)$ . Results of the proposed algorithm are presented in the following tables.

TABLE I:  $KS$  of squarefree numbers with 2 prime factors.

$N$	Pf of $N$	$KS(N)$
6	$2 * 3$	$\{4\}$
10	$2 * 5$	$\{4, 6\}$
14	$2 * 7$	$\{6, 8\}$
15	$3 * 5$	$\{4, 6, 7\}$
21	$3 * 7$	$\{5, 6, 9\}$
22	$2 * 11$	$\{12\}$
$N$	Pf of $N$	$KS(N)$
26	$2 * 13$	$\{14\}$
33	$3 * 11$	$\{9, 13\}$
34	$2 * 17$	$\{18\}$
35	$5 * 7$	$\{3, 6, 8, 11\}$ ,
38	$2 * 19$	$\{20\}$
39	$3 * 13$	$\{12, 15\}$

TABLE II:  $KS$  of squarefree numbers with 3 prime factors.

$N$	Pf of $N$	$KS(N)$
30	$2 * 3 * 5$	$\{4, 6\}$
42	$2 * 3 * 7$	$\{6\}$
66	$2 * 3 * 11$	$\{6, 10\}$
78	$2 * 3 * 13$	$\{\}$
102	$2 * 3 * 17$	$\{12\}$
$N$	Pf of $N$	$KS(N)$
105	$3 * 5 * 7$	$\{6, 9\}$
114	$2 * 3 * 19$	$\{\}$
138	$2 * 3 * 23$	$\{\}$
165	$3 * 5 * 11$	$\{-3, 4, 9\}$
174	$2 * 3 * 29$	$\{\}$

TABLE III:  $KS$  of squarefree numbers with 4 prime factors.

$N$	Pf of $N$	$KS(N)$
210	$2 * 3 * 5 * 7$	$\{6\}$
330	$2 * 3 * 5 * 11$	$\{\}$
390	$2 * 3 * 5 * 13$	$\{\}$
462	$2 * 3 * 7 * 11$	$\{12\}$
$N$	Pf of $N$	$KS(N)$
510	$2 * 3 * 5 * 17$	$\{\}$
570	$2 * 3 * 5 * 19$	$\{\}$
690	$2 * 3 * 5 * 23$	$\{\}$
770	$2 * 5 * 7 * 11$	$\{8, 14\}$

Also, to find all composite squarefree  $N \in [0, 1000]$  for any  $\alpha$ , we constructed a new algorithm to count the number of  $K_\alpha$ -numbers, in addition to it's value/s. The following flowchart (Figure 2) shows how to find them, which works in an opposite direction to find  $N$  by using  $\alpha$ .

Table 4 contains all existing composite squarefree  $K_\alpha$ -numbers of less than 1000 for  $\alpha \in \{-10, 20\}$

A summary representing the number of  $K_\alpha$ -numbers as  $\alpha \in [-10, 20]$  is depicted in Figure 3, there is no clear tend for the number of  $K_\alpha$  as  $\alpha \in [-10, 20]$ , making it difficult to describe the behaviour of number of  $K_\alpha$ -

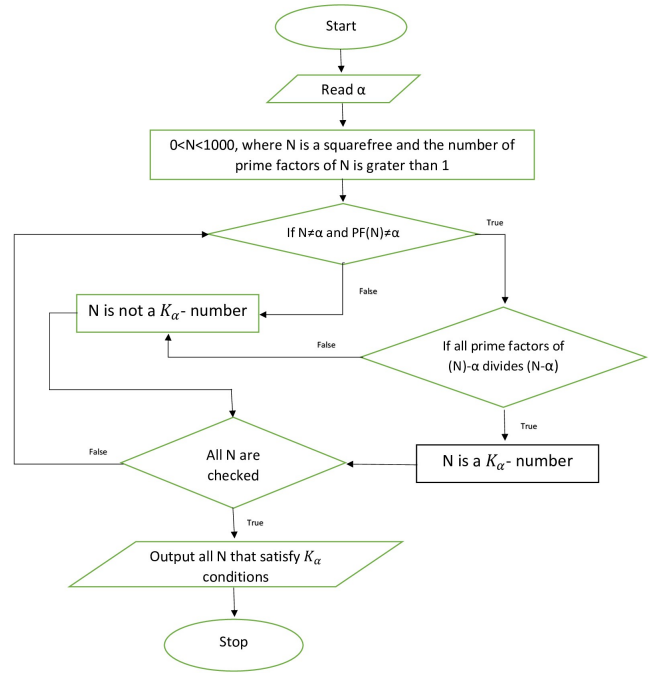


FIG. 2: Flowchart represents the way to find  $K_\alpha$ -numbers for a specific  $\alpha$  if exist.

number, but the results of the algorithm totally agree with definition of Korselt numbers which illustrate the theory involved.

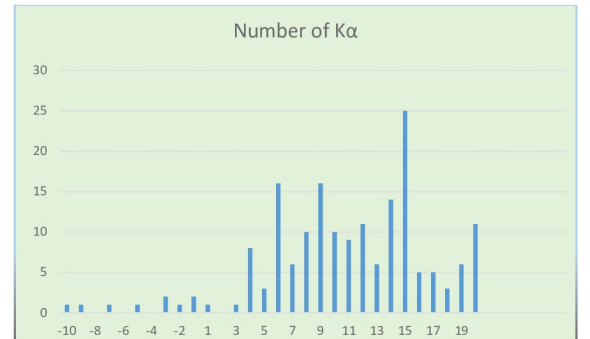


FIG. 3: Bar chart represents  $-10 \leq \alpha \leq 20$  with corresponding number of  $K_\alpha$ -numbers of less than 1000

### III. KORSELT SET OF $N = pq$ AND THE CORRECTION OF [7, THEOREM 14]

In this section, a focus on the Korselt set of a product of two distinct prime numbers is introduced by reproducing paper [7]. During that, we were able to discover and verify the existence of a fundamental error in [7, Theorem 14(6)], and after a lot of research and experimenting with numbers, we were able to find an alternative theory that can be considered as a correction to

TABLE IV: All  $K_\alpha$ -number of less than 1000  
for all  $\alpha \in \{-10, 20\}$ .

$\alpha$	Number of $K_\alpha$	$K_\alpha$
-10	1	935
-9	1	231
-8	0	-
-7	1	273
-6	0	-
-5	1	715
-4	0	-
-3	2	165,357
-2	1	598
-1	2	399,935
1	1	561
2	0	-
3	1	35
4	8	6,10,15,30,70,130,165,238
5	3	21,77,221
6	16	10,14,15,21,30,35,42,66,70, 105,195,210,231,266,286,805
7	6	15,55,187,247,715,759
8	10	14,35,77,110,143,170,273,638, 770,935
9	16	21,33,65,77,105,165,209,231, 273,345,385,399,429,561,609,969
10	10	55,66,91,130,154,255,322,385, 682,715
11	9	35,65,91,119,221,299,323,455,651
12	11	22,39,77,102,143,182,187,442,462, 782,962
13	6	33,85,133,253,493,589
14	14	26,77,91,119,143,182,209,221,230, 374,399,455,494, 770
15	25	39,51,55,65,85,95,119,143,187,195, 221, 231,247,255, 323,391,399,435, 455,527, 627, 663,715,759,935
16	5	133,170,247,506,646
17	5	65,77,209,377,437
18	3	34,323,663
19	6	51,91,187,391,403,943
20	11	38,95,110,209,290,323,437,506,551, 713,902

the theory presented by both Echi and Ghanmi in their paper [7]. Throughout the section,  $p$  and  $q$  are prime numbers with  $p < q$ ,  $q = ip + s$  such that  $i \geq 1$  and  $1 \leq s \leq p - 1$  and  $N = pq$ . The theme throughout this section is how are some conditions on  $p$  and  $q$  determines  $KS(N)$ . The next theorem was proved in [7], we provide it here to be used along with our new result at the end of this section in building algorithm that determine  $\alpha$ 's for which given positive integer is  $K_\alpha$  as well as the korselt set of that integer.

**Theorem 5.** [7]

1. If  $q > 2p^2$ , then  $KS(N) = \{p + q - 1\}$ .
2. If  $p^2 - p < q < 2p^2$  and  $p \geq 5$ , then  $KS(N) \subseteq \{ip, p + q - 1\}$ .
3. If  $4p < q < p^2 - p$ , then  $KS(N) \subseteq \{ip, (i+1)p, p + q - 1\}$ .

4. Suppose that  $3p < q < 4p$ . Then the following conditions are satisfied:

(a) If  $q = 4p - 3$ , then the following properties hold:

- i. If  $p \equiv 1 \pmod{3}$ , then  $KS(N) = \{4p, q - p + 1, p + q - 1\}$ .
- ii. If  $p \not\equiv 1 \pmod{3}$ , then  $KS(N) = \{q - p + 1, p + q - 1\}$  except when  $p = 5$ , because in this case  $KS(N) = \{3p, q - p + 1, p + q - 1\}$ .

(b) If  $q \neq 4p - 3$ , then  $KS(N) \subseteq \{3p, 4p, p + q - 1\}$ .

5. Suppose  $2p < q < 3p$ , then  $KS(N) \subseteq \{2p, 3p, 3q - 5p + 3, \frac{2p+q-1}{2}, q - p + 1, p + q - 1\}$ . [7]

The following examples illustrate the above mentioned properties:

**Example 6.** 1. Let  $N = 123 = 3 * 41$ . Here,  $p = 3$ ,  $q = 41$  and  $41 > 2 * 3^2 = 18$ . Therefore,  $KS(123) = \{3 + 41 - 1\} = \{43\}$ .

2. Let  $N = 185 = 5 * 37$ . Here,  $p = 5$ ,  $q = 37$  and  $5^2 - 5 = 20 < 37 < 2 * 5^2 = 50$ . Therefore,  $KS(123) \subseteq \{7 * 5, 5 + 37 - 1\} = \{35, 41\}$ .

3. Let  $N = 217 = 7 * 31$ . Here,  $p = 7$ ,  $q = 31$  and  $4 * 7 = 28 < 31 < 7^2 - 7 = 42$ . Therefore,  $KS(217) \subseteq \{4 * 7, 5 * 7, 7 + 31 - 1\} = \{28, 35, 37\}$ .

4. Let  $N = 1387 = 19 * 73$ . Here,  $p = 19$ ,  $q = 73$  where  $73 = 4 * 19 - 3$  and  $19 \equiv 1 \pmod{3}$ . Therefore,  $KS(1387) = \{4 * 19, 73 - 19 + 1, 19 + 73 - 1\} = \{76, 55, 91\}$ .

5. Let  $N = 2047 = 23 * 89$ . Here,  $p = 23$ ,  $q = 89$  where  $89 = 4 * 23 - 3$  and  $23 \not\equiv 1 \pmod{3}$ . Therefore,  $KS(2047) = \{89 - 23 + 1, 23 + 89 - 1\} = \{67, 111\}$ . Note that in case  $p = 5$ , then  $q = 4 * 5 - 3 = 17$  which leads  $N = 85$ . Therefore,  $KS(85) = \{3 * 5, 17 - 5 + 1, 5 + 17 - 1\} = \{15, 13, 21\}$

6. Let  $N = 473 = 11 * 43$ . Here,  $p = 11$ ,  $q = 43$  where  $43 \neq 4 * 11 - 3$ . Therefore,  $KS(473) \subseteq \{3 * 11, 4 * 11, 11 + 43 - 1\} = \{33, 44, 53\}$ .

7. Let  $N = 629 = 17 * 37$ . Here,  $p = 17$ ,  $q = 37$  where  $2 * 17 = 34 < 37 < 3 * 17 = 51$ . Therefore,  $KS(629) \subseteq \{2 * 17, 3 * 17, 3 * 37 - 5 * 17 + 3, \frac{2*17+37-1}{2}, 37 - 17 + 1, 17 + 37 - 1\} = \{34, 51, 29, 35, 21, 53\}$ .

While reproducing paper [7] which is related to Korselt numbers of the form  $N = p * q$ , we were able to introduce examples where Theorem 14(6) was not satisfied. Below are the result and the counterexample which ensures its mistake:

The claimed mistaken result ([7, Theorem 14(6)]) is:

Suppose that  $\alpha$  be an integer and  $p < q < 2p$ . If  $\alpha \in KS(N)$ , then  $\alpha \in (I(p, q) \cap J(p, q)) \cup \{2p\}$ , where

$$I(p, q) := \{p - \frac{q-1}{k} \mid k \text{ divides } q-1\}$$

$$J(p, q) := \{q - \frac{p-1}{l} \mid l \text{ divides } p-1\}.$$

The counterexample is:

**Example 7.** Let  $N = 77$ . Here,  $p = 7$ ,  $q = 11$  and  $p < q < 2p$ .

$$I(7, 11) = \{7 - \frac{10}{k} \mid k \text{ divides } 10\},$$

hence, getting  $k = 1, 2, 5$  and  $10$  which give  $I(7, 11) = \{-3, 2, 5, 6\}$ . Also,

$$J(7, 11) = \{11 - \frac{6}{l} \mid l \text{ divides } 6\},$$

hence, having  $l = 1, 2, 3$  and  $6$  which gives  $J(7, 11) = \{5, 8, 9, 10\}$ . Therefore,  $(I(p, q) \cap J(p, q)) \cup \{2p\} = \{5, 1, 4\}$ . Note that  $KS(77) = \{5, 8, 9, 12, 14, 17\} \not\subseteq \{5\}$ .

In the next theorem, we introduce a correction of aforementioned mistaken result along with it's proof, and hence we overcome the detected mistake.

**Theorem 8.** Suppose that  $p < q < 2p$ . Then, setting

$$I(p, q) := \{p + \frac{q-1}{k} \mid k \text{ divides } (q-1)\}$$

$$J(p, q) := \{q - \frac{p-1}{k} \mid k \text{ divides } (p-1)\},$$

we have  $KS(N) \subseteq \{2p\} \cup I(p, q) \cup J(p, q)$ .

*Proof.* The proof divided into two cases:

**Case1:**  $p$  divides  $\alpha$ . By [7, Lemma 7],  $\alpha = p$  or  $\alpha = 2p$ . But if  $\alpha = p$  then  $i-1$  must divide  $p+s-1$  with  $q = ip+s$ , and here,  $i=1$  that leads  $i-1=0$  which does not divide  $p+s-1$ , hence,  $\alpha = 2p$ .

**Case2:**  $p$  doesn't divide  $\alpha$ , which means that  $\gcd(p, \alpha) = 1$ . By [7, Proposition 4(2)], then

$$q - p + 1 \leq \alpha \leq p + q - 1,$$

so

$$q - (p-1) \leq \alpha \leq p + (q-1).$$

By Proposition [7, Proposition 4(1)],  $\gcd(q, \alpha) = 1$ . Hence, by Proposition [7, Lemma 5(2)],  $q - \alpha$  divides  $p-1$ . Thus,  $p-1 = l(q-\alpha)$  which implies  $\alpha = q - \frac{p-1}{l}$  with a non-zero integer  $l$ . Also, by hypothesis,  $\gcd(p, \alpha) = 1$ . Hence, by [7, Lemma 5(3)],  $p - \alpha$  divides  $q-1$  which yields  $\alpha - p$  divides  $q-1$ . Thus,  $q-1 = k(\alpha-p)$  which implies  $\alpha = p + \frac{q-1}{k}$  with a non-zero integer  $k$ . Therefore,  $\alpha \in \{q - \frac{p-1}{l_1}, q - \frac{p-1}{l_2}, \dots, q - \frac{p-1}{l_s}\} \cup \{p + \frac{q-1}{k_1}, p + \frac{q-1}{k_2}, \dots, p + \frac{q-1}{k_t}\}$ , where  $(k_1, \dots, k_t)$  are factors of  $q-1$  and  $(l_1, \dots, l_s)$  are factors of  $p-1$ . Hence, from case1 and case2, it is concluded that  $\alpha \in I(p, q) \cup J(p, q) \cup \{2p\}$ .  $\square$

**Example 9.** Let  $N = 77$ . Here,  $p = 7$ ,  $q = 11$  and  $7 < 11 < 22$ .

$$I(7, 11) = \{7 + \frac{10}{k} \mid k \text{ divides } 10\},$$

hence, getting  $k = 1, 2, 5$  and  $10$  which gives  $I(7, 11) = \{17, 12, 9, 8\}$ . Also,

$$J(7, 11) = \{11 - \frac{6}{l} \mid l \text{ divides } 6\},$$

hence, having  $l = 1, 2, 3$  and  $6$  which gives  $J(7, 11) = \{5, 8, 9, 10\}$ . Therefore,  $KS(77) \subseteq (I(7, 11) \cup J(7, 11)) \cup \{2 * 7\} = \{17, 14, 12, 10, 9, 8, 5\}$ .

In our final algorithm, we introduced a comprehend structure that takes  $N$  as an input and then selects only those values of  $N$  satisfying the condition  $N = p * q$  where  $p$  and  $q$  are primes to obtain first, the category which the algorithm used to find  $\alpha$ , secondly, the  $KS(N)$ . This algorithm puts our new theorem along with the old mentioned ones in this article and is used to give a modified new tables. The following diagram (Figure 4) illustrates the algorithm.

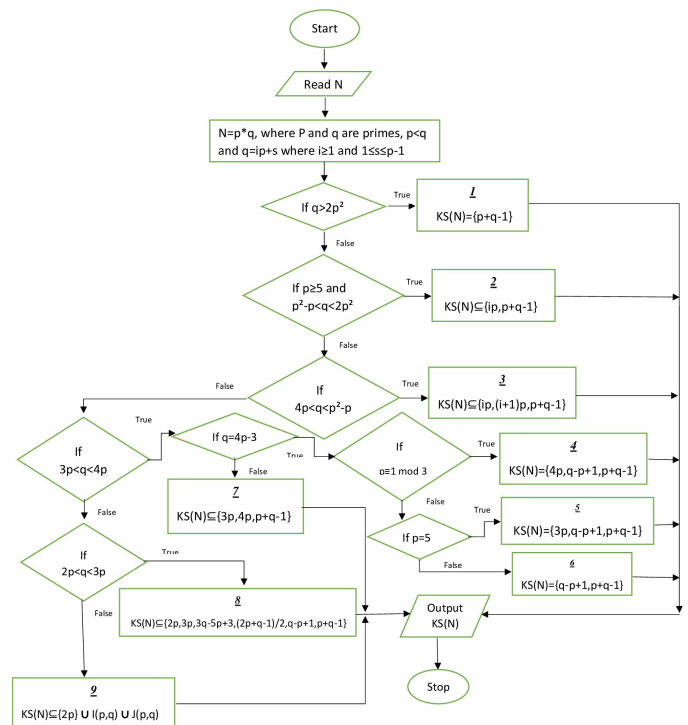


FIG. 4: A flowchart representing the fast approach to calculate the  $KS(N)$ .

Applying this algorithm on the values of  $N$  which is less than 10000 and satisfying the condition  $N = p * q$ , giving the outputs: The category and  $\alpha \in KS(N)$  which are presented in the next table (Table 5).

TABLE V: A collection of  $KS(N)$  for  $N = pq$  which are less than 10000.

$N$	$p$	$q$	Category	$\alpha \in KS(N)$
6	2	3	9	4
10	2	5	8	4, 6
14	2	7	7	6, 8
15	3	5	9	4, 6, 7
21	3	7	8	5, 6, 9
22	2	11	1	12
26	2	13	1	14
33	3	11	7	9, 13
34	2	17	1	18
35	5	7	9	3, 6, 8, 11
38	2	19	1	20
39	3	13	9	12, 15
46	2	23	1	24
51	3	17	9	15, 19
55	5	11	8	7, 10, 15
57	3	19	1	21
58	2	29	1	30
62	2	31	1	32
65	5	13	8	9, 11, 15, 17
69	3	23	1	25
74	2	37	1	38
77	7	11	9	5, 8, 9, 12, 14, 17
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
9939	3	3313	1	3315
9943	61	163	8	183, 223
9946	2	4973	1	4974
9953	37	269	3	305
9957	3	3319	1	3321
9959	23	433	3	455
9961	7	1423	1	1429
9965	5	1993	1	1997
9969	3	3323	1	3325
9974	2	4987	1	4988
9977	11	907	1	917
9979	17	587	1	603
9983	67	149	8	215
9985	5	1997	1	2001
9986	2	4993	1	4994
9987	3	3329	1	3331
9989	7	1427	1	1433
9991	97	103	9	91, 95, 99, 100, 199
9993	3	3331	1	3333
9995	5	1999	1	2003
9997	13	769	1	781
9998	2	4999	1	5000

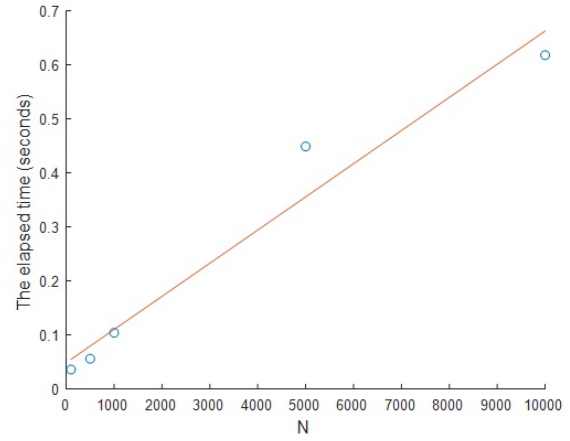


FIG. 5: The performance of the suggested algorithm.

2 Finally, the complexity of the suggested algorithms are of orders  $O(N)$  (linear running time); as the loop depends on  $N$ . An emphasis of the complexity was empirically proved through implementing the suggested modified algorithm with different values and measured corresponding elapsed times, the best regression representation was linear regression which complies with the  $O(N)$  complexity (See Figure 5 ). However a comparison between the different methods for calculating the Korselt numbers is made by defining composite square-free  $N$  from 1 to 10000 that have the form  $pq$ . Results showed that the way for calculating the Korselt number by checking all numbers between  $\frac{3q-N}{2}$  and  $\frac{N+p}{2}$  consumed more time rather than the proposed technique in this section, such that the first method needed 3.110 sec on a laptop with *i7* processor, while the improved technique consumed 0.618 sec. This gives us the right to say the modified technique is more efficient, although the program was not yet fully optimized for the time being.

## Summary

- This article for the first time introduces a set of algorithms implemented to enrich the literature with tables of Korselt relatively large numbers. In previous works, the authors provide tables without algorithms. Moreover, we expanded the set of tested numbers covering more than what the literature covered previously.
- While reproducing the different theorems and propositions in the literature, we detected an important mistake in [7, Theorem 14 (6)] and through a robust work, one original theorem is introduced by us to overcome the detected mistake.
- Through preparing the proper algorithms and writing program, we modified a compounded al-



gorithm which showed a remarkable performance compared to traditional ones.

#### **Ethics approval and consent to participate**

The authors confirm that they respect the publication ethics and that they consent the publication of their work.

#### **Consent for publication**

The authors consent the publication of this work. Availability of data and materials Data is available upon the request

#### **Funding**

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

#### **Author's contribution**

The results presented here are mainly based on the original ideas from Abeer Eshtaya and Khalid Adarbeh, Full Analysis and numerical analysis was Carried by Hadi Hamad. The original draft had been produced by Abeer Eshtaya in her master thesis.

#### **Conflicts of interest**

All authors declare that they have no conflicts of interest

**Acknowledgment:** The author's of the article express their deep grateful to both of the referee's for their careful reading of the article and their valuable comments and corrections.

- 
- [1] Al-Rasasi, I., Echi, O., and Ghanmi, N. (2013). On the korselt set of a squarefree composite number. *CR Math. Rep. Acad. Sci. Canada*, 35(1):1–15.
  - [2] Alford, W. R., Granville, A., and Pomerance, C. (1994). There are infinitely many carmichael numbers. *Annals of Mathematics*, 139(3):703–722.
  - [3] Beeger, N. (1950). On composite numbers  $n$  for which  $a^n - 1 \equiv 1 \pmod{n}$  for every  $a$  prime to  $n$ . *Scripta math*, 16:133–135.
  - [4] Bouallège, K., Echi, O., and Pinch, R. G. (2010). Korselt numbers and sets. *International Journal Of Number Theory*, 6(02):257–269.
  - [5] Carmichael, R. D. (1910). Note on a new number theory function. *Bulletin of the American Mathematical Society*, 16(5):232–238.
  - [6] Carmichael, R. D. (1912). On composite numbers  $p$  which satisfy the fermat congruence  $a^p - 1 \equiv 1 \pmod{p}$ . *The American Mathematical Monthly*, 19(2):22–27.
  - [7] Echi, O. and Ghanmi, N. (2012). The korselt set of pq. *International Journal of Number Theory*, 8(02):299–309.
  - [8] Erdős, P. and Monthly, A. M. (1956). On pseudo-primes and carmichael numbers. *Publ. Math. Debrecen*, 4(1956):201–206.
  - [9] Fletcher, C. R. (1991). A reconstruction of the frénicle-fermat correspondence of 1640. *Historia Mathematica*, 18(4):344–351.
  - [10] Korselt, A. (1899). Probleme chinois. *L'intermédiaire math*, 6:143–143.
  - [11] Lehmer, D. H. (1976). Strong carmichael numbers. *Journal of the Australian Mathematical Society*, 21(4):508–510.
  - [12] Williams, H. C. (1977). On numbers analogous to the carmichael numbers. *Canad. Math. Bull*, 20(1):133–143.