An-Najah National University

Faculty of Graduate Studies

Study of Korselt Numbers and Sets between Theory and Application

By

Abeer Adel Mohammad Eshtaya

Supervisors

Dr. Khalid Adarbeh

Dr. Hadi Hamad

This Thesis is submitted in Partial Fulfillment of the Requirements for the Degree of Master of Computational Mathematics, Faculty of Graduate Studies, An-Najah National University, Nablus-Palestine.

2020

Study of Korselt Numbers and Sets between Theory and Application

By

Abeer Adel Mohammad Eshtaya

This Thesis was defended successfully on 11/10/2020 and approved by:

<u>Defense Committee Members</u>	**<u>Signature</u>**
Dr. Khalid Adarbeh/ Supervisor	**…………………**
Dr. Hadi Hamad/ Co-Supervisor	**…………………**
Dr. Ala Talahmeh/ External examiner	**…………………**
Dr. Muath Karaki / Internal examiner	**…………………**

Dedication

This thesis is dedicated to my parents, my sisters and brothers for their support, as well as to my family and friends.

With respect and love.

Acknowledgement

First and foremost, I would like to thank Allah for giving me the strength and the ability to complete this work.

I would also like to express my special thanks to my supervisors Dr. Khalid Adarbeh and Dr. Hadi Hamad for their great effort and their continuous support. And thanks to all committee members for giving their time to improve this work.

Last but not least, thanks to my family and friends for their support and making me able to do this job.

الإقرار

أنا الموقع أدناه مقدم الرسالة التي تحمل العنوان:

Study of Korselt Numbers and Sets between Theory and Application

أقر بأن ما اشتملت عليه هذه الرسالة إنما هي نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه حيثما ورد، وأن هذا الرسالة ككل أو أي جزء منها لم يقدم من قبل لنيل أي درجة علمية أو بحث علمي لدى أي مؤسسة تعليمية أو بحثية أخرى.

Declaration

The work provided in this thesis, unless otherwise referenced, is the researcher's own work, and has not been submitted elsewhere for any degree or qualification.

Student's Name:	**اسم الطالب:**
Signature:	**التوقيع:**
Date:	**التاريخ:**

Table of Contents

Study of Korselt Numbers and Sets between Theory and Application

By

Abeer Eshtaya

Supervisors:

Dr. Khalid Adarbeh

Dr. Hadi Hamad

Abstract

The Korselt numbers and sets were discussed for the first time in 2007. The problem can be considered as a new one with limited literature making it as a new field of research.

Let N be a positive integer and α 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 α-Korselt number (K_α-number). The set of all α such that N is a K_α-number is called the Korselt set of N. The concept of K_α-number was introduced by Othman Echi in 2007 and recently studied for different situation of N by Othman Echi, Nejib Ghanmi, Kais Bouallgu and Richard Pinch.

Here it should be noted that the concept of Korselt numbers generalizes another concept called the Carmichael numbers which was presented as a counterexample for the converse of Fermat's little theorem.

This Thesis contributes to study, validate and develop all results mentioned in the papers. Also it contributes to use the developed results to build algorithms by MATLAB that will enrich the literature with Korselt sets of relatively large numbers (not included in the literature) as well as testing and illustrating the involved theory.

Introduction

In 1640, Fermat proved his well known result Fermat's Little Theorem, (Fletcher, 1991) 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 (Korselt, 1899): If N divides $a^N - a$ for any integer a, does it follow that N is prime? 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, Carmichael observed that the number 561 provides a counterexample that proves the converse of Fermat's little theorem giving him the conclusion that the theorem is not true in general (Carmichael, 1910), which helped in 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 $a \in \mathbb{Z}\backslash\{0\}$ and $gcd(a, N) = 1$, and it is called an absolute pseudoprime, or Carmichael number, if it is pseudoprime for all bases a with $gcd(a, N) = 1$ (Lehmer, 1976) (Erdös and Monthly, 1956). These numbers were first described by Robert D. Carmichael in 1910 (Carmichael, 1910), and the term Carmichael number was used by Beeger in 1950 (Beeger, 1950). Also, Alford, Granville and Pomerance showed that there are infinitely many Carmichael numbers in 1994 (Alford et al., 1994).

In 2010, Echi, Bouallegue and Pinch introduced the notion of the Korselt number. They defined that a natural number $N > 1$ is called an α-Korselt number with $\alpha \in \mathbb{Z}\backslash\{0\}$ (denoted K_α-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 $\alpha \in \mathbb{Z}\backslash\{0\}$ such that N is K_α-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 (Williams, 1977).

(Languasco et al., 2003) The Korselt numbers and sets depend on prime numbers which is implemented in many applications. One of the most important applications which is frequently used in daily life is **cryptography** which is based on prime numbers. One of our most widely used cryptographic systems is called R.S.A. cryptography, where the security of the R.S.A. method depends on the following facts:

- In order to encode the message, it is necessary to build large primes.
- On the other hand, in order to break the system, it is necessary to be able to factorize large natural numbers obtained as product of two primes.

Chapter one of this thesis introduces some basic definitions and theorems in number theory that help us in studying the Korselt numbers.

While chapter two is devoted to study the Korselt numbers and their main properties. For instance, it discusses the proof of the following main results:

1. If $\alpha \leq 1$, then each composite squarefree K_α-number has at least three prime factors.

2. There are only finitely many α-Korselt numbers with exactly two prime factors.

Chapter three provides the relation between Korselt numbers and other classes of numbers, as Y_α-numbers and Williams numbers, where a Williams number is a positive integer that is both K_α-number and $K_{-\alpha}$-number (Ghanmi and Al-Rassasi, 2013).

Chapter four is devoted to study the Korselt numbers of the squarefree numbers that have special forms as pq form and $6q$ form, where p and q are distinct primes.

Finally, paralleled to the theoretical part, we built our own algorithms using MATLAB to validate the involved results and to extend the numerical results depending on the theoretical proved facts in this work. Also, a comparison was made between the two different algorithms by computing the time that each of them consumed.

CHAPTER 1

PRELIMINARIES

In this chapter, the main number theory concepts and facts that are frequently used through the thesis are introduced. Starting by defining the prime and composite numbers.

1.1 Basic Definitions

Definition 1.1.1.

1. (Crandall and Pomerance, 2006) p is **a prime** if $p \in \mathbb{N}\backslash\{0, 1\}$ and has no factors (the only divisors are 1 and p).
e.g: $p = 5$ is a prime, because the only divisors of 5 are 1 and 5.

2. (Crandall and Pomerance, 2006) n is a **composite number** iff $n \in \mathbb{N}\backslash\{0, 1\}$ and is not a prime ($n = a * b$ where a, b are integers and $1 < a, b < n$).
e.g: $n = 30$ is composite, because $30 = 5 * 6$ where $< 15, 6 < 30$.

Definition 1.1.2.

1. (Stein, 2005) **The prime factorization of a number** n is defined as a list of distinct prime numbers $p_1, p_2, ..., p_k$ such that $p_1^{r_1} * p_2^{r_2} * ... * p_k^{r_k} = n$ where $r_1, r_2, ..., r_k$ are nonzero natural numbers.
e.g: The prime factorization of $126 = 2 * 3^2 * 7$.

2. (Weisstein, 2003) If prime factorization of n has no repeated factors ($r_1 = r_2 = ... = r_k = 1$), then n is said to be **squarefree number**.

e.g. 30 is squarefree, because $30 = 2^1 * 3^1 * 5^1$ and $2 \neq 3 \neq 5$ are all primes.

Definition 1.1.3.

1. (Andrews, 1994) An integer d is called **the greatest common divisor** of a and b ($gcd(a, b)$) where a, b are integers and at least one of them is not zero iff the following is satisfied:

   (a) $d \in \mathbb{N} \backslash \{0\}$,

   (b) d divides both a and b and

   (c) for all integer c divides both a and b is also a divisor of d.

2. (Andrews, 1994) **The least common multiple** of integers a and b ($lcm(a, b)$) is the smallest positive integer that is divisible by both a and b

Fact: (Andrews, 1994) $lcm(a, b) = \frac{a*b}{gcd(a,b)}$.

e,g. Let $a = 15$ and $b = 21$. Then $gcd(15, 21) = 3$ and $lcm(15, 21) = 105$. Note that $105 = \frac{15*21}{3}$.

Definition 1.1.4.

- (Nyblom, 2002) The **integer part or the floor function of a real number** y (denoted by $\lfloor y \rfloor$) equals $max\{z \in \mathbb{Z} : z \leq y\}$.

- (Nyblom, 2002) The **ceiling function of** y (denoted by $\lceil y \rceil$) equals $min\{z \in \mathbb{Z} : y \leq z\}$.

e.g. $\lfloor 3.75 \rfloor = 3$ *and* $\lceil 3.75 \rceil = 4$.

Theorem 1.1.1. (Raji, 2013) (**The Division Algorithm**) Let $a \in \mathbb{Z}$ and $b \in \mathbb{N} \backslash \{0\}$. Then there exist unique integers q and r such that $a = bq + r$ where

$0 \leq r \leq b - 1$.

e.g. If $a = 83$ and $b = 19$, then $83 = 19 * 4 + 7$ with $q = 4$ and $r = 7$.

Theorem 1.1.2. (Shoup, 2005) (**Fermat's Little Theorem**) If p is a prime number, then $a^p - a$ is a multiple of p for any integer a. ($a^{p-1} \equiv 1 \pmod{p}$).

e.g. If $5^{50} \equiv x \pmod{7}$, what is value of x?

by Fermat's Little Theorem, $5^6 \equiv 1 \pmod{7}$, hence, $5^{48} = 5^{6^8} \equiv 1^8 = 1 \pmod{7}$, thus, $5^{50} = 5^2 * 5^{48} \equiv 25 \pmod{7}$, this leads that $5^{50} \equiv 4 \pmod{7}$.

Definition 1.1.5. Let N be a composite number.

1. N is called a *pseudoprime to the base* a iff $gcd(a, N) = 1$ and $a^{N-1} \equiv 1 \pmod{N}$ where α is a non zero integer number.

2. N is called an *absolute pseudoprime* or *Carmichael number* if it is *pseudoprime for all bases a* with $gcd(a, N) = 1$.

e.g. $N = 10$ is a *pseudoprime to the base* 11, where $gcd(11, 10) = 1$ and $11^{10-1} = 2357947691 \equiv 1 \pmod{10}$. Also,the smallest absolute pseudoprime is $561 = 3 * 11 * 17 = N$ (Bouallègue et al., 2010).

CHAPTER 2

KORSELT NUMBERS WITH EXAMPLES AND SPECIFIC PROPERTIES

2.1 Korselt Numbers: Definitions and Examples

Definition 2.1.1. (Bouallègue et al., 2010) Assume that $N \in \mathbb{N}\backslash\{0,1\}$ and α be a nonzero integer. N is an α-Korselt number iff $N \neq \alpha$ and $p - \alpha$ divides $N - \alpha$ for every prime divisor p of N. If N is an α-Korselt number, then we write N is a K_α-number.

- The set of all α such that N is a K_α-number is called the Korselt set of N, and denoted by $KS(N)$.
- The cardinality of $KS(N)$ is called the Korselt weight of N, and denoted by $K_w(N)$.

Example 2.1.1.

- $N = 6$ is a K_4-number. Indeed, $N = 2 * 3$ 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 only K_8 and K_{14}-number (refer to Table 2.3). Hence, $KS(770) = \{8, 14\}$ and $K_w(770) = 2$.

Remark 2.1.1. (Bouallègue et al., 2010) K_1-numbers are exactly the Carmichael numbers (by definition).

2.2 Korselt Numbers: Properties

The following results help in finding the Korselt set of a given squarefree integer N.

Proposition 2.2.1. Let α be a nonzero integer and N be a composite squarefree number where the largest prime factor is q and the smallest prime factor is p. (e.g. $N = 30$, here, $p = 2$ and $q = 5$). If N is a K_α-number, then the following inequalities hold:

1. $\alpha \geq 2q - N + 1$. (Bouallègue et al., 2010)

2. $\alpha \geq \frac{3q-N}{2}$. (Al-Rasasi et al., 2013)

3. $\alpha \leq \frac{N+p}{2}$. (Bouallègue et al., 2010)

4. $\alpha \leq \frac{3N}{4}$. (Echi, 2007)

Proof.

1. α has two cases:

   Case1: $\alpha > 0$. Since p and q are primes with $p < q$, then $N \geq 2q$. So that, $2q - N \leq 0$ and $2q - N + 1 \leq 1$. Hence trivially $\alpha \geq 2q - N + 1$.

   Case2: $\alpha < 0$. Let N be a K_α-number. Then by definition; $q - \alpha$ divides $N - \alpha$ holds, and hence $\frac{N-\alpha}{q-\alpha} = x$ for some integer x. Now, as $\alpha < 0$, then both of $q - \alpha$ and $N - \alpha$ are positive. Moreover, $N > q$ implies that $N - \alpha > q - \alpha$, and hence $x \geq 2$, Consequently, $\frac{N-\alpha}{q-\alpha} \geq 2$. Thus, $\alpha \geq 2q - N$.

   Now, to prove that $\alpha \neq 2q - N$, using contradiction, suppose that $\alpha = 2q - N$. Here, $N \neq q$ because N is a composite number and q is a prime number. Also, α 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_α-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 $2m - 2 = 2 + 2(m-2) \lneq s + (m-2)q$ because $s \geq 2$ and $q \gneq 2$, so, there is a contradiction. Therefore, $\alpha \neq 2q - N$.

2. 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 $\alpha = 2q - N$. But by (1), $\alpha \neq 2q - N$, this gives a contradiction. Therefore, $y \geq 3$. This leads that $N - \alpha = y(q - \alpha) \geq 3(q - \alpha)$. Hence, $\alpha \geq \frac{3q-N}{2}$.

3. 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 $\alpha \leq \frac{N+p}{2}$. Now, 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_α-number), which implies that $\alpha - N = 0$, and hence $\alpha = N$. But by definition of the Korselt number, $N \neq \alpha$, a contradiction. Thus $\alpha < N$.

4. Let N be a K_α-number, then $h = p - \alpha$ divides $N - \alpha$ where p is a prime factor of N. As p divides N and $N > p$, then $N \geq 2p = 2(\alpha + h)$.

Thus, $\alpha \leq (N-\alpha) - 2h$. Also, h divides $N-\alpha$ and $\alpha < N$ ($N-\alpha$ is positive), hence, $-h \leq N-\alpha$. This yields $\alpha \leq (N-\alpha) - 2h \leq (N-\alpha) + 2(N-\alpha) = 3(N-\alpha)$, and consequently $\alpha \leq \frac{3N}{4}$.

Example 2.2.1. Let $N = 165 = 3 * 5 * 11$. Here, $q = 11$ and $p = 3$.

- $\alpha \geq 2q - N + 1 = 22 - 165 + 1 = -142$.
- $\alpha \geq \frac{3q-N}{2} = \frac{3*11-165}{2} = -66$.
- $\alpha \leq \frac{N+p}{2} = \frac{165+3}{2} = 84$.
- $\alpha \leq \frac{3N}{4} = \frac{3*165}{4} = 123.75$, thus, $\alpha \leq 123$.

Remark 2.2.1.

1. $\frac{N+p}{2} < \frac{3N}{4}$ and $\frac{3q-N}{2} > 2q - N + 1$.
2. $\frac{N+p}{2}$ can be reached. (Bouallègue et al., 2010)

Proof.

1. As p is the smallest prime factor of N, $N > 2p$. Hence, $\frac{N+p}{2} < \frac{N+\frac{N}{2}}{2} = \frac{3N}{4}$. Also, as q is the largest prime factor of N, $\frac{3q-N}{2} = \frac{2q-N}{2} + \frac{q}{2} > \frac{2q-N}{2} + 1$. But $2q - N \leq 0$, thus, $\frac{2q-N}{2} + 1 \geq 2q - N + 1$. Consequently $\frac{3q-N}{2} > 2q - N + 1$.

2. let q be an odd prime number. Hence, $\frac{p+N}{2} = \frac{2+N}{2} = q + 1$. Therefore, $N = 2q$ is a $(q+1)$-Korselt number.

The results in the Remark 2.2.1 leads that $[\frac{3q-N}{2}, \frac{N+p}{2}] \subset [2q-N+1, \frac{3N}{4}]$. So that, using part 1 and 2 of Proposition 2.2.1 in the following algorithm, which are more restricted. Also, part 4 helps to find the upper bound of α without knowing it's prime factors.

One application of the previous proposition it can be used to write a MATLAB program to find the Korselt set of numbers with $2, 3$ and 4 prime factors as described in the following flowchart (see Fig 2.1).

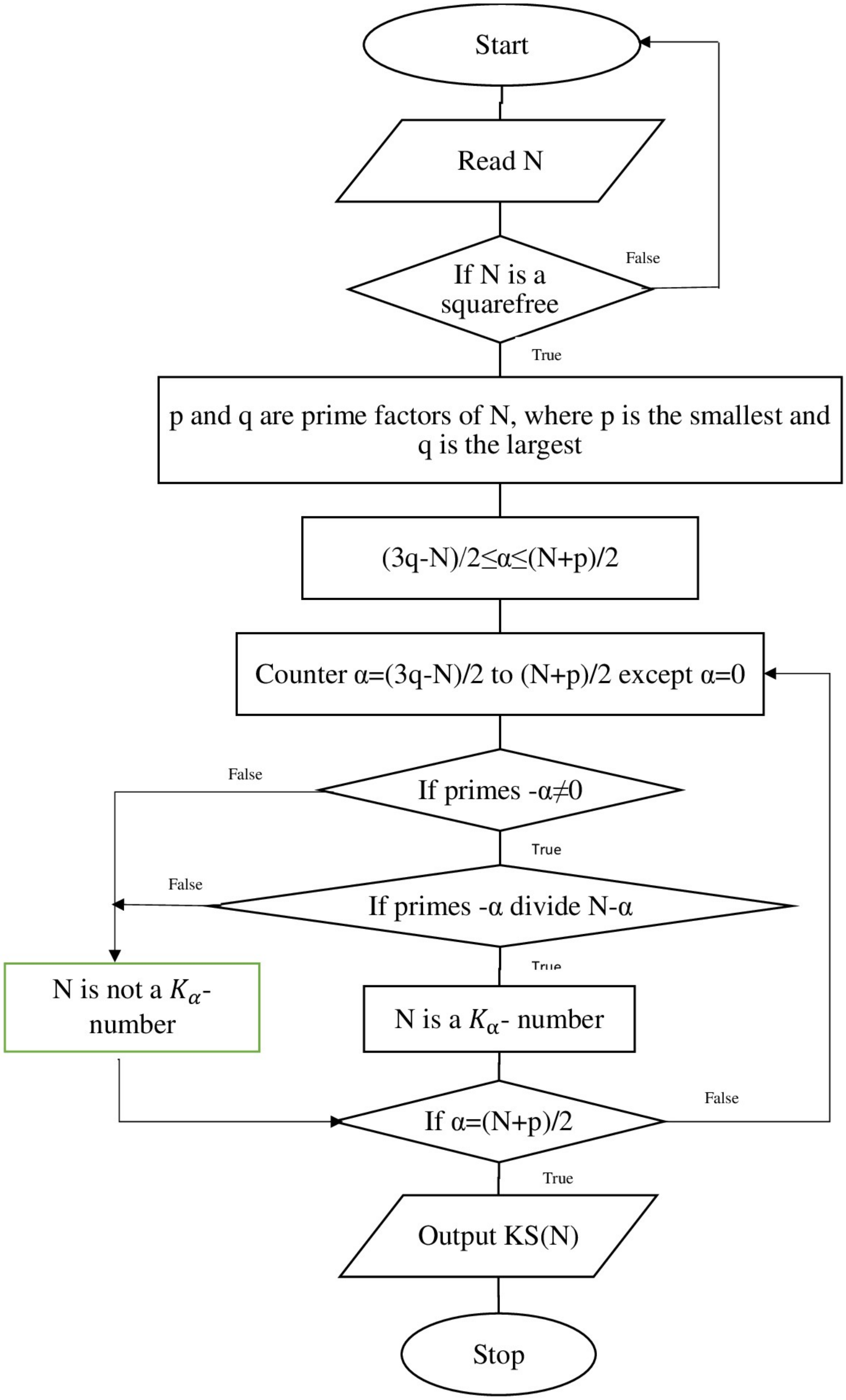

Figure 2.1: Flowchart represents the way to calculate the $KS(N)$.

The next tables contain some squarefree numbers N with their prime factorization (Pf) and $KS(N)$.

Table 2.1: 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 2.2: 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 2.3: 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 α, the following flowchart (see Fig 2.2) which shows how to find them.

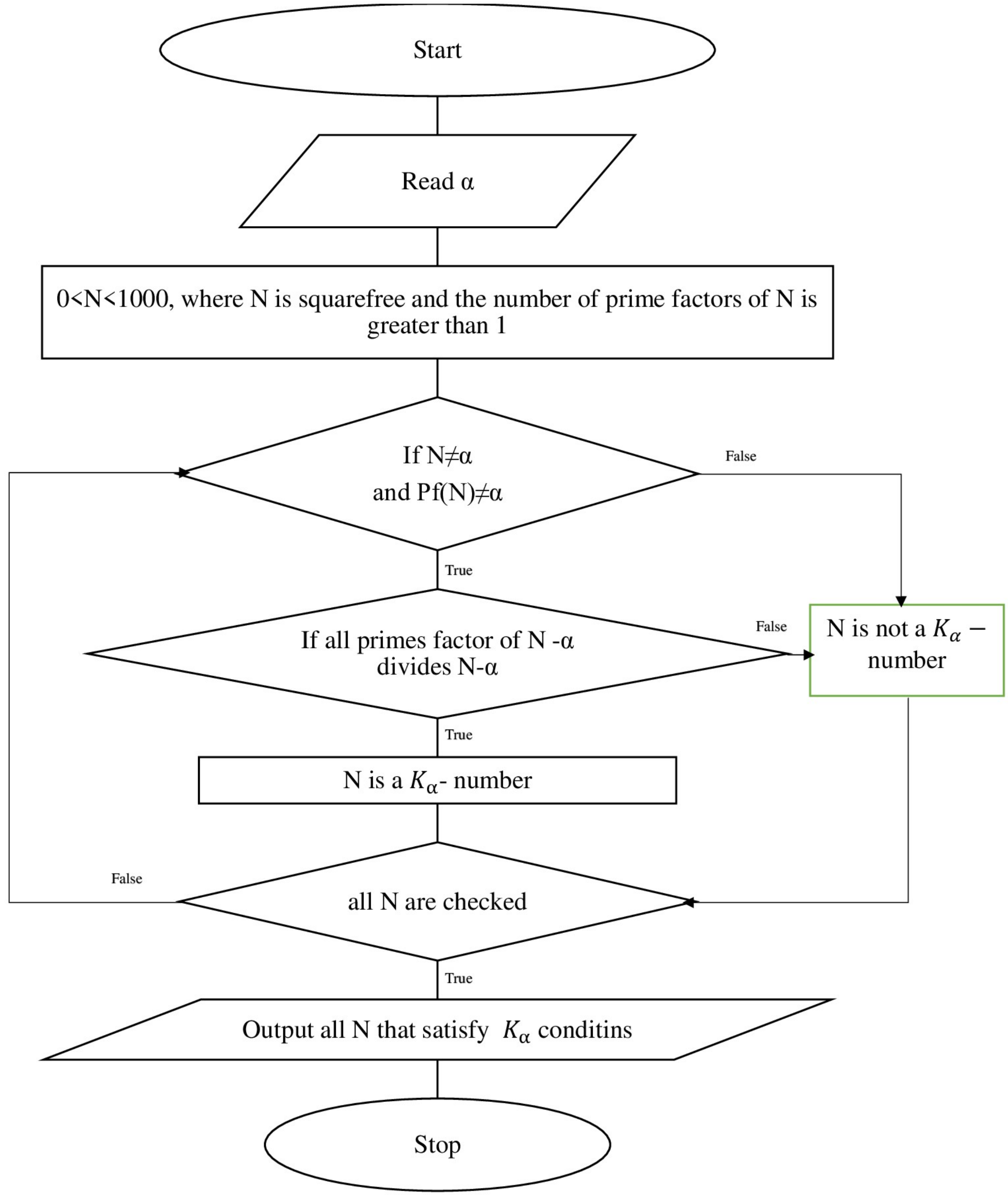

Figure 2.2: Flowchart represents the way to find K_α-numbers for a specific α if exist.

Table 2.4 contains all existing composite squarefree K_α-numbers of less than 1000 for $\alpha \in \{-10, 20\}$

Table 2.4: All K_α-numbers of less than 1000 for all $\alpha \in \{-10, 20\}$.

α	Number of K_α	K_α
-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

A summary representing the number of K_α-numbers which less than 1000 as $\alpha \in [-10, 20]$ is depicted in Fig 2.3

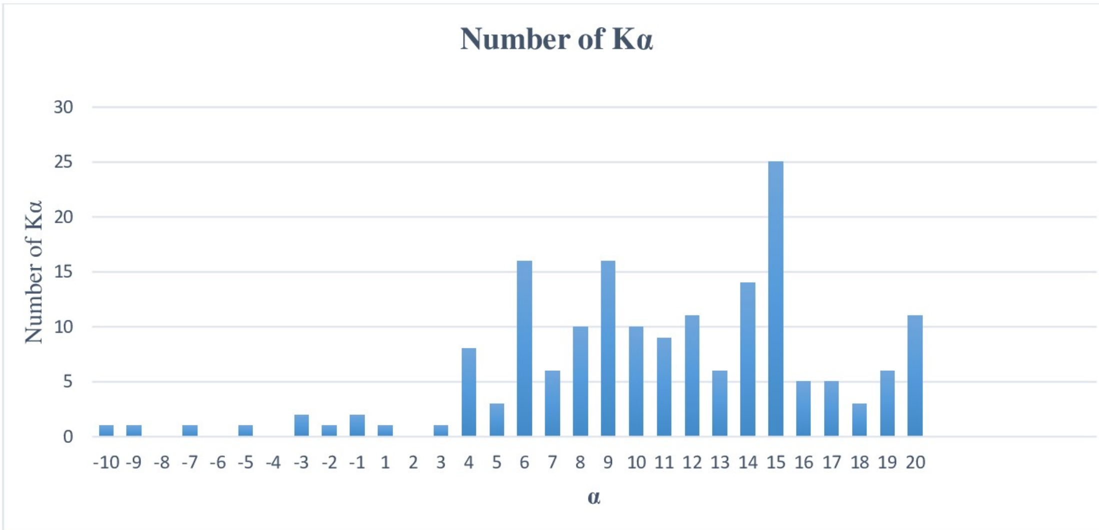

Figure 2.3: Bar chart represents $-10 \leq \alpha \leq 20$ with corresponding number of K_α-numbers of less than 1000

2.3 More Properties of Korselt Numbers

Another application of Proposition 2.2.1 is the following corollary.

Corollary 2.3.1. (Echi, 2007) If N is a K_α-number, then N is never K_{N-3} or K_{N-5}-number.

Proof. Using contradiction, let $\alpha = N - 3$. Then by Proposition 2.2.1, $\alpha = N - 3 \leq \frac{3N}{4}$. We deduce that $N \leq 12$, and since N is squarefree, hence, $N \in \{6, 10\}$. This means that 6 is a K_3-number and 10 is a K_7-number, which is not true.

Now, Let $\alpha = N - 5$, then by using Proposition 2.2.1, $\alpha = N - 5 \leq \frac{3N}{4}$. We conclude that $N \leq 20$. Therefore, $N \in \{6, 10, 14, 15\}$, thus 6 is a K_1-number, 10 is a K_5-number, 14 is a K_9-number and 15 is a K_{10}-number, which is not true.

Proposition 2.3.1. (Bouallègue et al., 2010) Let α be a non zero integer and N be a K_α-number such that $gcd(N, \alpha) = 1$. Then $p - \alpha$ divides $\frac{N}{p} - 1$ where p is a prime factor of N.

Proof. As N is a K_α-number, $N - \alpha = (p - \alpha)t$ for some integer t. Thus, $N - p = (p - \alpha)t + (\alpha - p) = (p - \alpha)(t - 1)$. Since p is a prime factor of N (p divides N), there exists a non zero integer number s such that $N = ps$, and hence, $N - p = p(s - 1) = (p - \alpha)(t - 1)$. So that p divides $(p - \alpha)(t - 1)$. But $gcd(\alpha, N) = 1 = gcd(\alpha, p)$, implies p divides $(t - 1)$. Therefore, $p(p - \alpha)$ divides $(N - p)$, equivalently $p - \alpha$ divides $\frac{N}{p} - 1$.

Example 2.3.1. If $N = 30$. Is N a K_7-number?

$N = 30 = 2 * 3 * 5$ and $gcd(2, 7) = gcd(3, 7) = gcd(5, 7) = 1$.

When $p = 2$, then $(p - \alpha) = (2 - 7) = -5$ does not divide $\frac{N}{p} - 1 = 14$.

Hence, N is not a K_7-number.

Example 2.3.2. This example shows that the condition $gcd(N, \alpha) = 1$ in Proposition 2.3.1 can not be deleted.

Let $N = 231 = 3 * 7 * 11$. Here 231 is a K_{-9}-number and $gcd(N, \alpha) = gcd(231, -9) = 3 \neq 1$. This implies that N and α are not relatively prime. $p = 3$ is a prime factor of N, then $(p - \alpha) = (3 - -9) = 12$, but $\frac{N}{p} - 1 = 77 - 1 = 76$ and 12 does not divide 76.

The following result adds further information about the Korselt set of a squarefree composite number.

Proposition 2.3.2. (Al-Rasasi et al., 2013) Assume that $N \neq 6$ is a K_α-number. If p and q are two prime factors of N, then the following properties hold.

1. If α and p are relatively prime and q divides α, then

$$\frac{2pq-N}{2q-1} \leq \alpha \leq \frac{2pq+N}{2q+1}$$

2. If q does not divide α, then

$$q+1-\frac{N}{q} \leq \alpha \leq \frac{N}{q}+q-1$$

Proof. The assumption that N is a squarefree composite number implies that $N = pqF$ with $F \in \mathbb{N}$ and p, q don't divide F.

1. Suppose that N is a K_α-number. Thus, $p-\alpha$ divides $N-\alpha = q(\frac{N-\alpha}{q})$. Here, p and q are primes, hence $gcd(p-\alpha, q) = gcd(p, q) = 1$, which implies that $p-\alpha$ divides $\frac{N-\alpha}{q}$. Hence, $\frac{N-\alpha}{q} = (p-\alpha)t$ with a nonzero integer t. Replacing N with pqF gives

$$\alpha(tq-1) = pq(t-F) \tag{2.1}$$

Claim: $|t| \neq 1$

By using contradiction, suppose that $t = 1$. Hence, equation 2.1 gives

$$\alpha(q-1) = pq(1-F) \tag{2.2}$$

$F \neq 1$, because $F = 1$ yields that either $\alpha = 0$ or $q-1 = 0$, this violates definition of the Korselt number, hence $F \geq 2$. Thus, equation 2.2 implies that $\alpha < 0$. Also, by equation 2.2, it can be concluded that p divides $\alpha(q-1)$. Hence, p divides $q-1$ because $gcd(\alpha, p) = 1$, therefore,

$p < q$. Now, let f be a prime factor of F, this means f is a prime factor of N. Replacing p with f in the beginning of the proof gives $f - \alpha = \frac{N-\alpha}{jq}$ with an integer $j \neq 1$ because $j = 1$ implies that $p - \alpha = f - \alpha$ and hence, $p = f$ which is not possible. Therefore, $f - \alpha \leq \frac{N-\alpha}{2q} = \frac{p-\alpha}{2}$, which yields that $f - p \leq \alpha - f$. By hypothesis, q divides α, and as $\alpha < 0$, hence $\alpha < -q$. Thus, we obtain that $-p < f - p \leq \alpha - f < \alpha < -q$. Consequently, $-p < -q$, contradicting inequality $p < q$. Therefore $t \neq 1$. Now, suppose that $t = -1$. Thus, equation 2.1 implies that $\alpha(q + 1) = pq(1 + F)$. q divides α which yields $\alpha = \alpha_1 q$ with $\alpha_1 \in \mathbb{Z}\backslash\{0, 1\}$. Hence,

$$\alpha_1(q + 1) = p(1 + F) \tag{2.3}$$

Then, proof has to deal with two cases:

Case1: $F = 1$. Equation 2.3 gives $\alpha_1(q + 1) = 2p$. We deduced that α_1 divides 2 because $gcd(\alpha_1, p) = gcd(\alpha, p) = 1$. Here, $\alpha_1 = 2$ because $\alpha_1 = 1$ yields that $\alpha = q$ which contradicts definition of the Korselt number. Thus $p = q + 1$. But p and q are primes, and the only two consecutive prime numbers are 2 and 3. Hence, $q = 2$ and $p = 3$. Consequently $N = 6$, which contradict the hypothesis.

Case2: $F \neq 1$. Hence $\alpha(q+1) = pq(1+F)$ yields that $q\alpha + \alpha = pq + N$, hence $N - \alpha = q(\alpha - p)$. Assume that f is a prime factor of F, thus $f - \alpha$ divides $N - \alpha = -q(p - \alpha)$. Note that $gcd(f - \alpha, q) = gcd(f, q) = 1$, therefore $f - \alpha$ divides $p - \alpha$ and consequently $f - \alpha = \frac{p-\alpha}{m}$ where m is a nonzero integer. But $f \neq p$, concluding $m \neq 1$. Hence, $f - \alpha \in$

$\{-\frac{N-\alpha}{2q}, -\frac{N-\alpha}{3q}, ..., \frac{N-\alpha}{2q}, \frac{N-\alpha}{q}\}$. By Proposition 2.2.1, $\alpha < N$, hence,

$$-\frac{N-\alpha}{2q} < -\frac{N-\alpha}{3q} < ... < 0 < ... < \frac{N-\alpha}{2q} < \frac{N-\alpha}{q}.$$

This leads to $f - \alpha \geq -\frac{N-\alpha}{2q} = \frac{p-\alpha}{2}$, and hence, $f \geq \frac{p-\alpha}{2} + \alpha = \frac{p+\alpha}{2}$. Thus, $2f \geq p + \alpha > \alpha$, then $2f > \alpha$. But, equation 2.3 gives

$$\alpha_1(q+1) = p(1+F) > pf > \frac{\alpha}{2}p = \alpha_1\frac{qp}{2},$$

so $2\alpha_1(q+1) > \alpha_1 qp$, thus, it is deduced that $q(p-2) < 2$. While from equation 2.3 it leads that p divides $q+1$ because $gcd(\alpha, p) = gcd(\alpha_1, p) = 1$. Hence, $p \leq q+1$ and $p-1 \leq q$. Multiplying $(p-1)$ by $(p-2)$ gives $(p-1)(p-2) \leq q(p-2) < 2$, this yields that $p = 2$. Therefore, $N = 2qF$, which follows that $q - \alpha = q(1-\alpha_1)$ divides $N - \alpha = 2qF - \alpha_1 q = q(2F - \alpha_1)$, and then, $1 - \alpha_1$ divides $2F - \alpha_1$. But α_1 is odd because $gcd(\alpha, p) = gcd(\alpha, 2) = 1$, so $2F - \alpha_1$ is odd and $1 - \alpha_1$ is even, this is contradicting the fact that $2F - \alpha_1$ is a multiple of $1 - \alpha_1$, hence, $|t| \neq 1$. Consequently,

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

Then, $\alpha \geq p - \frac{N-\alpha}{2q} = \frac{2pq-N}{2q} + \frac{\alpha}{2q}$, and gives $\alpha(1 - \frac{1}{2q}) \geq \frac{2pq-N}{2q}$, hence, $\alpha(\frac{2q-1}{2q}) \geq \frac{2pq-N}{2q}$. Therefore, $\alpha \geq \frac{2pq-N}{2q-1}$. Also, $\alpha \leq \frac{2pq+N}{2q+N}$. Consequently,

$$\frac{2pq-N}{2q-1} \leq \alpha \leq \frac{2pq+N}{2q+N}.$$

2. Assume that q does not divide α. Hence, $gcd(q, q-\alpha) = 1$. It is known that $q - \alpha$ divides $N - \alpha = N - q + q - \alpha$, concluding that $q - \alpha$ divides

$N-q = q\frac{N-q}{q}$. This yields $q-\alpha$ divides $\frac{N-q}{q}$. It follows that

$$-\frac{N-q}{q} \leq q-\alpha \leq \frac{N-q}{q}.$$

Thus finally

$$q+1-\frac{N}{q} \leq \alpha \leq \frac{N}{q}+q-1.$$

Example 2.3.3. Let $N = 30 = 2{*}3{*}5$. (By using MATLAB, $KS(30) = \{4, 6\}$)

1. Assume that $p = 3$, $q = 2$ and $\alpha = 4$. Note that $gcd(\alpha, p) = gcd(4, 3) = 1$, $2 = p$ divides $4 = \alpha$ and $\frac{2pq-N}{2q-1} = -6 \leq \alpha = 4 \leq \frac{2pq+N}{2q+N} = 8.4$.

2. Assume $q = 3$ and $\alpha = 4$, hence $q+1-\frac{N}{q} = -6 \leq \alpha = 4 \leq \frac{N}{q}+q-1 = 12$

The following remark is to illustrate Proposition 2.3.2.

Remark 2.3.1. (Al-Rasasi et al., 2013)

1. If $N = 6$, then the inequalities of part(1) in Proposition 2.3.2 do not hold, because when $N = 6$, then $p = 3, q = 2$ and $KS(N) = \{4\}$. Also, $\frac{2pq-N}{2q-1} = \frac{6}{3} = 2$ and $\frac{2pq+N}{2q+1} = \frac{18}{5} = 3\frac{3}{5}$. But $\alpha = 4 \notin [2, 3]$.

2. Let q be a prime factor of a squarefree composite number N, and let $\alpha \in \mathbb{Z}\backslash\{0\}$ such that $gcd(N, \alpha) = 1$. If N is an α-Korselt number, then

$$\alpha \in \bigcap_{\substack{q|N \\ q\ prime}} [q+1-\frac{N}{q}, q-1+\frac{N}{q}].$$

For example, let $N = 15 = 3.5$, then $KS(15) = \{4, 6, 7\}$.

When $q = 3$, $[q+1-\frac{N}{q}, q-1+\frac{N}{q}] = [-1, 7]$.

When $q = 5$, $[q + 1 - \frac{N}{q}, q - 1 + \frac{N}{q}] = [3, 7]$.

Also, $4, 6$ and $7 \in [-1, 7] \cap [3, 7] = [3, 7]$.

2.4 Finiteness K_α-Numbers with Exactly Two Prime Factors

An important fact concerning Korselt numbers is that for a given nonzero integer α, the number of the K_α-numbers that have exactly two prime factors is finite.

Theorem 2.4.1. Let α be a nonzero integer. There are a finite number of K_α-numbers that have exactly two prime factors

The proof of this theorem depends on the following facts.

Lemma 2.4.1. Assume that α is a nonzero integer with $\alpha \in \{-1, 1\}$. If N is a K_α-number, then N has at least three prime factors.

Proof. By contradiction, suppose that $N = pq$ such that $p < q$ are primes. Here, $\alpha = 1$ or -1. Thus, $gcd(\alpha, N) = 1$. Then by using Proposition 2.3.1, we get $q - \alpha$ divides $\frac{N}{q} - 1$, implies $q(q - \alpha)$ divides $N - q$. This yields that $N - q \geq q(q - \alpha)$ and $N \geq q + q(q - \alpha) \geq q + q(q - 1) = q^2$. Hence, $N = pq \geq q^2$, consequently, $p \geq q$ which is not true. Therefore, K_α-numbers with $\alpha = 1$ or -1 have at least three prime factors.

Lemma 2.4.2. Let α be an integer with $\alpha \leq -2$. If N is a K_α-number, then N must have at least three prime factors.

Proof. Assume that $N = pq$, where p and q are distinct prime numbers. Let $p - \alpha$ and $q - \alpha$ divide $N - \alpha$, where $\alpha \leq -2$. If $gcd(N, \alpha) = 1$, then by the previous lemma, a contradiction and conclude that a K_α-number has at least three prime factors. Now, suppose that $gcd(N, \alpha) \neq 1$. Then without loss of generality, one may suppose that p divides $-\alpha$. This leads that $-\alpha = pr$ for a nonzero natural r. But $p - \alpha$ divides $N - \alpha$, so that $p(1 + r)$ divides $p(q+r)$. Equivalently $1+r$ divides $q+r$. This yields that $q \equiv -r \pmod{1+r}$, and hence, $q \equiv 1 \pmod{1 + r}$. Thus, this gives $1 + r$ divides $q - 1$, which implies that $q - 1 \geq 1 + r$. On the other hand, $q - \alpha$ divides $N - \alpha$, where $N - \alpha = pq - \alpha = p(q - \alpha) + \alpha(p - 1)$. So $q - \alpha$ divides $\alpha(p - 1) = -p(p - 1)r$. But $gcd(q - \alpha, p) = 1$ because p divides α but does not divide q, then $q - \alpha$ divides $(p - 1)r$. Now, by claiming that $gcd(q - \alpha, r) = 1$, suppose that $gcd(q - \alpha, r) \neq 1$. This leads certainly to $gcd(q - \alpha, r) = q$ (q is a prime), then q divides r and $r = qs$ for a nonzero natural s. But $q - 1 \geq 1 + r$, which leads that $q \geq 2 + qs$, a contradiction, so the claim that $gcd(q - \alpha, r) = 1$ is true. Hence, $q - \alpha$ divides $p - 1$, but $q - \alpha = q + pr = q + (p - 1)r + r$, thus $q - \alpha$ divides $q + r$. Replacing α by pr, hence $q + pr$ divides $q + r$, which means that $q + pr < q + r$, but this is not possible. Therefore, each K_α-numbers with $\alpha \leq -2$ have at least three prime factors.

Proposition 2.4.1. Let α be a nonzero integer and less than 2. Then each K_α-number must have at least three prime factors.

Proof. Combine Lemma 2.4.1 and Lemma 2.4.2.

Lemma 2.4.3. Let α be an integer with $\alpha \geq 2$. If $N = pq$ with $p < q$ are two prime numbers, then $q \leq 4\alpha - 3$.

Proof. If $q \leq 2\alpha$, then $q + 2 \leq 2\alpha + 2 \lneq 2\alpha + 2\alpha$, hence, $q \lneq 4\alpha - 2$ is deduced, and this implies $q \leq 4\alpha - 3$. Now, assume that $q > 2\alpha > \alpha$. Clearly,

$N - \alpha = p(q - \alpha) + \alpha(p - 1)$ and $q - \alpha$ divides $N - \alpha$, this yields that $q - \alpha$ divides $\alpha(p - 1)$. But $gcd(q - \alpha, \alpha) = gcd(q, \alpha) = 1$, because 1 is only less than α and divides q. Hence, $q - \alpha$ divides $(p - 1)$. Thus, $p - 1 = k(q - \alpha)$ for a nonzero natural k. Now, if $k = 1$, then it gives $q - \alpha = p - 1$. But if $k \geq 2$, then $p - 1 = k(q - \alpha) \geq 2(q - \alpha)$. So that $q - \alpha \leq \frac{p-1}{2} \leq \frac{q}{2} - 1$, and implies that $q \leq 2\alpha - 2 < 2\alpha$, which is contradict the fact that $q > 2\alpha$. This leads that $q - \alpha = p - 1$. Now, $p - \alpha$ divides $(N - \alpha) - (p - \alpha)(p + 2\alpha - 1) = 2\alpha(\alpha - 1)$. Clearly, p does not divide α, because if not, this yields that $p \leq \alpha$ and hence, $q = p + \alpha - 1 \leq 2\alpha - 1$, a contradiction. Hence, $p - \alpha$ divides $2(\alpha - 1)$ and $p \leq 3\alpha - 2$. Therefore, $q = p + \alpha - 1 \leq 4\alpha - 3$.

Proof of Theorem 2.4.1

Let α be a nonzero integer. If $\alpha \leq 1$, then by Proposition 2.4.1, the number of the K_α-numbers with exactly two prime factors is 0. Now, assume that $\alpha > 1$ and let N be a K_α-number with exactly two prime factor. If q is the greatest prime factor of N, then by Lemma 2.4.3, it must be less than or equal $4\alpha - 3$. The proof ends by remarking that there are a finite number of prime numbers that are less than or equal to $4\alpha - 3$.

Example 2.4.1. (Bouallègue et al., 2010) The values of α up to 2000 for which there are no α-Korselt number with two prime factors are the following: $1, 2, 250, 330, 378, 472, 516, 546, 896, 1170, 1356, 1372, 1398, 1416, 1530, 1644, 1692, 1794, 1830$ and 1962.

CHAPTER 3

KORSELT NUMBERS AND OTHER CLASSES OF NUMBERS

3.1 K_α-Numbers and Y_α-Numbers

In this section, the relation between K_α-number and another class of numbers called Y_α-numbers is discussed. Similar to the case of Korselt numbers, Y_α-numbers started with the Y_1-numbers, and then a natural generalization to any α. Let's start by the definition of the Y_1-number.

Definition 3.1.1. Let N be a composite squarefree number. N is called a Y_1-number if for any p and q are distinct prime factors of N, $p \not\equiv 1 \pmod{q}$. The smallest Y_1-number is $N = 3 * 5 = 15$, and the smallest Y_1-number with three prime factors is $N = 3 * 5 * 17 = 255$. (Bouallègue et al., 2010)

The following proposition proves that any K_1-number is a Y_1-number.

Proposition 3.1.1. If N is a K_1-number, then it's also a Y_1-number.

Proof. Suppose that N is a K_1-number and not a Y_1-number. Then $p \equiv 1 \pmod{q}$ where p and q are distinct prime factor of N. This yields that q divides $p - 1$. But since N is a K_1-number, then $p - 1$ divides $N - 1$. Thus, q divides $N - 1$. But q divides N. Hence q divides $N - (N - 1) = 1$, which is a contradiction.

Now, a natural generalization of the Y_1-numbers to any α is illustrated through the following.

Definition 3.1.2. (Bouallègue et al., 2010) Suppose that α is a nonzero integer. A composite squarefree number N is called a Y_α-number if $p \not\equiv \alpha \pmod{q}$, where p and q are distinct prime divisors of N.

The following fact proves that any K_α-number is a Y_α-number.

Proposition 3.1.2. (Bouallègue et al., 2010) Let α be a nonzero integer number. If N is a K_α-number, then it's also a Y_α-number, but the opposite is not true.

Proof. Let $N = \prod_{i=1}^{k} p_i$ where p_i's are distinct prime factors. Now, suppose that N is a K_α-number and not a Y_α-number. Then there are distinct $s, t \in \{1, ..., k\}$ such that $p_s \equiv \alpha \pmod{p_t}$. Thus p_t divides $p_s - \alpha$. But as N is a K_α-number, then $p_s - \alpha$ divides $N - \alpha$, hence p_t divides $N - \alpha$, and then p_t divides α. This means that $\alpha \equiv 0 \pmod{p_t}$, and we conclude that $p_s \equiv 0 \pmod{p_t}$, and hence $p_s = p_t$, contradicting N being a squarefree. Therefore, any K_α-number is also a Y_α-number.

The next example is a counter example leads that the opposite of the previous proposition is not true.

Example 3.1.1. $N = 55$ is a Y_3-number ($\alpha = 3$), is 6 a K_3-number?
Here, $KS(N) = KS(55) = \{7, 10, 15\}$ (see Table 5.1).Thus, 55 is not a K_3-number.

3.2 Williams Numbers

Definition 3.2.1. (Bouallègue et al., 2010) Let $\alpha \in \mathbb{N}\backslash\{0\}$ and N is a positive integer. N is called an α-Williams number(W_α-number of short) if it is both a K_α-number and a $K_{-\alpha}$-number.

Proposition 3.2.1. (Echi, 2007) Let $\alpha \in \mathbb{Z}\backslash\{0\}$. If a squarefree composite number N is a W_α-number, then the prime factors of N is greater than or equal to 3.

Proof. By Proposition 2.4.1, it can be concluded that $\alpha > 0$ for all K_α-numbers that have the form pq, where p and q are primes. Hence, for all $N = pq$ is a K_α-number, there is no $-\alpha \in KS(N)$, so N is not a W_α-number.

The following algorithm is used to check if N is a W_α or not (see Fig 3.1), and in Tables 3.1 and 3.2 a list of both W_α-numbers and not are presented.

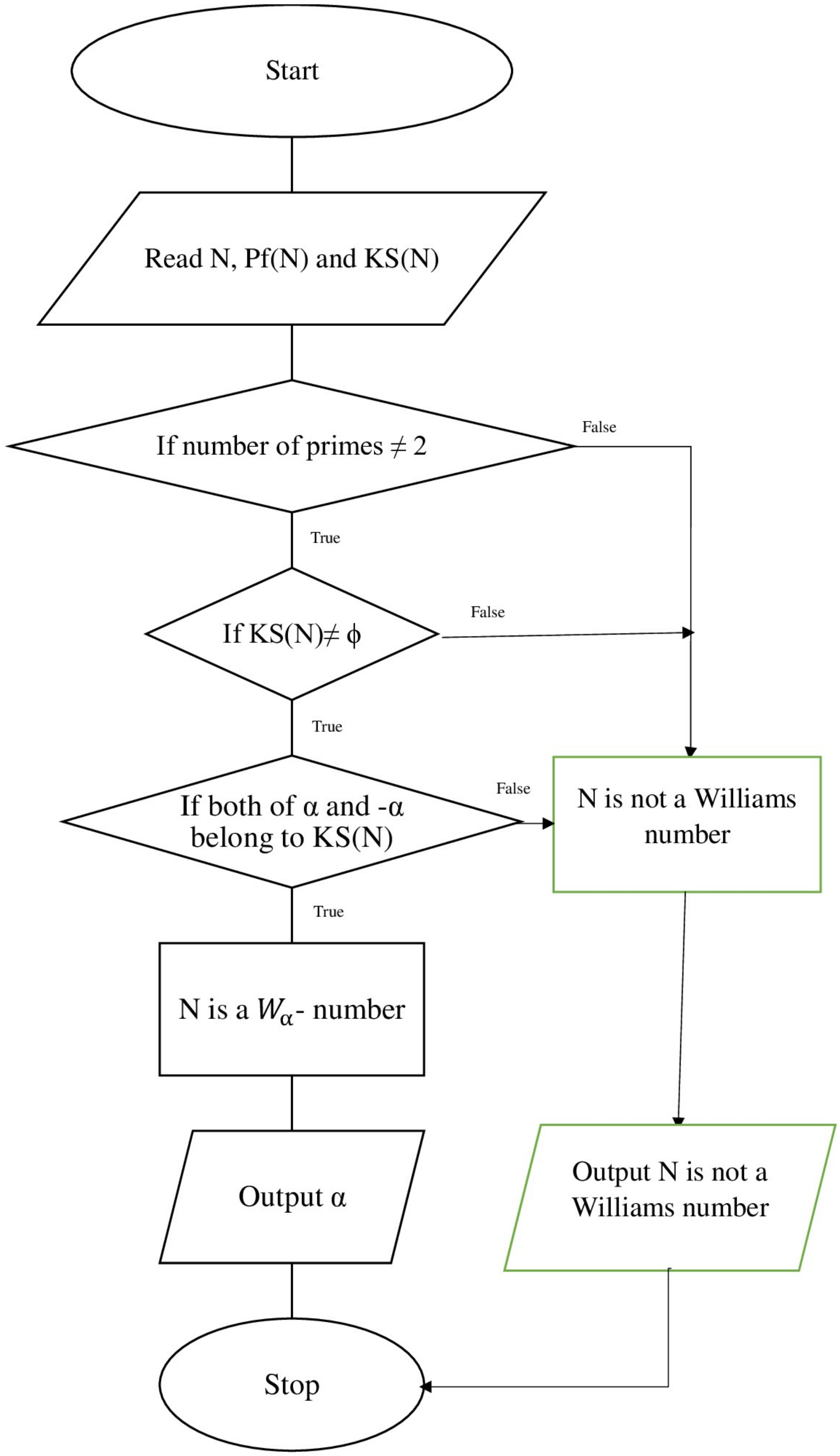

Figure 3.1: Flowchart to test if the number N is W_α-number or not.

Table 3.1: Some examples of Williams numbers

N	Pf(N)	$KS(N)$
231	$3*7*11$	$\{-9,6,9,15\}$
1105	$5*13*17$	$\{-15,1,9,15,16,25\}$
3059	$7*19*23$	$\{-21,11,21,35\}$
19721	$13*37*41$	$\{-39,9,39,65\}$
109411	$23*67*71$	$\{-69,64,69,115\}$
455729	$37*109*113$	$\{-111,111,185\}$
715391	$43*127*131$	$\{-129,129,215\}$
9834131	$103*307*311$	$\{-309,309,515\}$

Table 3.2: Some examples of non Williams numbers

N	Pf(N)	$KS(N)$
165	$3*5*11$	$\{-3,4,9\}$
462	$2*3*7*11$	$\{12\}$
770	$2*5*7*11$	$\{8,14\}$
3007	$31*97$	$\{127\}$
7663	$79*97$	$\{71,91,95,103,175\}$
11397	$3*29*131$	$\{\}$

Note that Pf of all numbers N in Table 3.1 is $p*(3p-2)*(3p+2)$ where p, $3p-2$ and $3p+2$ are all primes, and $N=p(3p-2)(3p+2)$ is a W_{3p}-number.

Definition 3.2.2. (Bouallègue et al., 2010) Let i be a nonzero natural number and p is a prime. Then it can be said that p is a T_i-prime number if $ip-(i-1)$ and $ip+(i-1)$ are prime numbers. Defining $T_i(p) := p[ip-(i-1)][ip+(i-1)]$.

Example 3.2.1. Is 13 a T_3-prime number?

Yes, as $p=13$ and $i=3$, then $ip-(i-1)=37$ and $ip+(i-1)=41$ are all primes. Also set $T_3(13)=13*37*41=19721$.

Example 3.2.2. The unique T_2-primes are 2 and 3.

Let p be a T_2-prime which is not in the set $\{2,3\}$. Then there are two cases, either $p\equiv 1 \pmod 3$ or $p\equiv 2 \pmod 3$. If $p\equiv 1 \pmod 3$, then $2p+1=3\equiv 0$

$\pmod 3$, which is not possible as p is a T_2-prime, and hence $2p+1$ must be a prime. Now, when $p \equiv 2 \pmod 3$. Then $2p-1 = 3 \equiv 0 \pmod 3$. Thus $2p-1$ is not a prime, which is a contradiction. Therefore, $p \in \{2, 3\}$.

Next, it is interesting to study the relation among the K_α-numbers, W_α-numbers and T_i-prime numbers by starting the following lemma.

Lemma 3.2.1. (Bouallègue et al., 2010) Let p be a T_i-prime number. Then $i-1$ divides p^2-1 iff $T_i(p)$ is a K_{ip}-number.

Proof. Assume that p is a T_i-prime number with $T_i(p) = p(ip-(i-1))(ip+(i-1))$. Now, p, $ip-(i-1)$ and $ip+(i-1)$ are all the prime factors of $T_i(p)$. Notice that $T_i(p)$ is K_{ip}-number iff $p - ip = (1-i)p$ divides $T_i(p) - ip$, $ip-(i-1)-ip = -(i-1)$ divides $T_i(p)-ip$ and $ip+(i-1)-ip = (i-1)$ divides $T_i(p)-ip$. Hence, concluding that $T_i(p)$ is K_{ip}-number iff $i-1$ divides $T_i(p)-ip$. But, clearly $T_i(p)-ip = p[(ip-(i-1))(ip+(i-1))-i]$ and $gcd(p, i-1) = 1$, hence, $i-1$ divides $(ip-(i-1))(ip+(i-1))-i$ where $(ip-(i-1))(ip+(i-1))-i = i^2p^2-(i-1)^2-i = i^2p^2-i^2+2i-1-i = i^2(p^2-1)+(i-1) = (i^2+1-1)(p^2-1)+(i-1) = (i^2-1)(p^2-1)+(p^2-1)+(i-1)$. Therefore, $T_i(p)$ is an ip-Korselt number iff $i-1$ divides p^2-1.

Theorem 3.2.1. (Bouallègue et al., 2010) Let p be a T_3-prime number ($T_3(p) = p(3p-2)(3p+2)$), then the following properties hold:

1. $\{-3p, 3p, 5p\} \subseteq KS(T_3(p))$.

2. In particular, $T_3(p)$ is a $3p$-Williams number.

Proof.

1. First Notice that p is an odd prime number, because if $p = 2$, then $3p+2 = 8$ is not a prime.

   Let us start by proving that $T_3(p)$ is K_{3p}-number. Indeed, p is an odd prime, so p^2 is an odd number and 2 divides $p^2 - 1$, and by using lemma 3.2.1, $T_3(p)$ is a K_{3p}-number. Next, to prove that $T_3(p)$ is a K_{-3p}-number, we have to show that each $p + 3p$, $(3p - 2) + 3p$ and $(3p + 2) + 3p$ divide $T_3(p) + 3p$. But $T_3(p) + 3p = p(3p - 2)(3p + 2) + 3p = p(9p^2 - 1) = p(3p - 1)(3p + 1)$. Both of $3p - 1$ and $3p + 1$ are even, and hence, 4 divides $(3p - 1)(3p + 1)$, consequently, $4p$ divides $p(3p - 1)(3p + 1) = T_3(p) + 3p$. But $4p = p + 3p$, giving $p + 3p$ divides $T_3(p) + 3p$. Also, $(3p - 2) + 3p = 2(3p - 1)$ and divides $p(3p - 1)(3p + 1)$, where $3p + 1$ is even, and $(3p + 2) + 3p = 2(3p + 1)$ and divides $p(3p - 1)(3p + 1)$, where $3p - 1$ is even. Hence, $T_3(p) + 3p$ is a multiple of $p + 3p$, $(3p - 2) + 3p$ and $(3p + 2) + 3p$, so $T_3(p)$ is a $-3p$-Korselt number. Finally, to prove that $T_3(p)$ is a $5p$-Korselt number, set $T_3(p) - 5p = p(3p - 2)(3p + 2) - 5p = p(9p^2 - 9) = 9p(p - 1)(p + 1)$. Both of $p - 1$ and $p + 1$ are even, so 4 divides $(p - 1)(p + 1)$ and $4p$ divides $9p(p - 1)(p + 1) = T_3(p) - 5p$, thus, $p - 5p$ divides $T_3(p) - 5p$. On the other hand, $(3p - 2) - 5p = -2(p + 1)$ and divides $9p(p - 1)(p + 1)$, where $p - 1$ is even, and $(3p + 2) - 5p = -2(p - 1)$ and divides $9p(p - 1)(p + 1)$, where $p + 1$ is even. so that $T_3(p)$ is a $5p$-Korselt number. Hence, $\{-3p, 3p, 5p\} \subseteq KS(T_3(p))$

2. $T_3(p)$ is a $3p$-Williams number. It is clear from 1 where each $3p$,$-3p \in KS(T_3(p))$.

Refer to Table 3.1 for some examples which confirms the validity of Theorem 3.2.1.

CHAPTER 4

THE KORSELT SET OF SOME SPECIFIC NUMBERS

4.1 Some Theorems and Examples about Korselt Numbers that Have pq Form

In this chapter, a focus on the Korselt set of a product of two distinct prime numbers is introduced. Throughout the chapter, 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 chapter is how are some conditions on p and q determines $KS(N)$. Starting by the following proposition.

Proposition 4.1.1. If $\alpha \in KS(N)$, then the following properties hold:

1. $p + q - 1 \in KS(N)$.

2. q does not divide α.

3. $q - p + 1 \leq \alpha \leq p + q - 1$.

4. If $T = \{\alpha, \text{where } N \text{is a } K_\alpha - \text{number}\}$ and
   $T' = \{(i-1)p + r \text{ with } 2 \leq r \leq 3p - 2\}$, then $T \subseteq T'$.

5. $p - 1$ is a multiple of $q - \alpha$.

6. $p - 1$ is a multiple of $p + s - r$.

Proof. In view of Propositions 2.4.1 and 2.2.1(3), it can be deduced that $2 \leq \alpha \leq N$.

1. Let $\alpha = p+q-1$. Then $N-\alpha = pq-p-q+1 = p(q-1)-(q-1) = (p-1)(q-1)$. Now, $p-\alpha = p-p-q+1 = -(q-1)$ which divides $N-\alpha$, and $q-\alpha = q-p-q+1 = -(p-1)$ which also divides $N-\alpha$. Thus, by definition of Korselt number, N is a K_α-number.

2. On the contrary, assume that q divides α. Then $\alpha = \beta q$ for some $\beta \in \mathbf{Z}$. Now, in view of Proposition 2.4.1, β must be greater than 1. There are two possible cases:

   Case1: p divides $p-\alpha$. If p divides $p-\alpha$, then p divides α as(p divides p). q divides α implies that $N = pq$ divides α. Hence, $N \leq \alpha$, which contradicts $\alpha < N$.

   Case2: p does not divide $p-\alpha$. As N is a K_α- number, $p-\alpha$ divides $N-\alpha$, where $N-\alpha = p(q-1)+(p-\alpha)$. This makes the conclution that $p-\alpha$ divides $p(q-1)$. But p does not divide $p-\alpha$, so $gcd(p, p-\alpha) = 1$. Thus, $p-\alpha$ divides $q-1$ and $p-\beta q$ divides $q-1$. But $p-\beta q$ is negative because $p < q < \beta q$. This yields that $|p-\beta q| = \beta q-p$ which divides $q-1$, hence, $\beta q - p \leq q-1$, which is not possible, since $\beta q - p \geq 2q-p > q$. Therefore, q does not divide α.

3. By definition of K_α-number, $q-\alpha$ divides $N-\alpha$, and $N-\alpha = pq-q+q-\alpha = q(p-1)+(q-\alpha)$, this implies that $q-\alpha$ divides $q(p-1)$. By using (2), $gcd(q, q-\alpha) = 1$. Thus $q-\alpha$ divides $p-1$ which means that

$q-\alpha \leq p-1$ and $\alpha \geq q-p+1$. Also $-(q-\alpha) \leq p-1$, so $\alpha \leq p+q-1$. Therefore, $q-p+1 \leq \alpha \leq p+q-1$.

4. Note that $q = ip + s > ip$, and $s < p$, so $q < ip + p = (i+1)p$. By (3), $q-p+1 \leq \alpha \leq q+p-1$. Thus, $q-p+1 > ip-p+1 = (i-1)p+1$ and $q+p-1 < (i+1)p+p-1 = (i+2)p-1$. This yields $(i-1)p+1 < \alpha < (i+2)p-1$. But $(i+2)p-1 = (i-1+3)p-1 = (i-1)p+(3p-1)$, hence, one can write $\alpha = (i-1)p + r$, with $r \in [2, 3p-2]$.

5. Let N be a K_α-number. By definition of the Korselt number, $q-\alpha$ divides $N-\alpha$. Now, $N-\alpha = pq-\alpha = pq-q+q-\alpha = q(p-1)+(q-\alpha)$. Hence, $q-\alpha$ divides $q(p-1)$ can be deduced. By(2) $gcd(q,\alpha) = 1$, so $q-\alpha$ divides $p-1$.

6. $q = ip + s$ with $i \geq 1$ and $s \in \{1, 2, ..., p-1\}$. By (5), $q-\alpha$ divides $p-1$. And by (4), $\alpha = (i-1)p + r$, with $r \in [2, 3p-2]$. Therefore, $q-\alpha = ip+s-(i-1)p-r = p+s-r$ and divides $p-1$.

Remark. By part 1 of Proposition 4.1.1, one may conclude that the Korselt set of any squarefree number with two distinct prime factors **is not empty**.

Proposition 4.1.2. If $p \geq 5$ and $q = 2p-3$ are prime numbers, then N is a $(q-p+1)$-Korselt number.

Proof. Definition of the Korselt number implies that $N = pq$ is a K_α-number iff $p-\alpha$ and $q-\alpha$ both divide $N-\alpha$. Here, $q = 2p-3$, hence $\alpha = 2p-3-p+1 = p-2$ and $N = p(2p-3)$. Also, $p-\alpha = p-(p-2) = 2$ divides $N-\alpha = p(2p-3)-(p-2) = 2(p-1)^2$ and $q-\alpha = 2p-3-(p-2) = p-1$ divides $2(p-1)^2$. Therefore, N is a K_{q-p+1}-number.

Example 4.1.1. Let $N = 77 = 7 * 11$. Note that $11 = q = 2p - 3$ and $q - p + 1 = 5 \in KS(77)$.

The following is an illustrative example of Proposition 4.1.1.

Example 4.1.2. Let $N = 4453 = 61 * 73$. Here, $p = 61$ and $q = 73$.

- Proposition 4.1.1(1) yields that $p + q - 1 = 133 \in KS(4453)$.

- Proposition 4.1.1(2) yields that for any $\alpha \in KS(4453)$, $q = 73$ does not divide any α.

- Proposition 4.1.1(3) yields $q - p + 1 \leq \alpha \leq p + q - 1$, and hence, $13 \leq \alpha \leq 133$.

- Proposition 4.1.1(4) in case $i = 1$, this yields that $(i-1)p + r = r$ with $2 \leq r \leq 3p - 2 = 181$. And hence, $\alpha \in \{2, .., 181\}$.

- Proposition 4.1.1(5) yields that $73 - \alpha$ divides 60, with $\alpha \in [2, 181]$. Note that $\{13, 43, 53, 58, 61, 63, 67, 68, 69, 70, 71, 72, 74, 75, 76, 77, 78, 79, 83, 85, 88, 93, 103, 133\}$ satisfy that $73 - \alpha$ divides 60.

- Proposition 4.1.1(6) yields that $73 - r$ divides 60, with $r = \alpha$. Hence, $\{13, 43, 53, 58, 61, 63, 67, 68, 69, 70, 71, 72, 74, 75, 76, 77, 78, 79, 83, 85, 88, 93, 103, 133\}$ satisfy $73 - r$ divides 60.

Now, using MATLAB, $KS(4453) = \{43, 53, 58, 63, 67, 69, 70, 79, 85, 133\}$ (see Table 5.1). This insures that all the above items are true.

The case of $gcd(p, \alpha) = 1$ has some particular results described in the following proposition.

Proposition 4.1.3. Let $\alpha \in KS(N)$ where α is a nonzero integer and $gcd(p, \alpha) = 1$, then the following properties hold:

1. $q - 1$ is a multiple of $p - \alpha$.

2. $(i-2)p + r$ divides $2p - r + s - 1$.

3. (a) If $F = \{\alpha,\ where\ N\ is\ an\ K_\alpha - number\ and\ \alpha \neq p + q - 1\}$ and $F' = \{(i-1)p + r\ with\ 2 \leq r \leq 2p - 1\}$, then $F \subseteq F'$.

   (b) $i \in \{1, 2, 3\}$.

Proof.

1. N is a K_α-number, so by definition of the Korselt number, $p - \alpha$ divides $N - \alpha$. Now, $N - \alpha = pq - p + p - \alpha = p(q-1) + (p - \alpha)$. Thus, $p - \alpha$ divides $p(q-1)$, By the hypothesis $gcd(\alpha, p) = 1$. Hence, $p - \alpha$ divides $q - 1$.

2. By (1), $\alpha - p$ divides $q - 1$, and by Proposition 4.1.1(4), $\alpha - p = (i-1)p + r - p = (i-2)p + r$. Also, $q - 1 = ip + s - 1 = (i - 2 + 2)p + r - r + s - 1 = [(i-2)p + r] + 2p - r + s - 1$. Hence, $(i-2)p + r$ divides $[(i-2)p + r] + 2p - r + s - 1$. Thus, $(i-2)p + r$ divides $2p - r + s - 1$.

3. (a) By Proposition 4.1.1(4), $\alpha = (i-1)p + r$ with $r \geq 2$. Now, using contradiction to prove that $r \leq 2p - 1$, suppose that $r \geq 2p$. Then by Proposition 4.1.1(4), $2p \leq r \leq 3p - 2$. Thus, $0 \leq r - 2p \leq p - 2$ and $2 - p \leq 2p - r \leq 0$. Next, $1 \leq s \leq p - 1$, so $0 \leq s - 1 \leq p - 2$. Hence, one infer that $-p + 2 \leq 2p - r + s - 1 \leq p - 2$. That means $|2p - r + s - 1| \leq p - 2$. it can be claimed that $2p - r + s - 1 \neq 0$.

By hypothesis $\alpha \neq p+q-1$, then $p+q-1-\alpha = p+(ip+s)-1-(i-1)p-r = 2p-r+s-1 \neq 0$. By (2), $(i-2)p+r$ divides $2p-r+s-1$. And as $2p-r+s-1 \neq 0$, this leads that $(i-2)p+r \leq |2p-r+s-1|$. Therefore, $p \leq ip = (i-2)p+2p \leq (i-2)p+r \leq |2p-r+s-1| \leq p-2$, which is not true. So, $2 \leq r \leq 2p-1$.

(b) By (3)(a), $r < 2p$. Then, getting $2p-r+s-1 > 0$. And by (2), $(i-2)p+r$ divides $2p-r+s-1$. Hence, $(i-2)p+r \leq 2p-r+s-1$. Which yields $(i-4)p \leq (s-r)-r-1$. By Proposition 4.1.1(6), $-p+1 \leq p+s-r \leq p-1$, so $r-s \geq 1$, and hence, $s-r \leq -1$. It is deduced that $(i-4)p \leq -r-2$. Giving $i \in \{1,2,3\}$.

Example 4.1.3. Let $N = 1147$. Here, $p = 31$, $q = 37$, $i = 1$ and $s = 6$. Note that $gcd(\alpha, 31) = 1$.

- Proposition 4.1.3(1) yields that $31-\alpha$ divides 36 for all $\alpha \in KS(1147)$.
- Proposition 4.1.3(2) yields that $-31+r$ divides $67-r$ with $r = \alpha$.
- Proposition 4.1.3(3) yields that $(i-1)p+r = r$ with $2 \leq r \leq 2.31-1 = 61$. Hence, $\alpha \in \{2,..,61\}$, where $\alpha \neq p+q-1 = 67$.

Now, by using MATLAB, $KS(1147) = \{22, 27, 32, 34, 35, 40, 43, 67\}$ (see Table 5.1) which agrees with the Proposition 4.1.3.

The following proposition concerns with the case $q > 2p^2$. It proves that in this case the result set is a singleton.

Proposition 4.1.4. (Echi and Ghanmi, 2012) If $q > 2p^2$, then $KS(N) = \{p+q-1\}$.

The proof of this proposition depends on the following lemma, which discusses the case p divides α.

Lemma 4.1.1. (Echi and Ghanmi, 2012) N is a K_α-number with an integer α and p divides α iff the following properties hold:

(I) $\alpha = ip$, s divides $p-1$ and $i-1$ divides $p+s-1$.

(II) $\alpha = (i+1)p$ and $lcm(p-s, i)$ divides $s-1$.

Proof. Assume that N is a K_α-number. In view of Proposition 4.1.1(4), $\alpha = (i-1)p+r$ with $2 \leq r \leq 3p-2$. Since p divides α, one concludes that p divides $r \in \{2, 3, ..., 3p-2\}$. This yields that $r = p$ or $r = 2p$. Therefore, $\alpha = ip$ or $\alpha = (i+1)p$.

Case1: $\alpha = ip$. Set $N - \alpha = p(q-1) + p - \alpha$. p divides α implies that

$$p - \alpha \,\text{divides}\, N - \alpha \quad \Leftrightarrow \quad \frac{p-\alpha}{p} \,\text{divides}\, q-1.$$

In this case, $\frac{p-\alpha}{p} = -i+1$ and $q-1 = ip+s-1 = (i-1)p+(p+s-1)$. Hence, $p-\alpha$ divides $N-\alpha \Leftrightarrow i-1$ divides $p+s-r$. Now, set $N-\alpha = q(p-1)+q-\alpha$. By Proposition 4.1.1(2), $gcd(q, \alpha) = 1$. Then

$$q - \alpha \,\text{divides}\, N - \alpha \quad \Leftrightarrow \quad q - \alpha \,\text{divides}\, p-1.$$

Here, $q - \alpha = ip + s - ip = s$. Thus, $q - \alpha$ divides $N - \alpha \Leftrightarrow s$ divides $p-1$. Therefore, N is a K_α-number iff $i-1$ divides $p+s-1$ and s divides $p-1$.

Case2: $\alpha = (i+1)p$. Here, $\frac{p-\alpha}{p} = -i$ and $q-1 = ip+(s-1)$. As in the case1, $p-\alpha$ divides $N-\alpha \Leftrightarrow i$ divides $s-1$. Also, $q-\alpha = ip+s-(i+1)p = s-p$

and $p-1 = p-s+(s-1)$. Thus, $q-\alpha$ divides $N-\alpha \Leftrightarrow p-s$ divides $s-1$. Therefore, N is an K_α-number iff i divides $s-1$ and $p-s$ divides $s-1$. These mean that $lcm(i, p-s)$ divides $s-1$.

Example 4.1.4.

- Is 10 a K_4-number?

  Here, $N = 10, p = 2, q = 5, i = 2$ and $s = 1$, where $q = ip + s$. Now, $p = 2$ which divides 4, also, $4 = ip$, $s = 1$ divides $p-1 = 1$ and $i-1 = 1$ divides $p+s-1 = 2$. Therefore, by using the first case of Lemma 4.1.1, 10 is a K_4-number.

- Is 77 a K_{14}-number?

  Here, $N = 77, p = 7, q = 11, i = 1$ and $s = 4$, where $q = ip + s$. Now, $p = 7$ which divides 14, also, $14 = (i+1)p$ and $lcm(p-s, i) = lcm(3,1) = 3$ divides $s-1 = 3$. So, by using the second case of Lemma 4.1.1, 77 is a 14-Korselt number.

Remark. (Raji, 2013) If p divides α, then $\alpha \in \{\lfloor \frac{q}{p} \rfloor p, \lceil \frac{q}{p} \rceil p\}$.

Proof. Note that $\frac{q}{p} = \frac{ip+s}{p} = i + \frac{s}{p}$ with $s < p$. Hence, $\lfloor \frac{q}{p} \rfloor = i$ and $\lceil \frac{q}{p} \rceil = i+1$. Thus, $\{\lfloor \frac{q}{p} \rfloor p, \lceil \frac{q}{p} \rceil p\} = \{ip, (i+1)p\}$. By Lemma 4.1.1, $\alpha \in \{ip, (i+1)p\}$, therefore $\alpha \in \{\lfloor \frac{q}{p} \rfloor p, \lceil \frac{q}{p} \rceil p\}$.

Corollary 4.1.1. (Echi and Ghanmi, 2012) Assume that N is an K_α-number with an integer α and $gcd(p, \alpha) = 1$. if $q \geq 4p$, then $\alpha = p+q-1$.

Proof. Proposition 4.1.3(3) leads that for all $\alpha \in KS(N)$ except $\alpha = p+q-1$, $i \in \{1, 2, 3\}$. Which yields $q < 4p$. Therefore, if $q \geq 4p$, then $\alpha = p+q-1$.

Now, it is time to prove Proposition 4.1.4.

Proof of Proposition 4.1.4: By contraposition, suppose that there is $\alpha \in KS(N)$ such that $\alpha \neq q+p-1$. By Lemma 4.1.1, $i-1$ divides $p+s-1>0$. Then, $i-1 \leq p+s-1$, but $s \leq p-1$, this yields that $i \leq p+s \leq 2p-1$. Which yields $q = ip+s \leq (2p-1)p+p-1 = 2p^2-1$. This implies that, if $q > 2p^2-1$, finally $KS(N) = \{p+q-1\}$.

Example 4.1.5. Let $N = 471347 = 61 * 7727$. Here, $p = 61$, $q = 7727$ and $7727 > 2 * 61^2 = 7442$. Therefore, by Proposition 4.1.4, $KS(471347) = \{61+7727-1\} = \{7787\}$.

Proposition 4.1.5. (Echi and Ghanmi, 2012) If $p^2-p < q < 2p^2$ and $p \geq 5$, then $KS(N) \subseteq \{ip, p+q-1\}$.

Proof. Let $p \geq 5$ and $p^2-p < q < 2p^2$. Start by the claim that $q > 4p$ and $i > s-1$. It is clear that $q > p^2-p = p(p-1) \geq 4p$. Hence, by Corollary 4.1.1, $p+q-1$ is a possible value of α. Now, to show that $i > s-1$, let $i \leq s-1$, then from $q = ip+s$ and $s \leq p-1$, it gives

$$q \leq (s-1)p+s \leq p(p-2)+p-1 = p^2-p-1,$$

which is a contradiction, since $q > p^2-p$. Hence, $i > s-1$, which leads that i does not divide $s-1$. So, by Lemma 4.1.1, $(i+1)p$ is not a possible value of α. Therefore, it is concluded that the possible values of $\alpha \in KS(N)$ are ip and $p+q-1$.

Example 4.1.6. Let $N = 145 = 5 * 29$. Here, $p = 5$, $q = 29$ and $5^2 - 5 = 20 < 29 < 2 * 5^2 = 50$. Therefore, by Proposition 4.1.5, $KS(145) \subseteq \{5i, 33\} = \{25, 33\}$

Proposition 4.1.6. (Echi and Ghanmi, 2012) If $4p < q < p^2 - p$, then $KS(N) \subseteq \{ip, (i+1)p, p+q-1\}$.

Proof. Let $4p < q < p^2 - p$. Here, $q > 4p$, then by Corollary 4.1.1, $\alpha = p+q-1 \subseteq KS(N)$. Also, by Lemma 4.1.1, the possible values of α are ip and $(i+1)p$. Thus, $KS(N) \subseteq \{ip, (i+1)p, p+q-1\}$.

Example 4.1.7. Let $N = 203 = 7 * 29$. Here, $p = 7$, $q = 29$ and $4 * 7 = 28 < 29 < 7^2 - 7 = 42$. Therefore, by Proposition 4.1.6, $KS(203) \subseteq \{7i, 7(i+1), 35\} = \{28, 35\}$.

The next lemma helps to prove Proposition 4.1.7, which discuss the case $3p < q < 4p$

Lemma 4.1.2. (Echi and Ghanmi, 2012) Assume that N is an K_α-number with an integer $\alpha \neq p+q-1$ such that $gcd(p, \alpha) = 1$. If $3p < q < 4p$, then $q = 4p-3$ and $\alpha = q - p + 1 = 3p - 2$.

Proof. Assuming $3p < q < 4p$ gives $q = 3p + s$ with $1 \leq s \leq p - 1$. Now, Suppose $\alpha \neq p + q - 1$. Thus, by Proposition 4.1.3, $\alpha = 2p + r$ with $2 \leq r \leq 2p - 1$. Also, as $gcd(p, \alpha) = 1$, $r \neq p$. By Proposition 4.1.3.(2), $p + r$ divides $2p-r+s-1$. And $2p-r+s-1 = 2p+2r-3r+s-1 = 2(p+r)-(3r-s+1)$. This yields that $p + r$ divides $3r - s + 1$. By Proposition 4.1.1(6), it can be concluded that $1 \leq r - s \leq 2p - 1$. So, Add $2r + 1$ to this inequality, giving

$2r+2 \leq 3r-s+1 \leq 2p+2r = 2(p+r)$. But $p+r$ divides $3r-s+1$, so two cases can be had:

Case1: $3r-s+1 = 2(p+r)$. We conclude that $r = 2p+s-1$, which implies $\alpha = 2p+r = 2p+2p+s-1 = 4p+s-1 = (3p+s)+p-1 = q+p-1$, a contradiction.

Case2: $3r-s+1 = p+r$. By subtract $2r-s$ to this equation, giving $p+s-r = r+1$. By Proposition 4.1.1.(6), Thus, $r+1$ divides $p-1$, where $p-1 = 2r-s = 2r+2-2-s = 2(r+1)-(s+2)$. Hence, $r+1$ divides $s+2$. But, by Proposition 4.1.1(6), $1 \leq r-s$. Add $s+1$ to this inequality, giving $s+2 \leq r+1$. Consequently, $r+1 = s+2$. Therefore, $p-1 = 2r-s = r+(r-s) = r+1$, which yields $q = 3p+s = 3p+(r+1)-2 = 3p+p-1-2 = 4p-3$ and $\alpha = 2p+r = 2p+p-2 = 3p-2 = q-p+1$.

Example 4.1.8. Let $N = 14701$. Here, $p = 61$ and $q = 241 = 4p-3$. $KS(14701) = \{181, 244, 301\}$. Note that, $181 = 3p-2$, $244 = 4p$ (here, p divides α) and $301 = p+q-1$.

Proposition 4.1.7. (Echi and Ghanmi, 2012) Suppose that $3p < q < 4p$. Then the following conditions are satisfied:

1. If $q = 4p-3$, then the following properties hold:

   (a) If $p \equiv 1 \pmod 3$, then $KS(N) = \{4p, q-p+1, p+q-1\}$.

   (b) If $p \not\equiv 1 \pmod 3$ and $p \neq 5$, then $KS(N) = \{q-p+1, p+q-1\}$.

   (c) If $p = 5$, then $KS(N) = \{3p, q-p+1, p+q-1\}$.

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

Proof.

1. To prove this item, it is needed to prove that each $p+q-1$ and $q-p+1$ $\in KS(N)$ for all $N = pq$ such that p and q are primes, $p \neq 3$ and $q = 4p-3$. Also, it is necessary to prove that $4p \in KS(N)$ just in case $p \equiv 1 \pmod 3$. By Proposition 4.1.1(1), $p+q-1 \in KS(N)$. Now, one must prove that $q-p+1 \in KS(N)$. Let $\alpha = q-p+1 = 4p-3-p+1 = 3p-2$. Hence, $p-\alpha = p-(3p-2) = -2(p-1)$, $q-\alpha = 4p-3-(3p-2) = p-1$ and $N-\alpha = pq-(3p-2) = p(4p-3)-(3p-2) = 4p^2-3p-3p+2 = 4p^2-6p+2 = 2(p-1)(2p-1)$. Both of $p-\alpha$ and $q-\alpha$ divide $N-\alpha$. Therefore, by definition of the Korselt number $\alpha = q-p+1 \in KS(N)$. Now, $q = 4p-3 = 3p+(p-3)$. Thus, $i = 3$ and $s = p-3$. Note that s does not divide $p-1$ (Counter example: Let $p = 11$. Thus, $11-3 = 8$ does not divide $11-1 = 10$), so by Lemma 4.1.1(I), $3p \notin KS(N)$. In view of Lemma 4.1.1(II), $lcm(p-s,i) = lcm(3,3) = 3$.

   - If $p \equiv 1 \pmod 3$, then $p-4 \equiv 0 \pmod 3$. This yields that $lcm(p-s,i) = 3$ divides $s-1 = p-4$. Hence, $4p \in KS(N)$.
   - If $p \not\equiv 1 \pmod 3$, then $p \equiv 2 \pmod 3$ (p is a prime and not equal 3). Thus, $p-4 \equiv 1 \pmod 3$. This means that $lcm(p-s,i) = 3$ does not divide $s-1 = p-4$. Hence, $4p \notin KS(N)$.

2. By using Lemma 4.1.2 and Lemma 4.1.1, it can be concluded that $KS(N) \subseteq \{3p, 4p, p+q-1\}$.

The following examples discuss the previous proposition cases.

Example 4.1.9. Let $N = 1387 = 19 * 73$. Here, $p = 19$, $q = 73$. Note that $q = 4p-3$ and $p \equiv 1 \pmod 3$ Therefore, $KS(1387) = \{55, 76, 91\}$.

Example 4.1.10. • Let $N = 85 = 5 * 17$. Here, $p = 5$, $q = 17$. Note that $q = 4p - 3$ with $p = 5$. Therefore, $KS(85) = \{13, 15, 21\}$.

• Let $N = 451 = 11 * 41$. Here, $p = 11$, $q = 41$. Note that $q = 4p - 3$ and $p \equiv 2 \pmod 3$ where $p \neq 5$. Therefore, $KS(451) = \{31, 51\}$

Example 4.1.11. Let $N = 14 = 2 * 7$. Here, $p = 2$, $q = 7$. Note that $3p < q < 4p$ and $q \neq 4p - 3$. Therefore, $KS(14) \subseteq \{6, 8\}$.

To study the case $2p < q < 3p$, the following lemma helps.

Lemma 4.1.3. (Echi and Ghanmi, 2012) Suppose that N is a K_α-number with an integer $\alpha \neq p + q - 1$ and $gcd(p, \alpha) = 1$. If $2p < q < 3p$. then $\alpha \in \{3q - 5p + 3, \frac{2p+q-1}{2}, q - p + 1\}$.

Proof. Assume $2p < q < 3p$. Thus, $q = 2p+s$ with $1 \leq s \leq p-1$. $\alpha \neq p+q-1$, so by Proposition 4.1.3(3), $\alpha = p + r$ with $2 \leq r \leq 2p - 1$, and $\alpha \neq p$. By using Proposition 4.1.3.(2), r divides $q - 1 = 2p + s - 1$. This means that $2p + s - 1 = lr$, where l be a non zero integer. Then the proof has four cases.

Case1: When $l \geq 4$; will obtain the inequality

$$r \leq \frac{2p + s - 1}{4}.$$

Claim: $p + s - r \leq p - 1 < 2(p + s - r)$.

By Proposition 4.1.1.(6), $p + s - r \leq p - 1$. Also, $s \geq 1$, giving $s > -1$, $3s > -3$, $s - 1 < 4s + 2$ and $\frac{s-1}{2} < 2s + 1$. Hence, $p + \frac{s-1}{2} < p + 2s + 1$. Then $r \leq \frac{2p+s-1}{4}$, giving $2r \leq \frac{2p+s-1}{2} = p + \frac{s-1}{2} < p+2s+1$. Note that $2r < p+2s+1$ is equivalent to $p-1 < 2(p+s-r)$. Therefore, $p+s-r \leq p-1 < 2(p+s-r)$.

By Proposition 4.1.1.(6), $p+s-r$ divides $p-1$. This yields that $p-1 = p+s-r$ and $r = s+1$. Hence, $\alpha = p+r = (2p+s)-p+1 = q-p+1$.

Case2: When $l = 3$, then $r = \frac{2p+s-1}{3}$. Now, $q-\alpha = 2p+s-(p+r) = p+s-r = p+s-\frac{2p+s-1}{3} = \frac{p+2s+1}{3}$. Also, By Proposition4.1.1.(5), $q-\alpha$ divides $p-1$. hence, $\frac{p+2s+1}{3}$ divides $p-1$. Giving $p+2s+1$ divides $3(p-1) = 3(p+2s+1)-(6s+6)$. This implies that $p+2s+1$ divides $6s+6$. Also, as $3(p-1)$ is positive, then it gives $0 < 6s+6 < 3(p+2s+1)$. Thus, to deal with two cases:

- $6s+6 = p+2s+1$. Then $p = 4s+5$ and $r = \frac{2p+s-1}{3} = 3s+3$. Consequently, $\alpha = p+r = p+3s+3 = 6p+3s-5p+3 = 3(2p+s)-5p+3 = 3q-5p+3$.

- $6s+6 = 2(p+2s+1)$. Then $p = s+2$ and $r = \frac{2p+s-1}{3} = \frac{2(s+2)+s-1}{3} = \frac{3s+3}{3} = s+1$. It follows that $\alpha = p+r = p+s+1 = (2p+s)-p+1 = q-p+1$.

Case3: When $l = 2$, then $r = \frac{2p+s-1}{2}$. In this case, it has $\alpha = p+r = p+\frac{2p+s-1}{2} = \frac{4p+s-1}{2} = \frac{2p+q-1}{2}$.

Case4: When $l = 1$, then $r = 2p+s-1 = q-1$. Hence, $\alpha = p+r = p+q-1$, contradicting the hypothesis.

Example 4.1.12. Let $N = 19109 = 97 * 197$. Here, $p = 97$, $q = 197$ and $2p < q < 3p$. Also, $KS(19109) = \{101, 194, 195, 293\}$. Note that $101 = q-p+1$, $194 = 2p$ (p which divides α), $195 = \frac{2p+q-1}{2}$ and $293 = p+q-1$. one can conclude that $\{101, 195\} \subseteq \{101, 109, 195\} = \{q-p+1, 3q-5p+3, \frac{2p+q-1}{2}\}$.

Proposition 4.1.8. (Echi and Ghanmi, 2012) Suppose $2p < q < 3p$, then

$$KS(N) \subseteq \{2p, 3p, 3q - 5p + 3, \frac{2p + q - 1}{2}, q - p + 1, p + q - 1\}.$$

Proof. It is clear by using Lemma 4.1.3 and Lemma 4.1.1.

Example 4.1.13. Let $N = 10 = 2 * 5$. Here, $p = 2$, $q = 5$ and $2p < q < 3p$. Therefore, by Proposition 4.1.8, $KS(10) \subseteq \{4, 6, 8\}$.

The following result was proved by Echi and Ghanmi (Echi and Ghanmi, 2012).

Proposition 4.1.9. Set

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

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

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

But it is possible to find a counter example that make this result not true in general. Next, an example is provided as well as a suggested correction to the theorem.

Example 4.1.14. Let $N = 77$. Here, $p = 7$, $q = 11$ and $p < q < 2p$.

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

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

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

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

The following proposition is a correction of Theorem 14 part 6 in (Echi and Ghanmi, 2012).

Proposition 4.1.10. Set

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

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

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

Proof. Here it has two cases:

Case1: p divides α. By Lemma 4.1.1, $\alpha = p$ 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 not divide $p + s - 1$, hence, $\alpha = 2p$.

Case2: p doesn't divide α, which means that $gcd(p, \alpha) = 1$. By Proposition 4.1.1(3), then

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

so

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

By Proposition 4.1.1(2), $gcd(q,\alpha)=1$. Hence, by Proposition 4.1.1(5), $q-\alpha$ 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 Proposition 4.1.3(1), $p-\alpha$ 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, $\alpha \in \{q-\frac{p-1}{l_1}, q-\frac{p-1}{l_2}, ..., q-\frac{p-1}{l_s}\} \cup \{p+\frac{q-1}{k_1}, p+\frac{q-1}{k_2}, ..., p+\frac{q-1}{k_t}\}$, where $(k_1, ..., k_t)$ are factors of $q-1$ and $(l_1, ..., l_s)$ are factors of $p-1$. Hence, from case1 and case2, it is concluded that $\alpha \in I(p,q) \cup J(p,q) \cup \{2p\}$.

Example 4.1.15. Let $N=77$. Here, $p=7$, $q=11$ and $p<q<2p$.

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

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

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

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

4.2 The Korselt Set of $6q$. (Al-Rasasi et al., 2013)

This section is about the Korselt set of an integer that has the form $6q$, where q is a prime number distinct from 2 and 3.

Proposition 4.2.1. Let $N = 6q$ with a prime $q \geq 5$. If $\alpha \in KS(N)$, then $\alpha \in \{q+1, q-1, q+5, q-5\}$.

Proof. Suppose that $\alpha \in KS(N)$. Thus, $q - \alpha$ divides $N - \alpha$. Here, $N - \alpha = 6q - \alpha = 5q + (q - \alpha)$. Hence, $q - \alpha$ divides $5q$. This yields $q - \alpha \in \{\pm 1, \pm 5, \pm q, \pm 5q\}$.

- $q - \alpha \neq q$ and $q - \alpha \neq -5q$, because by definition of the Korselt number, $\alpha \neq 0$ and $\alpha \neq N$.

- Suppose that $q - \alpha = -q$. Hence, $\alpha = 2q$. Now, 2 is a prime factor of N implies that $2 - \alpha = 2(1 - q)$ divides $N - \alpha = 4q$. This yields that $q - 1$ divides $2q$. But $gcd(q-1, q) = 1$, so $q - 1$ divides 2. This leads that either $q - 1 = 1$ or $q - 1 = 2$. Consequently, $q = 2$ or $q = 3$, which contradict the hypotheses.

- Suppose that $q - \alpha = 5q$. Hence, $\alpha = -4q$. Again $2 - \alpha = 2(1 + 2q)$ divides $N - \alpha = 10q$. Thus, $1 + 2q$ divides $5q$. Now, $gcd(1 + 2q, q) = 1$ implies that $1 + 2q$ divides 5. This yields that $1 + 2q = 1$ or $1 + 2q = 5$. Consequently, $q = 0$ or $q = 2$, which again contradict the hypotheses.

Therefore, this indicates that $q - \alpha \in \{\pm 1, \pm 5\}$, hence $\alpha \in \{q+1, q-1, q+5, q-5\}$.

In the following theorem, the previous proposition will be used to prove that the $KS(6q) = \emptyset$ for all values of q except when $q \in \{5, 7, 11, 17\}$.

Theorem 4.2.1. Let $N = 6q$, where q is a prime number greater than or equal to 5. Then the following results satisfied:

1. If $\alpha = q + 1$, then $q = 5$.

2. If $\alpha = q - 1$, then $q \in \{5, 7, 11\}$.

3. It is not possible to have $\alpha = q + 5$.

4. If $\alpha = q - 5$, then $q \in \{11, 17\}$

Proof.

1. Suppose that $\alpha = q + 1$. N is a K_α-number and 2 is a prime factor of N, so $2 - \alpha = 1 - q$ divides $N - \alpha$, with $N - \alpha = 5q - 1 = 5(q - 1) + 4$. It can be deduced that $q - 1$ divides 4. Hence, $q - 1 \in \{1, 2, 4\}$. and then, $q \in \{2, 3, 5\}$. Also, 3 is a prime factor of N, so $3 - \alpha = 2 - q$ divides $N - \alpha$, where $N - \alpha = 5q - 1 = 5(q - 2) + 9$. Thus, $q - 2$ divides 9 can be concluded. Hence, $q - 2 \in \{1, 3, 9\}$ and $q \in \{3, 5, 11\}$. Therefore, $q \in \{3, 5\}$. But $q \geq 5$, thus $q = 5$.

2. Suppose that $\alpha = q - 1$. Then $2 - \alpha = 3 - q$ divides $N - \alpha$, where $N - \alpha = 5q + 1 = 5(q - 3) + 16$. It gives $q - 3$ divides 16, so that, $q - 3 \in \{1, 2, 4, 8, 16\}$ and $q \in \{5, 7, 11, 19\}$. Also, $3 - \alpha = 4 - q$ divides $N - \alpha$ where $N - \alpha = 5q + 1 = 5(q - 4) + 21$, concluding that $q - 4$ divides 21. Thus, $q - 4 \in \{1, 3, 7, 21\}$ and $q \in \{5, 7, 11\}$. It follows that $q \in \{5, 7, 11\}$.

3. Suppose that $\alpha = q + 5$, Then $2 - \alpha = -3 - q$ divides $N - \alpha$, where $N - \alpha = 5q - 5 = 5(q + 3) - 20$. It gives $q + 3$ divides 20. Hence, $q + 3 \in \{1, 2, 4, 5, 10, 20\}$ and $q \in \{7, 17\}$. Also $3 - \alpha = -2 - q$ divides $N - \alpha$, where $N - \alpha = 5q - 5 = 5(q + 2) - 15$. Thus, $q + 2$ divides

15, and consequently, $q+2 \in \{1,3,5,15\}$ and $q \in \{3,13\}$. There is no intersection between $\{7,17\}$ and $\{3,13\}$. Therefore, it is not possible to have $\alpha = q+5$

4. Suppose that $\alpha = q-5$. Then $2-\alpha = 7-q$ divides $N-\alpha$, where $N-\alpha = 5q+5 = 5(q-7)+40$. Hence, $q-7$ divides 40 can be deduced. And since $q-7 \geq 5-7 = -2$, it gives $q-7 \in \{-2,-1,1,2,4,5,8,10,20,40\}$ and $q \in \{5,11,17,47\}$. But $\alpha \neq 0$ gives $q \in \{11,17,47\}$. Also, $3-\alpha-8-q$ divides $N-\alpha$, where $N-\alpha = 5q+5 = 5(q-8)+45$. This yields $q-8$ divides 45. Since $q-8 \geq 5-8 = -3$, it gives $q-8 \in \{-3,-1,1,3,5,9,15,45\}$ and $q \in \{7,11,13,17,23,53\}$. Therefore, in this case, $q \in \{11,17\}$.

Corollary 4.2.1. Combining the previous results, the only values of q for which $KS(6q) \neq \phi$ are $5,7,11$ and 17.

Example 4.2.1. (Al-Rasasi et al., 2013)

- For $q=5$, then $KS(6q) = \{q-1, q+1\} = \{4,6\}$.
- For $q=7$, then $KS(6q) = \{q-1\} = \{6\}$.
- For $q=11$, then $KS(6q) = \{q-1, q-5\} = \{6,10\}$.
- For $q=17$, then $KS(6q) = \{q-5\} = \{12\}$.

CHAPTER 5

RESULTS AND CONCLUSION

5.1 Algorithms and Tables

The following propositions that were proven in the previous chapter are used in the following diagram (see Figure 5.1) to find the $KS(N)$ for all N that have the form $p * q$. After that, $KS(N)$ for all $N = pq$ where p and q are less than 100 is found. (See Table 5.1.)

- If $q > 2p^2$, then $KS(N) = \{p + q - 1\}$.
- If $p^2 - p < q < 2p^2$ and $p \geq 5$, then $KS(N) \subseteq \{ip, p + q - 1\}$.
- If $4p < q < p^2 - p$, then $KS(N) \subseteq \{ip, (i + 1)p, p + q - 1\}$.
- Suppose that $3p < q < 4p$. Then the following conditions are satisfied:
  1. If $q = 4p - 3$, then the following properties hold:
     (a) If $p \equiv 1 \pmod 3$, then $KS(N) = \{4p, q - p + 1, p + q - 1\}$.
     (b) If $p \not\equiv 1 \pmod 3$, then $KS(N) = \{q - p + 1, p + q - 1\}$ except when $p = 5$, because in this case $KS(N) = \{3p, q - p + 1, p + q - 1\}$
  2. If $q \neq 4p - 3$, then $KS(N) \subseteq \{3p, 4p, p + q - 1\}$.

- Suppose $2p < q < 3p$, then

$$KS(N) \subseteq \{2p, 3p, 3q - 5p + 3, \frac{2p + q - 1}{2}, q - p + 1, p + q - 1\}.$$

- Suppose that $p < q < 2p$. Then, setting

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

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

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

The following flowchart is used to make MATLAB program to calculate the $KS(N)$ for all $N = pq$.

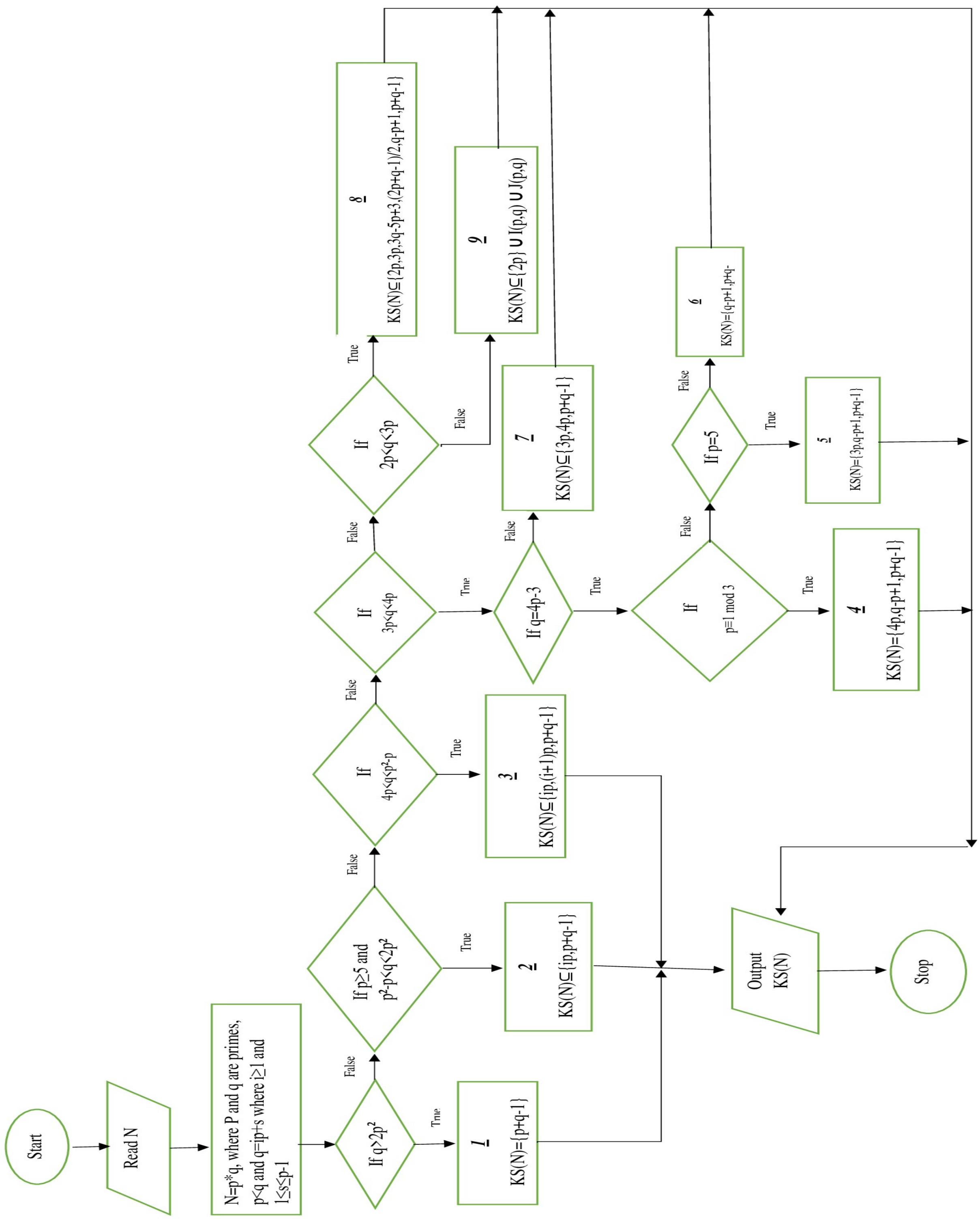

Figure 5.1: A flowchart representing a fast approach to calculate the $KS(N)$.

Table 5.1: $KS(N)$ for all $N = pq$ where p and q are less than 100.

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

Continued on next page

Table 5.1 – continued from previous page

N	p	q	**Category**	$\alpha \in KS(N)$
77	7	11	9	5, 8, 9, 12, 14, 17
82	2	41	1	42
85	5	17	5	15, 21, 13
86	2	43	1	44
87	3	29	1	31
91	7	13	9	10, 11, 14, 19
93	3	31	1	33
94	2	47	1	48
95	5	19	7	15, 20, 23
106	2	53	1	54
111	3	37	1	39
115	5	23	1	27
118	2	59	1	60
119	7	17	8	11, 14, 15, 23
122	2	61	1	62
123	3	41	1	43
129	3	43	1	45
133	7	19	8	13, 16, 21, 25
134	2	67	1	68
141	3	47	1	49
142	2	71	1	72

Continued on next page

Table 5.1 – continued from previous page

N	p	q	**Category**	$\alpha \in KS(N)$
143	11	13	9	8, 12, 14, 15, 23
145	5	29	2	25, 33
146	2	73	1	74
155	5	31	2	30, 35
158	2	79	1	80
159	3	53	1	55
161	7	23	7	21, 29
166	2	83	1	84
177	3	59	1	61
178	2	89	1	90
183	3	61	1	63
185	5	37	2	35, 41
187	11	17	9	7, 12, 15, 19, 22, 27
194	2	97	1	98
201	3	67	1	69
203	7	29	3	35
205	5	41	2	45
209	11	19	9	9, 14, 17, 20, 29
213	3	71	1	73
215	5	43	2	47
217	7	31	3	28, 37

Continued on next page

Table 5.1 – continued from previous page

N	p	q	**Category**	$\alpha \in KS(N)$
219	3	73	1	75
221	13	17	9	5, 11, 14, 15, 21, 29
235	5	47	2	51
237	3	79	1	81
247	13	19	9	7, 15, 16, 22, 31
249	3	83	1	85
253	11	23	8	13, 22, 33
259	7	37	3	35, 43
265	5	53	1	57
267	3	89	1	91
287	7	41	3	35, 42, 47
291	3	97	1	99
295	5	59	1	63
299	13	23	9	11, 24, 26, 35
301	7	43	2	49
305	5	61	1	65
319	11	29	8	39
323	17	19	9	11, 15, 18, 20, 23, 35
329	7	47	2	53
335	5	67	1	71
341	11	31	8	21, 26, 33, 41

Continued on next page

Table 5.1 – continued from previous page

N	p	q	**Category**	$\alpha \in KS(N)$
355	5	71	1	75
365	5	73	1	77
371	7	53	2	59
377	13	29	8	17, 26, 27, 41
391	17	23	9	15, 19, 39
395	5	79	1	83
403	13	31	8	19, 28, 43
407	11	37	7	47
413	7	59	2	65
415	5	83	1	87
427	7	61	2	67
437	19	23	9	17, 20, 21, 41
445	5	89	1	93
451	11	41	6	31, 51
469	7	67	2	73
473	11	43	7	33, 44, 53
481	13	37	8	25, 31, 39, 49
485	5	97	1	101
493	17	29	9	13, 21, 31, 45
497	7	71	2	77
511	7	73	2	70, 79

Continued on next page

Table 5.1 – continued from previous page

N	p	q	**Category**	$\alpha \in KS(N)$
517	11	47	3	57
527	17	31	9	15, 23, 27, 32, 47
533	13	41	7	39, 53
551	19	29	9	20, 23, 26, 38, 47
553	7	79	2	85
559	13	43	7	39, 55
581	7	83	2	89
583	11	53	3	55, 63
589	19	31	9	13, 22, 25, 29, 34, 49
611	13	47	7	59
623	7	89	2	95
629	17	37	8	21, 29, 35, 53
649	11	59	3	69
667	23	29	9	27, 30, 51
671	11	61	3	66, 71
679	7	97	2	91, 103
689	13	53	3	65
697	17	41	8	25, 37, 57
703	19	37	9	28, 31, 38, 55
713	23	31	9	20, 29, 33, 53
731	17	43	8	51, 59

Continued on next page

Table 5.1 – continued from previous page

N	p	q	**Category**	$\alpha \in KS(N)$
737	11	67	3	77
767	13	59	3	71
779	19	41	8	23, 38, 39, 59
781	11	71	3	66, 81
793	13	61	3	65, 73
799	17	47	8	51, 63
803	11	73	3	83
817	19	43	8	25, 40, 61
851	23	37	9	26, 35, 59
869	11	79	3	77, 89
871	13	67	3	79
893	19	47	8	38, 65
899	29	31	9	24, 27, 30, 32, 35, 59
901	17	53	7	51, 69
913	11	83	3	93
923	13	71	3	83
943	23	41	9	19, 43, 63
949	13	73	3	85
979	11	89	3	99
989	23	43	9	21, 44, 65
1003	17	59	7	51, 75

Continued on next page

Table 5.1 – continued from previous page

N	p	q	**Category**	$\alpha \in KS(N)$
1007	19	53	8	71
1027	13	79	3	91
1037	17	61	7	77
1067	11	97	3	99, 107
1073	29	37	9	23, 30, 33, 35, 38, 41, 65
1079	13	83	3	95
1081	23	47	8	25, 46, 69
1121	19	59	7	57, 77
1139	17	67	7	51, 68, 83
1147	31	37	9	22, 27, 32, 34, 35, 40, 43, 67
1157	13	89	3	101
1159	19	61	7	79
1189	29	41	9	27, 34, 37, 39, 69
1207	17	71	3	87
1219	23	53	8	75
1241	17	73	3	89
1247	29	43	9	15, 36, 50, 71
1261	13	97	3	91, 109
1271	31	41	9	11, 26, 35, 36, 39, 51, 71
1273	19	67	7	76, 85
1333	31	43	9	28, 33, 37, 38, 45, 73

Continued on next page

Table 5.1 – continued from previous page

N	p	q	**Category**	$\alpha \in KS(N)$
1343	17	79	3	95
1349	19	71	7	89
1357	23	59	8	81
1363	29	47	9	75
1387	19	73	4	76, 55, 91
1403	23	61	8	83
1411	17	83	3	99
1457	31	47	9	32, 62, 77
1501	19	79	3	76, 97
1513	17	89	3	85, 105
1517	37	41	9	29, 32, 35, 38, 39, 42, 45, 47, 77
1537	29	53	9	25, 55, 81
1541	23	67	8	45, 56, 69, 89
1577	19	83	3	101
1591	37	43	9	31, 34, 39, 40, 44, 79
1633	23	71	7	69, 93
1643	31	53	9	83
1649	17	97	3	113
1679	23	73	7	95
1691	19	89	3	95, 107
1711	29	59	8	31, 58, 87

Continued on next page

Table 5.1 – continued from previous page

N	p	q	**Category**	$\alpha \in KS(N)$
1739	37	47	9	35, 38, 83
1763	41	43	9	35, 38, 39, 42, 44, 47, 48, 83
1769	29	61	8	33, 59, 89
1817	23	79	7	101
1829	31	59	9	29, 60, 62, 89
1843	19	97	3	95, 115
1891	31	61	9	46, 51, 62, 91
1909	23	83	7	105
1927	41	47	9	39, 42, 43, 87
1943	29	67	8	95
1961	37	53	9	35, 41, 50, 89
2021	43	47	9	41, 44, 45, 89
2047	23	89	6	67, 111
2059	29	71	8	43, 64, 99
2077	31	67	8	37, 62, 64, 97
2117	29	73	8	87, 101
2173	41	53	9	43, 45, 54, 93
2183	37	59	9	95
2201	31	71	8	41, 66, 101
2231	23	97	3	119
2257	37	61	9	25, 43, 49, 52, 57, 67, 97

Continued on next page

Table 5.1 – continued from previous page

N	p	q	**Category**	$\alpha \in KS(N)$
2263	31	73	8	43, 67, 103
2279	43	53	9	39, 47, 56, 95
2291	29	79	8	107
2407	29	83	8	87, 111
2419	41	59	9	39, 99
2449	31	79	8	109
2479	37	67	9	31, 70, 103
2491	47	53	9	51, 99
2501	41	61	9	21, 51, 53, 56, 71, 101
2537	43	59	9	45, 101
2573	31	83	8	93, 113
2581	29	89	7	87, 117
2623	43	61	9	40, 47, 55, 58, 63, 103
2627	37	71	9	35, 72, 74, 107
2701	37	73	9	55, 61, 74, 109
2747	41	67	9	47, 63, 107
2759	31	89	8	119
2773	47	59	9	105
2813	29	97	7	125
2867	47	61	9	59, 62, 107
2881	43	67	9	46, 65, 109

Continued on next page

Table 5.1 – continued from previous page

N	p	q	**Category**	$\alpha \in KS(N)$
2911	41	71	9	31, 51, 76, 111
2923	37	79	8	43, 76, 115
2993	41	73	9	33, 53, 65, 77, 113
3007	31	97	7	127
3053	43	71	9	29, 50, 57, 78, 113
3071	37	83	8	74, 119
3127	53	59	9	55, 111
3139	43	73	9	31, 52, 67, 79, 115
3149	47	67	9	44, 69, 113
3233	53	61	9	48, 57, 59, 63, 65, 113
3239	41	79	9	39, 80, 119
3293	37	89	8	125
3337	47	71	9	48, 94, 117
3397	43	79	9	37, 82, 86, 121
3403	41	83	8	43, 82, 123
3431	47	73	9	50, 71, 119
3551	53	67	9	54, 119
3569	43	83	9	41, 84, 86, 125
3589	37	97	8	61, 85, 133
3599	59	61	9	60, 62, 63, 119
3649	41	89	8	49, 85, 129

Continued on next page

Table 5.1 – continued from previous page

N	p	q	**Category**	$\alpha \in KS(N)$
3713	47	79	9	125
3763	53	71	9	58, 67, 123
3827	43	89	8	47, 86, 87, 131
3869	53	73	9	47, 71, 77, 125
3901	47	83	9	129
3953	59	67	9	65, 125
2977	41	97	8	57, 89, 137
4087	61	67	9	55, 62, 63, 64, 72, 127
4171	43	97	8	55, 91, 139
4183	47	89	9	43, 91, 135
4187	53	79	9	27, 66, 92, 131
4189	59	71	9	69, 73, 129
4307	59	73	9	71, 131
4331	61	71	9	51, 56, 59, 66, 68, 75, 131
4399	53	83	9	135
4453	61	73	9	43, 53, 58, 63, 67, 69, 70, 79, 85, 133
4559	47	97	8	51, 95, 143
4661	59	79	9	137
4717	53	89	9	141
4757	67	71	9	60, 65, 68, 69, 72, 74, 77, 137
4819	61	79	9	59, 64, 67, 74, 139

Continued on next page

Table 5.1 – continued from previous page

N	p	q	**Category**	$\alpha \in KS(N)$
4891	67	73	9	70, 71, 75, 76, 79, 139
4897	59	83	9	141
5063	61	83	9	63, 143
5141	53	97	9	45, 101, 149
5183	71	73	9	59, 63, 68, 72, 74, 75, 80, 83, 143
5251	59	89	9	60, 118, 147
5293	67	79	9	68, 73, 80, 145
5429	61	89	9	59, 69, 83, 149
5561	67	83	9	149
5609	71	79	9	65, 69, 72, 74, 77, 84, 149
5723	59	97	9	155
5767	73	79	9	67, 70, 71, 75, 76, 151
5893	71	83	9	69, 73, 153
5917	61	97	9	37, 67, 77, 85, 93, 109, 157
5963	67	89	9	23, 56, 78, 111, 155
6059	73	83	9	71, 74, 75, 155
6319	71	89	9	75, 79, 82, 159
6497	73	89	9	65, 71, 77, 81, 95, 161
6499	67	97	9	64, 75, 91, 99, 163
6557	79	83	9	77, 80, 81, 161
6887	71	97	9	83, 87, 95, 167

Continued on next page

Table 5.1 – continued from previous page

N	p	q	**Category**	$\alpha \in KS(N)$
7031	79	89	9	83, 87, 90, 167
7081	73	97	9	25, 61, 79, 85, 89, 105, 121, 169
7387	83	89	9	87, 91, 171
7663	79	97	9	71, 91, 95, 103, 175
8051	83	97	9	95, 99, 179
8633	89	97	9	86, 93, 95, 101, 105, 185

a

b

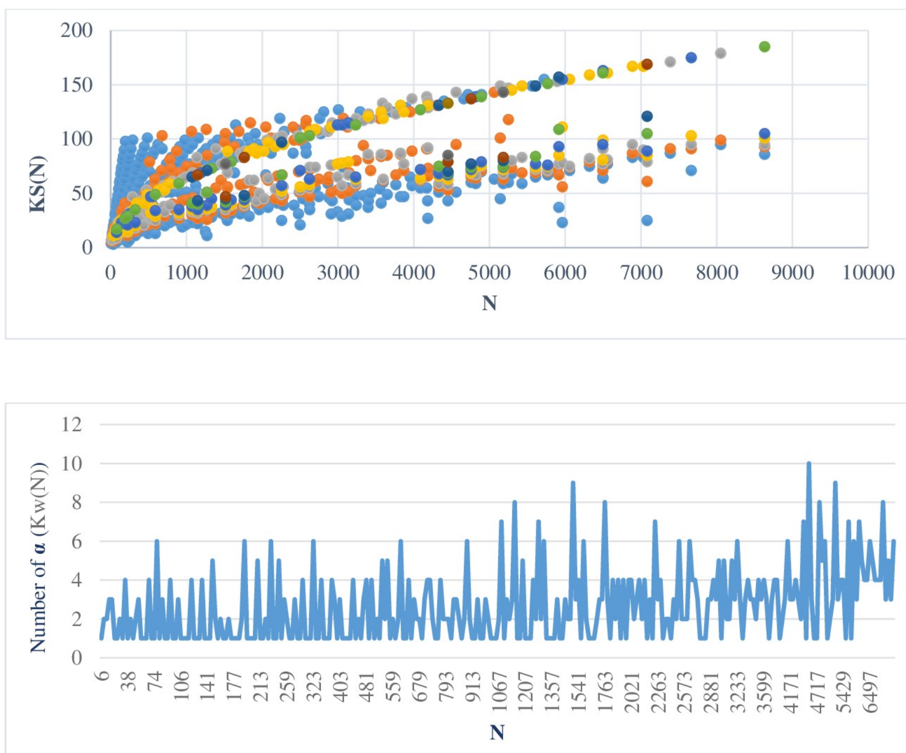

Figure 5.2: a and b are scatter and line charts in order represents relation between N, $KS(N)$ and $K_w(N)$

In the final stage, a comparison between methods for calculating the Korselt numbers is made by defining composite squarefree N from 1 to 1000 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 chapter, such that the first method needed 0.39 sec on a laptop with $i7$ processor, while the improved technique consumed 0.11 sec which is more than 3 times faster than the traditional way of calculating. This gives us the right to say the modified technique is more efficient, although the program was not fully optimized for the time being.

5.2 Observations and Remarks on Literature

Here are some notes about the literature relevant to this work.

- Theorem 1.10 in (Bouallègue et al., 2010) is divided into several parts. Section 2.4 (Finiteness K_α-Number with Exactly Two Prime Factors) was devoted to it because of it's importance and to being able to demonstrate it in a detailed way, so that the reader can easily understand it.

- Theorem 2.1 in (Al-Rasasi et al., 2013) is divided into two propositions. Section 4.2 (The Korselt Set of $6q$) was devoted to it in order to simplify it for the reader.

- Because of the algorithms that were developed in this thesis, enabled us to discover errors in the literature. Some numerical errors are observed in one of the tables in (Bouallègue et al., 2010) (page 262), and the correction of them is in Table 2.4 in this thesis.

- While solving some examples related to Theorem 14 in (Echi and Ghanmi, 2012), some mistakes are discovered. Items (4) and (6) of that theorem has some errors, so Propositions 4.1.7 and 4.1.10 are provided as well as suggested correction in order.

Conclusion

In this work, we have presented a new type of numbers which are not mentioned much in the literature, namely, Korselt numbers. Several methods to find Korselt numbers and the relation between Korselt numbers and other classes of numbers as Williams numbers and Carmichael numbers have been studied. The work developed complicated algorithms to find these numbers very efficiently and in a short time. Although these algorithms were an important addition to this thesis, still we believe this topic has a lot to improve.

References

Al-Rasasi, I., Echi, O., and Ghanmi, N. (2013). **On the korselt set of a square-free composite number**. CR Math. Rep. Acad. Sci. Canada, 35(1):1–15.

Alford, W. R., Granville, A., and Pomerance, C. (1994). **There are infinitely many carmichael numbers**. Annals of Mathematics, 139(3):703–722.

Andrews, G. E. (1994). **Number theory**. Courier Corporation.

Beeger, N. (1950). **On composite numbers n for which $a^{n-1} \equiv$ 1 (mod n) for every a prime to n.** Scripta math, 16(1950):133–135.

Bouallègue, K., Echi, O., and Pinch, R. G. (2010). **Korselt numbers and sets**. International Journal Of Number Theory, 6(02):257–269.

Carmichael, R. D. (1910). **Note on a new number theory function**. Bulletin of the American Mathematical Society, 16(5):232–238.

Crandall, R. and Pomerance, C. B. (2006). **Prime numbers: a computational perspective**, volume 182. Springer Science & Business Media.

Echi, O. (2007). **Williams numbers**. Mathematical Reports of the Academy of Sciences, 29(2):41–47.

Echi, O. and Ghanmi, N. (2012). **The korselt set of pq**. International Journal of Number Theory, 8(02):299–309.

Erdös, P. and Monthly, A. M. (1956). **On pseudoprimes and carmichael numbers**. Publ. Math. Debrecen, 4(1956):201–206.

Fletcher, C. R. (1991). **A reconstruction of the frénicle-fermat correspondence of 1640**. Historia Mathematica, 18(4):344–351.

Ghanmi, N. and Al-Rassasi, I. (2013). **On williams numbers with three prime factors**. Missouri Journal of Mathematical Sciences, 25:134–152.

Korselt, A. (1899). **Probleme chinois**. Lintermédiaire math, 6:143–143.

Languasco, Alessandro and Perelli. (2003) **Prime numbers and cryptography**,

Lehmer, D. H. (1976). **Strong carmichael numbers**. Journal of the Australian Mathematical Society, 21(4):508–510.

Nyblom, M. (2002). **Some curious sequences involving floor and ceiling functions**. The American mathematical monthly, 109(6):559–564.

Raji, W. (2013). **An introductory course in elementary number theory**. The Saylor Foundation.

Shoup, V. (2005) **A computational introduction to number theory and algebra**. Cambridge University Press.

Stein, W. (2005). **Elementary number theory**. Springer-Verlag, URL.

Weisstein, E. W. (2003). **Squarefree**. Wolfram Research, Inc.

Williams, H. C. (1977). **On numbers analogous to the carmichael numbers**. Canad. Math. Bull, 20(1):133–143.

جامعة النجاح الوطنية

كلية الدراسات العليا

دراسة لأعداد ومجموعات كورسلت بين النظريـة والتطبيق

إعداد

عبير عادل محمد اشتية

إشراف

د. خالد عداربه

د. هادي حمد

قدمت هذه الأطروحة استكمالا لمتطلبات الحصول على درجة الماجستير في الرياضيات المحوسبة بكلية الدراسات العليا، جامعة النجاح الوطنية، نابلس–فلسطين.

2020

دراسة لأعداد ومجموعات كورسلت بين النظرية والتطبيق

إعداد

عبير عادل محمد اشتية

إشراف

د.خالد عداربه

د. هادي حمد

الملخص

لقد تم مناقشة أعداد ومجموعات كورسلت لأول مرة عام 2007، حيث يمكن اعتبار المشكلة مسألة جديدة ذات مؤلفات محدودة مما يجعلها مجالاً جديداً للبحث.

ولتوضيح أعداد كورسلت نبدأ بفرض أن (N) عدد صحيح موجب و (α) عدد صحيح لا يساوي صفراً، إذا كانت $(N \neq \alpha)$ و $(p - \alpha)$ تقسم $(N - \alpha)$ بحيث أن (p) تمثل جميع العوامل الأولية لِ (N)، في هذه الحالة تسمى (N) بِ $(\alpha -$ Korselt number$)$ ويرمز لها بِ (Kα–number)، وتسمى مجموعة كل قيم (α) بحيث أن (N) هي(Kα–number) بمجموعة كورسلت التابعة لِ (N).

إن مفهوم أعداد كورسلت قد طرح لأول مرة بواسطة عثمان عشي عام 2007، وتم دراسته فيما بعد ضمن حالات مختلفة بواسطة عثمان عشي وآخرون عام 2010، 2012، ...، وتجدر الإشارة هنا إلى أن مفهوم أعداد كورسلت يعمم مفهوماً آخر يسمى بأعداد كرمايكل والذي تم تقديمه كمثال ينقض النظرية الصغيرة العكسية لفيرمات.

تساهم هذه الأطروحة في دراسة العديد من النتائج المذكورة في المؤلفات بهدف التأكد منها والعمل على تطويرها، فقد تم تدوين العديد من الملاحظات التي ساعدت في بناء خوارزميات بواسطة MATLAB التي ستثري المؤلفات بمجموعات كورسلت ذات الأعداد الكبيرة نسبياً (غير المدرجة في المؤلفات) بطريقة فعالة تستغرق وقتاً قصيراً والتي قد تتطلب وقتاً وجهداً كبيراً في حال إيجادها يدوياً أو بإستخدام النظريات التقليدية، وبالإضافة إلى عمل مقارنة لاختبار النظريات المعنية.