Hacettepe Journal of Mathematics & Statistics

Hacet. J. Math. Stat.
Volume 50 (1) (2021), 135 – 143
DOI : 10.15672/hujms.659265

Research Article

Connections on the rational Korselt set of pq

Nejib Ghanmi

Preparatory Institute of Engineering Studies of Tunis, Tunis university, Tunisia

Abstract

For a positive integer N and $\mathbb{A}$, a subset of $\mathbb{Q}$, let $\mathbb{A}$-$\mathcal{KS}(N)$ denote the set of $\alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{A}\backslash\{0, N\}$, where $\alpha_2 r - \alpha_1$ divides $\alpha_2 N - \alpha_1$ for every prime divisor r of N. The set $\mathbb{A}$-$\mathcal{KS}(N)$ is called the set of N-Korselt bases in $\mathbb{A}$. Let p, q be two distinct prime numbers. In this paper, we prove that each pq-Korselt base in $\mathbb{Z}\backslash\{q + p - 1\}$ generates at least one other in $\mathbb{Q}$-$\mathcal{KS}(pq)$. More precisely, we prove that if $(\mathbb{Q}\backslash\mathbb{Z})$-$\mathcal{KS}(pq) = \emptyset$, then $\mathbb{Z}$-$\mathcal{KS}(pq) = \{q + p - 1\}$.

Mathematics Subject Classification (2020). 11Y16, 11Y11, 11A51

Keywords. prime number, Carmichael number, squarefree composite number, Korselt base, Korselt number, Korselt set

1. Introduction

A Carmichael number [2] N is a positive composite integer that satisfies $a^N \equiv 1 \pmod N$ for any a with $\gcd(a, N) = 1$, it follows that a Carmichael number N meets Korselt's criterion:

Korselt's criterion 1.1 ([10]). A squarefree composite integer $N > 1$ is a Carmichael number if and only if $p - 1$ divides $N - 1$ for all prime factors p of N.

In [1, 3], Bouallègue-Echi-Pinch introduced the notion of an α-Korselt number, where $\alpha \in \mathbb{Z}\backslash\{0\}$, as a generalized Carmichael number when $\alpha = 1$ as follows:

Definition 1.2. An α-Korselt number is a number N such that $p - \alpha$ divides $N - \alpha$ for all prime divisors p of N.

The α-Korselt numbers for $\alpha \in \mathbb{Z}$ have been thoroughly investigated in recent years, especially in [1, 3, 4, 8, 9]. In [5], Ghanmi proposed another generalization for $\alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q}\backslash\{0\}$ by setting the following definitions:

Definition 1.3. Let $N \in \mathbb{N}\backslash\{0, 1\}$, $\alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q}\backslash\{0\}$ with $\gcd(\alpha_1, \alpha_2) = 1$ and $\mathbb{A}$ a subset of $\mathbb{Q}$. Then,

(1) N is said to be an *α-Korselt number* (*K_α-number*) if $N \neq \alpha$ and $\alpha_2 p - \alpha_1$ divides $\alpha_2 N - \alpha_1$ for every prime divisor p of N.

Email address: nejib.ghanmi@ipein.rnu.tn, neghanmi@yahoo.fr
Received: 13.12.2019; Accepted: 11.05.2020

(2) By the $\mathbb{A}$-*Korselt set* of a number N (or the Korselt set of N over $\mathbb{A}$), we mean the set $\mathbb{A}$-$\mathcal{KS}(N)$ of all $\beta \in \mathbb{A}\backslash\{0, N\}$ such that N is a K_β-number.

(3) If $\mathbb{A}$-$\mathcal{KS}(N)$ has a finite number of elements, then its cardinality is the $\mathbb{A}$-*Korselt weight* of N. Otherwise, if the cardinality is infinite, we say that N has an infinite weight over $\mathbb{A}$. The $\mathbb{A}$-*Korselt weight* of N is simply denoted by $\mathbb{A}$-$\mathcal{KW}(N)$.

Carmichael numbers are exactly the 1-Korselt squarefree composite numbers. Furthermore, in [6,7], Ghanmi defined the notion of Korselt bases as follows:

Definition 1.4. Let $N \in \mathbb{N}\backslash\{0, 1\}$, $\alpha \in \mathbb{Q}\backslash\{0\}$ and $\mathbb{B}$ be a subset of $\mathbb{N}$. Then,

(1) α is called an *N-Korselt base* (*K_N-base*) if N is a *K_α-number.*

(2) By the $\mathbb{B}$-*Korselt set* of base α (or the Korselt set of base α over $\mathbb{B}$), we mean the set $\mathbb{B}$-$\mathcal{KS}(B(\alpha))$ of all $M \in \mathbb{B}$ such that α is a K_M-base.

(3) If $\mathbb{B}$-$\mathcal{KS}(B(\alpha))$ has a finite number of elements, then its cardinality is called the $\mathbb{B}$-*Korselt weight* of base α. Otherwise, if the cardinality is infinite, we say that α has an infinite weight over $\mathbb{B}$. The $\mathbb{B}$-*Korselt weight* of base α is denoted by $\mathbb{B}$-$\mathcal{KW}(B(\alpha))$.

The set $\mathbb{Q}$-$\mathcal{KS}(N)$ is simply called the rational Korselt set of N. In this paper, we are concerned only with a squarefree composite number N.

After extending the notion of a Korselt number to $\mathbb{Q}$, and in order to study the Korselt numbers and their Korselt sets over $\mathbb{Q}$, it is natural to ask about the existence of connections between the Korselt bases of a number N over the sets $\mathbb{Z}$ and $\mathbb{Q}\backslash\mathbb{Z}$. The answer is affirmative for a squarefree composite number N with two prime factors. Indeed, when we look deeply at a list of Korselt numbers and their Korselt sets (see Table 1 and Table 2), we note the absence of any squarefree composite number N with two prime factors such that $\mathbb{Z}$-$\mathcal{KW}(N) \geq 2$ and $(\mathbb{Q}\backslash\mathbb{Z})$-$\mathcal{KS}(N) = \emptyset$. This finding inspired us to claim that such a relation between $\mathbb{Z}$-$\mathcal{KS}(N)$ and $(\mathbb{Q}\backslash\mathbb{Z})$-$\mathcal{KS}(N)$ exists. The case when N is squarefree and has more than two prime factors remains untreated. To explain this (these) connection(s), we organize our work as follows. In Section 2, we give some numerical data showing connections between the Korselt bases of N over $\mathbb{Z}$ and $(\mathbb{Q}\backslash\mathbb{Z})$. In Section 3, we prove that for each squarefree composite number N with two prime factors, some N-Korselt bases in $\mathbb{Z}$ generate others in the same set $\mathbb{Z}$-$\mathcal{KS}(N)$. Finally, in Section 4, we show that for each squarefree composite number $N = pq$ with two prime factors, each N-Korselt base in $\mathbb{Z}\backslash\{q + p - 1\}$ generates a Korselt base in $\mathbb{Q}\backslash\mathbb{Z}$.

2. Preliminaries

The following data illustrate some cases of Korselt numbers and their Korselt sets. Table 1 provides all $N = pq$ and $\mathbb{Z}$-$\mathcal{KS}(N)$ with p, q primes and $p < q \leq 53$ for which $(\mathbb{Q}\backslash\mathbb{Z})$-$\mathcal{KS}(N) = \emptyset$. Table 2 lists, for each integer $1 \leq i \leq 7$, the smallest squarefree composite number $N_i = pq$ with p, q primes, $p < q < 10^3$ such that $\mathbb{Z}$-$\mathcal{KW}(N_i) = i$ and $(\mathbb{Q}\backslash\mathbb{Z})$-$\mathcal{KW}(N_i)$ is the smallest.

N	$\mathbb{Z}$-$\mathcal{KS}(N)$	N	$\mathbb{Z}$-$\mathcal{KS}(N)$	N	$\mathbb{Z}$-$\mathcal{KS}(N)$
2×11	$\{12\}$	2×31	$\{32\}$	5×43	$\{47\}$
2×13	$\{14\}$	3×31	$\{33\}$	2×47	$\{48\}$
2×17	$\{18\}$	2×37	$\{38\}$	3×47	$\{49\}$
2×19	$\{20\}$	3×37	$\{39\}$	5×47	$\{51\}$
3×19	$\{21\}$	2×41	$\{42\}$	13×47	$\{59\}$
2×23	$\{24\}$	3×41	$\{43\}$	2×53	$\{54\}$
3×23	$\{25\}$	5×41	$\{45\}$	3×53	$\{55\}$
2×29	$\{30\}$	2×43	$\{44\}$	5×53	$\{57\}$
3×29	$\{31\}$	3×43	$\{45\}$		

Table 2. $\mathbb{Z}$-$\mathcal{KS}(N)$ where $N = pq; p, q$ primes , $p < q \leq 53$ and $(\mathbb{Q}\backslash\mathbb{Z})$-$\mathcal{KS}(N) = \emptyset$.

i	N_i	$\mathbb{Z}$-$\mathcal{KS}(N_i)$	$(\mathbb{Q}\backslash\mathbb{Z})$-$\mathcal{KW}(N_i)$
1	2×11	$\{12\}$	0
2	2×7	$\{6,8\}$	1
3	5×19	$\{15,20,23\}$	2
4	31×59	$\{29,60,62,89\}$	5
5	67×97	$\{64,75,91,99,163\}$	12
6	757×881	$\{755,773,797,845,867,1637\}$	17
7	37×61	$\{25,43,49,52,57,67,97\}$	22

Table 2. The smallest $N_i = pq$ with p, q primes, $p < q < 10^3$ such that $\mathbb{Z}$-$\mathcal{KW}(N_i) = i$ and $(\mathbb{Q}\backslash\mathbb{Z})$-$\mathcal{KW}(N_i)$ is the smallest.

Based on Table 1 and Table 2, we remark that there is no squarefree composite number N with two prime factors such that $\mathbb{Z}$-$\mathcal{KW}(N) \geq 2$ and $(\mathbb{Q}\backslash\mathbb{Z})$-$\mathcal{KS}(N) = \emptyset$. This leads to the following result:

Theorem 2.1 (**Main Theorem**)**.** *Let $N = pq$. If $(\mathbb{Q}\backslash\mathbb{Z})$-$\mathcal{KS}(N) = \emptyset$, then $\mathbb{Z}$-$\mathcal{KS}(N) = \{q+p-1\}$.*

Moreover, it appears that for numbers N that satisfy Theorem 2.1, the sets $\mathbb{Z}$-$\mathcal{KS}(N)$ and $(\mathbb{Q}\backslash\mathbb{Z})$-$\mathcal{KS}(N)$ are somewhat related. To highlight this relation, we show that each N-Korselt base in $\mathbb{Z}\backslash\{p+q-1\}$ induces at least one other N-Korselt base in $(\mathbb{Q}\backslash\mathbb{Z})$-$\mathcal{KS}(N)$. Hence, the main theorem is deduced immediately.

For the rest of this paper, let $p < q$ be two primes and let $N = pq$ and i, s be the integers given by the Euclidian division of q by p: $q = ip + s$ with $s \in \{1, \ldots, p-1\}$.

Our work is based on the following result given by Echi-Ghanmi [4].

Theorem 2.2. [4, Theorem 14] *Let $N = pq$ such that $p < q$. Then, the following properties hold:*

(1) *If $q > 2p^2$, then $\mathbb{Z}$-$\mathcal{KS}(N) = \{p+q-1\}$.*

(2) *If $p^2 - p < q < 2p^2$ and $p \geq 5$, then*

$$\mathbb{Z}\text{-}\mathcal{KS}(N) \subseteq \{ip, p+q-1\}.$$

(3) *If $4p < q < p^2 - p$, then*

$$\mathbb{Z}\text{-}\mathcal{KS}(N) \subseteq \{ip, (i+1)p, p+q-1\}.$$

(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*

$$\mathbb{Z}\text{-}\mathcal{KS}(N) = \{4p, q-p+1, p+q-1\}.$$

(*ii*) *If $p \not\equiv 1 \pmod 3$, then*

$$\mathbb{Z}\text{-}\mathcal{KS}(N) = \{q-p+1, p+q-1\}.$$

(*b*) *If $q \neq 4p-3$, then*

$$\mathbb{Z}\text{-}\mathcal{KS}(N) \subseteq \{3p, 4p, p+q-1\}.$$

(5) *If $2p < q < 3p$, then*

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

(6) *If $p < q < 2p$, then*

$$\mathbb{Z}\text{-}\mathcal{KS}(N) \subseteq \{q+p-1\} \cup [2, 2p] \setminus \{p\}.$$

Next, we establish the following two results to serve us for the rest of the paper:

Lemma 2.3. *For each $N = pq$ with $p < q$ and both being prime, the set $\mathbb{Z}\text{-}\mathcal{KS}(N)$ is characterized by Theorem 2.2, except for $(p, q) \in \{(3, 13), (3, 17)\}$, where $\mathbb{Z}\text{-}\mathcal{KS}(3 \times 13) = \{12, 15\}$ and $\mathbb{Z}\text{-}\mathcal{KS}(3 \times 17) = \{15, 19\}$.*

Proof. Let $N = pq$ with $p < q$ both being prime.

- If $p \geq 5$, then $\mathbb{Z}\text{-}\mathcal{KS}(N)$ is simply given by one of the six cases of Theorem 2.2.

- Suppose that $p = 2$. If $q < 8 = 4p$ (resp. $q > 8 = 2p^2$), then $\mathbb{Z}\text{-}\mathcal{KS}(N)$ is completely determined by one of states 4, 5, and 6 (resp. state 1) of Theorem 2.2.

- Similarly, for the case $p = 3$, if $q < 4p = 12$ (resp. $q > 2p^2 = 18$), then $\mathbb{Z}\text{-}\mathcal{KS}(N)$ is determined by one of cases 4, 5, and 6 (resp. case 1) of Theorem 2.2. Therefore, the remaining values for the prime number q are 13 and 17, where $\mathbb{Z}\text{-}\mathcal{KS}(3 \times 13) = \{12, 15\}$ and $\mathbb{Z}\text{-}\mathcal{KS}(3 \times 17) = \{15, 19\}$ (see [4, Proposition 15]). □

Proposition 2.4. [9, Corollary 3.6] *Let p and q be two prime numbers such that $p < q$ and $N = pq$. If $\alpha \in \mathbb{Z}\text{-}\mathcal{KS}(N)$, then the following statements hold:*

(1) $\gcd(\alpha, q) = 1$.

(2) $2 \leq q - p + 1 \leq \alpha \leq p + q - 1$.

(3) *If p divides α, then $\alpha \in \{ip, (i + 1)p\}$.*

3. Connections in $\mathbb{Z}\text{-}\mathcal{KS}(N)$

In the following result, we prove that certain N-Korselt bases in $\mathbb{Z}$ induce others in the same set $\mathbb{Z}\text{-}\mathcal{KS}(N)$.

Proposition 3.1. *Suppose that $2p < q < 3p$. Then, the following statements hold:*

(1) $\dfrac{2p + q - 1}{2} \in \mathbb{Z}\text{-}\mathcal{KS}(N)$ *if and only if* $q - p + 1 \in \mathbb{Z}\text{-}\mathcal{KS}(N)$.

(2) *If $3q - 5p + 3 \in \mathbb{Z}\text{-}\mathcal{KS}(N)$, then $q - p + 1 \in \mathbb{Z}\text{-}\mathcal{KS}(N)$.*

Proof. First, since $q = 2p + s$, the integer s must be odd, and therefore, $s < p - 1$.

(1) We have $\alpha = \dfrac{2p + q - 1}{2} \in \mathbb{Z}\text{-}\mathcal{KS}(N)$ if and only if

$$\begin{cases} p - \alpha = \dfrac{-q + 1}{2} & \mid \quad p(q - 1) \\ q - \alpha = \dfrac{s + 1}{2} & \mid \quad q(p - 1) \end{cases}$$

which is equivalent to $s + 1$ divides $2q(p - 1)$.

However, we have $\gcd(q, s + 1) = 1$ (as $s < p - 1 < q - 1$) and $2(p - 1) = q - 1 - (s + 1)$. Therefore, we conclude that

$$\frac{2p + q - 1}{2} \in \mathbb{Z}\text{-}\mathcal{KS}(N) \quad \text{if and only if} \quad s + 1 \mid q - 1. \tag{3.1}$$

Similarly, $\beta = q - p + 1 \in \mathbb{Z}\text{-}\mathcal{KS}(N)$ is equivalent to

$$\begin{cases} p - \beta = -s - 1 & \mid \quad p(q - 1) \\ q - \beta = p - 1 & \mid \quad q(p - 1) \end{cases}$$

which is equivalent to $s + 1$ divides $p(q - 1)$.

However, we know that $\gcd(p, s + 1) = 1$ since $s < p - 1$, which shows that

$$q - p + 1 \in \mathbb{Z}\text{-}\mathcal{KS}(N) \quad \text{if and only if} \quad s + 1 \mid q - 1. \tag{3.2}$$

Therefore, by (3.1) and (3.2), we conclude that

$$\frac{2p + q - 1}{2} \in \mathbb{Z}\text{-}\mathcal{KS}(N) \quad \text{if and only if} \quad q - p + 1 \in \mathbb{Z}\text{-}\mathcal{KS}(N).$$

(2) Suppose that $\gamma = 3q - 5p + 3 \in \mathbb{Z}\text{-}\mathcal{KS}(N)$. Then,

$$p - \gamma = 6p - 3q - 3 = -3(s+1) \mid p(q-1). \tag{3.3}$$

We consider two cases:

• If $p \neq 3$, then since $s < p - 1$, we have $\gcd(p, 3(s+1)) = 1$. Hence, by (3.3), $3(s+1)$ divides $q - 1$. Thus, by (3.2), $q - p + 1 \in \mathbb{Z}\text{-}\mathcal{KS}(N)$.

• Now, assume that $p = 3$. First, because $1 \leq s \leq p - 2 = 1$, we know that $s = 1$, $q = 2p + s = 7$ and $q - p + 1 = 5$. Therefore, we can easily check that $N = 3 \times 7 = 21$ is a 5-Korselt number. □

Corollary 3.2. *If $q > 2p$ and $q - p + 1 \notin \mathbb{Z}\text{-}\mathcal{KS}(N)$, then*

$$\mathbb{Z}\text{-}\mathcal{KS}(N) \subseteq \{ip, (i+1)p, p+q-1\}.$$

Proof. By Theorem 2.2 and Lemma 2.3, the solution is straightforward when $q > 3p$.

Now, suppose that $2p < q < 3p$ (i.e., $i = 2$). Let $\beta \in \mathbb{Z}\text{-}\mathcal{KS}(N)$. Then, again by Theorem 2.2, we obtain

$$\beta \in \left\{2p, 3p, 3q - 5p + 3, \frac{2p+q-1}{2}, q - p + 1, p + q - 1\right\}.$$

However, since $q - p + 1 \notin \mathbb{Z}\text{-}\mathcal{KS}(N)$, using Proposition 3.1, we obtain $\beta \neq 3q - 5p + 3, \frac{2p+q-1}{2}$. Thus, $\beta \in \{2p, 3p, p + q - 1\}$, as desired. □

4. Connections between $\mathbb{Z}\text{-}\mathcal{KS}(N)$ and $(\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N)$

The following result concerns the case when $q < 2p$.

Proposition 4.1. *Suppose that $q < 2p$ and $\beta \in \mathbb{Z}\backslash\{0\}$ with $\beta \neq p+q-1$ and $\gcd(p, \beta) = \gcd(pq, p+q-\beta) = 1$. Then, $\beta \in \mathbb{Z}\text{-}\mathcal{KS}(N)$ if and only if $\frac{qp}{p+q-\beta} \in (\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N)$.*

Proof. Since $\gcd(p, \beta) = \gcd(pq, p+q-\beta) = 1$, we have

$$\begin{aligned}
\beta \in \mathbb{Z}\text{-}\mathcal{KS}(N) \quad &\Leftrightarrow \quad \begin{cases} p - \beta & \mid \quad q - 1 \\ q - \beta & \mid \quad p - 1 \end{cases} \\
&\Leftrightarrow \quad \begin{cases} (p+q-\beta)p - pq = (p-\beta)p & \mid \quad p(q-1) \\ (p+q-\beta)q - pq = (q-\beta)q & \mid \quad q(p-1) \end{cases} \\
&\Leftrightarrow \quad \frac{qp}{p+q-\beta} \in \mathbb{Q}\text{-}\mathcal{KS}(N).
\end{aligned}$$

Because $\beta \notin \{p, q\}$, $p+q-\beta \notin \{p, q\}$. Moreover, if $\beta \in \mathbb{Z}\text{-}\mathcal{KS}(N)$, then since $p < q < 2p$, we have $2 \leq \beta < 2p$ by Theorem 2.2; hence, $p+q-\beta \geq 2p-\beta+1 \geq 2$, that is, $p+q-\beta \neq 1$. Therefore, $\frac{qp}{p+q-\beta} \notin \mathbb{Z}$, and we conclude that $\frac{qp}{p+q-\beta} \in (\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N)$. □

The next two results concern the case when p divides β.

Proposition 4.2. *If $ip \in \mathbb{Z}\text{-}\mathcal{KS}(N)$, then there exists $k_1 \in \mathbb{N}\backslash\{0, 1\}$ such that $\frac{(k_1+1)q}{ik_1+1} \in (\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N)$.*

Proof. Let $ip \in \mathbb{Z}\text{-}\mathcal{KS}(N)$. Then,

$$\begin{cases} p - ip & \mid \quad pq - ip = p(q-1) + p - ip \\ q - ip & \mid \quad pq - ip = q(p-1) + q - ip. \end{cases}$$

As $\gcd(s,q)=1$, this is equivalent to

$$\begin{cases} i-1 & | & q-1 \\ s & | & p-1 \end{cases}$$

and hence, there exist k_1 and k_2 in $\mathbb{Z}$ such that

$$\begin{cases} q-1 & = & k_2(i-1) \\ p-1 & = & k_1 s. \end{cases}$$

As $q=ip+s$, $k_1q=ik_1p+k_1s=ik_1p+p-1$, and therefore,

$$(k_1+1)q-(ik_1+1)p=q-1. \tag{4.1}$$

Let $k=\gcd(k_1+1,ik_1+1)$, $\alpha_1^{'}=\dfrac{k_1+1}{k}$ and $\alpha_2=\dfrac{ik_1+1}{k}$. Therefore, using (4.1), we obtain

$$\alpha_1^{'}q-\alpha_2p=\frac{q-1}{k}. \tag{4.2}$$

Now, let us prove that $\alpha_2-\alpha_1^{'}$ divides $p-1$. First, note that

$$\alpha_2-\alpha_1^{'}=\frac{k_1}{k}(i-1). \tag{4.3}$$

Since $q-1=(i-1)p+(k_1+1)s$ and $i-1\mid q-1$, we deduce that $i-1\mid(k_1+1)s$. Furthermore, because $\gcd(k_1+1,i-1)=\gcd(k_1+1,ik_1+1)=k$, it follows that $m=\dfrac{i-1}{k}\mid\dfrac{k_1+1}{k}s$. However, $\gcd\left(\dfrac{k_1+1}{k},\dfrac{i-1}{k}\right)=1$; hence, $m\mid s$. Therefore, we conclude by (4.3) that

$$\alpha_2-\alpha_1^{'}=k_1m\mid k_1s=p-1. \tag{4.4}$$

Now, by (4.2) and (4.4), we obtain

$$\begin{cases} \alpha_2p-\alpha_1^{'}q & | & q-1 \\ \alpha_2-\alpha_1^{'} & | & p-1. \end{cases}$$

Thus,

$$\alpha=\frac{\alpha_1^{'}q}{\alpha_2}=\frac{(k_1+1)q}{ik_1+1}\in\mathbb{Q}\text{-}\mathcal{KS}(N).$$

As $\gcd(\alpha_1^{'},\alpha_2)=1$, $\gcd(q,\alpha_2)=1$ by (4.2) and $\alpha_2\neq1$, we conclude that $\dfrac{(k_1+1)q}{ik_1+1}\in(\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N)$. ☐

In the following result, we need $(i+1)p\neq q+p-1$ (i.e., $s>1$) to show that $(i+1)p$ generates an element in $\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N)$.

Proposition 4.3. *If $(i+1)p\in\mathbb{Z}\text{-}\mathcal{KS}(N)$ and $s>1$, then there exists $k_1\in\mathbb{N}\backslash\{0,1\}$ such that $\dfrac{(k_1-1)q}{(i+1)k_1-1}\in(\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N)$.*

Proof. If $(i+1)p\in\mathbb{Z}\text{-}\mathcal{KS}(N)$, then

$$\begin{cases} p-(i+1)p & | & pq-(i+1)p=p(q-1)+p-(i+1)p \\ q-(i+1)p & | & pq-(i+1)p=q(p-1)+q-(i+1)p. \end{cases}$$

This is equivalent to

$$\begin{cases} i & | & q-1 \\ p-s & | & p-1 \end{cases}$$

and hence, there exist k_1 and k_2 in $\mathbb{N}\backslash\{0\}$ such that

$$\begin{cases} q-1 & = & k_2i \\ p-1 & = & k_1(p-s). \end{cases}$$

First, as $s > 1$, it follows that $k_1 > 1$. Since $q = (i+1)p+s-p$, $k_1 q = (i+1)k_1 p - p + 1$. Therefore, we can write

$$((i+1)k_1 - 1)p - (k_1 - 1)q = q - 1. \tag{4.5}$$

Let $k = \gcd(k_1 - 1, (i+1)k_1 - 1)$, $\alpha_1^{'} = \dfrac{k_1 - 1}{k}$ and $\alpha_2 = \dfrac{(i+1)k_1 - 1}{k}$.

Then, we use (4.5) to obtain

$$\alpha_2 p - \alpha_1^{'} q = \frac{q-1}{k}. \tag{4.6}$$

Next, let us prove that $\alpha_2 - \alpha_1^{'} \mid p - 1$. First, we have

$$\alpha_2 - \alpha_1^{'} = \frac{ik_1}{k}. \tag{4.7}$$

Since $i \mid q - 1 = ip + s - 1$, we know that $i \mid s - 1 = (k_1 - 1)(p - s)$. Moreover, as $\gcd(k_1 - 1, i) = \gcd(k_1 - 1, (i+1)k_1 - 1) = k$, it follows that $m = \dfrac{i}{k} \mid \dfrac{k_1 - 1}{k}(p - s)$. Hence, $m \mid p - s$ since $\gcd\left(\dfrac{k_1 - 1}{k}, \dfrac{i}{k}\right) = 1$. Therefore, we deduce by (4.7) that

$$\alpha_2 - \alpha_1^{'} = k_1 m \mid k_1(p - s) = p - 1. \tag{4.8}$$

Now, by (4.6) and (4.8), we obtain

$$\begin{cases} \alpha_2 p - \alpha_1^{'} q & \mid \quad q - 1 \\ \alpha_2 - \alpha_1^{'} & \mid \quad p - 1. \end{cases}$$

Therefore,

$$\alpha = \frac{\alpha_1^{'} q}{\alpha_2} = \frac{(k_1 - 1)q}{(i+1)k_1 - 1} \in \mathbb{Q}\text{-}\mathcal{KS}(N).$$

As $\gcd(\alpha_1^{'}, \alpha_2) = 1$, $\gcd(q, \alpha_2) = 1$ by (4.6) and $\alpha_2 \neq 1$, we deduce that $\dfrac{(k_1 - 1)q}{(i+1)k_1 - 1} \in (\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N)$. □

Now, it remains to prove that each N-Korselt base $\beta \in \mathbb{Z}$ generates an N-Korselt base in $(\mathbb{Q}\backslash\mathbb{Z})$, where $\gcd(\beta, p) = 1$, $2p < q < 4p$ and $\beta \neq q + p - 1$. This is equivalent to discuss only the cases when $\beta \in \{3q - 5p + 3, \dfrac{2p + q - 1}{2}, q - p + 1\}$. It follows by Corollary 3.2 that we can restrain our work only for $\beta = q - p + 1$ with $\gcd(q + 1, p) = \gcd(\beta, p) = 1$.

Proposition 4.4. *Suppose that* $2p < q < 4p$ *with* $\gcd(q+1, p) = 1$. *If* $q - p + 1 \in \mathbb{Z}\text{-}\mathcal{KS}(N)$, *then* $\dfrac{pq}{2p - 1} \in (\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N)$.

Proof. First, if $i = 3$, then by Theorem 2.2, we must have $q = 4p - 3$, and it is easy to verify that $\dfrac{pq}{2p - 1}$ is an N-Korselt base. Furthermore, since $\gcd(pq, 2p - 1) = 1$ and $2p - 1 \neq 1$, we know that $\dfrac{pq}{2p - 1} \notin \mathbb{Z}$. Therefore, we conclude that $\dfrac{pq}{2p - 1} \in (\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N)$.

Next, assume that $q = 2p + s$. Then, s is odd, so $s \neq p - 1$. If $q - p + 1 \in \mathbb{Z}\text{-}\mathcal{KS}(N)$, then $s + 1 \mid p(q - 1)$. However, we know that $\gcd(p, s + 1) = 1$ because $s < p - 1$, which implies that $s + 1 \mid q - 1$. Hence, by taking $\alpha_1^{''} = 1$ and $\alpha_2 = 2p - 1$, we show that $\alpha_2 p - \alpha_1^{''} pq = -p(s + 1) \mid p(q - 1)$. Thus, as $\alpha_2 q - \alpha_1^{''} pq = q(p - 1)$, we can write

$$\begin{cases} \alpha_2 p - \alpha_1^{''} pq & \mid \quad p(q - 1) \\ \alpha_2 q - \alpha_1^{''} pq & \mid \quad q(p - 1). \end{cases}$$

This implies that $\dfrac{pq}{2p - 1}$ is an N-Korselt base.

Now, as $\gcd(pq, 2p-1) = \gcd(q, q-1-s) = \gcd(q, s+1) = 1$ and $2p-1 \neq 1$, we deduce that $\dfrac{pq}{2p-1} \notin \mathbb{Z}$. Thus, $\dfrac{pq}{2p-1} \in (\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N)$. □

Example 4.5. Let $N = 2 \times 7$. Then, $\mathbb{Z}\text{-}\mathcal{KS}(N) = \{6, 8\}$ and $(\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N) = \left\{\dfrac{7}{2}\right\}$ is exactly the set generated by $\mathbb{Z}\text{-}\mathcal{KS}(N)$. However, for $N = 3 \times 7$, we have $\mathbb{Z}\text{-}\mathcal{KS}(N) = \{5, 6, 9\}$ and $(\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N) = \left\{\dfrac{7}{2}, \dfrac{7}{3}, \dfrac{21}{5}, \dfrac{21}{4}, \dfrac{15}{2}, \dfrac{33}{5}\right\}$, which is composed of more than the N-Korselt bases in $(\mathbb{Q}\backslash\mathbb{Z})$ generated by $\mathbb{Z}\text{-}\mathcal{KS}(N)$.

Proof of the Main Theorem. Let $N = pq$, where $p < q$ are two prime numbers such that $(\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N) = \emptyset$. Assume by contradiction that there exists $\beta \neq q + p - 1$ in $\mathbb{Z}\text{-}\mathcal{KS}(N)$. By Propositions 4.2 and 4.3, we know that $\beta \neq ip$ and $\beta \neq (i+1)p$, respectively. It follows that $\gcd(p, \beta) = \gcd(q, \beta) = 1$ by Proposition 2.4 and $q < 4p$ by Theorem 2.2.

Suppose that $q > 2p$. Then, by Corollary 3.2, we should have $\beta = q - p + 1$, and by Proposition 4.4, $\gcd(q + 1, p) \neq 1$. However, since in our case, $2p < q = ip + s < 4p$ and q is prime, this forces $q = 4p - 1$, and therefore, $\beta = q - p + 1 = 3p$, which contradicts $\gcd(p, \beta) = 1$.

Next, assume that $q < 2p$. Then, by Proposition 4.1, $\gcd(pq, p + q - \beta) \neq 1$; otherwise, β generates an element in $(\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N) = \emptyset$, which is impossible. This result implies that either p or q divides $p + q - \beta$, and one of the following holds:

- If p divides $p + q - \beta$, then since $1 \leq p + q - \beta \leq 2p - 1$ by Proposition 2.4, we obtain $p = p + q - \beta$. Therefore, $\beta = q$, which is impossible.
- If q divides $p + q - \beta$, then as $1 \leq p + q - \beta \leq 2p - 1 < 2q$ by Proposition 2.4, we obtain $q = p + q - \beta$. Hence, $\beta = p$, which is also impossible.

Thus, all cases lead to absurdity. Therefore, we conclude that $\beta = q + p - 1$ and $\mathbb{Z}\text{-}\mathcal{KS}(N) = \{q + p - 1\}$. □

Remark 4.6. The converse of the main theorem is not true. For instance, if $N = 6 = 2\times 3$, then

$$\mathbb{Q}\text{-}\mathcal{KS}(N) = \left\{4, \frac{3}{2}, \frac{10}{3}, \frac{14}{5}, \frac{8}{3}, \frac{5}{2}, \frac{18}{7}, \frac{12}{5}, \frac{9}{4}\right\}.$$

This study motivates us to begin a deeper investigation of the rational Korselt set of a number N with more than two prime factors. We believe that the study of a possible relation or relations between $(\mathbb{Q}\backslash\mathbb{Z})\text{-}\mathcal{KS}(N)$ and $\mathbb{Z}\text{-}\mathcal{KS}(N)$ can simplify this task, but not enough. The simple case when $N = pq$ is still full of unsolved problems. For instance, after examining the Korselt sets over $\mathbb{Q}$ of some values of $N = pq$, since $\mathbb{Q}\text{-}\mathcal{KW}(N)$ is finite (see [5, Theorem 2.3]), we state the following conjecture:

Conjecture 4.7. *For all $N = pq$, $\mathbb{Q}\text{-}\mathcal{KW}(N)$ is odd.*

Acknowledgment. I am grateful to the referee for his comments which have led to improvements in the paper.

References

[1] K. Bouallegue, O. Echi and R. Pinch, *Korselt Numbers and Sets*, Int. J. Number Theory, **6**, 257–269, 2010.

[2] R.D. Carmichael, *On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$*, Amer. Math. Monthly, **19**, 22–27, 1912.

[3] O. Echi, *Williams Numbers*, C. R. Math. Acad. Sci. Soc. R. Can. **29**, 41–47, 2007.

[4] O. Echi and N. Ghanmi, *The Korselt Set of pq*, Int. J. Number Theory, **8** (2), 299–309, 2012.

[5] N. Ghanmi, $\mathbb{Q}$-*Korselt Numbers*, Turkish J. Math. **42**, 2752–2762, 2018.

[6] N. Ghanmi, *Rationel Korselt Bases of Prime Powers*, Stu. Sci. Math. Hungarica, 56 (4), 388-403 2019.
[7] N. Ghanmi, *The* $\mathbb{Q}$*-Korselt Set of* pq, Period. Math. Hungarica, **81**, 174–193, 2020.
[8] N.Ghanmi and I. Al-Rassasi, *On Williams Numbers With Three Prime Factors*, Missouri J. Math. Sci. **25** (2), 134–152, 2013.
[9] N. Ghanmi, O. Echi and I. Al-Rassasi, *The Korselt Set of a Squarefree Composite Number*, C. R. Math. Rep. Acad. Sci. Canada, **35** (1), 1–15, 2013.
[10] A. Korselt, *Problème chinois*, Interméd. Math. **6**, 142–143, 1899.