Korselt Rational Bases of Prime Powers
Nejib Ghanmi

To cite this version:
Nejib Ghanmi. Korselt Rational Bases of Prime Powers. 2018. hal-01884182

HAL Id: hal-01884182
https://hal.archives-ouvertes.fr/hal-01884182
Preprint submitted on 30 Sep 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
KORSELT RATIONAL BASES OF PRIME POWERS

NEJIB GHANMI

Abstract. Let $N$ be a positive integer, $A$ be a subset of $\mathbb{Q}$ and $\alpha = \frac{\alpha_1}{\alpha_2} \in A \setminus \{0, N\}$. $N$ is called an $\alpha$-Korselt number (equivalently $\alpha$ is said an $N$-Korselt base) if $\alpha_2 p - \alpha_1$ divides $\alpha_2 N - \alpha_1$ for every prime divisor $p$ of $N$. By the Korselt set of $N$ over $A$, we mean the set $A$-KS($N$) of all $\alpha \in A \setminus \{0, N\}$ such that $N$ is an $\alpha$-Korselt number.

In this paper we determine explicitly for a given prime number $q$ and an integer $l \in \mathbb{N} \setminus \{0, 1\}$, the set $\mathbb{Q}$-KS($q^l$) and we establish some connections between the $q^l$-Korselt bases in $\mathbb{Q}$ and others in $\mathbb{Z}$. The case of $A = \mathbb{Q} \cap [-1, 1]$ is studied where we prove that $(\mathbb{Q} \cap [-1, 1]$)-KS($q^l$) is empty if and only if $l = 2$.

Moreover, we show that each nonzero rational $\alpha$ is an $N$-Korselt base for infinitely many numbers $N = q^l$ where $q$ is a prime number and $l \in \mathbb{N}$.

1. Introduction

By extending the Korselt criterion, Bouallegue-Echi-Pinch [3, 7] stated the notion of Korselt numbers and gave rise to a new kind of generalized Carmichael numbers. As known, Carmichael numbers [5, 8] are squarefree composite numbers $N$ verifying $a^{N−1} \equiv 1 \pmod{N}$ for each integer $a$ with gcd($a, N) = 1$. These numbers are characterized by Korselt as follows:

Korselt’s criterion (1899) [9]: A composite integer $N > 1$ is carmichael if and only if $N$ is squarefree and $p − 1$ divides $N − 1$ for all prime factors $p$ of $N$.

In 1910, Carmichael [6] found $561 = 3.11.17$ as the first and smallest number verifying the Korselt criterion, this explains the name "Carmichael numbers". Although, Korselt was the first who state the basic properties of Carmichael numbers, he could not find any example; if he had just done a few computation, then surely “Carmichael numbers” would have been known as "Korselt numbers".

In honor to Korselt, Bouallegue-Echi-Pinch [3, 7] introduced the concept of $\alpha$-Korselt numbers with $\alpha \in \mathbb{Z}$, where the Carmichael numbers are exactly the squarefree composite 1-Korselt numbers.

Ghanmi [4] introduced the notion of $\mathbb{Q}$-Korselt numbers as extension of Korselt numbers to $\mathbb{Q}$ by setting the following definitions:

2010 Mathematics Subject Classification. Primary 11Y16; Secondary 11Y11, 11A51.

Key words and phrases. Prime number, Carmichael number, Square free composite number, Korselt base, Korselt number, Korselt set.
Definition 1.1. Let \( N \in \mathbb{N} \setminus \{0, 1\}, \alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q} \setminus \{0\} \) with \( A \) a subset of \( \mathbb{Q} \). Then

1. \( N \) is said to be an \( \alpha \)-Korselt number (\( K_\alpha \)-number, for short), if \( N \neq \alpha \) and \( \alpha_2 p - \alpha_1 \) divides \( \alpha_2 N - \alpha_1 \) for every prime divisor \( p \) of \( N \).
2. By the \( A \)-Korselt set of the number \( N \) (or the Korselt set of \( N \) over \( A \)), we mean the set \( A-KS(N) \) of all \( \beta \in A \setminus \{0, N\} \) such that \( N \) is a \( K_\beta \)-number.
3. The cardinality of \( A-KS(N) \) will be called the \( A \)-Korselt weight of \( N \) (or the Korselt weight of \( N \) over \( A \)); we denote it by \( A-KW(N) \).

In this paper we will concentrate on the study of the rational numbers \( \alpha \in \mathbb{Q} \setminus \{0\} \) for which a given number \( N \) is an \( \alpha \)-Korselt number, for this we state the following definition.

Definition 1.2. Let \( N \in \mathbb{N} \setminus \{0, 1\}, \alpha \in \mathbb{Q} \setminus \{0\} \) and \( B \) be a subset of \( \mathbb{N} \). Then

1. \( \alpha \) is called \( N \)-Korselt base (\( K_N \)-base, for short) if \( N \) is a \( K_\alpha \)-number.
2. By the \( B \)-Korselt set of the base \( \alpha \) (or the Korselt set of the base \( \alpha \) over \( B \)), we mean the set \( B-KS(B(\alpha)) \) of all \( M \in B \) such that \( \alpha \) is a \( K_M \)-base.
3. The cardinality of \( B-KS(B(\alpha)) \) will be called the \( B \)-Korselt weight of the base \( \alpha \) (or the Korselt weight of the base \( \alpha \) over \( B \)); we denote it by \( B-KW(B(\alpha)) \).

For more convenience, the set \( \bigcup_{\alpha \in \mathbb{Q}} (B-KS(B(\alpha))) \) is simply called the set of \( \mathbb{Q} \)-Korselt numbers or the set of rational Korselt numbers or the set of Korselt numbers over \( \mathbb{Q} \). Also, the set \( \bigcup_{N \in \mathbb{N}} (\mathbb{Q}-KS(N)) \) is called the set of Korselt rational bases or the set of \( \mathbb{N} \)-Korselt bases in \( \mathbb{Q} \) or the set of Korselt rational bases over \( \mathbb{N} \).

Since their creation, Korselt numbers are well investigated specially in \([1, 2, 3, 4, 7]\), where the majority of cases except in \([1]\), the authors restrict their studies on the case of squarefree composite numbers. In this paper we focus our study on the prime power Korselt numbers, where we manage to determine explicitly the Korselt set and the Korselt weight of a prime power number over \( \mathbb{Q} \). Therefore many properties of prime power Korselt number over \( \mathbb{Z} \) immediately follows.

We organize this work as follows. In section 1 we recall some useful properties of the \( q^l \)-Korselt rational bases. The \( q^l \)-Korselt set over the sets \( \mathbb{Q} \) and \( \mathbb{Z} \) are determined explicitly in section 2. Hence, we simply deduce each of the weights \( \mathbb{Q}-KW(q^l) \) and \( \mathbb{Z}-KW(q^l) \). Moreover, we establish some relations between the \( q^l \)-Korselt bases in \( \mathbb{Z} \) and others in \( \mathbb{Q} \). In section 3, we prove that each nonzero rational \( \alpha \) is a \( K_N \)-base for infinitely many prime powers \( N \). Finally, the section 4 is devoted to study the \( q^l \)-Korselt rational
bases in $[-1,1]$, where we present a necessary and sufficient condition for a given $\alpha \in \mathbb{Q} \cap [-1,1]$ to be a $q^l$-Korselt rational base. This leads to conclude that for each prime number $q$, the $q^2$-Korselt set over $\mathbb{Q} \cap [-1,1]$ is empty.

Throughout this paper we assume that $l \geq 2$ and for $\alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q}$, we will suppose without loss of generality that $\alpha_2 > 0$, $\alpha_1 \in \mathbb{Z}$ and $\gcd(\alpha_1, \alpha_2) = 1$.

2. Properties of $q^l$-Korselt rational bases

Proposition 2.1. Let $q$ be a prime number, $\alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q} \setminus \{0\}$ and $l \in \mathbb{N} \setminus \{0\}$.

(1) If $\gcd(\alpha_1, q) = 1$, then

\[ \alpha \in \mathbb{Q} \text{-} KS(q^l) \text{ if and only if } (\alpha_2 q - \alpha_1) | (q^l - 1). \]

(2) If $\alpha_1 = \alpha' q$, then

\[ \alpha \in \mathbb{Q} \text{-} KS(q^l) \text{ if and only if } (\alpha_2 - \alpha'_1) | (q^l - 1). \]

Proof. We have $\alpha \in \mathbb{Q} \text{-} KS(q^l)$ if and only if $(\alpha_2 q - \alpha_1) = \alpha_2 q(q^l - 1) + \alpha_2 q - \alpha_1$. As $\gcd(\alpha_2 q - \alpha_1, \alpha_2) = 1$, it follows that

\[ \alpha \in \mathbb{Q} \text{-} KS(q^l) \iff \alpha_2 q - \alpha_1 | q(q^l - 1) \]  \hspace{1cm} (2.1)

Hence, if $\gcd(\alpha_1, q) = 1$ then (2.1) gives

\[ \alpha \in \mathbb{Q} \text{-} KS(q^l) \iff (\alpha_2 q - \alpha_1) | (q^l - 1), \]

and if $\alpha_1 = \alpha' q$, then by (2.1) we get

\[ \alpha \in \mathbb{Q} \text{-} KS(q^l) \iff (\alpha_2 - \alpha'_1) | (q^l - 1). \]

□

The following result is an immediate consequence of Definition 1.1.

Corollary 2.2. Let $q$ be a prime number, $l \in \mathbb{N} \setminus \{0\}$ and $\frac{\alpha'_1 q}{\alpha_2} \in \mathbb{Q} \setminus \{0\}$ with $\gcd(\alpha'_1 q, \alpha_2) = 1$. Then, $\frac{\alpha'_1 q}{\alpha_2} \in \mathbb{Q} \text{-} KS(q^l)$ if and only if $\frac{\alpha_2 q}{\alpha_1} \in \mathbb{Q} \text{-} KS(q^l)$.

By the next two results, we give information about $\mathbb{Q} \text{-} KS(q^l)$.

Proposition 2.3. Let $\alpha \in \mathbb{Q} \text{-} KS(q^l)$. If $\alpha = \alpha' q$, then

\[ 2 - q^l \leq \alpha' \leq \frac{q^{l-1} + 1}{2}. \]

Proof. Let $N = q^l$ and $\alpha = \frac{\alpha_1}{\alpha_2} = \alpha' q \in \mathbb{Q} \text{-} KS(q^l)$ with $\gcd(\alpha_2, \alpha_1) = 1$. 


Proposition 2.4. Assume that \( \alpha' > 0 \). First, we show by contradiction that \( \alpha' < q^l-1 \). If \( \alpha' \geq q^l-1 \), then \( \alpha_1 - \alpha_2 N = \alpha_2 q (\alpha' - q^l-1) \geq 0 \), hence \( \alpha_1 - \alpha_2 N \geq \alpha_1 - \alpha_2 N \). But as \( \alpha_1 - \alpha_2 q \) divides \( \alpha_1 - \alpha_2 N \), it follows that \( \alpha_1 - \alpha_2 N = 0 \), and so \( \alpha = N \) which is impossible. Thus, \( \alpha' < q^l-1 \).

Now, let us show that \( \alpha' \leq \frac{q^l-1 + 1}{2} \). We can suppose that \( \alpha' > 1 \) (otherwise \( \alpha' \leq 1 \) and so the result is immediate).

Since \( \alpha_2 N - \alpha_1 = k(\alpha_2 q - \alpha_1) \) with \( k \in \mathbb{Z} \setminus \{0\} \), it follows by dividing both sides by \( \alpha_2 q \), that \( q^l-1 - \alpha' = k(1 - \alpha') \). As \( \alpha' > 1 \), it yields that \( \alpha' - 1 = |1 - \alpha'| \leq |q^l-1 - \alpha'| = q^l-1 - \alpha' \), and so \( \alpha' \leq \frac{q^l-1 + 1}{2} \).

Case 2: Now, suppose that \( \alpha' < 0 \) (i.e. \( \alpha_1 < 0 \)). Since \( \alpha_2 N - \alpha_1 = k(\alpha_2 q - \alpha_1) \) with \( k \in \mathbb{N} \), we claim that \( k \geq 2 \), otherwise \( l = 1 \) which is impossible. So, \( N - \alpha = k(q - \alpha) \geq 2(q - \alpha) \), which implies that \( 2q - N \leq \alpha \). Thus, \( 2 - q^l-1 \leq \alpha' \).

\[\square\]

Proposition 2.4. Assume that \( \alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q} \cdot KS(q^l) \) with \( \gcd(\alpha_1, q) = 1 \). Then
\[1 + q - q^l-1 \leq \alpha \leq q^l-1 + q - 1.\]

Proof. Let \( N = q^l \) and \( \alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q} \cdot KS(N) \). Then, by Proposition 2.1(1) we have \( \alpha_2 q - \alpha_1 \mid q^l-1 - 1 \), hence \( 1 - q^l-1 \leq \alpha_2 q - \alpha_1 \leq q^l-1 - 1 \). Since \( \alpha_2 \geq 1 \), this implies that
\[1 - q^l-1 \leq \frac{1 - q^l-1}{\alpha_2} \leq q - \alpha \leq \frac{q^l-1 - 1}{\alpha_2} \leq q^l-1 - 1.\]

Thus,
\[1 + q - q^l-1 \leq \alpha \leq q^l-1 + q - 1.\]

\[\square\]

The following two examples show that in Propositions 2.3 and 2.4 the upper and lower bounds are attained (except in Proposition 2.3 where only the upper bound is attained for \( N = 2^2 \)).

Examples 2.5. (1) Let \( \alpha = \frac{q^l + q}{2} \). Then \( q^l - \alpha = \frac{q^l - q}{2} = -(q - \alpha) \), therefore \( \alpha \) is a \( q^l \)-Korselt base.

Now, by taking \( \beta = 2q - q^l \), we get \( q^l - \beta = 2(q^l - q) = 2(q - \beta) \). Thus \( \beta \) is a \( q^l \)-Korselt base.

(2) Let \( \alpha = \frac{q^l-1 + q - 1}{2} \). Then \( q^l - \alpha = (1 - q)(1 - q^l-1) = (1 - q)(q - \alpha) \), hence \( \alpha \) is a \( q^l \)-Korselt base.

If \( \beta = 1 + q - q^l-1 \), then \( q^l - \beta = (q + 1)(q^l-1 - 1) = (q + 1)(q - \beta) \). Hence \( \beta \) is a \( q^l \)-Korselt base.
The following result gives relations between the Korselt sets of two powers of the same prime number as an immediate consequence of Definition 1.1.

**Proposition 2.6.** Let \( l, k \in \mathbb{N} \setminus \{0, 1\} \), \( q \) be a prime number and \( \mathcal{A} \) be a subset of \( \mathbb{Q} \). Then

1. \( \mathcal{A} \cdot \mathcal{KS}(q^2) \subseteq \mathcal{A} \cdot \mathcal{KS}(q^l) \).
2. In general, if \( (k - 1) \mid (l - 1) \) then \( \mathcal{A} \cdot \mathcal{KS}(q^k) \subseteq \mathcal{A} \cdot \mathcal{KS}(q^l) \).

This result can be generalized as follows.

**Proposition 2.7.** Let \( l, k \in \mathbb{N} \setminus \{0, 1\} \), \( q \) be a prime number and \( \mathcal{A} \) be a subset of \( \mathbb{Q} \). Then the following hold.

1. If \( \gcd(l - 1, k - 1) = m - 1 \), then
   \[
   \mathcal{A} \cdot \mathcal{KS}(q^l) \cap \mathcal{A} \cdot \mathcal{KS}(q^k) = \mathcal{A} \cdot \mathcal{KS}(q^m).
   \]
2. If \( 1 \in \mathcal{A} \) then
   \[
   \bigcap_{t \in \mathbb{N} \setminus \{0, 1\}} q \text{ prime } (\mathcal{A} \cdot \mathcal{KS}(q^t)) = \{1\}.
   \]

**Proof.** (1) Since \( m - 1 \) divides each of \( l - 1 \) and \( k - 1 \), then by Proposition 2.6, we get

\[
\mathcal{A} \cdot \mathcal{KS}(q^m) \subseteq \mathcal{A} \cdot \mathcal{KS}(q^l) \cap \mathcal{A} \cdot \mathcal{KS}(q^k).
\]

On the other hand, if \( \alpha = \frac{\alpha_1}{\alpha_2} \in \mathcal{A} \cdot \mathcal{KS}(q^l) \cap \mathcal{A} \cdot \mathcal{KS}(q^k) \) then

\[
\begin{align*}
\alpha_2 q - \alpha_1 & \mid q^l - q = q(q^{l-1} - 1) \\
\alpha_2 q - \alpha_1 & \mid q^k - q = q(q^{k-1} - 1)
\end{align*}
\]

hence

\[
\alpha_2 q - \alpha_1 \mid q \gcd(q^{l-1} - 1, q^{k-1} - 1).
\]

But as

\[
\gcd(q^{l-1} - 1, q^{k-1} - 1) = q^{\gcd(l-1,k-1)} - 1 = q^{m-1} - 1,
\]

it follows that \( (\alpha_2 q - \alpha_1) \mid q(q^{m-1} - 1) \). Thus \( \alpha \in \mathcal{A} \cdot \mathcal{KS}(q^m) \).

So, we conclude that \( \mathcal{A} \cdot \mathcal{KS}(q^l) \cap \mathcal{A} \cdot \mathcal{KS}(q^k) = \mathcal{A} \cdot \mathcal{KS}(q^m) \).

(2) By Proposition 2.7(1) we have

\[
\bigcap_{t \in \mathbb{N} \setminus \{0, 1\}} q \text{ prime } (\mathcal{A} \cdot \mathcal{KS}(q^t)) = \mathcal{A} \cdot \mathcal{KS}(q^2),
\]

hence

\[
\bigcap_{t \in \mathbb{N} \setminus \{0, 1\}} q \text{ prime } (\mathcal{A} \cdot \mathcal{KS}(q^t)) = \bigcap_{q \text{ prime}} (\mathcal{A} \cdot \mathcal{KS}(q^2)).
\]

Let \( \alpha \in \bigcap_{q \text{ prime}} (\mathcal{A} \cdot \mathcal{KS}(q^2)) \). We claim that if \( (q^2 - \alpha) / (q - \alpha) \in \mathbb{Z} \) for all primes \( q \) and \( \alpha \neq 0 \) then \( \alpha = 1 \). Well,
\[
\frac{q^2 - \alpha}{q - \alpha} = q + (\alpha + \frac{\alpha^2 - \alpha}{q - \alpha}),
\]
and taking \( q \) sufficiently large so that \( \frac{\alpha^2 - \alpha}{q - \alpha} \) is smaller than the reciprocal of the denominator of \( \alpha \) we get a contradiction unless \( \alpha^2 = \alpha \), and with \( \alpha \neq 0 \) that forces \( \alpha = 1 \).
Finally, we conclude that
\[
\bigcap_{q \text{prime}} \left( \mathbb{A} \text{-KS}(q^l) \right) = \{1\}.
\]

3. Connections between Korselt rational bases of \( q^l \).

In this section we will determine explicitly for a given prime number \( q \) and an integer \( l \in \mathbb{N} \setminus \{0, 1\} \), the set \( \mathbb{Q} \text{-KS}(q^l) \). Further, we state some connections between \( q^l \)-Korselt bases in \( \mathbb{Q} \) and others in \( \mathbb{Z} \).

First, we determine by the next two results, the Korselt sets of a prime power over \( \mathbb{Z} \) and \( \mathbb{Q} \).

**Theorem 3.1.** Let \( N = q^l \) be such that \( l \geq 2 \). Then
\[
\mathbb{Q} \text{-KS}(N) = \bigcup_{s \in \mathbb{Z} \setminus \{0\}} \{ q + \frac{d}{s}; \text{ where } d \in \mathbb{N} \text{ and } d \mid (q^l - q) \} \setminus \{0, N\}.
\]

**Proof.** Suppose that \( \alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q} \text{-KS}(N) \). Then, two cases are to be considered
- If \( \alpha_1 = \alpha_1' q \), then \( d = \alpha_1' - \alpha_2 \mid (q^{l-1} - 1) \) by Proposition 2.1(2). Hence, \( \alpha = q(1 + \frac{d}{\alpha_2}) \).
- If \( \gcd(q, \alpha_1) = 1 \), then as \( d = \alpha_1 - \alpha_2 q \mid (q^{l-1} - 1) \) by Proposition 2.1(1), we get \( \alpha = q + \frac{d}{\alpha_2} \).

The converse, in the two cases, is immediate. \hfill \Box

Now, immediately by Theorem 3.1, we get the following result.

**Theorem 3.2.** Let \( N = q^l \) be such that \( l \geq 2 \). Then
\[
\mathbb{Z} \text{-KS}(N) = \{ q \pm d; \text{ where } d \in \mathbb{N} \text{ and } d \mid (q^l - q) \} \setminus \{0, N\}.
\]

For a prime number \( q \) and \( l \in \mathbb{N} \setminus \{0, 1\} \), it's clear by Theorem 3.2 that the set \( \mathbb{Z} \text{-KS}(q^l) \) is finite and the \( \mathbb{Z} \)-Korselt weight of \( q^l \) is equal to the cardinality of the divisors in \( \mathbb{Z} \) of \( q^l - q \) minus two. Hence, \( \mathbb{Z} \text{-KW}(q^l) = \)
4σ₀(q⁻¹ - 1) - 2 where σ₀ is the divisor count function. Also, It’s obvious to see by Theorem 3.1 that the sets $(\mathbb{Q} \setminus \mathbb{Z})$-$KS(q^l)$ and $\mathbb{Q}$-$KS(q^l)$ are infinite.

Now, in the rest of this section, we will prove the existence of connections between some $q^l$-Korselt bases in $\mathbb{Q}$ by establishing relations between $q^l$-Korselt bases in $\mathbb{Z}$ and others in $\mathbb{Q} \setminus \mathbb{Z}$. These relations provide us to determine the Korselt set of $q^l$ over $\mathbb{Q}$ from the knowledge of its Korselt set over $\mathbb{Z}$.

**Proposition 3.3.** Let $N = q^l$ be such that $l \geq 2$. Then, $\beta \in \mathbb{Z}$-$KS(q^l)$ if and only if $\alpha = q + \frac{\beta - q}{s}$ where $\alpha = \frac{\alpha_1}{\alpha_2}$ and $\alpha_1 = sq + \beta - q$ and $\alpha_2 = s$.

Proof. Let $\beta \in \mathbb{Z}$, $s \in \mathbb{N} \setminus \{0, 1\}$ with $gcd(s, \beta - q) = 1$.

Let $\alpha = q + \frac{\beta - q}{s} = \frac{\alpha_1}{\alpha_2}$ where $\alpha_1 = sq + \beta - q$ and $\alpha_2 = s$.

Since $gcd(s, \beta - q) = 1$, $\alpha_2 q - \alpha_1 = sq - (sq - (\beta - q)) = \beta - q$ and $\alpha_2 q - \alpha_1 = sq - (sq - (\beta - q)) = s(q^l - \beta) + (s + 1)(\beta - q)$,

the following equivalence holds

$$(q - \beta) | (q^l - \beta) \Leftrightarrow (\alpha_2 q - \alpha_1) | (\alpha_2 q^l - \alpha_1).$$

As, in addition, $\beta \neq q^l$ if and only if $\alpha \neq q + \frac{q^l - q}{s}$, we conclude that

$$\beta \in \mathbb{Z}$-KS$(q^l)$ if and only if $\alpha \in (\mathbb{Q} \setminus \mathbb{Z})$-$KS(q^l) \setminus \{q + \frac{q^l - q}{s}\}$. \hfill \Box$$

By Proposition 3.3, we determine in the next example, the sets $\mathbb{Z}$-$KS(q^l)$ and $\mathbb{Q}$-$KS(q^l)$ for some chosen numbers $q$ and $l$.

**Example 3.4.** (1) Let $N_2 = q^2$ where $q = 2p + 1$ and $p$ are prime numbers. As $q^2 - q = 2pq$, we get

$$Z$-KS$(N_2) = \{q \pm d; \ d \mid 2pq\} \setminus \{0, N_2\} = \{q \pm d; \ d \in \{1, 2, p, q, 2p, 2q, pq, 2pq\}\} \setminus \{0, N_2\} = \{q \pm 1, q \pm 2, q \pm p, 2q, 2p, q \pm 2p, q \pm q, q \pm pq, q \pm 2pq\}.$$  

Hence,

$$(\mathbb{Q} \setminus \mathbb{Z})$-KS$(N_2) = \bigcup_{s \in \mathbb{N} \setminus \{0, 1\}} \{q \pm \frac{d}{s}; \ gcd(d, s) = 1 \text{ and } d \mid 2pq\} \setminus \{0, N_2\} = \bigcup_{s \in \mathbb{N} \setminus \{0, 1\}} \{q \pm \frac{1}{s}, q \pm \frac{2}{s}, q \pm \frac{p}{s}, q \pm \frac{q}{s}, q \pm \frac{2p}{s}, q \pm \frac{2q}{s}, q \pm \frac{pq}{s}, q \pm \frac{2pq}{s}\} \setminus \{0, N_2\}.$$
Thus, we obtain
\[
\mathbb{Q} \cdot \mathcal{KS}(N_2) = \mathbb{Z} \cdot \mathcal{KS}(N_2) \cup (\mathbb{Q} \setminus \mathbb{Z}) \cdot \mathcal{KS}(N_2)
\]
\[
= \bigcup_{s \in \mathbb{N} \setminus \{0\}, \gcd(s,2pq)=1} \{ q \pm \frac{1}{s} q \pm \frac{2}{s} q \pm \frac{p}{s} q \pm \frac{q}{s} q \pm \frac{2p}{s} q \pm \frac{2q}{s} q \pm \frac{pq}{s} q \pm \frac{2pq}{s} \} \setminus \{0, N_2\}.
\]

(2) Let \( N_3 = q^2 \) where \( q = 2p + 1, \ p = 2r - 1 \) and \( r \) are prime numbers.
We denote the positive divisors of \( q^3 - q = 8pqr \) by \( D(q^3 - q) \). Hence,
\[
D(q^3 - q) = \{ d \in \mathbb{N} \text{ such that } d \mid 8pqr \}
\]
\[
= \{ 1, 2, 4, 8, p, q, r, 2p, 2q, 2r, 4p, 4q, 4r, 8p, 8q, 8r, pq, pr, qr, 2pq, 2pr, 2qr, 4pq, 4pr, 4qr, 8pq, 8pr, 8qr, pqr, 2pqr, 4pqr, 8pqr \}.
\]
Therefore
\[
\mathbb{Z} \cdot \mathcal{KS}(N_3) = \{ q \pm d \mid d \in D(q^3 - q) \} \setminus \{0, N_3\}
\]
and
\[
(\mathbb{Q} \setminus \mathbb{Z}) \cdot \mathcal{KS}(N_3) = \bigcup_{s \in \mathbb{N} \setminus \{0,1\}} \{ q \pm \frac{d}{s} \mid \gcd(d,s) = 1, d \in D(q^3 - q) \} \setminus \{0, N_3\}.
\]
Thus,
\[
\mathbb{Q} \cdot \mathcal{KS}(N_3) = \mathbb{Z} \cdot \mathcal{KS}(N_3) \cup (\mathbb{Q} \setminus \mathbb{Z}) \cdot \mathcal{KS}(N_3)
\]
\[
= \bigcup_{s \in \mathbb{N} \setminus \{0\}} \{ q \pm \frac{d}{s} \mid \gcd(d,s) = 1, d \in D(q^3 - q) \} \setminus \{0, N_3\}.
\]

4. KORSLET WEIGHT OF A \( q^l\)-RATIONAL BASE

**Proposition 4.1.** Let \( \alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q} \setminus \{0,1\} \) and \( N = q^l \) be such that \( l \geq 2 \) and \( \gcd(q,\alpha_1) = 1 \). If \( \alpha \in \mathbb{Q} \cdot \mathcal{KS}(q^l) \), then \( 2 \leq q \leq \alpha + |\alpha \alpha_1^{-2} - \alpha_2^{-2}| \).

**Proof.** Let \( \alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q} \cdot \mathcal{KS}(N) \). Then, by Proposition 2.1(1) we have \( \alpha_2 q - \alpha_1 \mid (q^{l-1} - 1) \). So, we can write
\[
\alpha_2 q - \alpha_1 \mid \alpha_2^{l-1} (q^{l-1} - 1) = (\alpha_2 q)^{l-1} - \alpha_1^{l-1} + \alpha_1^{l-1} - \alpha_2^{l-1},
\]

hence \( \alpha_2 q - \alpha_1 \mid (\alpha_1^{l-1} - \alpha_2^{l-1}) \). Since in addition \( \alpha \neq 1 \) (i.e \( \alpha_1 \neq \alpha_2 \)), it follows that \( \alpha_2 q - \alpha_1 \leq |\alpha_1^{l-1} - \alpha_2^{l-1}| \). Thus, \( q \leq \alpha + |\alpha \alpha_1^{-2} - \alpha_2^{-2}| \).

\( \square \)

By Proposition 4.1 and for a fixed integer \( l \geq 2 \), we can see that every nonzero rational number \( \alpha \neq 1 \) can belong only to a finite number of sets \( \mathbb{Q} \cdot \mathcal{KS}(q^l) \). However, we will prove in the rest of this section that for each \( \alpha \neq 0 \), there exist infinitely many couples \( (l, q) \) (equivalently \( N = q^l \)) such that \( \alpha \) is an \( N \)-Korselt base.
The following result shows for \( N = q^l \) that the exponent \( l \) of \( q \) can generate some \( N \)-Korselt rational bases.

**Proposition 4.2.** Let \( N = q^l \) be such that \( l \geq 2 \) and \( \varphi(.) \) denote the Euler’s totient function. Then each number \( d \) where \( \varphi(d) \mid (l-1) \), generates a Korselt base of \( N \) in \( \mathbb{Q} \).

**Proof.** First, by Euler’s theorem, we have \( d \mid (q^{\varphi(d)} - 1) \). Furthermore, since \( \varphi(d) \mid (l-1) \), we get \( (q^{\varphi(d)+1} - q) \mid (q^l - q) \). Hence

\[
d \mid (q^l - q).
\]

By the euclidian division of \( d \) by \( q \) there exist \( t_d \geq 0 \) and \( 0 \leq r_d < q \) such that \( d = tq + r_d \). Three cases are to be discussed:

1. Suppose that \( t_d = 0 \) (i.e. \( d < q \)). Then by (4.1) and for each \( m \in \mathbb{N} \setminus \{0\} \), we get \( mq - (mq - r_d) = r_d = d \mid (q^l - q) \). Hence,

\[
\alpha_d = \frac{mq - r_d}{m} \in \mathbb{Q}\text{-KS}(q^l).
\]

2. If \( r_d = 0 \) (i.e. \( q \mid d \)), then there exist \( t'_d \) and \( t''_d \) integers such that \( t_d = t'_d - t''_d \) and \( t'_d t''_d \neq 0 \). Consequently, by (4.1) we obtain \( t'_d - t''_d = t_d \mid (q^{l-1} - 1) \), this implies that \( \alpha_d = \frac{t'_dt''_d}{t_d} \in \mathbb{Q}\text{-KS}(q^l) \).

3. Now, assume that \( r_d \neq 0 \) and \( t_d \neq 0 \). Then for each \( m \in \mathbb{Z} \) where \( t_d + m \neq 0 \), we have \( (t_d + m)q - (mq - r_d) = d \mid (q^l - q) \). Thus,

\[
\alpha_d = \frac{mq - r_d}{t_d + m} \in \mathbb{Q}\text{-KS}(q^l).
\]

\( \square \)

It follows by Proposition 4.2, that for each \( N = q^l \) the set \( \mathbb{Q}\text{-KS}(q^l) \) is non empty (\( d = 2 \) is valid for all cases). Now, one may ask if the converse is true. The answer is yes, moreover by the following result we show that for each \( \alpha \in \mathbb{Q} \setminus \{0\} \), there exist infinitely many \( N = q^l \) such that \( \alpha \) is an \( N \)-Korselt base.

**Theorem 4.3.** Let \( \alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q} \setminus \{0\} \). Then the following assertions hold.

1. There exist a prime number \( p \) and \( k \in \mathbb{N} \) such that \( \gcd(\alpha_1, p) = 1 \) and \( \alpha \in \mathbb{Q}\text{-KS}(p^k) \).
2. If \( \alpha_1 \neq 1 \), then there exist a prime number \( q \) and \( l \in \mathbb{N} \) such that \( q \) divides \( \alpha_1 \) and \( \alpha \in \mathbb{Q}\text{-KS}(q^l) \).

**Proof.** Let \( \alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q} \setminus \{0\} \).

1. Let \( p > \alpha_1 \) be a prime number and \( k_1 = \alpha_2p - \alpha_1 \geq 1 \). Since \( \gcd(k_1, p) = 1 \), we get by Euler’s theorem \( \alpha_2p - \alpha_1 = k_1 \mid (p^{\varphi(k_1)} - 1) \). Hence \( \alpha \in \mathbb{Q}\text{-KS}(p^k) \) where \( k = \varphi(k_1) + 1 \).
(2) Let \( q \) be a prime number such that \( \alpha_1 = \alpha'_1 q \).

By taking \( l - 1 = \varphi(\alpha_2 - \alpha'_1) \), Euler’s theorem implies that
\[
(\alpha_2 - \alpha'_1) \mid (q^{\varphi(\alpha_2 - \alpha'_1)} - 1) = q^{l-1} - 1.
\]
Hence \( (\alpha_2 q - \alpha_1) \mid (q^l - q) \), and so \( \alpha \in \mathbb{Q}^{-KS}(q^l) \).

\[\square\]

The next result follows immediately

**Corollary 4.4.** For each \( \alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q} \setminus \{0\} \), the following assertions hold.

1. There exist infinitely many \( N = p^k \) with \( p \) a prime number and \( k \) a positive integer such that \( \gcd(\alpha_1, p) = 1 \) and \( \alpha \) is a \( K_N \)-base.
2. If \( \alpha_1 \neq 1 \), then there exist infinitely many \( N = q^l \) with \( q \) a prime number and \( l \) a positive integer such that \( q \) divides \( \alpha_1 \) and \( \alpha \) is a \( K_N \)-base.

**Proof.**

(1) Follows directly from Theorem 4.3(1).

(2) Let \( \alpha = \frac{\alpha'_1 q}{\alpha_2} \in \mathbb{Q} \setminus \{0\} \) and \( l_1 = \varphi(\alpha_2 - \alpha'_1) + 1 \). Then by Theorem 4.3(2), we have \( \alpha \in \mathbb{Q}^{-KS}(q^{l_1}) \). Hence, for each integer \( l \) where \( (l_1 - 1) \mid (l - 1) \), we get by Proposition 2.6(2),
\[
\alpha \in \mathbb{Q}^{-KS}(q^{l_1}) \subseteq \mathbb{Q}^{-KS}(q^l).
\]
Therefore \( \alpha \) is a \( q^l \)-Korselt base, and so \( \alpha \) is an \( N \)-Korselt base for infinitely many numbers \( N = q^l \).

\[\square\]

By Corollary 4.4, we deduce that for each rational \( \alpha \neq 0 \) the korselt weight of a base \( \alpha \) over the set of prime powers is infinite.

5. **Korselt set of \( q^l \) over \([-1, 1] \cap \mathbb{Q} \)**

We begin this section by giving some examples of \( q^l \)-Korselt rational bases in \([-1, 1] \].

**Proposition 5.1.** Let \( q \) be a prime number and \( l \) be a positive integer. Then \( \frac{1}{q^{s-1}} \in \mathbb{Q}^{-KS}(q^l) \) for each integer \( s \) dividing \( l - 1 \).

**Proof.** Since \( s \mid (l - 1) \) that is \( s \mid (l + s - 1) \), it follows that \( q^{s-1}q - 1 = (q^s - 1) \mid (q^{l+s-1} - 1) = q^{s-1}N - 1 \). Thus, \( \frac{1}{q^{s-1}} \in \mathbb{Q}^{-KS}(q^l) \).

\[\square\]

Similarly, we obtain the following result

**Proposition 5.2.** Let \( q \) be a prime number and \( l \) be a positive integer. Then \( \frac{1}{q^{s-1}} \in \mathbb{Q}^{-KS}(q^l) \) for each positive integer \( s \) dividing \( l - 1 \) where \( \frac{l - 1}{s} \) is even.
Proof. Since \( s \mid (l-1) \) hence \( s \mid (l+s-1) \) and \( \frac{l+s-1}{s} \) is odd, it follows that \( q^{s-1}q + 1 = (q^s + 1) \mid (q^{l+s-1} + 1) = q^{s-1}N + 1 \). Therefore \( \frac{-1}{q^{s-1}} \in \mathbb{Q} - \mathcal{K}_S(q^l) \). □

If \( \frac{l-1}{s} \) is odd the assertion in Proposition 5.2 is false, for instance, if \( l = 3 \) and \( q \) a prime number, it’s forward to verify that \( \frac{-1}{q} \notin \mathbb{Q} - \mathcal{K}_S(q^3) \).

By the next two results, we give some relations between the Korselt sets over \( \mathbb{Q} \) of the prime powers \( p^l \) and \( q^l \).

**Proposition 5.3.** Let \( p, q \) be two distinct prime numbers and \( l \) a positive integer. Then, \( \frac{1}{p} \in \mathbb{Q} - \mathcal{K}_S(q^l) \) if and only if \( \frac{1}{q} \in \mathbb{Q} - \mathcal{K}_S(p^l) \).

Proof. We have

\[
\frac{1}{p} \in \mathbb{Q} - \mathcal{K}_S(q^l) \iff pq - 1 \mid pq^l - 1 \\
\iff pq - 1 \mid p^{l-1}(pq^l - 1) = (pq)^l - 1 - p^{l-1} + 1 \\
\iff pq - 1 \mid p^{l-1} - 1 \\
\iff q(p - 1) \mid qp(p^{l-1} - 1) + q - 1 = qp^l - 1 \\
\iff \frac{1}{q} \in \mathbb{Q} - \mathcal{K}_S(p^l)
\]

□

**Proposition 5.4.** Let \( p, q \) be two distinct prime numbers and \( l \) a positive odd integer. Then the following assertion holds

\( \frac{-1}{p} \in \mathbb{Q} - \mathcal{K}_S(q^l) \) if and only if \( \frac{-1}{q} \in \mathbb{Q} - \mathcal{K}_S(p^l) \).

Proof. We have

\[
\frac{-1}{p} \in \mathbb{Q} - \mathcal{K}_S(q^l) \iff pq + 1 \mid pq^l + 1 \\
\iff pq + 1 \mid p^{l-1}(pq^l + 1) = (pq)^l + 1 + p^{l-1} - 1 \\
\iff pq + 1 \mid p^{l-1} - 1 \\
\iff pq + 1 \mid pq(p^{l-1} - 1) + pq + 1 = qp^l + 1 \\
\iff \frac{-1}{q} \in \mathbb{Q} - \mathcal{K}_S(p^l)
\]

□

If \( l \) is even the assertion in Proposition 5.4 is not true, for instance when \( q = 3, p = 2 \) and \( l = 2 \), we have \( \frac{-1}{2} \notin \mathbb{Q} - \mathcal{K}_S(3^2) \) but \( \frac{-1}{3} \notin \mathbb{Q} - \mathcal{K}_S(2^2) \).

Now, by the next two propositions and for a given prime number \( q \) and \( l \in \mathbb{N} - \{0, 1\} \), we determine the set \( (-1, 1 - \mathbb{Q}) - \mathcal{K}_S(q^l) \).
Proposition 5.5. Let $q$ be a prime number, $l \in \mathbb{N} \setminus \{0, 1\}$ and
$\alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q} \setminus \mathcal{KS}(q^l)$. Then, $\alpha \in [0, 1]$ if and only if there exists $d \mid (q^l - q)$ such that
$$\alpha = q - \frac{d}{\alpha_2} \quad \text{and} \quad \alpha_2 \in \left\{ \left\lfloor \frac{d}{q} \right\rfloor + 1, ..., \left\lfloor \frac{d}{q-1} \right\rfloor - 1 \right\}.$$  

Proof. By Theorem 3.1, $\alpha = \frac{\alpha_1}{\alpha_2} \in [0, 1] \cap (\mathbb{Q} \setminus \mathcal{KS}(q^l))$ is equivalent to the existence of a positive integer $d$ such that $d \mid (q^l - q)$ and $\alpha = q - \frac{d}{\alpha_2}$. Further, we have

$$\alpha \in [0, 1] \cap (\mathbb{Q} \setminus \mathcal{KS}(q^l)) \iff 0 < \alpha = q - \frac{d}{\alpha_2} < 1$$
$$\iff \frac{d}{q} < \alpha_2 < \frac{d}{q-1}$$
$$\iff \left\lfloor \frac{d}{q} \right\rfloor + 1 \leq \alpha_2 \leq \left\lfloor \frac{d}{q-1} \right\rfloor - 1$$
$$\iff \alpha_2 \in \left\{ \left\lfloor \frac{d}{q} \right\rfloor + 1, ..., \left\lfloor \frac{d}{q-1} \right\rfloor - 1 \right\},$$

which complete the proof. □

Corollary 5.6. Let $q$ be a prime number and $\mathbb{A} = [0, 1] \cap \mathbb{Q}$. Then
$$\mathbb{A} \setminus \mathcal{KS}(q^2) = \emptyset.$$  

Proof. Suppose that there exists $\alpha \in [0, 1] \cap (\mathbb{Q} \setminus \mathcal{KS}(q^2))$. This is equivalent by Theorem 3.1 and Proposition 5.5, to the existence of $d \mid (q^2 - q)$ such that $\alpha = q - \frac{d}{\alpha_2}$ and

$$\left\lfloor \frac{d}{q} \right\rfloor + 1 \leq \alpha_2 \leq \left\lfloor \frac{d}{q-1} \right\rfloor - 1. \quad (5.1)$$

Since, in addition $d \mid (q^2 - q) = q(q - 1)$, two cases are to be considered:

- If $\gcd(q, d) = 1$, then $d$ divides $q - 1$ and so $d < q$. Hence, by (5.1)
  $$1 = \left\lfloor \frac{d}{q} \right\rfloor + 1 \leq \left\lfloor \frac{d}{q-1} \right\rfloor - 1 = 0$$
  which is impossible.

- Assume that $d = d'q$. Then, since $d = d'q \mid q(q-1)$ hence $d' \mid (q-1)$, it follows by (5.1) that
  $$d' + 1 = \left\lfloor \frac{d}{q} \right\rfloor + 1 \leq \left\lfloor \frac{d}{q-1} \right\rfloor - 1 = d'$$
  which is again impossible. □
Proposition 5.7. Let \( q \) be a prime number, \( l \in \mathbb{N} \setminus \{0,1\} \) and
\[
\alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{Q} - \mathbb{K}S(q^l).
\]
Then, \( \alpha \in [-1,0[ \) if and only if there exists \( d \mid (q^l - q) \) such that
\[
\alpha = q - \frac{d}{\alpha_2} \quad \text{and} \quad \alpha_2 \in \left\{ \left\lfloor \frac{d}{q+1} \right\rfloor, ..., \left\lfloor \frac{d}{q} \right\rfloor - 1 \right\}.
\]

Proof. By Theorem 3.1, \( \alpha = \frac{\alpha_1}{\alpha_2} \in [-1,0[ \cap (\mathbb{Q} - \mathbb{K}S(q^l)) \) is equivalent to the existence of an integer \( d > 0 \) such that \( d \mid (q^l - q) \) and \( \alpha = q - \frac{d}{\alpha_2} \). Also, the following equivalences hold
\[
\begin{align*}
\alpha \in [-1,0[ \cap (\mathbb{Q} - \mathbb{K}S(q^l)) & \iff -1 \leq \alpha = q - \frac{d}{\alpha_2} < 0 \\
& \iff \frac{d}{q+1} \leq \frac{d}{q} < 0 \\
& \iff \left\lfloor \frac{d}{q+1} \right\rfloor \leq \alpha_2 < \left\lfloor \frac{d}{q} \right\rfloor - 1 \\
& \iff \alpha_2 \in \left\{ \left\lfloor \frac{d}{q+1} \right\rfloor, ..., \left\lfloor \frac{d}{q} \right\rfloor - 1 \right\}.
\end{align*}
\]
Thus the proposition is proved. \( \square \)

Corollary 5.8. Let \( q \) be a prime number and \( A = [-1,0[ \cap \mathbb{Q} \). Then
\[
A - \mathbb{K}S(q^2) = \emptyset.
\]

Proof. Suppose by contradiction that there exists \( \alpha \in [-1,0[ \cap (\mathbb{Q} - \mathbb{K}S(q^2)) \). This is equivalent by Proposition 5.7, to the existence of a positive integer \( d \mid (q^2 - q) \) such that \( \alpha = q - \frac{d}{\alpha_2} \) and
\[
\left\lfloor \frac{d}{q+1} \right\rfloor \leq \alpha_2 \leq \left\lfloor \frac{d}{q} \right\rfloor - 1. \tag{5.2}
\]
Since \( d \mid (q^2 - q) = q(q - 1) \), two cases are to be discussed:

- If \( \gcd(q,d) = 1 \), then \( d \) divides \( q - 1 \) and so \( d < q \). Hence, by (5.2)
\[
1 = \left\lfloor \frac{d}{q+1} \right\rfloor \leq \left\lfloor \frac{d}{q} \right\rfloor - 1 = 0
\]
which is impossible.

- If \( q \mid d \), then \( d = dq \) with \( d' \in \mathbb{N} \). Since \( d = dq \mid q(q - 1) \) hence \( d' \mid (q - 1) \), it follows by (5.2), that
\[
d' + 1 = \left\lfloor \frac{d}{q} \right\rfloor + 1 \leq \left\lfloor \frac{d}{q-1} \right\rfloor - 1 = d'
\]
which is again impossible.
So, we conclude that \(\mathcal{KS}(q^2)\) is empty. \(\square\)

References

[5] N. G. W. H. Beeger; On composite numbers \(n\) for which \(a^{n-1} \equiv 1 \pmod{n}\) for every a prime to \(n\), *Scripta Math.*, 16(1950), 133 – 135.
[8] R. D. Carmichael; On composite numbers \(P\) which satisfy the Fermat congruence \(a^{P-1} \equiv 1 \pmod{P}\), *Amer. Math. Monthly*, 19(1912), 22 – 27.

(Ghanmi) (1) Preparatory Institut of Engineering Studies of Tunis, Montfleury, Tunisia.

(2) University College of Jammum, Department of Mathematics, Mekkah, Saudi Arabia.

E-mail address: neghanmi@yahoo.fr and naghanmi@uqu.edu.sa