C. R. Math. Rep. Acad. Sci. Canada Vol. **35** (1) 2013, pp. 1–15

On the Korselt Set of a Squarefree Composite Number

Ibrahim Al-Rasasi, Othman Echi, and Nejib Ghanmi

Presented by Pierre Milman, FRSC

Abstract. Let $\alpha \in \mathbb{Z} \setminus \{0\}$. A positive composite squarefree integer N is said to be an *α-Korselt number* (*K_α-number*, for short) if $N \neq \alpha$ and $p - \alpha$ divides $N - \alpha$ for each prime divisor p of N. By the *Korselt set* of N, we mean the set of all $\alpha \in \mathbb{Z} \setminus \{0\}$ such that N is a K_α-number. This set will be denoted by $\mathcal{KS}(N)$.

In a recent paper [3], Bouallegue–Echi–Pinch have asked whether there are infinitely many squarefree composite numbers with empty Korselt set. This paper aims to solve this question by showing that for each prime number $q \geq 19$, $6q$ has an empty Korselt set.

We also show that for each integer $l \geq 3$, there are infinitely many squarefree composite numbers with l prime divisors whose Korselt sets are empty.

Résumé. Soit N un nombre composé sans facteur carré et $\alpha \in \mathbb{Z} \setminus \{0\}$. On dit que N est *α-Korselt* si $N \neq \alpha$ et $p - \alpha$ divise $N - \alpha$ pour tout facteur premier p de N.

L'ensemble constitué de tous les α tels que N est α-Korselt, noté $\mathcal{KS}(N)$, est appelé *l'ensemble de Korselt* de N.

Bouallegue–Echi–Pinch se sont posés la question d'existence d'une infinité de nombres composés sans facteur carré possédant des ensembles de Korselt vides.

Dans ce papier on donne une réponse positive à cette question en démontrant que pour tout premier $q \geq 19$, $6q$ a un ensemble de Korselt vide.

On prouve aussi que pour tout entier $l \geq 3$, il existe une infinité de nombres composés sans facteur carré ayant l facteurs premiers et d'ensembles de Korselt vides.

1. Introduction.

In 1640, Fermat proved that if p is a prime number, then p divides $a^p - a$ for every integer a. This is known as Fermat's Little Theorem. The question then arose whether the converse of this theorem might be true: if n divides $a^n - a$ for every integer a, does it follow that n is prime?

In 1899, Korselt showed in [8] that a composite odd number n has this property if and only if n is squarefree and $p-1$ divides $n-1$ for each prime divisor p of n. It is worth noting that, in 1910, Carmichael gave a counterexample to the converse

Received by the editors on September 1, 2012; revised November 18, 2012.

AMS Subject Classification: Primary: 11Y16; secondaries: 11Y11, 11A51.

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

of Fermat's little theorem ($n = 561 = 3 * 11 * 17$). He also exhibited a method for constructing such numbers, known nowadays as Carmichael numbers. The term Carmichael number was introduced by Beeger [2] in 1950.

In 1912, Carmichael conjectured that there are infinitely many such numbers. This conjecture has been solved by Alford, Granville, and Pomerance in a remarkable paper [1]. Indeed, it is shown that if $C(x)$ denotes the number of Carmichael numbers not exceeding x, then $C(x) > x^{2/7}$ for x sufficiently large. Improving this result, Harman showed in [7] that there are more than x^{σ} Carmichael numbers up to x, where $\sigma > 1/3$.

In studying the converse of Fermat's little theorem, Korselt did not exhibit any numerical example; if he had just done few computations, then surely the so-called "Carmichael numbers" would have been known as "Korselt numbers".

In honor of Korselt, Bouallegue, Echi, and Pinch have recently introduced the concept of "Korselt numbers" (see [3] and [6]).

DEFINITION 1.1 ([3]). Let $N \in \mathbb{N} \setminus \{0, 1\}$ be a squarefree composite number and $\alpha \in \mathbb{Z} \setminus \{0\}$. Then N is said to be an *α-Korselt number* (*K_α-number*, for short), if $N \neq \alpha$ and $p - \alpha$ divides $N - \alpha$ for every prime divisor p of N.

Note that, by definition, if N is a composite α-Korselt number, then α is not a prime factor of N.

The following two concepts are also introduced in [3].

DEFINITION 1.2. Let $N \in \mathbb{N} \setminus \{0, 1\}$ be a squarefree composite number.

(i) By the *Korselt set* of N, we mean the set $\mathcal{KS}(N)$ of all $\alpha \in \mathbb{Z} \setminus \{0, N\}$ such that N is a K_α-number.
(ii) The cardinality of $\mathcal{KS}(N)$ will be called the *Korselt weight* of N; we denote it by $Kw(N)$.

In [3], the authors asked if there are infinitely many integers with empty *Korselt sets*; *i.e.*, integers N that are not K_α-numbers for any $\alpha \in \mathbb{Z} \setminus \{0, N\}$.

Our main goal in this paper is to show that there are infinitely many integers whose Korselt sets are empty. This will be achieved in two ways. The first one consists of providing an infinite sequence of squarefree composite numbers with empty Korselt sets (Section 2). The second way is more theoretical: we prove that for each integer $l \geq 3$, there are infinitely many squarefree composite numbers with l prime divisors whose Korselt sets are empty.

2. Introductory result: The Korselt set of $6q$.

The aim of this section is to give an infinite sequence of squarefree composite numbers with empty Korselt sets using an elementary proof. This may be considered as a direct answer to the question stated in [3].

THEOREM 2.1. *Let $q \geq 5$ be a prime number and $N = 6q$. Then the only values of q for which $\mathcal{KS}(N) \neq \varnothing$ are 5, 7, 11, and 17.*

Proof. We break the proof into five steps.

Step 1: If $\alpha \in \mathcal{KS}(N)$, then $\alpha \in \{q+1, q-1, q+5, q-5\}$. Indeed, $q-\alpha$ divides $6q-\alpha = 5q+(q-\alpha)$. Hence $q-\alpha$ divides $5q$; thus $q-\alpha \in \{\pm 1, \pm 5, \pm q, \pm 5q\}$. Of course, $q-\alpha \neq q$ and $q-\alpha \neq -5q$, as $\alpha \neq 0$ and $\alpha \neq N$, by definition.

Suppose that $q-\alpha = -q$. Then $\alpha = 2q$. But, $2-\alpha = 2(1-q)$ divides $N-\alpha = 4q$. This implies that $q-1$ divides $2q$. Consequently $q-1$ divides 2, showing that $q=2$ or $q=3$, against the hypotheses.

Now suppose that $q-\alpha = 5q$. Then $\alpha = -4q$. As $2-\alpha = 2(1+2q)$ and $N-\alpha = 10q$, we see that $1+2q$ divides $5q$. Since, in addition $\gcd(1+2q, q) = 1$, we deduce that $1+2q$ divides 5. This yields $q=0$ or $q=2$, which is again against the hypotheses.

We conclude that $q-\alpha \in \{\pm 1, \pm 5\}$, so that

$$\alpha \in \{q+1, q-1, q+5, q-5\}.$$

The next four steps deal with these possible values of α.

Step 2: If $\alpha = q+1$, then $q=5$. First, we have $N-\alpha = 5q-1$, $2-\alpha = 1-q$ and $3-\alpha = 2-q$. As $2-\alpha = 1-q$ divides $N-\alpha = 5q-1 = 5(q-1)+4$, we deduce that $q-1$ divides 4. Hence, $q-1 \in \{1,2,4\}$. Thus, $q \in \{2,3,5\}$.

Also, $3-\alpha = 2-q$ divides $N-\alpha = 5q-1 = 5(q-2)+9$ implies that $q-2$ divides 9; so that $q-2 \in \{1,3,9\}$. Thus $q \in \{3,5,11\}$.

We conclude that $q=5$.

Step 3: If $\alpha = q-1$, then $q \in \{5,7,11\}$. On one hand, $2-\alpha = 3-q$ divides $N-\alpha = 5q+1 = 5(q-3)+16$. Then $q-3$ divides 16; so that $q-3 \in \{1,2,4,8,16\}$. This implies that $q \in \{5,7,11,19\}$.

On the other hand, $3-\alpha = 4-q$ divides $N-\alpha = 5q+1 = 5(q-4)+21$. Hence, $q-4$ divides 21, and consequently, $q-4 \in \{1,3,7,21\}$. Therefore, $q \in \{5,7,11\}$.

It follows that $q \in \{5,7,11\}$.

Step 4: It is not possible to have $\alpha = q+5$. Suppose that $\alpha = q+5$. Then $2-\alpha = -3-q$ divides $N-\alpha = 5q-5 = 5(q+3)-20$. Hence, $q+3$ divides 20; so that $q+3 \in \{1,2,4,5,10,20\}$. Thus $q \in \{7,17\}$.

Also, $3-\alpha = -2-q$ divides $N-\alpha = 5q-5 = 5(q+2)-15$. Hence, $q+2$ divides 15, and consequently, $q \in \{3,13\}$.

It follows that it is not possible to have $\alpha = q+5$.

Step 5: If $\alpha = q-5$, then $q \in \{11,17\}$. Indeed, as $2-\alpha = 7-q$ divides $N-\alpha = 5q+5 = 5(q-7)+40$, we see that $q-7$ divides 40. Since $q-7 \geq 5-7 = -2$, we get $q-7 \in \{-2,-1,1,2,4,5,8,10,20,40\}$. This gives $q \in \{5,11,17,47\}$. But since $\alpha \neq 0$, we have $q \in \{11,17,47\}$.

Also, $3-\alpha = 8-q$ divides $N-\alpha = 5q+5 = 5(q-8)+45$. Hence, $q-8$ divides 45. Since $q-8 \geq 5-8 = -3$, we have $q-8 \in \{-3,-1,1,3,5,9,15,45\}$. This yields $q \in \{7,11,13,17,23,53\}$.

Therefore, in this case, $q \in \{11,17\}$.

Combining the previous steps, the only values of q for which $\mathcal{KS}(6q) \neq \varnothing$ are 5, 7, 11, and 17.

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

3. **Korselt numbers and sets.** We start this section by improving Proposition 1.5 in [3] that sheds some light on Korselt sets. Note that the proof of the following proposition is extracted from [3], with a slight change.

PROPOSITION 3.1. *Let $N \in \mathbb{N} \setminus \{0, 1\}$ be a composite squarefree number and q (resp., p) be the largest (resp., smallest) prime factor of N. If $\alpha \in \mathcal{KS}(N)$, then we have the following inequalities:*

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

PROOF. Let $\alpha \in \mathcal{KS}(N)$. We consider two cases.

Case 1: $\alpha < 0$. By hypothesis, there exists an integer $k \in \mathbb{N}$ such that $N - \alpha = k(q - \alpha)$. Since $N > q$, we have $k \geq 2$.

Next we show that $k \neq 2$. Suppose that $k = 2$. Then we get $\alpha = 2q - N$. As N is composite, $N \neq q$. Also, $N \neq 2q$; otherwise $\alpha = 0$, which is impossible. Therefore, $N = rq$ where $r \geq 3$, and so $\alpha = -(r-2)q < 0$.

If t is a prime factor of r, then $t - \alpha = t + (r-2)q$ divides $N - \alpha = q(2r-2)$. Now, $\gcd\big(t + (r-2)q, q\big) = \gcd(t, q) = 1$ and so $t + (r-2)q$ divides $2r - 2$. But $2r - 2 = 2 + (r-2)2 < t + (r-2)q$, a contradiction. Therefore $k \geq 3$ and so $N - \alpha = k(q - \alpha) \geq 3(q - \alpha)$. Thus, $\alpha \geq \frac{3q-N}{2}$.

Case 2: $\alpha > 0$. Suppose that $\alpha \geq N$; then $\alpha - q > \alpha - N \geq 0$; but since in addition, $q - \alpha$ divides $N - \alpha$, we have necessarily $\alpha - N = 0$, which is not possible. Therefore, $\alpha \leq N - 1$.

Now, let us show that $\alpha \leq \frac{N+p}{2}$. If $\alpha \leq p$, then this is clear. If $p < \alpha < N$, then since $p - \alpha$ divides $N - \alpha$, we have $|p - \alpha| \leq |N - \alpha|$ which gives $\alpha - p \leq N - \alpha$ and hence $\alpha \leq \frac{p+N}{2}$.

Finally, we combine the two cases to get the inequalities $\frac{3q-N}{2} \leq \alpha \leq \frac{p+N}{2}$. □

REMARK 3.2. The upper bound of Proposition 3.1 may be reached. Indeed, let p be an odd prime number. Then $N := 2p$ is a $(p+1)$-Korselt number (and $\frac{2+N}{2} = p + 1$).

Next, we recall a result dealing with the number of prime factors of a composite squarefree Korselt number [3].

Theorem 3.3 ([3]). *Let $\alpha \in \mathbb{Z} \setminus \{0\}$. Then the following properties hold.*

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

(ii) *Suppose that $\alpha > 1$. Let $p < q$ be two prime numbers and $N := pq$. If N is an α-Korselt number, then $p < q \leq 4\alpha - 3$. In particular, there are only finitely many α-Korselt numbers with exactly two prime factors.*

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

Proposition 3.4. *Let $N \neq 6$ be a squarefree composite number and $\alpha \in \mathcal{KS}(N)$. Let p, q be two prime factors of N. Then the following properties hold.*

(i) *If $\gcd(\alpha, p) = 1$ and q divides α, then*

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

(ii) *If q does not divide α, then $q + 1 - \frac{N}{q} \leq \alpha \leq \frac{N}{q} + q - 1$.*

Proof. Let R be the natural number such that $N = pqR$.

(i) If q divides α, then there exists an integer $\alpha_1 \in \mathbb{Z}\setminus\{0, 1\}$ such that $\alpha = \alpha_1 q$. Now, $p - \alpha$ divides $q(\frac{N-\alpha}{q})$; as, in addition, $\gcd(p - \alpha, q) = \gcd(p, q) = 1$, we conclude that $p - \alpha$ divides $\frac{N-\alpha}{q}$. It follows that there exists $k \in \mathbb{Z} \setminus \{0\}$ such that $(p - \alpha)k = \frac{N-\alpha}{q}$. Thus, we have

$$qp(k - R) = \alpha(kq - 1). \tag{3.1}$$

We will prove that $|k| \neq 1$. Suppose that $k = 1$. Then equation (3.1) gives

$$qp(1 - R) = \alpha(q - 1). \tag{3.2}$$

Consequently, $R \neq 1$ and $\alpha < 0$.

As $\gcd(\alpha, p) = 1$, by equation (3.2), p divides $q - 1$, which implies that

$$p < q. \tag{3.3}$$

Let r be a prime factor of R. Replacing the factor p of N by r, we deduce, as in the beginning of the proof, that there exists an integer l such that $r - \alpha = \frac{N-\alpha}{lq}$. Since $r \neq p$, we have $l \neq 1$. So $r - \alpha \leq \frac{N-\alpha}{2q} = \frac{p-\alpha}{2}$, and consequently, $r - p \leq \alpha - r$. But, we have $-p < r - p$ and $\alpha - r < \alpha < -q$. This implies that $-p < -q$, that is to say $p > q$, contradicting inequality (3.3).

Now suppose that $k = -1$. Then equation (3.1) gives

$$p(1 + R) = \alpha_1(q + 1). \tag{3.4}$$

Two cases are to be considered.

• If $R = 1$, then by equation (3.4), we have $2p = \alpha_1(q+1)$. As $\gcd(\alpha, p) = 1$, we conclude that α_1 divides 2. Now, since $\alpha_1 > 1$, we get $\alpha_1 = 2$. Hence $p = q + 1$ and consequently $q = 2$ and $p = 3$, that is to say $N = 6$, contradicting the fact that $N \neq 6$.
• Suppose that $R \neq 1$.

Let r be a prime divisor of R. Then there exists an integer $s \in \mathbb{Z} \setminus \{0\}$ such that $r - \alpha = -\frac{N-\alpha}{sq} = \frac{p-\alpha}{s}$.

As $r \neq p$, we claim that $s \neq 1$. This implies that $r - \alpha$ is in the set $\{-\frac{N-\alpha}{2q}, -\frac{N-\alpha}{3q}, \ldots, \frac{N-\alpha}{2q}, \frac{N-\alpha}{q}\}$.

Since $\alpha < N$ (by Proposition 3.1), we have

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

This implies that $r - \alpha \geq -\frac{N-\alpha}{2q} = \frac{p-\alpha}{2}$, so $r \geq \frac{p+\alpha}{2}$. Then, we obtain $2r > \alpha$. But, equation (3.4) gives

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

so $2q + 2 > qp$, that is to say $q(p-2) < 2$. Since $\gcd(\alpha, p) = \gcd(\alpha_1, p) = 1$, then by equation (3.4) we get p divides $q + 1$ and hence $p \leq q + 1$. Thus $(p-1)(p-2) \leq q(p-2) < 2$ and so $p = 2$. Hence, $N = 2qR$; so that $q - \alpha$ divides $N - \alpha = q(2R - \alpha_1)$. This implies that $1 - \alpha_1$ divides $2R - \alpha_1$. As $1 = \gcd(\alpha, p) = \gcd(\alpha, 2)$, α_1 is odd. Then, $2R - \alpha_1$ is odd and $1 - \alpha_1$ is even, contradicting the fact that $2R - \alpha_1$ is a multiple of $1 - \alpha_1$.

So we conclude that $|k| \neq 1$ and consequently we get

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

and hence

$$\frac{2pq - N}{2q-1} \leq \alpha \leq \frac{2pq + N}{2q+1}, \quad \text{as desired.}$$

(ii) Suppose that q does not divide α. Then $\gcd(q, q - \alpha) = 1$. Knowing that $q - \alpha$ divides $N - \alpha$ and $N - \alpha = N - q + q - \alpha$, we deduce that $q - \alpha$ divides $N - q = q\frac{N-q}{q}$. This implies that $q - \alpha$ divides $\frac{N-q}{q}$.

It follows that

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

so

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

REMARKS 3.5.

(i) For $N = 6$, the inequalities of part (i) in Proposition 3.4 do not hold.

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

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

More precisely, let $N=p_1p_2\cdots p_n$ be such that the p_i's are primes and $p_1<p_2<\cdots<p_n$.
Let $b_i=p_i+1-\frac{N}{p_i}$ and $c_i=p_i-1+\frac{N}{p_i}$ for $i\in\{1,\dots,n\}$. Then $(b_i)_i$ and $(c_i)_i$ are respectively increasing and decreasing sequences.
Therefore, $\alpha\in[b_n,c_n]=[p_n+1-\frac{N}{p_n}, p_n-1+\frac{N}{p_n}]$.

For a real number x, we recall that $\lfloor x\rfloor$ (resp., $\lceil x\rceil$) denotes the greatest (resp., least) integer less (resp., greater) than or equal to x.

Corollary 3.6. *Let p and q be prime numbers such that $p<q$ and $N=pq$. Let α be an integer such that N is an α-Korselt number. Then the following properties hold.*
(i) $\gcd(\alpha,q)=1$.
(ii) $2\le q-p+1=q+1-\frac{N}{q}\le\alpha\le\frac{N}{q}+q-1=p+q-1$.
(iii) *If p divides α, then, $\alpha\in\{\lfloor\frac{q}{p}\rfloor p, \lceil\frac{q}{p}\rceil p\}$.*

Proof. (i) Let $N=pq$ such that $p<q$.
If $N=6$, then by Proposition 3.1 we have $2\le\alpha\le 4$. Thus, N is only a 4-Korselt number and then $\gcd(\alpha,q)=\gcd(4,3)=1$.
Suppose that $N\neq 6$ and q divides α. Then by Proposition 3.4(1), we have

$$0<\frac{pq}{2q-1}=\frac{2pq-N}{2q-1}\le\alpha\le\frac{2pq+N}{2q+1}=\frac{3pq}{2q+1}<2p.$$

Hence there exists $r\in\{1,\dots,2p-1\}$ such that $\alpha=2p-r$.
As q divides α, we obtain $\alpha=2p-r=kq$, with $k\ge 2$. It follows that

$$q\le\frac{2p-r}{2}=p-\frac{r}{2}<q,$$

a contradiction. We conclude that $\gcd(\alpha,q)=1$.
(ii) This is an immediate consequence of Proposition 3.4 (ii).
(iii) Suppose that p divides α. Let β be an integer such that $\alpha=\beta p$. By (ii), we have $q-p+1\le\alpha\le p+q-1$.
Then $b_1:=\frac{q}{p}-\frac{p-1}{p}=\frac{q-p+1}{p}\le\beta\le\frac{p+q-1}{p}=\frac{q}{p}+\frac{p-1}{p}:=b_2$, as the interval $[b_1,b_2]$ is centered on $\frac{q}{p}$ and of length $b_2-b_1=2-\frac{2}{p}<2$, we get $\beta\in\{\lfloor\frac{q}{p}\rfloor,\lceil\frac{q}{p}\rceil\}$. □

EXAMPLE 3.7. Let p and q be distinct prime numbers such that $p < q$ and $N = pq$.

(i) The upper and the lower bounds of the inequalities in Corollary 3.6 are reached. Indeed, we have, always N is a $(p+q-1)$-Korselt number. Besides, if p and $q = 2p-3$ are prime numbers (*e.g.*, $p \in \{5, 7, 11, 13, 17, \dots\}$), then N is also a $(q-p+1)$-Korselt number.

(ii) If p divides α, then the two values $\lfloor \frac{q}{p} \rfloor p$ and $\lceil \frac{q}{p} \rceil p$ are reached by α. Indeed, for $N = 10 = 2 * 5$, N is a 6-Korselt number and $\lceil \frac{5}{2} \rceil 2 = 6$. Also, N is a 4-Korselt number and $\lfloor \frac{5}{2} \rfloor 2 = 4$.

Corollary 3.6 may provide the following immediate consequence, which is already mentioned in Theorem 3.3 (i).

COROLLARY 3.8. *Let $\alpha \leq 1$ be a nonzero integer and N be a squarefree composite number. If N is an α-Korselt number, then it has at least three prime factors.*

REMARK 3.9. Let $N = p_1 p_2 \dots p_n$ be such that the p_i's are distinct primes, $\alpha \in \mathbb{Z} - \{0\}$ and $d_i = \gcd(\alpha, p_i)$ for all $i \in \{1, 2, \dots, n\}$.

Then N is an α-Korselt number if and only if, for each $i \in \{1, 2, \dots, n\}$, $\frac{p_i - \alpha}{d_i}$ divides $\frac{N}{p_i} - 1$.

PROOF. As $d_i = \gcd(\alpha, p_i)$, we have $\gcd(\frac{p_i}{d_i}, \frac{\alpha}{d_i}) = 1$.

For each $i \in \{1, 2, \dots, n\}$, $p_i - \alpha$ divides $N - \alpha = N - p_i + p_i - \alpha$, that is to say $p_i - \alpha$ divides $N - p_i = p_i(\frac{N}{p_i} - 1)$, which is equivalent to $(\frac{p_i}{d_i} - \frac{\alpha}{d_i})$ divides $\frac{p_i}{d_i}(\frac{N}{p_i} - 1)$.

As $\gcd(\frac{p_i}{d_i}, \frac{\alpha}{d_i}) = 1$, we conclude that $(\frac{p_i}{d_i} - \frac{\alpha}{d_i})$ divides $\frac{p_i}{d_i}(\frac{N}{p_i} - 1)$ if and only if $\frac{p_i - \alpha}{d_i}$ divides $\frac{N}{p_i} - 1$. □

PROPOSITION 3.10. *Let N be a squarefree composite number, α be a nonzero integer, $Q = \gcd(\alpha, N)$ and $P = \frac{N}{Q}$. Let n (resp., n_1) be the number of prime factors of N (resp., P).*

Suppose that N is an α-Korselt number. Then the following properties hold.

(i) $1 \leq n_1 \leq n$.

(ii) *If $n \geq 4$, then $2 \leq n_1 \leq n$.*

PROOF. (i) Straightforward.

(ii) Suppose that $n \geq 4$ and $n_1 = 1$. We will show that this leads to a contradiction. There exists a prime number p such that $N = pQ$. Let $\alpha_1 = \frac{\alpha}{Q}$.

As $p - \alpha$ divides $N - \alpha$, $p - \alpha$ divides $\frac{N}{p} - 1 = Q - 1$, by Remark 3.9.

Hence, there exists an integer k such that $Q - 1 = k(p - \alpha_1 Q)$. Consequently we have $\alpha_1 > 0$ and

$$(Q-1)(1 + k\alpha_1) = k(p - \alpha_1). \tag{3.5}$$

Also, for each prime divisor q of Q, $q-\alpha$ divides $N-\alpha = Q(p-\alpha_1)$. Hence, $1-\frac{\alpha_1 Q}{q}$ divides $\frac{Q}{q}(p-\alpha_1)$. Thus, $\frac{\alpha_1 Q}{q}-1$ divides $p-\alpha_1$. It follows that, according to equation (3.5),

$$\frac{\alpha_1 Q}{q}-1 \text{ divides } \frac{(1+k\alpha_1)}{k}(Q-1).$$

As $Q-1=k(p-\alpha)$, we remark that, if $p<\alpha$, then $k<0$ and if $p>\alpha$, then $k>0$.

In any case, if we let $\varepsilon=\frac{|k|}{k}$, then

$$\frac{\alpha_1 Q}{q}-1 \text{ divides } \frac{k\alpha_1+1}{k}(Q-1)=\frac{|k|\alpha_1+\varepsilon}{|k|}(Q-1). \tag{3.6}$$

Let $q_2,\ q_3,\ \ldots,\ q_n$ be the prime factors of Q with $q_2<q_3<\cdots<q_n$.

By (3.6), $\frac{\alpha_1 Q}{q_i}-1$ divides $\frac{(|k|\alpha_1+\varepsilon)}{|k|}(Q-1)$, for each i.

Thus, $|k|(\frac{\alpha_1 Q}{q_i}-1)$ divides

$$(|k|\alpha_1+\varepsilon)(Q-1)=q_i|k|\Big(\frac{\alpha_1 Q}{q_i}-1\Big)+|k|(q_i-\alpha_1)+\varepsilon(Q-1),$$

which implies that

$$|k|\Big(\frac{\alpha_1 Q}{q_i}-1\Big) \text{ divides } |k|(q_i-\alpha_1)+\varepsilon(Q-1) \quad \text{for each } i. \tag{3.7}$$

Two cases are to be considered.

Case 1: $\varepsilon=-1$ By (3.7), $|k|(\frac{\alpha_1 Q}{q_i}-1)$ divides $|k|(q_i-\alpha_1)-(Q-1)$.

If there exists an i such that $q_i<\alpha_1$, then, $(Q-1)-|k|(q_i-\alpha_1)>0$ and $|k|(\frac{\alpha_1 Q}{q_i}-1)\le (Q-1)-|k|(q_i-\alpha_1)$. This implies that

$$|k|\Big(\frac{\alpha_1 Q}{q_i}-1\Big)-(Q-1)\le |k|(\alpha_1-q_i);$$

so that $\frac{Q}{q_i}\le \frac{|k|(\alpha_1-q_i+1)-1}{|k|\alpha_1-q_i}<1$, which is not possible. Thus $q_i>\alpha_1$ for all i.

Now, suppose that $q_2>\alpha_1$.

First, we claim that $|k|>q_n$. Indeed, by (3.7), $\frac{\alpha_1 Q}{q_2}-1$ divides $\alpha_1|k|(q_2-\alpha_1)-\alpha_1(Q-1)=\alpha_1|k|(q_2-\alpha_1)-\big(q_2(\frac{\alpha_1 Q}{q_2}-1)+q_2-\alpha_1\big)$, which yields that $\frac{\alpha_1 Q}{q_2}-1$ divides $\alpha_1|k|(q_2-\alpha_1)-(q_2-\alpha_1)=(\alpha_1|k|-1)(q_2-\alpha_1)$.

We conclude that $\frac{\alpha_1 Q}{q_2}\le(\alpha_1|k|-1)(q_2-\alpha_1)+1<\alpha_1|k|q_2$. Therefore, $q_3\cdots q_n=\frac{Q}{q_2}<|k|q_2$. As $q_2<q_3$ and $n\ge 4$, we have $q_n<|k|$.

By relation (3.7), we have $|k|(\frac{\alpha_1 Q}{q_i}-1)$ divides $|k|(q_i-\alpha_1)-(Q-1)$, for each i. Again, we consider two cases:

(i) If $|k|(q_2-\alpha_1)-(Q-1)>0$, then, we obtain $\frac{Q}{q_2}\leq\frac{|k|(q_2-\alpha_1+1)+1}{|k|\alpha_1+q_2}<q_2$, which is impossible.
(ii) If $|k|(q_2-\alpha_1)-(Q-1)<0$, then we have

$$\frac{Q}{q_2}\leq\frac{|k|(\alpha_1-q_2+1)-1}{|k|\alpha_1-q_2}<0,$$

which is again not possible.

Case 2: $\varepsilon=1$.

Suppose that there is an i such that $q_i<\alpha_1$. By relation (3.7), $k(\frac{\alpha_1 Q}{q_i}-1)$ divides $k(q_i-\alpha_1)+(Q-1)$. We consider two cases:
(i) If $k(q_i-\alpha_1)+(Q-1)>0$, then we obtain

$$\frac{Q}{q_i}\leq\frac{k(q_i-\alpha_1+1)-1}{k\alpha_1-q_i}<0,$$

which is impossible.
(ii) If $k(q_i-\alpha_1)+(Q-1)<0$, then we get

$$\frac{Q}{q_i}\leq\frac{k(\alpha_1-q_i+1)+1}{k\alpha_1+q_i}<1,$$

which is again not possible. Thus $q_i\geq\alpha_1$ for all i.

Suppose that $q_2>\alpha_1$.

First, we claim that $k\geq q_n$. In fact, by relation (3.7) we have that $\frac{\alpha_1 Q}{q_2}-1$ divides $k(q_2-\alpha_1)+(Q-1)$.

This implies that $\frac{\alpha_1 Q}{q_2}-1$ divides

$$\alpha_1 k(q_2-\alpha_1)+\alpha_1(Q-1)=\alpha_1 k(q_2-\alpha_1)+q_2\Big(\frac{\alpha_1 Q}{q_2}-1\Big)+(q_2-\alpha_1),$$

which yields that $\frac{\alpha_1 Q}{q_2}-1$ divides $\alpha_1 k(q_2-\alpha_1)+(q_2-\alpha_1)=(\alpha_1 k+1)(q_2-\alpha_1)$. This implies that $\frac{\alpha_1 Q}{q_2}-1\leq(\alpha_1 k+1)(q_2-\alpha_1)$. Hence, $\frac{\alpha_1 Q}{q_2}-1+(\alpha_1 k+1)\alpha_1\leq(\alpha_1 k+1)q_2$. Thus, $\frac{\alpha_1 Q}{q_2}<(\alpha_1 k+1)q_2$, which leads to

$$q_3\cdots q_n=\frac{Q}{q_2}<\frac{\alpha_1 k+1}{\alpha_1}q_2. \tag{3.8}$$

As $q_2<q_3$ and $n\geq 4$, we have $q_n\leq k$.

Relation (3.7) gives $k(\frac{\alpha_1 Q}{q_2}-1)$ divides $k(q_2-\alpha_1)+(Q-1)$, which implies that

$$\frac{Q}{q_2}\leq\frac{k(q_2-\alpha_1+1)-1}{k\alpha_1-q_2}. \tag{3.9}$$

If $\alpha_1 = 1$, then (3.9) gives $\frac{Q}{q_2} \leq \frac{kq_2-1}{k-q_2}$ which implies that $k \leq \frac{Q-1}{\frac{Q}{q_2}-q_2}$ and by equation (3.8) we obtain

$$\begin{aligned}\frac{Q}{q_2} < (k+1)q_2 &\leq \Big[\frac{Q-1}{\frac{Q}{q_2}-q_2}+1\Big]q_2 < \Big[\frac{Q}{\frac{Q}{q_2}-q_2}+1\Big]q_2 \\ &= \frac{Qq_2^2}{Q-q_2^2}+q_2.\end{aligned}$$

But, as $\frac{Qq_2^2}{Q-q_2^2} < q_2(q_2+1)$, we get

$$\frac{Q}{q_2} = q_3q_4\cdots q_n < q_2(q_2+1)+q_2 = q_2(q_2+2),$$

which is not possible.

Suppose that $\alpha_1 > 1$.

As $k(q_2-\alpha_1+1)-1-(k\alpha_1-q_2)q_2 = -(q_2+1)\big(k(\alpha_1-1)-q_2+1\big) < 0$, we have $\frac{k(q_2-\alpha_1+1)-1}{k\alpha_1-q_2} < q_2$. And by equation (3.9) we obtain $\frac{Q}{q_2} < q_2$, which is impossible.

Finally, we conclude that, if $N = PQ$ and $\alpha = \alpha_1 Q$ such that N is an α-Korselt number and has $n \geq 4$ prime factors, then P has at least two prime factors. □

Examples 3.11. Here we conserve the same notation as in Proposition 3.10.

(i) The following examples show that, for $n \in \{2,3\}$, n_1 may reach all values in $\{1,\ldots,n\}$.
   - Let $N = 10 = 2*5$; then N is a 4-Korselt number, $P = 5$ and $n_1 = 1$.
   - Let $N = 15 = 3*5$; then N is a 7-Korselt number, $P = N$ and $n_1 = n = 2$.
   - Let $N = 30 = 2*3*5$; then N is a 6-Korselt number, $P = 5$ and $n_1 = 1$.
   - Let $N = 273 = 3*7*13$; then N is a (-7)-Korselt number, $P = 3*17$ and $n_1 = 2$.
   - Let $N = 3913 = 7*13*43$; then N is a (-2)-Korselt number, $P = N$ and $n_1 = n = 3$.

(ii) For $N = 5530 = 2*5*7*79 = P*Q$ with $P = 553 = 7*79$ and $\alpha = Q = 10 = 2*5$. Then N is an α-Korselt number and $n_1 = 2$.

The next proposition gives an improvement of the inequalities (i) in Proposition 3.4 whenever $\gcd(N,\alpha) > 1$.

Proposition 3.12. *Let N be a squarefree composite number. Let $\alpha \in \mathbb{Z} - \{0\}$. Set $Q = \gcd(\alpha, N)$, $P = \frac{N}{Q}$ and $\alpha_1 = \frac{\alpha}{Q}$. Let p be a prime factor of P and $R = \frac{P}{p}$. Suppose that N is an α-Korselt number and $Q > 1$. Then the following properties hold.*

(1) $\frac{2Qp-N}{2Q-1} \leq \alpha \leq \frac{Qp+N}{Q+1}$.
(2) *If $N \neq 6$ and the number of prime factors of N is distinct from 3, then the following are satisfied:*
   (a) $\frac{2Qp-N}{2Q-1} \leq \alpha \leq \frac{2Qp+N}{2Q+1}$.
   (b) *Let p_1 and r_1 be respectively the smallest and the largest prime factors of P and $R_1 = \frac{P}{r_1}$. Then we have*
      (i) $\frac{2Qr_1-N}{2Q-1} \leq \alpha \leq \frac{2Qp_1+N}{2Q+1}$.
      (ii) $\alpha_1 \in \{\lceil \frac{r_1}{Q} \rceil + j, -R_1 \leq j \leq R_1 - 1\}$.

PROOF. (1) If N has two prime factors, then the result follows from Proposition 3.4 and Remark 3.5.

Suppose that N has more than or equal to 3 prime factors.

As N is squarefree, we have $\gcd(P, Q) = 1$.

Since N is an α-Korselt number, $p - \alpha$ divides $N - \alpha = Q(\frac{N}{Q} - \frac{\alpha}{Q})$. Hence, as $\gcd(p - \alpha, Q) = \gcd(p, Q) = 1$, $p - \alpha$ divides $\frac{N-\alpha}{Q}$.

Thus, there exists a nonzero integer k such that $p - \alpha = \frac{N-\alpha}{kQ}$. This leads to the equality $Qp(k - R) = \alpha(kQ - 1)$, which gives

$$p(k - R) = \alpha_1(kQ - 1). \tag{3.10}$$

We claim that $k \neq 1$. Indeed, let us suppose that it is not the case.

By equation (3.10), we get $p(1 - R) = \alpha_1(Q - 1)$, so that $R \neq 1$ and $\alpha < 0$.

Let r be a prime factor of R. As $\gcd(\alpha, P) = 1$, then $\gcd(\alpha, p) = 1$, we deduce that p divides $Q - 1$, which implies that

$$p < Q. \tag{3.11}$$

As in the beginning of the proof, replacing p by r, there exists a nonzero positive integer l such that $r - \alpha = \frac{N-\alpha}{lQ}$. Clearly, we have $l \neq 1$ (since $r \neq p$). Hence, $r - \alpha \leq \frac{N-\alpha}{2Q} = \frac{p-\alpha}{2}$. This gives $r - p \leq \alpha - r$. Thus, as $-p < r - p$ and $\alpha - r < \alpha < -Q$, we get $-p < -Q$. Consequently, $p > Q$, contradicting inequality (3.11). Thus $k \neq 1$.

This gives

$$-\frac{N - \alpha}{Q} \leq p - \alpha \leq \frac{N - \alpha}{2Q}$$

which leads to

$$\frac{2Qp - N}{2Q - 1} \leq \alpha \leq \frac{Qp + N}{Q + 1}.$$

(2) Now, suppose that N has more than or equal to 4 prime factors. Then by Proposition 3.10, P has more than or equal to 2 prime factors.

(a) We claim that, in equation (3.10), $k \neq -1$. Indeed, let us assume that $k = -1$. Then equation (3.10) becomes $p(1 + R) = \alpha_1(Q + 1)$; so that $\alpha > 0$.

Let r be a prime factor of R. Then there exists a nonzero integer l such that $r-\alpha = \frac{N-\alpha}{lQ}$. Of course, $l \neq -1$ since $r \neq p$; which leads to $r-\alpha \geq -\frac{N-\alpha}{2Q} = \frac{p-\alpha}{2}$. It follows that

$$r > \frac{\alpha}{2}. \tag{3.12}$$

As $\alpha_1(Q+1) = p(1+R) > pR > pr$ and by inequality (3.12), we obtain $\alpha_1(Q+1) > \frac{\alpha p}{2} = \frac{\alpha_1 Q p}{2}$, which implies that $Q(\frac{p}{2}-1) < 1$. Since, in addition, $Q \geq 2$ and p is prime, we get necessarily $p = 2$. Thus, $N = 2RQ$.

Let q be a prime factor of Q. Then $q - \alpha$ divides $N - \alpha = Q(P - \alpha_1) = Q(2R - \alpha_1)$. This implies that $1 - \frac{\alpha}{q}$ divides $\frac{Q}{q}(2R - \alpha_1)$. As $1 = \gcd(\alpha, P) = \gcd(\alpha_1, p) = \gcd(\alpha_1, 2)$, α_1 is odd. Then, since N is squarefree, $\frac{Q}{q}(2R - \alpha_1)$ is odd and $1 - \frac{\alpha}{q} = 1 - \alpha_1\frac{Q}{q}$ is even, contradicting the fact that $1 - \frac{\alpha}{q}$ divides $\frac{Q}{q}(2R - \alpha_1)$.

We conclude that $k \neq -1$; and accordingly

$$-\frac{N-\alpha}{2Q} \leq p - \alpha \leq \frac{N-\alpha}{2Q}$$

which implies that

$$\frac{2Qp - N}{2Q-1} \leq \alpha \leq \frac{2Qp+N}{2Q+1},$$

for each prime divisor p of P.

(b) (i) This is an immediate consequence of (a).

(ii) By Proposition 3.4, we have $r_1 - \frac{N}{r_1} + 1 \leq \alpha \leq r_1 + \frac{N}{r_1} - 1$. Since $\alpha = \alpha_1 Q$, $N = PQ$, and $P = r_1 R_1$, then dividing by Q, we obtain $|\alpha_1 - \frac{r_1}{Q}| \leq R_1 - \frac{1}{Q} < R_1$. This implies that

$$\alpha_1 \in \Big\{ \Big\lceil \frac{r_1}{Q} \Big\rceil + j \;\Big|\; -R_1 \leq j \leq R_1 - 1 \Big\}. \qquad \square$$

Remark 3.13. This remark is related to the restrictions of Proposition 3.12 ($N = 6$ and $n = 3$).

– For $N = 6$, N is an α-Korselt number (with $\alpha = 4$) and

$$\frac{2Qp+N}{2Q+1} = \frac{18}{5} < \alpha = 4.$$

– For $N = 2 * 5 * 11$, N is a 20-Korselt number and

$$\frac{2Qp+N}{2Q+1} = \frac{110}{7} < \alpha = 20.$$

Corollary 3.14. *Let N be a squarefree composite number, $\alpha \in \mathbb{Z} - \{0\}$, and $Q = \gcd(\alpha, N)$ such that $\alpha \equiv 0 \pmod{Q}$. Suppose that $N = 2pQ$, with p an odd prime number and $3p < Q$. Then N is not an α-Korselt number.*

PROOF. Suppose N is an α-Korselt number. Then, according to Proposition 3.12, we have:

$$0 = \frac{2pQ - N}{2Q - 1} \leq \alpha \leq \frac{pQ + N}{Q + 1} = \frac{3pQ}{Q + 1} < 3p,$$

which implies that $0 < \alpha < 3p < Q$. As Q divides α, we obtain a contradiction. □

4. **Numbers with empty Korselt set.** The main result of this work is the following theorem.

THEOREM 4.1. *Let $n \geq 2$ be an integer. Let $p_1, p_2, \ldots, p_n$ be fixed distinct prime numbers. Then there exists an integer q_0 such that, for each prime number $q > q_0$, $N := p_1 p_2 \cdots p_n q$ has an empty Korselt set.*

PROOF. Let $P_1 = p_1 p_2 \cdots p_n$, q be a prime number such that q is greater than $\max\{p_1, p_2, \ldots, p_n\}$, and $N = P_1 q$. Let $\alpha \in \mathbb{Z}$ be such that N is an α-Korselt number, $Q := \gcd(\alpha, N)$, and $N = PQ$. Then, we consider two cases.

First case: Suppose that q does not divide Q. Then, by Proposition 3.4, we have

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

which means that

$$1 - P_1 = 1 - \frac{N}{q} \leq \alpha - q \leq \frac{N}{q} - 1 = P_1 - 1,$$

so $\alpha = q + i$ such that $i \in \{1 - P_1, 2 - P_1, \ldots, P_1 - 2, P_1 - 1\}$.

We have $p_j - \alpha = p_j - q - i$ divides $N - \alpha = P_1 q - q - i$, this gives $p_j - q - i$ divides $(P_1 - 1)(q + i - p_j) + (p_j - i)(P_1 - 1) - i$. It follows that $q + i - p_j$ divides $(p_j - i)(P_1 - 1) - i$.

Then, $q + i - p_j \leq |(p_j - i)(P_1 - 1) - i| \leq |i| P_1 + p_j (P_1 - 1)$. Thus, we get

$$q \leq |i|(P_1 + 1) + p_j P_1 \leq (P_1 - 1)(P_1 + 1) + p_j P_1 \leq 2P_1^2 - 1. \tag{4.1}$$

Second case: Suppose that q divides Q. Let $\alpha = \alpha_1 Q$ and p_j such that $\gcd(p_j, \alpha) = 1$; by Proposition 3.12, we have

$$\frac{2Qp_j - N}{2Q - 1} \leq \alpha \leq \frac{Qp_j + N}{Q + 1}.$$

This gives

$$\frac{2p_j - P}{2Q - 1} \leq \alpha_1 \leq \frac{p_j + P}{Q + 1}.$$

As P divides P_1, we get

$$-\frac{P_1}{2Q-1} \leq -\frac{P}{2Q-1} < \alpha_1 < \frac{p_j+P}{Q} < \frac{2P}{Q} \leq \frac{2P_1}{Q}. \tag{4.2}$$

Now, if we let q be a prime number such that $q > 2P_1^2 - 1$, then inequalities (4.1) and (4.2) do not hold. Indeed, under this assumption we have $-1 < \alpha_1 < 1$, which implies that $\alpha_1 = 0$, contradicting the fact that $\alpha \neq 0$.

So, for each prime number $q > 2P_1^2 - 1$, $N = P_1 q$ has an empty Korselt set. □

Acknowledgement. The authors thank the referee for his comments. Al-Rasasi and Echi would like to thank King Fahd University of Petroleum and Minerals (Saudi Arabia) for its support (IN100026).

References

1. W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*. Ann. of Math. **139** (1994), 703–722.
2. 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.
3. K. Bouallegue, O. Echi, and R. Pinch, *Korselt Numbers and Sets*. Internat. J. Number Theory **6** (2010), 257–269.
4. R. D. Carmichael, *Note on a new number theory function*. Bull. Amer. Math. Soc. **16** (1910), 232–238.
5. 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.
6. O. Echi, *Williams Numbers*. C. R. Math. Acad. Sci. Soc. R. Can. **29** (2007), 41–47.
7. G. Harman, *Watt's mean value theorem and Carmichael numbers*. Internat. J. Number Theory **4** (2008), 241–248.
8. A. Korselt, *Problème chinois*. L'intermédiaire des mathématiciens **6** (1899), 142–143.

King Fahd University of Petroleum and Minerals, Department of Mathematics and Statistics
PO Box 5046, Dhahran 31261, Saudi Arabia
e-mail: irasasi@kfupm.edu.sa

King Fahd University of Petroleum and Minerals, Department of Mathematics and Statistics
PO Box 5046, Dhahran 31261, Saudi Arabia
e-mail: echi@kfupm.edu.sa
othechi@yahoo.com

Umm Al-Qura University, University College in Makkah, Department of Mathematics, Azizia
PO.Box 2064, Makkah, Kingdom of Saudi Arabia
e-mail: naghanmi@uqu.edu.sa
neghanmi@yahoo.fr