

WILLIAMS NUMBERS

OTHMAN ECHI

ABSTRACT. Let N be a composite squarefree number; N is said to be a Carmichael number if $p - 1$ divides $N - 1$ for each prime divisor p of N . In [On numbers analogous to the Carmichael numbers, *Canad. Math. Bull.* 20(1977), 133 – 143], Williams (H.C) has stated an interesting problem of whether there exists a Carmichael number N such that $p + 1$ divides $N + 1$ for each prime divisor p of N . This is a long standing open question; and it is possible that there is no such number.

For a given nonzero integer a , we call N an a -Korselt number if N is composite, squarefree and $p - a$ divides $N - a$ for all primes p dividing N . We will say that N is an a -Williams number if N is both an a -Korselt number and a $(-a)$ -Korselt number.

Extending the problem of Williams, one may ask more generally, the following:

For a given nonzero integer a , is there an a -Williams number?

We give an affirmative answer to the above problem, for $a = 3p$, where p is a prime number such that $3p - 2$ and $3p + 2$ are primes. We, also, prove that each a -Williams number has at least three prime factors.

RÉSUMÉ. Soit N un nombre composé et sans facteur carré; N est dit un nombre de Carmichael si $p - 1$ divise $N - 1$ pour tout diviseur premier p de N . Dans [On numbers analogous to the Carmichael numbers, *Canad. Math. Bull.* 20(1977), 133 – 143], Williams (H.C) a posé un problème concernant l'existence d'un nombre de Carmichael N tel que $p + 1$ divise $N + 1$ pour tout diviseur premier p de N . C'est donc un ancien problème; et il se peut qu'il n'existe pas de tel nombre.

Pour un entier naturel non nul a , on dit que N est un nombre a -Korselt si N est composé, sans facteur carré et $p - a$ divise $N - a$ pour tout diviseur premier p de N . On dira que N est un nombre a -Williams si N est à la fois a -Korselt et $(-a)$ -Korselt.

On a, alors, le problème suivant:

Pour un entier naturel non nul a , existe-t-il un nombre a -Williams?

On donne une réponse affirmative à ce problème, dans le cas où $a = 3p$, où p est un nombre premier tel que $3p - 2$ et $3p + 2$ sont premiers. On montre aussi que tout nombre a -Williams possède au moins 3 facteurs premiers.

INTRODUCTION

A composite number N such that $a^{N-1} \equiv 1 \pmod{N}$ and $\gcd(a, N) = 1$ is called a *pseudoprime to the base a* . This N is called an *absolute pseudoprime* or *Carmichael number* if it is pseudo prime for all bases a with $\gcd(a, N) = 1$. These numbers were first described by Robert Carmichael in 1910. The term Carmichael number was introduced by Beeger [2] in 1950. The smallest number of this kind is $N = 3.11.17 = 561$.

Considerable progress has been made investigating Carmichael numbers in the past several years.

In 1994, Alford, Granville and Pomerance showed, in a remarkable paper [1], that there are infinitely many Carmichael numbers.

Carmichael numbers meet the following criterion,

2000 *Mathematics Subject Classification*. Primary 11Y16; Secondary 11Y11, 11A51.

Key words and phrases. Prime number, Carmichael number, squarefree composite number.

“Korselt’s criterion (1899): A composite odd number N is a Carmichael number if and only if N is squarefree and $p - 1$ divides $N - 1$ for every prime p dividing N .”

For a given nonzero integer a , we call N an a -Korselt number if N is composite, square-free and $p - a$ divides $N - a$ for all primes p dividing N .

Note that the concept of a -Korselt number have been introduced and studied by Echi, Pinch and Bouallègue (in a preprint; not yet published).

Let N be a composite squarefree number. The first section of this short note deals with the set of all $a \in \mathbb{Z} \setminus \{0\}$, for which N is an a -Korselt number.

In [7], Williams has stated the problem of whether there exists a Carmichael number N such that $p + 1$ divides $N + 1$ for each prime divisor p of N . This is a long standing open question; and it is possible that there is no such number.

For any given non-zero-integer a , we say that N is an a -Williams number if N is both an a -Korselt number and a $(-a)$ -Korselt number. We are interested in determining whether there are any a -Williams numbers, and state and prove some results in Section 2.

1. KORSELT NUMBERS

Proposition 1.1. *Let q be the largest prime factor of an a -Korselt number N . Then*

$$2q - N \leq a \leq \frac{3N}{4}.$$

Proof. Suppose that $a < 0$. Then there exists an integer $k \in \mathbb{N}$ such that $N - a = k(q - a)$. Since $N > q$, we have $k \geq 2$. Hence, $N - a = k(q - a) \geq 2(q - a)$. Thus, $N \geq 2q - a$.

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

Now, let us show that $a \leq \frac{3N}{4}$. Let p be a prime factor of N . Then $p - a$ divides $N - a$. Set $d := p - a$; then $N \geq 2p = 2(a + d)$ (since p divides N and $N > p$). Thus $a \leq (N - a) - 2d$.

On the other hand, d divides $N - a$ and $a \leq N$ imply that $-d \leq N - a$, this yields $a \leq 3(N - a)$; and accordingly $a \leq \frac{3N}{4}$. \square

Corollary 1.2. *If N is an a -Korselt number, then a is never $N - 3$ or $N - 5$.*

Proof. Suppose that $a = N - 3$. Then $N \leq 12$, by Proposition 1.1. Hence $N = 6$, since N is squarefree. It follows that 6 is an $(N - 3)$ -Korselt number; which is not true.

Now, Suppose that $a = N - 5$. Then $N \leq 20$, by Proposition 1.1. Hence $N \in \{6, 10, 14, 15\}$, since N is squarefree; which is not true, for the simple reason that 6 is not a 1-Korselt number, 10 is not a 5-Korselt number, 14 is not a 9-Korselt number, and 15 is not a 10-Korselt number. \square

Proposition 1.3. *Let N be a squarefree composite number. Then*

$$\{a \in \mathbb{Z} \setminus \{0\} : N \text{ is an } a\text{-Korselt number}\} = \bigcap_{\substack{p|N \\ p \text{ prime}}} \{p - d : d \text{ divides } N - p\}.$$

Proof.

– Suppose that N is an a -Korselt number. Let p be a prime dividing N . Then $d := p - a$ divides $N - a$; so that d divides $N - p$ (since $N - p = N - a - d$). Thus

$$a \in \bigcap_{\substack{p|N \\ p \text{ prime}}} \{p - d : d \text{ divides } N - p\}.$$

– Conversely, let $a \in \bigcap_{\substack{p|N \\ p \text{ prime}}} \{p - d : d \text{ divides } N - p\}$; then for each prime p dividing N , there exists a divisor d of $N - p$ such that $a = p - d$. Hence, $p - a = d$ divides $N - a = N - p + d$. Therefore, N is an a -Korselt number. \square

Now, the following corollary is an immediate consequence of Proposition 1.3 (it is also a consequence of Proposition 1.1).

Corollary 1.4. *For any given integer N , there are only finitely many integers a for which N is an a -Korselt number.*

Next, we give some comments on Proposition 1.1.

Remarks 1.5.

(a) The upper bound $\lfloor \frac{3N}{4} \rfloor$ of the inequality in Proposition 1.1 is attained for $N = 6$.

We do not know whether this upper bound is attained for another value of N .

(b) The lower bound in Proposition 1.1 is never attained. Indeed, suppose that $a = 2q - N$. As N is composite, $N \neq q$. Also, $N \neq 2q$ else $a = 0$ which is impossible. Therefore, $N = rq$ where $r \geq 3$, and so $a = -(r - 2)q$ is < 0 .

If p is a prime factor of r , then $p - a = p + (r - 2)q$ divides $N - a = q(2r - 2)$. Now, $\gcd(p + (r - 2)q, q) = \gcd(p, q) = 1$ and so $p + (r - 2)q$ divides $2r - 2$. Thus, $2r - 2 = 2 + (r - 2)2 \leq p + (r - 2)q \leq 2r - 2$. But, since $q > p \geq 2$, we have $p + (r - 2)q > 2 + (r - 2)2 = 2r - 2$, a contradiction.

(c) Corollary 1.2 provides examples of integers $1 \leq i$ such that for each squarefree composite number N satisfying the inequality $i \leq N \leq 4i$, N is not an $(N - i)$ -Korselt number. The only such integers i (up to 100) are: 1, 3, 5, 7, 13, 14, 17, 19, 21, 23, 25, 31, 33, 34, 35, 37, 38, 39, 41, 43, 47, 49, 51, 53, 55, 57, 59, 61, 62, 67, 71, 73, 74, 76, 79, 83, 85, 86, 87, 89, 91, 93, 94, 95, 97, 98.

Of course, one may write an easy computer program which detects all such integers i up to a given integer A .

2. WILLIAMS NUMBERS

Theorem 2.1. *Let p be a prime number such that $3p - 2$ and $3p + 2$ are primes. Let $N = p(3p - 2)(3p + 2)$ and $a \in \{-3p, 3p, 5p\}$; then N is an a -Korselt number. In particular, N is a $(3p)$ -Williams number.*

Proof. First, remark that p is an odd prime number.

– Let $a := 3p$ and $N = p(3p - 2)(3p + 2)$. Then, $N - a = p(9p^2 - 7)$. Hence, $2p$ divides $N - a$. Thus, N is an a -Korselt number.

– Now, let us show that N is a $(-a)$ -Korselt number. Indeed, we have $N + a = p[9p^2 - 1] = p(3p - 1)(3p + 1)$. Since $3p - 1$ and $3p + 1$ are even, $4p$ divides $N + a$; that is $p + a$ divides $N + a$. On the other hand, $(3p - 2) + a = 2(3p - 1)$ and $(3p + 2) + a = 2(3p + 1)$; so that $N + a$ is a multiple of the numbers $(3p - 2) + a$ and $(3p + 2) + a$.

– It remains to prove that N is a $(5p)$ -Korselt number. Indeed, $N - 5p = 9p(p-1)(p+1)$; $p - 1 \equiv 0 \pmod{2}$ and $p + 1 \equiv 0 \pmod{2}$. So that $p - 5p$ divides $N - 5p$.

On the other hand, $(3p - 2) - 5p = -2(p + 1)$ and $(3p + 2) - 5p = -2(p - 1)$; hence $(3p - 2) - 5p$ and $(3p + 2) - 5p$ divide $N - 5p$. \square

Examples 2.2. An easy computer program gives us the following data:

List of squarefree composite numbers N (up to 10^8) such that there exists an $a \in \mathbb{Z} \setminus \{0\}$ for which N is an a -Williams number.

N	Prime factorization of N	Integers a such that N is an a -Korselt Number
231	3.7.11	-9, 6, 9, 15
1105	5.13.17	-15, 1, 9, 15, 16, 25
3059	7.19.23	-21, 11, 21, 35
19721	13.37.41	-39, 9, 39, 65
109411	23.67.71	-69, 64, 69, 115
455729	37.109.113	-111, 111, 185
715391	43.127.131	-129, 129, 215
9834131	103.307.311	-309, 309, 515
18434939	127.379.383	-381, 381, 635
38976071	163.487.491	-489, 489, 815
41916499	167.499.503	-501, 501, 835

Williams has observed that, if there exists a squarefree composite number N such that $p - 1$ divides $N - 1$ and $p + 1$ divides $N + 1$ for each prime factor p of N , then N must have an odd number ≥ 5 of prime factors [7, Page 142]. In the general case, Corollary 2.4 asserts that, if N is an a -Williams number, then it has at least three prime factors.

Theorem 2.3. *Let b be a positive integer or -1 . If N is composite, squarefree and $p + b$ divides $N + b$ for all primes p dividing N (that is, N is a $(-b)$ -Korselt number), then N has at least three prime factors.*

Proof. We break the proof into three steps.

Step 1. Let $a \in \mathbb{Z} \setminus \{0\}$ and N be an a -Korselt number such that $\gcd(N, a) = 1$. If p is a prime dividing N , then $N \equiv p \pmod{p(p-a)}$ (extracted from [5]).

Let $\beta \in \mathbb{Z}$ such that $N - a = (p - a)\beta$. Then $N - p = (p - a)(\beta - 1)$. This forces p to divide $(p - a)(\beta - 1)$. But, since $\gcd(a, N) = 1$, we conclude that p divides $\beta - 1$. Thus $p(p - a)$ divides $N - p$; that is to say, $N \equiv p \pmod{p(p - a)}$.

Step 2. If $a \leq 1$ is an integer and N is an a -Korselt number such that $\gcd(N, a) = 1$, then N has at least three prime factors (extracted from [5]).

Suppose that $N = pq$ such that $p < q$ are primes. By Step 1, $N \equiv q \pmod{q(q - a)}$; hence $N \geq q + q(q - a) \geq q + q(q - 1) = q^2$. This yields $p \geq q$, a contradiction, completing the proof of Step 2.

As a consequence of Step 2, each Carmichael number (resp., (-1) -Korselt number) has at least three prime factors.

Thus we may suppose that $b \geq 2$.

Step 3. If $b \geq 2$, then there is no $(-b)$ -Korselt number with exactly two prime factors.

Suppose that there exists $N = pq$, with p, q are distinct primes and $p + b, q + b$ dividing $N + b$. Then, according to Step 2, $\gcd(N, b) \neq 1$. Thus, we may suppose, without loss of generality, that p divides b .

Let us write $b = pt$, where t is a nonzero positive integer.

The fact that $p + b (= p(1 + t))$ divides $N + b (= p(q + t))$ implies that $1 + t$ divides $q + t$. Hence, $q + t \equiv 0 \pmod{(1 + t)}$; and consequently, we get the congruence

$$(C_q) : q \equiv 1 \pmod{(1 + t)}.$$

On the other hand, $q + b$ divides $N + b [= p(q + b) + b(p - 1)]$. This implies that $q + b$ divides $p(p - 1)t$. But, since $\gcd(q + b, p) = 1$, we conclude that $q + b$ divides $(p - 1)t$.

We claim that $\gcd(q + b, t) = 1$. Indeed, if it is not the case, we get $\gcd(q + b, t) = q$; so that q divides t . Thus, there exists $s \in \mathbb{N} \setminus \{0\}$ such that $t = qs$. According to Congruence (C_q) , we have $q \geq 1 + (1 + t) = 2 + qs$, which is not true. It follows that $\gcd(q + b, t) = 1$.

As a consequence of the previous claim, $q + b$ divides $p - 1$. But, $q + b = q + pt = q + (p - 1)t + t$; which forces $q + b$ to divide $q + t$. Therefore, $q + pt$ divides $q + t$, which is impossible, since $q + t < q + pt$. \square

Corollary 2.4. *Let N be a squarefree composite number and α a nonzero integer. If N is an α -Williams number, then N has at least three prime factors.*

A Carmichael number has at least three prime factors, but a Korselt one may have exactly two prime factors, as shown by the following proposition (which is extracted from [5]).

Proposition 2.5. *Let p, q be any odd distinct primes and $a = p + q - 1$. Then $n = pq$ is an a -Korselt number.*

Proof. Just write $n - a = pq - p - q + 1 = (p - 1)(q - 1)$ and this is divisible by $p - a = -(q - 1)$ and by $q - a = -(p - 1)$. \square

Corollary 2.6. *If Goldbach's conjecture is true (that is, if every even integer ≥ 8 can be written as the sum of two distinct primes), then for each odd integer $a > 1$, there is an a -Korselt number with two prime factors (just apply Proposition 2.5).*

However, there are even integers $a > 1$ such that there is no a -Korselt number with two prime factors (see Example 2.8).

The following result deals with Korselt numbers with two prime factors.

Theorem 2.7 ([5]). *Let $a > 1$ be an integer, $p < q$ be two prime numbers and $N = pq$. If N is an a -Korselt number, then $p < q \leq 4a - 3$. In particular, there are only finitely many a -Korselt numbers with exactly two prime factors.*

Proof. We may assume that $q > 2a$ else we are done. Therefore, $\gcd(q - a, a) = \gcd(q, a) \leq a < q$ and divides q , so must equal 1. Now $q - a$ divides $(N - a) - p(q - a) = (p - 1)a$ so that $q - a$ divides $p - 1$ (as $\gcd(q - a, a) = 1$). Therefore, $q - a = p - 1$ else $q - a \leq (p - 1)/2 \leq q/2 - 1$, which contradicts the fact that $q > 2a$. Now, $p - a$ divides $(N - a) - (p - a)(p + 2a - 1) = 2a(a - 1)$. Clearly, p does not divide a , else $q = p + a - 1 \leq 2a - 1$ a contradiction, and so $\gcd(p - a, a) = \gcd(p, a) = 1$, which implies that $p - a$ divides $2(a - 1)$. Hence $q = p + a - 1 \leq 4a - 3$. \square

It is easy to write a computer program listing integers a less than or equal to a given integer; and for which there are no a -Korselt number with two prime factors.

Example 2.8. The values of a up to 1000 for which there are no a -Korselt number with two prime factors are 1, 2, 250, 330, 378, 472, 516, 546 and 896.

Remark 2.9. The upper bound of Theorem 2.7 cannot be improved. For, if $p = 3a - 2$ and $q = 4a - 3$ are both primes (for example, $a = 5$, $p = 13$, $q = 17$) and $N = pq$, then $lcm(p - a, q - a) = lcm(2a - 2, 3a - 3) = 6(a - 1)$ divides $N - a = pq - a = 6(a - 1)(2a - 1)$.

In fact the prime k -tuplets conjecture implies that there are infinitely many prime pairs of the form $3a - 2$, $4a - 3$.

Following the heuristic ideas of Erdos, which inspired the proof that there are infinitely many Carmichael numbers [1], we believe that there are infinitely many a -Korselt numbers, for all nonzero integers a . The proof of [1] does not seem to be easily modified to obtain this result.

The prime k -tuplets conjecture suggests that there are infinitely many primes triplets p , $3p - 2$, $3p + 2$, so we believe that there should be infinitely many examples of a -Williams numbers as in Theorem 2.1. Following the calculations described in Examples 2.2, it could be that the examples described in Theorem 2.1 provide the only examples of a -Williams numbers.

Acknowledgement. The author gratefully acknowledges the detailed referee report that helped to improve both the presentation and the mathematical content of this paper. The author thanks the referee for communicating to him Proposition 1.3, Remark 2.9 and shortening the proof of Theorem 2.7.

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] R. D. Carmichael, *Note on a new number theory function*. Bull. Amer.Math. Soc. **16**(1910), 232 – 238.
- [4] 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.
- [5] O. Echi, R. Pinch, K. Bouallegue, *Korselt numbers*. Preprint.
- [6] A. Korselt, *Problème chinois*, L'intermédiaire des Mathématiciens **6**(1899), 142 – 143.
- [7] H. C. Williams, *On numbers analogous to the Carmichael numbers*. Canad. Math. Bull. **20**(1977), 133 – 143.

DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCES OF TUNIS. UNIVERSITY OF TUNIS-EL MANAR “CAMPUS UNIVERSITAIRE” 2092 TUNIS, TUNISIA.

E-mail address: othechi@yahoo.com and othechi@math.com