International Journal of Number Theory

The Korselt Set of a Power of a Prime

Liyuan Wang
School of Mathematics and Statistics, Wuhan University
Wuhan 430072, China
2014202010017@whu.edu.cn

Received (Day Month Year)
Accepted (Day Month Year)

A Carmichael number is a composite number n such that n divides $a^{n-1}-1$ for all integers a coprime to n. Korselt discovered that n is a Carmichael number if and only if n is square-free and $p-1 \mid n-1$ for each prime divisor p of n. Let $\alpha \in \mathbb{Z}\backslash\{0\}$, a K_α-number is defined to be a composite number N, such that $N \neq \alpha$ and $p-\alpha \mid N-\alpha$ for each prime $p \mid N$. The set of all $\alpha \in \mathbb{Z}\backslash\{0\}$ such that N is a K_α-number is called the *Korselt set* of N and we denote this set by $\mathcal{KS}(N)$. In this paper, we investigate some properties of $\mathcal{KS}(N)$ when N is a power of a prime.

Keywords: Korselt's Criterion; Korselt set; Williams numbers; prime number.

Mathematics Subject Classification 2010: 11xxx, 11xxx, 11xxx

1. Introduction

Fermat's little theorem states that if p is a prime, then $a^{p-1} \equiv 1 \pmod{p}$ for each integer a coprime to p. The converse of this theorem is very interesting: If $n \geq 2$ is an integer and $a^{n-1} \equiv 1 \pmod{n}$ for every a coprime to n, does n has to be a prime? Actually, n is not necessarily a prime. In 1910, Carmichael found the first and smallest such number: $561 = 3 \cdot 11 \cdot 17$(see [5]), which explains the name "Carmichael number".

Carmichael's method of searching for Carmichael number is based on Korselt's Criterion, which states that n is a Carmichael number if and only if n is square-free and $p-1 \mid n-1$ for all prime divisors of n. However, Korselt did not give any example in his paper[8]. Carmichael conjectured in 1912 that there are infinitely many Carmichael numbers, which was not confirmed until 1994 when Alford-Granville-Pomerance published their remarkable paper[1]. Indeed, if $C(x)$ denotes the number of Carmichael number less than or equal to x, in their paper they proved that for sufficiently large x, $C(x) > x^{\frac{2}{7}}$.

Inspired by Korselt's Criterion, O. Echi and R. Pinch introduced the concept of K_α-number and *Korselt set*. In [3], they gave the following definition.

Definition 1.1. *Let $N \in \mathbb{N}$ be a composite number and $\alpha \in \mathbb{Z}\backslash\{0\}$.*

(1) *N is said to be a K_α-number, if $N \neq \alpha$ and $p - \alpha \mid N - \alpha$ for every prime divisor p of N.*
(2) *The Korselt set of N, denoted by $\mathcal{KS}(N)$, is the set of all $\alpha \in \mathbb{Z}\backslash\{0, N\}$ such that N is a K_α-number.*

By Definition 1.1 and Korselt's Criterion, Carmichael numbers are precisely K_1-numbers. Carmichael numbers are interesting since they behave like primes: they satisfy Fermat's little theorem. However, when α takes other values other than one, it seems K_α-number no longer possesses such good property as K_1-number does.

In 1977, H. C. Williams asked(see [9]): Do there exist Carmichael number N that also satisfies: $p+1 \mid N+1$ for all prime divisor p of N. In other words, can we find a composite N such that both $p-1 \mid N-1$ and $p+1 \mid N+1$ hold for each prime $p \mid N$? No such number has been found yet. This question has led the author of [6] to give the following definition.

Definition 1.2. *Let $N \in \mathbb{N}$ be a composite number and α be a positive integer.*

(1) *N is said to be a W_α-number, if $\alpha, -\alpha \in \mathcal{KS}(N)$.*
(2) *The Williams set of N, denoted by $\mathcal{WS}(N)$, is the set of all positive integers α such that N is a W_α-number.*

O. Echi and N. Ghanmi studied $\mathcal{KS}(N)$ when $N = pq$ is the product of two different primes [7]. The author of [2] concentrated on the case when N is the square of a prime. He fully described $\mathcal{KS}(q^2)$ and proved some interesting propositions about $\mathcal{KS}(q^2)$ and $\mathcal{WS}(q^2)$.

In this paper, we follow their steps and investigate $\mathcal{KS}(N)$ and $\mathcal{WS}(N)$ when $N = p^l$ is the power of a prime (where $l \geq 3$ is an integer). For $\mathcal{KS}(p^l)$, we mainly discuss the case when $l = 3$. $\mathcal{KS}(q^l)$ and $\mathcal{WS}(q^l)$ will be discussed in Section 2 and Section 3 respectively.

2. The Korselt Set and Weight of q^l

Let $|\mathcal{KS}(q^l)|$ denotes the number of elements in $\mathcal{KS}(q^l)$. The following theorem analyzed $\mathcal{KS}(q^l)$ and $|\mathcal{KS}(q^l)|$.

Theorem 2.1. *Let q be a prime number, $\alpha \in \mathbb{Z}$ and $l \geq 3$ be an integer. We denote by $\mathcal{D}^+(q^{l-1}-1)$ the set of all positive divisors of $q^{l-1}-1$; then the following properties hold.*

(1) *$\alpha \in \mathcal{KS}(q^l)$ if and only if $\alpha = q + \delta q^\varepsilon r$, for some $r \in \mathcal{D}^+(q^{l-1}-1)$, $\delta \in \{-1, 1\}$, $\varepsilon \in \{0, 1\}$, and $(\delta, \varepsilon, r) \notin \{(-1, 1, 1), (1, 1, q^{l-1}-1)\}$.*
(2) *$|\mathcal{KS}(q^l)| = 4\tau(q^{l-1}-1) - 2$, where $\tau(q^{l-1}-1)$ denotes the number of all positive divisors of $q^{l-1}-1$.*

Proof.

(1) As $q^l - \alpha = q^l - q + (q - \alpha)$, we deduce that $\alpha \in \mathcal{KS}(q^l)$ if and only if $q - \alpha$ divides $q^l - q = q(q^{l-1} - 1)$. But , as $\alpha \neq 0$ and $\alpha \neq q^l$, we conclude that $\alpha \in \mathcal{KS}(q^l)$ if and only if $\alpha = q + \delta q^{\varepsilon} r$, for some $r \in \mathcal{D}^+(q^{l-1} - 1)$, $\delta \in \{-1, 1\}$, $\varepsilon \in \{0, 1\}$, and $(\delta, \varepsilon, r) \notin \{(-1, 1, 1), (1, 1, q^{l-1} - 1)\}$.

(2) If we let $\mathcal{D}(q^l - q)$ be the set of all divisors of $q^l - q$, then from (1), $\mathcal{KS}(q^l)$ and $\mathcal{D}(q^l - q)\backslash\{-q, q^l - q\}$ are numerically equipotent. Hence

$$|\mathcal{KS}(q^l)| = |\mathcal{D}(q^l - q)| - 2.$$

But $|\mathcal{D}(q^l - q)| = 2\tau(q^l - q)$; and as the function τ is multiplicative and $\gcd(q, q^{l-1} - 1) = 1$, we get $\tau(q^l - q) = \tau(q) \times \tau(q^{l-1} - 1) = 2\tau(q^{l-1} - 1)$.

Therefore, $|\mathcal{KS}(q^l)| = 4\tau(q^{l-1} - 1) - 2$. □

Notice that $q \geq 2$ and $l \geq 3$, so $q^{l-1} - 1 > 1$. Thus by the above theorem, $|\mathcal{KS}(q^l)| \geq 4 \cdot 2 - 2 = 6$.

We now ask: given an integer α, does it always belong to $\mathcal{KS}(q^l)$ for some prime q? Obviously, for some α, this is always true (simply let $\alpha = p - 1$ and $q = p$, where p is any prime number). What we really want to know is that can we find an α such that $\alpha \notin \mathcal{KS}(q^l)$ for any prime q and that how many such "strange" α there exist. We first consider the simplest case: $l = 3$.

Suppose $\alpha \in \mathcal{KS}(q^3)$ for some prime q, which means $q - \alpha \mid q^3 - \alpha$. Notice that

$$\begin{aligned} q^3 - \alpha &= q^3 - \alpha^3 + \alpha^3 - \alpha \\ &= (q - \alpha)(q^2 + q \cdot \alpha + \alpha^2) + \alpha^3 - \alpha. \end{aligned} \tag{2.1}$$

So

$$\alpha \in \mathcal{KS}(q^3) \text{ if and only if } q - \alpha \mid \alpha^3 - \alpha. \tag{$*$}$$

With this, our task is to find α such that there doesn't exist prime q which satisfy $q - \alpha \mid \alpha^3 - \alpha$. By condition $(*)$ and a computer program, we found that the first such "strange" α is 21362 and there are only seven such α between 1 and 50000. When we enlarge the scope of α, we can find more. It is natural to conjecture that there are infinitely such α. This question is not as elementary as it seems. We can't give a definite answer to that. However, it is not so hard to partly answer this question. Notice that q is a prime, so that for any q, either $q \mid \alpha$ or $\gcd(q, \alpha) = 1$. We only discuss the first case in this paper. Actually, we proved the following theorem.

Theorem 2.2. *There exist infinitely many α such that $\alpha \notin \mathcal{KS}(q^3)$ for any prime $q \mid \alpha$.*

In order to prove this theorem, we need Dirichlet's theorem on arithmetic progressions, which is the following lemma. The proof can be found in [10].

Lemma 2.3 (Dirichlet's theorem). *For any two positive coprime integers a and d, there are infinitely many primes of the form $a + nd$, where n is a non-negative integer.*

Proof of Theorem 2.2. We will prove our theorem by constructing such α. Let p be any odd prime number, so $\gcd(p^2, 2) = 1$. Thus by Lemma 2.3, there exists an integer n_1 such that $p_1 = p^2 \cdot n_1 + 2$ is a prime. Since $p_1 - 1 = p^2 \cdot n_1 + 1$,

$$\gcd(p_1 - 1, p) = \gcd(p^2 \cdot n_1 + 1, p) = 1. \tag{2.2}$$

By Lemma 2.3 again, there are infinitely many primes in the arithmetic progression $(p_1 - 1)n + p$. So we can find an integer n_2 large enough so that $p_2 = (p_1 - 1)n_2 + p$ is a prime and $p_2 > {p_1}^2$.

We claim that $\alpha = p_1p_2$ satisfy our needs. "Infinity" follows from the fact that there are infinitely many choices for both p_1 and p_2.

If on the contrary, there is a prime q such that $q \mid \alpha$ and $\alpha \in \mathcal{KS}(q^3)$. Since $\alpha = p_1p_2$, q is either p_1 or p_2. If $q = p_1$, then $\alpha \in \mathcal{KS}(p_1^3)$. By the condition $(*)$, we have

$$p_1 - \alpha \mid \alpha^3 - \alpha. \tag{2.3}$$

Replace α by p_1p_2 in the above equation, we get

$$p_1 - p_1p_2 \mid p_1p_2(p_1p_2 - 1)(p_1p_2 + 1), \tag{2.4}$$

or equivalently,

$$p_2 - 1 \mid (p_1p_2 - 1)(p_1p_2 + 1). \tag{2.5}$$

Since

$$\begin{aligned}(p_1p_2 - 1)(p_1p_2 + 1) &= (p_1p_2 - p_1 + p_1 - 1)(p_1p_2 - p_1 + p_1 + 1)\\ &= (p_1(p_2 - 1) + p_1 - 1)(p_1(p_2 - 1) + p_1 + 1),\end{aligned}$$

(2.5) is equivalent to

$$p_2 - 1 \mid (p_1 - 1)(p_1 + 1) = {p_1}^2 - 1. \tag{2.6}$$

Similarly, if $q = p_2$, then $\alpha \in \mathcal{KS}(p_2^3)$ and we will have

$$p_1 - 1 \mid {p_2}^2 - 1. \tag{2.7}$$

We next prove that both (2.6) and (2.7) are impossible.
According to our choice, $p_2 > {p_1}^2$, which implies $p_2 - 1 > {p_1}^2 - 1$. So (2.6) is impossible.
If (2.7) holds, then

$$0 \equiv {p_2}^2 - 1 \equiv ((p_1 - 1)n_2 + p)^2 - 1 \equiv p^2 - 1 \pmod{p_1 - 1}. \tag{2.8}$$

However

$$p_1 = p^2n_1 + 2 \implies p_1 - 1 = p^2n_1 + 1 > p^2 - 1,$$

this contradicts (2.8). □

Notice that the above theorem did not answer our question completely. If there are indeed infinitely many "strange" α, to prove that I think we have to provide a certain form of α and control the number of divisors of $\alpha^3-\alpha$. This, however, is not an easy task. Besides the conjecture we made before Theorem 2.2, if we consider $\mathcal{KS}(q^l)$(where $l \geq 3$ is any integer) a conjecture in more general form arises. We simply list that below and leave it to some experts.

Conjecture 2.4. *For any integer $l \geq 3$, there exist infinitely many $\alpha \in \mathbb{Z}$ such that no prime q satisfies $q-\alpha \mid \alpha^l - \alpha$.*

3. Williams Numbers

As defined in the introduction, a W_α-number is a composite number N such that $\alpha, -\alpha \in \mathcal{KS}(N)$. The *Williams set* of N, denoted by $\mathcal{WS}(N)$, is the set of all $\alpha > 0$ such that N is a W_α-number. The author of [2] discussed some propositions of $\mathcal{WS}(N)$ when $N = q^2$. Here, we are concerned with $N = p^l$, for $l \geq 3$. For any prime q, there are only four possible values $\mod 12$, namely $q \equiv 1, 5, 7, \text{or } 11 \pmod{12}$. Our discussion will split into two cases, we first prove the following proposition.

Proposition 3.1. *If q is a prime and $q \equiv 1, 5, or\ 7 \pmod{12}$ then $\mathcal{WS}(q^l) \neq \varnothing$ for any integer $l \geq 3$.*

Proof. Since q^l has only one prime factor, we get

$$\alpha \in \mathcal{WS}(q^l) \iff q-\alpha \mid q^l - \alpha,\ q+\alpha \mid q^l+\alpha. \tag{3.1}$$

Notice that

$$\begin{aligned} q^l - \alpha &= q^l - q + q - \alpha, \\ q^l + \alpha &= q^l - q + q + \alpha. \end{aligned} \tag{3.2}$$

So

$$\alpha \in \mathcal{WS}(q^l) \iff q-\alpha \mid q^l - q,\ q+\alpha \mid q^l - q. \tag{3.3}$$

We next find α such that $q \pm \alpha \mid q^l - q$.
If $q \equiv 1, 5 \pmod{12}$, then $q - 1 \equiv 0 \pmod 4$. So

$$\begin{aligned} q^l - q &= q(q^{l-1}-1) \\ &= q(q-1)(1+q+\cdots+q^{l-2}) \\ &\equiv 0 \pmod{4q}. \end{aligned} \tag{3.4}$$

Thus $q \pm 3q \mid q^l - q$. By (3.3), we get $3q \in \mathcal{WS}(q^l)$.
If $q \equiv 7 \pmod{12}$, then $q-1 \equiv 0 \pmod 3$. This gives

$$\begin{aligned} q^l - q &= q(q^{l-1}-1) \\ &= q(q-1)(1+q+\cdots+q^{l-2}) \\ &\equiv 0 \pmod{3q}. \end{aligned} \tag{3.5}$$

By similar arguments, we can see that $\alpha = 2q \in \mathcal{WS}(q^l)$. Thus we have proved that $\mathcal{WS}(q^l) \neq \varnothing$, for any $l \geq 3$. □

Different from the case we discussed in Proposition 3.1, when $q \equiv 11 \pmod{12}$ whether $\mathcal{WS}(q^l) \neq \varnothing$ or not will have a relation with the parity of l. We first let l be odd. In this case, $l-1$ is even, $q \equiv -1 \pmod{12}$, thus

$$\begin{aligned} q^l - q &= q(q^{l-1}-1) \\ &\equiv q((-1)^{l-1}-1) \\ &\equiv 0 \pmod{12q}. \end{aligned} \tag{3.6}$$

Combining (3.6) with (3.3) we can see that $2q, 3q \in \mathcal{WS}(q^l)$. We summarize the above statements in the following proposition.

Proposition 3.2. *If q is a prime such that $q \equiv 11 \pmod{12}$ and $l \geq 3$ is an odd integer, then $\mathcal{WS}(q^l) \neq \varnothing$.*

By now, we have already discussed some cases when $\mathcal{WS}(q^l) \neq \varnothing$. With the above two propositions and some further research, we are in a position to provide a necessary and sufficient condition on $\mathcal{WS}(q^l) = \varnothing$. This is shown in the following theorem.

Theorem 3.3. *$\mathcal{WS}(q^l) = \varnothing$ if and only if $q \equiv 11 \pmod{12}$, l is even, and for any integer k, $q^{l-1} \not\equiv 1 \pmod{36k^2 - q^2}$, $q^{l-1} \not\equiv 1 \pmod{36k^2 - 1}$.*

Proof. We first suppose $\mathcal{WS}(q^l) = \varnothing$.

In this case, by Proposition 3.1 and Proposition 3.2, we know that $q \equiv 11 \pmod{12}$ and l is even. It is sufficient to prove that for any integer k both $q^{l-1} \not\equiv 1 \pmod{36k^2 - q^2}$ and $q^{l-1} \not\equiv 1 \pmod{36k^2 - 1}$. We prove this by contradiction.

- Assume there exists $k_0 \in \mathbb{Z}$ such that
$$q^{l-1} \equiv 1 \pmod{36k_0^2 - q^2}.$$
Since
$$36k_0^2 - q^2 = (6k_0 - q)(6k_0 + q),$$
we have
$$q - 6k_0 \mid q^{l-1} - 1 \text{ and } q + 6k_0 \mid q^{l-1} - 1,$$
which imply $q \pm 6k_0 \mid q(q^{l-1} - 1)$. So $\alpha = 6k_0 \in \mathcal{WS}(q^l)$, a contradiction.
- If there exists $k_1 \in \mathbb{Z}$ such that
$$q^{l-1} \equiv 1 \pmod{36k_1^2 - 1},$$
then
$$1 \pm 6k_1 \mid q^{l-1} - 1,$$
or equivalently,
$$q \pm 6k_1 q \mid q^l - q.$$
This leads to $\alpha = 6k_1 q \in \mathcal{WS}(q^l)$, a contradiction.

We now prove the other direction. Suppose $q \equiv 11 \pmod{12}$ and l is even. We claim that if $\mathcal{WS}(q^l) \neq \varnothing$, then there exists an integer k such that

$$q^{l-1} \equiv 1 \pmod{36k^2 - q^2} \tag{3.7}$$

or

$$q^{l-1} \equiv 1 \pmod{36k^2 - 1} \tag{3.8}$$

holds. Let $\alpha \in \mathcal{WS}(q^l)$, by (3.3) we get $q \pm \alpha \mid q^l - q$. Since q is a prime, either $q \mid \alpha$ or $\gcd(q, \alpha) = 1$. We will prove our claim according to these two cases.

If $q \mid \alpha$, we can write $\alpha = rq$ for some integer r. Replace α by rq in $q \pm \alpha \mid q^l - q$, we get $q \pm rq \mid q^l - q$ or equivalently,

$$r - 1 \mid q^{l-1} - 1 \text{ and } r + 1 \mid q^{l-1} - 1. \tag{3.9}$$

Notice that $q \equiv 11 \equiv -1 \pmod{12}$ and l is even, so

$$q^{l-1} - 1 \equiv (-1)^{l-1} - 1 \equiv -1 - 1 \equiv 10 \pmod{12}. \tag{3.10}$$

We now show that $6 \mid r$. This can be done by proving $2 \mid r$ and $3 \mid r$. If $2 \nmid r$, then $r \equiv \pm 1 \pmod 4$. So either $4 \mid r-1$ or $4 \mid r+1$. By (3.9), we always have $4 \mid q^{l-1}-1$, contradicting (3.10). If $3 \nmid r$, then $r \equiv \pm 1 \pmod 3$. By similar arguments we can prove that $3 \mid q^{l-1} - 1$, which also contradicts (3.10).

Since $6 \mid r$ we can write $r = 6k$ and (3.9) will become

$$6k - 1 \mid q^{l-1} - 1 \text{ and } 6k + 1 \mid q^{l-1} - 1.$$

However, $\gcd(6k - 1, 6k + 1) = \gcd(6k - 1, 2) = 1$. So the above statements imply

$$(6k - 1)(6k + 1) \mid q^{l-1} - 1.$$

Thus we have found an integer k such that (3.8) holds.

If $\gcd(q, \alpha) = 1$, then $\gcd(q \pm \alpha, q) = 1$. So

$$q \pm \alpha \mid q^l - q \iff q \pm \alpha \mid q^{l-1} - 1.$$

Notice that $q \equiv 11 \pmod{12}$ implies $q \equiv 3 \pmod 4$. So if α is odd, then either $4 \mid q - \alpha$ or $4 \mid q + \alpha$. Any case will imply $4 \mid q^{l-1} - 1$ since $q \pm \alpha \mid q^l - q$. This contradicts (3.10). So α must be even. Thus $q + \alpha$ is odd. Combining this with $\gcd(q, \alpha) = 1$ we will get

$$\gcd(q - \alpha, q + \alpha) = \gcd(2q, q + \alpha) = \gcd(q, q + \alpha) = 1.$$

So

$$q - \alpha \mid q^{l-1} - 1, q + \alpha \mid q^{l-1} - 1 \implies q^2 - \alpha^2 \mid q^{l-1} - 1. \tag{3.11}$$

If we are able to prove $6 \mid \alpha$, then letting $\alpha = 6k$, (3.11) will become

$$q^2 - 36k^2 \mid q^{l-1} - 1,$$

namely (3.7) holds. This will complete the proof.

To prove $6 \mid \alpha$, it is sufficient to prove $3 \mid \alpha$ since we have already proved that α is even. Notice that $q \equiv -1 \pmod 3$. If $3 \nmid \alpha$, then $\alpha \equiv \pm 1 \pmod 3$. So

$$q^2 - \alpha^2 \equiv (-1)^2 - (\pm 1)^2 \equiv 0 \pmod 3.$$

By (3.11), $3 \mid q^{l-1} - 1$, contradicting (3.10). □

Given a prime q and an integer $l \geq 3$, it will be quite cumbersome to check whether or not $\mathcal{WS}(q^l) = \varnothing$ directly. However, by Theorem 3.3 we only need to check if there is an integer k that satisfies one of the two conditions: $q^{l-1} \equiv 1 \pmod{36k^2 - q^2}$, $q^{l-1} \equiv 1 \pmod{36k^2 - 1}$. Notice that these conditions require $36k^2 - q^2 \leq q^{l-1}$ and $36k^2 - 1 \leq q^{l-1}$. So we only have to test these conditions for a finite number of values for k. For instance, when $l = 4$, of all the primes $2 < q < 1000$ that satisfy $q \equiv 11 \pmod{12}$, there are only ten primes

$$q = 11, 23, 71, 191, 239, 419, 431, 491, 647, 911$$

for which we can find an integer k such that $q^2 - 36k^2 \mid q^{l-1} - 1$ or $36k^2 - 1 \mid q^{l-1} - 1$ holds. Thus by Theorem 3.3, $\mathcal{WS}(q^l) = \varnothing$ for all primes $q < 1000$ and $q \equiv 11 \pmod{12}$ except these ten primes.

Acknowledgement

In the process of writing this paper, I get many instructions from Prof. Jianhua Chen, Prof. Jihua Ma and some classmates. My family also give me lots of love and support. I would like to thank them all. In the end, I am eager to express my sincere gratitude to the anonymous referee for reading this paper and putting forward valuable opinions, which assist me in revising my paper.

References

[1] W. R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, *Ann.Math.* **139** (1994) 703–722.
[2] I. Alrasasi, The Korselt set of the square of a prime, *Int. J. Number Theory* **10** (2014) 875–884.
[3] K. Bouallegue, O. Echi and R. Pinch, Korselt numbers and sets, *Int. 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 $a^{P-1} \equiv 1 \bmod P$, *Amer. Math. Monthly* **19** (1912) 22–27.
[6] O. Echi, Williams numbers, *C. R. Math. Acad. Sci. Soc. Roy. Canad.* **29** (2007) 41–47.
[7] O. Echi and N. Ghanmi, The Korselt set of pq, *Int. J. Number Theory* **8** (2012) 299–309.
[8] A. Korselt, Problème chinois, *L'Intermédiaire des Mathématiciens* **6** (1899) 142–143.
[9] H. C. Williams, On numbers analogous to the Carmichael numbers, *Canad. Math. Bull.* **20** (1977) 151–163.
[10] J. P. Serre, A course in arithmetic, New York: Springer-Verlag (1973) 73–76.