Really strong Carmichael numbers

Mohamed Ayad, Rachid Bouchenna

Really strong Carmichael numbers

Mohamed Ayad, Laboratoire de Mathématiques Pures et Appliquées, Université du Littoral, F-62228 Calais. France

E-mail: ayadmohamed502@yahoo.com

Rachid Bouchenna, ACC (Arithmétique, Codage et Combinatoire), Université des Sciences et Technologies Houari Boumediene, 16324, El Alia, Alger, Algérie.

E-mail: rbouchenna@usthb.dz

MSC : 11A07, 11A51.

Keywords : λ function, Carmichael numbers, Strong Carmichael numbers, Congruences.

Abstract. A composite number n is called a Carmichael number if $a^{n-1} \equiv 1 \pmod{n}$ for any integer a coprime with n. D. H. Lehmer considered the class of these numbers n such that $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$ for any integer a coprime with n. Here $\left(\frac{a}{n}\right)$ denotes the Jacobi symbol. It turns out and it is shown by Lehmer himself that this class is empty. Here, we replace $\equiv \left(\frac{a}{n}\right) \pmod{n}$ in Lehmer's congruence by $\equiv 1 \pmod{n}$ and get a new class which is not empty.

1 introduction

In 1910, R. D. Carmichael [2] defined the number theory function $\lambda(n)$ by $\lambda(2) = \Phi(2) = 1$, $\lambda(2^2) = \Phi(2^2) = 2$,

$$\lambda(p^e) = \begin{cases} \Phi(p^e) = p^{e-1}(p-1) \text{ if } p \text{ is odd and } e \geq 1 \\ \frac{\Phi(2^e)}{2} = 2^{e-2} \text{ if } p = 2 \text{ and } e \geq 3 \end{cases}$$

and in general $\lambda(p_1^{e_1} \cdots p_r^{e_r}) = lcm(\lambda(p_1^{e_1}), \ldots, \lambda(p_r^{e_r}))$.

Let $n \geq 2$ be an integer. It is easy to see that the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^\star$ divides $\lambda(n)$. Indeed, even better that this divisibility property alone, the paper [2] proves equality, that is there exists an element of the group whose order is equal to $\lambda(n)$.

The famous Fermat's little theorem asserts that if p is a prime number, then for any $a \in \mathbb{Z}$, $gcd(a, p) = 1$, we have $a^{p-1} \equiv 1 \pmod{p}$. The converse of this theorem is false. Carmichael [3] gave the first counter-example, namely $n = 561 = 3.11.17$, so we are led to the following definition. A composite number n is called a Carmichael number if for any $a \in \mathbb{Z}$, $gcd(a, n) = 1$ we have $a^{n-1} \equiv 1 \pmod{n}$.

The known criteria for a Carmichael number are sumarized in the following result.

Theorem 1. *Let $n \geq 2$ be a composite number, then the following conditions are equivalent.*

(i) n *is a Carmichael number.*

(ii) n *is square-free and any prime factor* p *of* n *satisfies the condition* $p-1 \mid n-1$.

(iii) $\lambda(n) \mid n-1$.

The equivalence of (i) with (ii) (resp. (i) with (iii)) are due to A. R. Korselt [4] and to R. D. Carmichael respectively [3].

In [1] the authors proved that there are infinitely many Carmichael numbers.

In [5], D. H. Lehmer defined what he called a strong Carmichael number to be an odd composite number n for which $a^{(n-1)/2} \equiv (\frac{a}{n}) \pmod{n}$ for any $a \in \mathbb{Z}$, $gcd(a,n) = 1$, where $(\frac{a}{n})$ denotes the Jacobi symbol. He showed, in the same paper, that these numbers do not exist.

In the rest of the text, we discuss the possibility for an integer n to satisfy the congruence $a^{(n-1)/2} \equiv 1 \pmod{n}$ for any $a \in \mathbb{Z}$, $gcd(a,n) = 1$. Such numbers will be called really strong Carmichael numbers.

2 Really strong Carmichael numbers.

An odd composite number n for which $a^{(n-1)/2} \equiv (\frac{a}{n}) \pmod{n}$ for any $a \in \mathbb{Z}$, $gcd(a,n) = 1$ is called by D. H. Lehmer a strong Carmichael number. Here $\left(\frac{a}{n}\right)$

denotes the Jacobi symbol. If n is strong, then

$$\left(a^{(n-1)/2}\right)^2 \equiv \left(\frac{a}{n}\right)^2 \pmod{n} \equiv 1 \pmod{n},$$

hence n is a Carmichael number. For example for $n = 561$ which is the smallest Carmichael number, we have $2^{560/2} = 2^{280} \equiv -1 \pmod{561} \equiv \left(\frac{2}{561}\right) \pmod{561}$ and $5^{280} \equiv 67 \pmod{561} \not\equiv \pm 1 \pmod{561}$, hence 561 is not a strong Carmichael number. Indeed, in his paper Lehmer proved that there exists no strong Carmichael number.

Let $e(n) = \nu_2(n-1) \geq 1$. For any k, $1 \leq k \leq e(n)$, we consider the conditions:

$$(C_k) \quad a^{(n-1)/2^k} \equiv 1 \pmod{n} \quad \text{for any} \quad a \in \mathbb{Z}, \quad gcd(a, n) = 1.$$

It is clear that if (C_k) is satisfied, then all the conditions $(C_k), (C_{k-1}), \cdots (C_1)$ are verified. A number n which satisfies (C_k) for some $1 \leq k \leq e(n)$, hence for $k = 1$, will be called a really strong Carmichael number. We will show that contrary to strong Carmichael numbers, really strong Carmichael numbers exist.

Notice that, since the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^\star$ is equal to $\lambda(n)$, then the condition (C_k) is equivalent to $\lambda(n) \mid (n-1)/2^k$.

Proposition 1. *If $n \equiv -1 \pmod{4}$ and n is a Carmichael number, then any prime factor of n is congruent to -1 modulo 4. The number of these primes is odd and n is not really strong.*

Proof. Since $n \equiv -1 \pmod{4}$, then $n - 1 \equiv 2 \pmod{4}$. Let p be a prime factor of n. Since p is odd and $p - 1 \mid n - 1$, then $p - 1 \equiv 2 \pmod{4}$, hence $p \equiv -1 \pmod{4}$.

Let r be the number of prime factors of n, then $-1 \equiv n \pmod 4 \equiv (-1)^r \pmod 4$, hence r is odd. Now $(n-1)/2$ is odd and $\lambda(n)$ is even, hence $\lambda(n) \nmid (n-1)/2$ and n is not really strong. □

Example. The integer $n = 8911 = 7 \times 19 \times 67$ satisfies the conditions of this proposition.

Theorem 2. *Let $n \geq 3$ be an odd integer and k be an integer such that $1 \leq k \leq e(n)$.*

1. *The following conditions are equivalent.*

   (i) n is a prime number or a Carmichael number.

   (ii) For any $a \in \mathbb{Z}$, $gcd(a,n) = 1$, we have $\overline{a^{(n-1)/2^k}}$ is a 2^k-th root of 1 in $\mathbb{Z}/n\mathbb{Z}$.

2. *Suppose that n satisfies the above equivalent conditions. Let A_k be the set of prime numbers p dividing n such that $\nu_2(p-1) > \nu_2((n-1)/2^k)$.*

   Let $\theta : (\mathbb{Z}/n\mathbb{Z})^\star \to (\mathbb{Z}/n\mathbb{Z})^\star$ be the map such that $\theta(\bar{x}) = \overline{x^{(n-1)/2^k}}$. Then θ is a homomorphism of groups and

$$Im\theta \simeq \prod_{p_i \in A_k} (\mathbb{F}_{p_i}^\star)^{u_i} \simeq \prod_{p_i \in A_k} \{2^{s_i}\text{-th roots of } \quad 1 \quad \text{in} \quad \mathbb{Z}/p_i\mathbb{Z}\} \simeq \prod_{p_i \in A_k} < \xi_i^{(p_i-1)/2^{s_i}} >,$$

   where ξ_i is a generator of $(\mathbb{Z}/p_i\mathbb{Z})^\star$, $s_i = \nu_2(p_i-1)-(e-k)$ and $u_i = (p_i-1)/2^{s_i}$. Moreover,

$$Im\theta = \{\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\star |\, x \equiv 1 \; or \; x^{2^k} \equiv 1 \pmod p \text{ according to } p \notin A_k \text{ or } \quad p \in A_k\}.$$

Proof. 1. • $(i) \Rightarrow (ii)$. Let $a \in \mathbb{Z}$ such that $gcd(a,n) = 1$ and let $b = a^{(n-1)/2^k}$. Since $\overline{a^{n-1}} = \overline{1}$, then $\overline{b}^{2^k} = \overline{a^{(n-1)/2^k}}^{2^k} = \overline{a^{n-1}} = \overline{1}$, hence b is a 2^k-th root of 1 modulo n.

• $(ii) \Rightarrow (i)$. Suppose that n is not a prime number, that is n is composite. Let $a \in \mathbb{Z}$ such that $gcd(a,n) = 1$, then $\overline{1} = \overline{a^{(n-1)/2^k}}^{2^k} = \overline{a^{n-1}}$, hence n is a Carmichael number.

2. Obviously, θ is a homomorphism of groups. We compute the image of θ. We will use the following:

Claim. Let p be a prime divisor of n, then $p-1 \mid (n-1)/2^k$ if and only if $p \notin A_k$.

Proof. For any odd prime l, we have $\nu_l((n-1)/2^k) = \nu_l(n-1)$, hence

$$\begin{aligned} p-1 \mid (n-1)/2^k &\Leftrightarrow \nu_l(p-1) \leq \nu_l((n-1)/2^k) \quad \text{for any prime} \quad l \\ &\Leftrightarrow \nu_2(p-1) \leq \nu_2((n-1)/2^k) = \nu_2(n-1) - k \\ &\Leftrightarrow p \notin A_k. \end{aligned}$$

This claim being proved, let $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\star$. We have

$$\begin{aligned} \overline{a} \in Ker\theta &\Leftrightarrow \overline{a^{(n-1)/2^k}} = \overline{1} \\ &\Leftrightarrow a^{(n-1)/2^k} \equiv 1 \pmod{p} \quad \text{for any} \quad p \mid n \\ &\Leftrightarrow (\text{ by the claim}), \quad a^{(n-1)/2^k} \equiv 1 \pmod{p_i} \quad \text{for} \quad p_i \in A_k. \end{aligned}$$

For i such that $p_i \in A_k$, let $\xi_i \in \mathbb{Z}$ be such that its reduction modulo p_i is a primitive p_i-th root of unity and let u_i be such that $a \equiv \xi_i^{u_i} \pmod{p_i}$. Then

$$\begin{aligned} a^{(n-1)/2^k} \equiv 1 \pmod{p_i} &\Leftrightarrow \xi_i^{u_i(n-1)/2^k} \equiv 1 \pmod{p_i} \\ &\Leftrightarrow p_i - 1 \mid u_i(n-1)/2^k \\ &\Leftrightarrow (\text{by the fact that} \quad p_i - 1 \mid n-1), \nu_2(p_i-1) \leq \nu_2(u_i(n-1)/2^k) \\ &= \nu_2(u_i) + \nu_2((n-1)/2^k) \end{aligned}$$

Since $\nu_2(p_i - 1) > \nu_2((n-1)/2^k) = e - k$, set $\nu_2(p_i - 1) = e - k + s_i$, where s_i is a positive integer. Then

$$\begin{aligned} p_i - 1 \mid u_i(n-1)/2^k &\Leftrightarrow e - k + s_i \leq \nu_2(u_i) + e - k \\ &\Leftrightarrow \nu_2(u_i) \geq s_i. \end{aligned}$$

We deduce that

$$\begin{aligned} \overline{a} \in Ker\theta &\Leftrightarrow \nu_2(u_i) \geq s_i = \nu_2(p_i - 1) - (e - k) \quad \text{for} \quad p_i \in A_k \\ &\Leftrightarrow 2^{s_i} \mid u_i \quad \text{for} \quad p_i \in A_k \\ &\Leftrightarrow a \quad \text{modulo} \quad p_i \quad \text{is a} \quad 2^{s_i} - \text{th power in} \quad \mathbb{Z}/p_i\mathbb{Z} \quad \text{for} \quad p_i \in A_k \end{aligned}$$

Therefore $Ker\theta \simeq (\prod_{p_i \notin A_k} \mathbb{F}_{p_i}^{\star}) \times (\prod_{p_j \in A_k} \mathbb{F}_{p_j}^{\star 2^{s_j}})$.

This implies that

$$\begin{aligned} Im\theta &\simeq \prod_{p_j \in A_k} (\mathbb{F}_{p_j}^{\star})^{u_j} \\ &\simeq \prod_{p_j \in A_k} \{2^{s_j}\text{-th roots of} \quad 1 \quad \text{in} \quad \mathbb{Z}/p_j\mathbb{Z}\} \\ &\simeq \prod_{p_j \in A_k} < \xi_j^{(p_j-1)/2^{s_j}} >, \end{aligned}$$

where $u_j = (p_j - 1)/2^{s_j}$. Moreover,

$$Im\theta = \{\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^{\star} |\, x \equiv 1 \,\text{or}\, x^{2^k} \equiv 1 \pmod{p} \,\text{according to}\ p \notin A_k \,\text{or}\, p \in A_k\}.$$

□

3 The role of the square roots of 1.

This theorem shows that if n a prime number or a Carmichael number, then as a runs over $\mathbb{Z}$ and $gcd(a, n) = 1$, $a^{(n-1)/2}$ takes $2^{|A_1|}$ distinct values modulo n all of them being square roots of 1.

Corollary 1. *Let $n \geq 3$ be an odd integer and*

$$V = \{\overline{a^{(n-1)/2}}, a \in \mathbb{Z} | \quad gcd(a, n) = 1\} \subset (\mathbb{Z}/n\mathbb{Z})^{\star}$$

1. *V contains an element which is not a square root of 1 if and only if n is not prime nor a Carmichael number.*

2. *If all the elements of V are square roots of 1, then n is a prime number if and only if $V = \{-1, 1\}$.*

Proof. 1. Let $x \in V$ be such that x is not a square root of 1, and let $a \in \mathbb{Z}$, $gcd(a, n) = 1$ and $x = \overline{a}^{(n-1)/2}$. Since $x^2 \neq 1$, then $a^{n-1} \not\equiv 1 \pmod{n}$. Fermat's little theorem implies immediately that n is not a prime number, hence n is composite not a Carmichael number.

Conversely, suppose that $n = p^e$ or $n = p_1^{e_1} \cdots p_r^{e_r}$, where $r \geq 2$, $p, p_1, \ldots p_r$ are odd prime numbers, $e \geq 2$ and $e_1, \ldots e_r$ are positive integers. Let ξ_n be an element of $(\mathbb{Z}/n\mathbb{Z})^\star$ of order $\lambda(n)$. Then $\xi_n^{(n-1)/2} \in V$. We show that this element of V is not a square root of 1. Suppose the contrary. We have

$$\bar{1} = (\xi_n^{(n-1)/2})^2 = \xi_n^{n-1} = \begin{cases} \xi_n^{p^e-1} \text{ in the first case} \\ \xi_n^{p_1^{e_1}\cdots p_r^{e_r}-1} \text{ in the second case} \end{cases}.$$

In the first case this implies $\lambda(n) = \Phi(n) = p^{e-1}(p-1)$ divides $p^e - 1$. This is a contradiction because $p \nmid p^e - 1$. In the second case $\lambda(n) = lcm(\Phi(p_i^{e_i}), i = 1, \ldots, r) = lcm(p_i^{e_i-1}(p_i - 1), i = 1, \ldots, r)$ divides $p_1^{e_1} \cdots p_r^{e_r} - 1$. If some $e_j \geq 2$, then $p_j \mid p_1^{e_1} \cdots p_r^{e_r} - 1$, which is a contradiction. If all the e_i are equal to 1, then $p_i - 1 \mid n - 1$ for all i, hence n is a Carmichael number, a contradiction again.

2. Suppose $n = p$ is a prime number and let $x = \overline{a^{(n-1)/2}} = \overline{a^{(p-1)/2}} \in V$, then $x^2 = \overline{a^{p-1}} = \bar{1}$, hence $x = \pm 1$.

Conversely, suppose that $V = \{-1, 1\}$. Let $a \in \mathbb{Z}$ such that $gcd(a, n) = 1$. Since $a^{(n-1)/2} \equiv \pm 1 \pmod{n}$, then $a^{n-1} \equiv 1 \pmod{n}$. By 1., n is a prime or a Carmichael number. We must eliminate the second possibility. If $n = p_1 \cdots p_r$ is a Carmichael number, then the assumption on V shows that $|B_1| = 1$ and $|A_1| \geq 2$, thus $|A_1| = r - 1$. This means that $a^{(n-1)/2} \equiv 1 \pmod{p_i}$ for $i = 1, \ldots r_1$ and $a^{(n-1)/2} \equiv \pm 1 \pmod{p_r}$. Equivalently, we have

$$a^{(n-1)/2} \equiv \begin{cases} 1 \pmod{\prod_{i=1}^{r-1} p_i} \\ 1 \pmod{p_r} \end{cases}$$

or

$$a^{(n-1)/2} \equiv \begin{cases} 1 \pmod{\prod_{i=1}^{r-1} p_i} \\ -1 \pmod{p_r}. \end{cases}$$

The first case shows that the unique solution is $a^{(n-1)/2} \equiv 1 \pmod{n}$. The solution for the second case is never equal to 1, nor -1.

□

Example Let $n = 3367$, then $(n-1)/2 = 1683$, $2^{(n-1)/2} \equiv 1807 \pmod{n}$ and $1807^2 \equiv 2626 \pmod{n} \not\equiv 1 \pmod{n}$, hence by the corollary, n is not a prime nor a Carmichael number.

Remark 1. *If all the elements of V are square roots of 1, then by 1., n is a prime number or a Carmichael number, thus item 2. of the above corollary may be replaced by the following:*

If all the the elements of V are square roots of 1, then n is a Carmichael number if and only if $V \neq \{-1, 1\}$.

Notice that if $a^{(n-1)/2}$ is a square root of 1 for any $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\star$, then the set V is a subgroup of the group S of square roots of unity, so $\{1\} \subset V \subset S \subset (\mathbb{Z}/n\mathbb{Z})^\star$.

Corollary 2. *Let $n = p_1 \cdots p_r$ be a square free integer such that all the elements of V are square roots of 1. Let r_1 (resp. r_2) be the number of p_i's such that $\nu_2(p_i - 1) < \nu_2(n-1)$ (resp. $\nu_2(p_i - 1) = \nu_2(n-1)$). Then the first three (resp. the last three) following conditions are equivalent.*

(i) $r_2 = 0$.

(ii) $V = \{1\}$.

(iii) *n is really strong.*

(iv) $r_1 = 0$.

(v) $-1 \in V$.

(vi) $V = \{\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\star \mid \overline{x}^2 = 1\}$.

Proof. $(i) \Rightarrow (ii)$. Since for any $i = 1, \ldots, r$, $\nu_2(p_i - 1) < \nu_2(n-1)$, then $\nu_2(p_i - 1) \leq \nu_2((n-1)/2)$, hence $p_i - 1 \mid (n-1)/2$. Since for any $a \in \mathbb{Z}$, $gcd(a, n) = 1$, we have $a^{p_i - 1} \equiv 1 \pmod{p_i}$, then $a^{(n-1)/2} \equiv 1 \pmod{n}$ for $i = 1, \ldots, r$. This implies $a^{(n-1)/2} \equiv 1 \pmod{n}$ for any $a \in \mathbb{Z}$ such that $gcd(a, n) = 1$. Therefore, $V = \{1\}$.

$(ii) \Rightarrow (iii)$. Obvious.

$(iii) \Rightarrow (i)$. By contradiction, suppose that there exists $i \in \{1, \ldots, r\}$ be such that $\nu_2(p_i - 1) = \nu_2(n-1)$. Since $p_i - 1 \mid n-1$, then we may set $n-1 = (p_i-1)q$, where q is an odd integer. Let $a \in \mathbb{Z}$ be such that $a^{(p_i-1)/2} \equiv -1 \pmod{p_i}$, then $a^{(n-1)/2} = (a^{(p_i-1)/2})^q \equiv (-1)^q \pmod{p_i} \equiv -1 \pmod{p_i}$, hence $a^{(n-1)/2} \not\equiv 1 \pmod{n}$, which is a contradiction.

$(iv) \Rightarrow (v)$. For any $i = 1, \ldots, r$, $\nu_2(p_i-1) = \nu_2(n-1)$, hence $n-1 = (p_i-1)q_i$, where q_i is an odd positive integer. By the Chinese remainder theorem, let $a \in \mathbb{Z}$ be such that $a^{(p_i-1)/2} \equiv -1 \pmod{p_i}$ for $i = 1, \ldots, r$. Then $a^{(n-1)/2} = (a^{((p_i-1)/2)})^q \equiv (-1)^q \pmod{p_i} \equiv -1 \pmod{p_i}$ for $i = 1, \ldots, r$, hence $a^{(n-1)/2} \equiv -1 \pmod{n}$. This implies $-1 \in V$.

$(v) \Rightarrow (vi)$. By assumption any element of V is a square root of 1. We show the converse. Let $a \in \mathbb{Z}$ be a fixed integer such that $a^{(n-1)/2} \equiv -1 \pmod{n}$, then for $i = 1, \ldots, r$, $a^{(n-1)/2} \equiv -1 \pmod{p_i}$. Let $\overline{x}$ be a square root of 1 in $\mathbb{Z}/n\mathbb{Z}$, then x is a square root of 1 modulo p_i for $i = 1, \ldots, r$, hence $x \equiv \epsilon_i$ for $i = 1, \ldots r$, where $\epsilon_i = \pm 1$. Set

$$b_i = \begin{cases} a \text{ if } \epsilon_i = -1 \\ \\ \epsilon_i \text{ if } \epsilon_i = 1 \end{cases}$$

and let $b \in \mathbb{Z}$ be such that $b \equiv b_i \pmod{p_i}$ for $i = 1, \ldots, r$. We have $b^{(n-1)/2} \in V$, $b^{(n-1)/2} \equiv b_i^{(n-1)/2} \pmod{p_i}$.

$(vi) \Rightarrow (iv)$. Since $\overline{-1} \in V$, then there exists $a \in \mathbb{Z}$ such that $a^{(n-1)/2} \equiv -1 \pmod{n}$.

This implies that $a^{(n-1)/2} \equiv -1 \pmod{p}$ for any prime factor p of n. We deduce that $p-1 \nmid (n-1)/2$, and since $p-1 \mid n-1$, then $\nu_2(p-1) = \nu_2(n-1)$. Therefore, $r_1 = 0$.

Here is the list of the sixteen first Carmichael numbers n with the factorizations of n and $n-1$ along with the values of $\lambda(n)$ and (r_1, r_2).

n	$n-1$	$\lambda(n)$	(r_1, r_2)
561=3.11.17	$560 = 2^4.5.7$	$\lambda(561) = 2^4.5$	$(2,1)$
1105=5.13.17	$1104 = 2^4.3.23$	$\lambda(1105) = 2^4.3$	$(2,1)$
1729=7.13.19	$1728 = 2^6.3^3$	$\lambda(1729) = 2^2.3^2$	$(3,0)$
2465=5.17.29	$2464 = 2^5.7.11$	$\lambda(2465) = 2^4.7$	$(3,0)$
2821=7.13.31	$2820 = 2^2.3.5.47$	$\lambda(2821) = 2^2.3.5$	$(2,1)$
6601=7.23.41	$6600 = 2^3.3.5^2.11$	$\lambda(6601) = 2^3.3.5.11$	$(2,1)$
8911=7.19.67.	$8910 = 2.3^4.5.11$	$\lambda(8911) = 2.3^2.11$	$(0,3)$
10585=5.29.73	$10584 = 2^3.3^3.7^2$	$\lambda(2465) = 2^3.3^2.7$	$(2,1)$
15841=7.31.73	$15840 = 2^5.3^2.5.11$	$\lambda(15841) = 2^3.3^2.5$	$(3,0)$
29341=13.37.61.	$29340 = 2^2.3^2.5.163$	$\lambda(29341) = 2^2.3^2.5$	$(0,3)$
41041=7.11.13.41	$41040 = 2^4.3^2.5.19$	$\lambda(2465) = 2^3.3.5$	$(4,0)$
46657=13.37.97	$46656 = 2^6.3^6$	$\lambda(2465) = 2^5.3^2$	$(3,0)$
52633=7.73.103	$52632 = 2^3.3^2.17.43$	$\lambda(52633) = 2^3.3^2.17$	$(2,1)$
62745=3.5.47.89.	$62744 = 2^3.11.23.31$	$\lambda(62745) = 2^3.11.23$	$(3,1)$
63973=7.13.19.37	$63972 = 2^2.3^2.1777$	$\lambda(63973) = 2^3.11.23$	$(2,2)$

n	$n-1$	$\lambda(n)$	(r_1, r_2)
75361=11.13.17.31.	$75360 = 2^5.3.5.157$	$\lambda(63973) = 2^4.3.5$	$(4, 0)$

Among these Carmichael numbers, six of them are really strong Carmichael numbers, namely: $1729, 2465, 15841, 41041, 46657, 75361$. Clearly, if $n \equiv -1 \pmod 4$, then by proposition 1, $r_1 = 0$ and $r_2 = r$. The converse is false, as is shown by the number $n = 29341 = 13.37.61$ contained in the above table. Notice that in this table there is no number for which $(r_1, r_2) = (1, 2)$.

Questions. 1. Do there exist infinitely many Carmichael numbers $n \equiv -1 \pmod 4$?

2. Given non-negative integers r_1, r_2, r, such that $r \geq 3$ and $r_1 + r_2 = r$, can one find a Carmichael number n such that n has r prime factors, r_1 of them say $p_1, \ldots, p_{r_1}$ satisfy the condition $\nu_2(p_i - 1) < \nu_2(n-1)$ and the remaing ones $p_{r_1+1}, \ldots, p_r$ verify the condition $\nu_2(p_j - 1) = \nu_2(n-1)$?

References

[1] W. R. Alford , A. Granville, C. Pomerance, There are infinitely many Carmichael numbers, Annals of Math. 140, (1994) 703-722.

[2] R. D. Carmichael, Note on a new number theory function, Bull. A. M. S. 16 (1910) 232-238.

[3] 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.

[4] A. R. Korselt, Problème chinois, L'intermédiaire des mathématiciens 6 (1899) 142-143.

[5] D. H. Lehmer, Strong Carmichael numbers, J. Aust. Math. Soc. 21 (1976) 508-510.