On some Generalizations of Wilson's Theorem and How to Characterize Carmichael Numbers by Stirling Numbers

Khaled Ben Letaïef

Notes on Number Theory and Discrete Mathematics
ISSN 1310–5132
Vol. XX, XXXX, No. X, XX–XX

On some Generalizations of Wilson's Theorem and How to Characterize Carmichael Numbers by Stirling Numbers

Khaled Ben Letaïef[1]

[1] Aeronautics and aerospace high graduate engineer
16 Bd du Maréchal de Lattre, apt. 095, 21300 Chenove, France
e-mail : letaiev@gmail.com

Abstract : This work uses a combinatorial identity involving Stirling's numbers of the second kind to prove and generalize Wilson's theorem in an original manner. Then, again using this relation, we show new characterizations of Carmichael's numbers.

Keywords : Stirling Numbers, Carmichael Numbers, Wilson's Theorem.
AMS Classification : 11B73, 05A18.

Table des matières

1 New proof of the Wilson's theorem

Here, we will show the Wilson's theorem in a combinatorial way, i.e. without going through the traditional classes of congruences met in the literature. We will use the identity Φ below - a subtraction between two known combinatorial relations - to make emerge congruences properties

in a visible way.

Wilson's theorem : if $n+1$ prime, then $n! + 1 \equiv 0 \quad [n+1]$

Proof :

$\forall n \geq 1$, we have :

$$\sum_{i=0}^{n} (-1)^i C_n^i (X+i)^n = (-1)^n n! \quad (*)$$

This classical identity is obtained from the n-th finite difference of the polynomial X^n [5]. One starts then from the relation obtained by setting : $X = 0$ in $(*)$, that is to say :

$$\sum_{i=0}^{n} (-1)^i C_n^i i^n = (-1)^n n! \quad (**)$$

Then, by deriving k times $(*)$ for $k > 1$, we get :

$$\sum_{i=0}^{n} (-1)^i C_n^i (X+i)^{n-k} = 0$$

Hence, setting $X = 0$:

$$\sum_{i=0}^{n} (-1)^i C_n^i i^{n-k} = 0$$

In other words, $\forall \alpha$ integer, $\alpha < n$:

$$\sum_{i=0}^{n} (-1)^i C_n^i i^{\alpha} = 0 \quad (\Delta)$$

Now, let us cut off to $(**)$, member with member, the arithmetic equation :

$$\sum_{i=0}^{n} (-1)^i C_n^i = 0$$

obtained by posing $\alpha = 0$ in (Δ).

Hence, for $n+1$ an odd prime number ≥ 3 (thus n even) :

$$\sum_{i=1}^{n} (-1)^i C_n^i (i^n - 1) = n! + 1 \quad (\Phi)$$

Using the little Fermat's theorem, one sees that :

$\forall i = 1...n$,

$$i^n - 1 \equiv 0 \quad [n+1]$$

From which :

$$n! + 1 \equiv 0 \quad [n+1]$$

Q.E.D.

Always thanks to Φ, we note that if $n+1$ divides the terms $i^n - 1$, $\forall i$ varying from 1 to n, then it divides $n! + 1$. Thus, according to the equivalence of the Wilson's theorem, $n+1$ is prime - this result can also be found by using the theorem of Bézout.

We discovered later another proof of the Wilson's theorem starting from $(**)$ [2]. But this proof differs from ours in that it uses initially the formula :

$$C_{n+1}^i = C_n^i + C_n^{i-1}$$

and the following result : for all prime number $n+1$ and $i = 1...n$,

$$C_{n+1}^i \equiv 0 \quad [n+1]$$

Then :

$$\begin{aligned} C_n^i + C_n^{i-1} &\equiv 0 \quad [n+1] \\ C_n^i &\equiv -C_n^{i-1} \quad [n+1] \\ C_n^i \equiv (-1)^{i-1} C_n^1 &\equiv (-1)^i \quad [n+1] \end{aligned}$$

From which :

$$\begin{aligned} C_n^i &\equiv (-1)^i \quad [n+1] \\ (-1)^i C_n^i i^n \equiv (-1)^i (-1)^i i^n &\equiv i^n \quad [n+1] \\ \sum_{i=0}^{n} (-1)^i C_n^i i^n \equiv \sum_{i=1}^{n} i^n &\equiv (-1)^n n! = n! \quad [n+1] \end{aligned}$$

Then, the little Fermat's theorem is applied : $\forall i = 1...n$,

$$i^n \equiv 1 \quad [n+1]$$

Finally :

$$\sum_{i=1}^{n} i^n \equiv n \equiv n! \equiv -1 \quad [n+1]$$

This proof involves two different types of congruences, whereas we only use that of Fermat. Our method directly makes rise the result in a visual way while revealing the numbers of the form $k^n - k$ for all $k = 1...n$, and it is systematically as we will proceed thereafter to deduce new results of congruence.

2 Generalizations of Wilson's theorem

We have the following result using the Stirling numbers of the second kind.

Theorem S :

Let $m+1$ be a prime. Then, $\forall n \leq m$,

$$(-1)^n n! \left\{ {m \atop n} \right\} + 1 \equiv 0 \quad [m+1]$$

where the $\left\{ {m \atop n} \right\}$ are the Stirling's numbers of second kind, giving the number of n-partitions of a set of m elements.

Proof :

The Stirling numbers of the second kind $\left\{ {m \atop n} \right\}$ verify the following classical relation [1] :

$$\sum_{i=0}^{n} (-1)^i C_n^i i^m = (-1)^n n! \left\{ {m \atop n} \right\} \quad (1)$$

Applying the same method as in our proof of Wilson's theorem, (1) can be rewritten for all $m+1$ prime and $n \leq m$:

$$\sum_{i=1}^{n} (-1)^i C_n^i (i^m - 1) = (-1)^n n! \left\{ {m \atop n} \right\} + 1 \quad (2)$$

As again, $\forall i = 1...n$, $i^m - 1 \equiv 0 \quad [m+1]$.

Then,

$$(-1)^n n! \left\{ {m \atop n} \right\} + 1 \equiv 0 \quad [m+1]$$

Q.E.D.

One can still push our generalization further using the classical Euler's totient function $\varphi(n)$ which, to each integer n, associates the number of integers lower than n and prime with it.

Theorem E **:**

Let p, n be two integers such that $p > n$ and $\forall i \leq n, \quad i \wedge p = 1$.
We have then :

$$(-1)^n n! \left\{ \begin{matrix} \varphi(p) \\ n \end{matrix} \right\} + 1 \equiv 0 \quad [p]$$

Proof :

Let's make out first that if $\forall i \leq n, i \wedge p = 1$, we will have, by definition of $\varphi : \varphi(p) \geq n$, then $\left\{ \begin{matrix} \varphi(p) \\ n \end{matrix} \right\}$ is well-defined.

Besides, we know that the Euler's totient function allows us to generalize the little Fermat's theorem in the following way [4] :

$\forall i, p$ with $i \wedge p = 1$

$$i^{\varphi(p)} - 1 \equiv 0 \quad [p]$$

Let then p be an integer such that : $\forall i \leq n, i \wedge p = 1$.

By setting $m = \varphi(p)$ in (2), we obtain :

$$\sum_{i=0}^{n} (-1)^i C_n^i (i^{\varphi(p)} - 1) = (-1)^n n! \left\{ \begin{matrix} \varphi(p) \\ n \end{matrix} \right\} + 1$$

Yet, by hypothesis : $\forall i \leq n, i \wedge p = 1$

then :

$$\begin{aligned} \forall i \leq n, \quad & i^{\varphi(p)} - 1 \equiv 0 \quad [p] \\ \Rightarrow (-1)^n n! & \left\{ \begin{matrix} \varphi(p) \\ n \end{matrix} \right\} + 1 \equiv 0 \quad [p] \end{aligned}$$

Q.E.D.

Note : One finds the generalized theorem S, by setting $p = m + 1$ with $m + 1$ prime, which implies that : $\varphi(p) = m$.

Thus, the generalizations of the theorems of Wilson and Fermat are directly united in one and the same relation using the Stirling numbers of the second kind. Let us now turn to the characterization of the Carmichael numbers, on the basis of the same combinatorial relations again.

3 Characterizations of Carmichael's numbers

Definition :

We call Carmichael number every composed and non-negative integer κ verifying the following property :

$\forall a$ integer,

$$a^{\kappa} \equiv a \quad [\kappa]$$

The Carmichael numbers are also called absolutely pseudo-prime or "Fermat liars" because of their behaviour analogy with prime numbers, so much so that they defeat the Fermat primality test [3]. We will prove here a new very simple criterion for characterizing these numbers.

Criterion C_1 :

A composite integer κ is said of Carmichael if and only if :

$\forall n \leq \kappa - 1$,

$$n! \left\{ \begin{matrix} \kappa \\ n \end{matrix} \right\} \equiv 0 \quad [\kappa]$$

Proof :

Let's proceed in two steps.

Step 1

Let's prove first that a composite integer κ is of Carmichael if and only if : $\forall n$,

$$n! \left\{ \begin{matrix} \kappa \\ n \end{matrix} \right\} \equiv 0 \quad [\kappa]$$

Let us start from the relation (1) already mentioned at any n :

$$\sum_{i=0}^{n} (-1)^i C_n^i i^m = (-1)^n n! \left\{ \begin{matrix} m \\ n \end{matrix} \right\}$$

to which we subtract the relation :

$$\sum_{i=0}^{n} (-1)^i C_n^i i = 0$$

which is simply proved by setting $\alpha = 1$ in the Δ formula demonstrated at the beginning of our work.

One gets :

$$\sum_{i=0}^{n}(-1)^i C_n^i(i^m - i) = (-1)^n n! \left\{ {m \atop n} \right\} \quad (1')$$

sense $\Rightarrow$ *:*

Let κ be an integer of Carmichael. It verifies by definition : $\forall i$,

$$i^\kappa - i \equiv 0 \quad [\kappa]$$

Yet, for $m = \kappa$, $(1')$ becomes :

$$\sum_{i=0}^{n}(-1)^i C_n^i(i^\kappa - i) = (-1)^n n! \left\{ {\kappa \atop n} \right\}$$

Hence, by linearity of congruence :

$$(-1)^n n! \left\{ {\kappa \atop n} \right\} \equiv 0 \quad [\kappa]$$

That is to say :

$$n! \left\{ {\kappa \atop n} \right\} \equiv 0 \quad [\kappa]$$

sense $\Leftarrow$ *:*

Let now be a composed integer κ and let's suppose that : $\forall n$,

$$n! \left\{ {\kappa \atop n} \right\} \equiv 0 \quad [\kappa]$$

Let us show by recurrence on n that : $\forall n$,

$$n^\kappa - n \equiv 0 \quad [\kappa]$$

– This is verified for $n = 0$.
– Let's suppose the hypothesis is true for $n - 1$.
– We demonstrate it for n.

From :

$$\sum_{i=0}^{n}(-1)^i C_n^i(i^\kappa - i) = (-1)^n n! \left\{ {\kappa \atop n} \right\}$$

We deduce :

$$(-1)^n \left(n^\kappa - n\right) + \sum_{i=0}^{n-1}(-1)^i C_n^i(i^\kappa - i) = (-1)^n n! \left\{ {\kappa \atop n} \right\}$$

Then, according to our hypothesis :

$$\forall i \leq n-1, \quad i^\kappa - i \equiv 0 \quad [\kappa]$$

we get :

$$\sum_{i=0}^{n-1} (-1)^i C_n^i (i^\kappa - i) \equiv 0 \quad [\kappa]$$

and :

$$n! \left\{ \begin{matrix} \kappa \\ n \end{matrix} \right\} \equiv 0 \quad [\kappa]$$

Hence :

$$n^\kappa - n \equiv 0 \quad [\kappa]$$

The step 1 is completed. The obtained criterion can yet be simplified as follows.

Step 2

Let us prove that : κ is of Carmichael if and only if : $\forall n \leq \kappa - 1$,

$$n! \left\{ \begin{matrix} \kappa \\ n \end{matrix} \right\} \equiv 0 \quad [\kappa]$$

By definition of κ, the sense $\Rightarrow$ is immediate. As for the sense $\Leftarrow$, let us suppose that :

$$\forall n \leq \kappa - 1, \quad n! \left\{ \begin{matrix} \kappa \\ n \end{matrix} \right\} \equiv 0 \quad [\kappa]$$

We know that : $\forall n \geq \kappa, \quad n! \equiv 0 \quad (\kappa)$.

Then :

$$\begin{aligned} \forall n \geq \kappa, \quad & n! \left\{ \begin{matrix} \kappa \\ n \end{matrix} \right\} \equiv 0 \quad (\kappa) \\ \Rightarrow \quad \forall n, \quad & n! \left\{ \begin{matrix} \kappa \\ n \end{matrix} \right\} \equiv 0 \quad (\kappa) \end{aligned}$$

So, by definition, κ is a Carmichael number.

Q.E.D.

In the general case, let us prove the following result :

Lemma G :

$\forall n, m, p$ integers,

$$(\forall k \in [0,n], \quad k^m - k \equiv 0 \quad [p]) \Leftrightarrow \left(\forall l \in [0,n], \quad l! \left\{ {m \atop l} \right\} \equiv 0 \quad [p]\right)$$

Proof :

We start again from $(1')$:

$$\sum_{i=0}^{n} (-1)^i C_n^i (i^m - i) = (-1)^n n! \left\{ {m \atop n} \right\}$$

Let's set integers n, m, p.

- sense $\Rightarrow$:

We suppose that :

$$\forall k \in [0,n], \quad k^m - k \equiv 0 \quad [p]$$

Then, according to $(1')$ and by linearity of the congruence :

$\forall l \in [0,n]$,

$$\sum_{i=0}^{l} (-1)^i C_l^i (i^m - i) = (-1)^l l! \left\{ {m \atop l} \right\} \equiv 0 \quad [p]$$

- sense $\Leftarrow$:

Let us suppose :

$$\forall l \in [0,n], \quad l! \left\{ {m \atop l} \right\} \equiv 0 \quad [p]$$

Here, we remind the classical ***binomial inversion*** : given two sequences u_n and v_n, we have

$$u_n = \sum_{i=0}^{n} C_n^i v_i \Leftrightarrow v_n = \sum_{i=0}^{n} (-1)^{n-i} C_n^i u_i$$

We can apply the binomial inversion to $(1')$ to get :

$$\forall k, m, \quad \sum_{l=0}^{k} C_k^l l! \left\{ {m \atop l} \right\} = k^m - k$$

Then, by hypothesis, $\forall k \in [0,n]$ we have :

$$\forall l \in [0,k], \quad l! \left\{ {m \atop l} \right\} \equiv 0 \quad [p]$$

Thus, by linearity of congruence :

$$\forall k \in [0,n], \quad \sum_{l=0}^{k} C_k^l l! \left\{ {m \atop l} \right\} = k^m - k \equiv 0 \quad [p]$$

Q.E.D.

This lemma G highlights that a transfer of arithmetic properties is possible in both directions between $\{k^m - k\}_{k \in \mathbb{N}}$ numbers and Stirling numbers of the second kind. It allows us to prove in another manner this equivalent well-known definition of Carmichael numbers, which limits the number of congruences they must satisfy [3] :

A composite integer κ is a Carmichael number if and only if :

$\forall a \leq \kappa - 1,$

$$a^\kappa - a \equiv 0 \quad [\kappa]$$

Proof :

We just apply lemma G to criterion C_1, with κ a Carmichael number and $m = \kappa$, $n = \kappa - 1$, $p = \kappa$. *Q.E.D.*

Yet, we have a stronger result :

Criterion C_2 :

Let m be a composite square free integer whose largest prime factor is p. Then, m is a Carmichael number if and only if :

$\forall a \leq p - 1,$

$$a^m - a \equiv 0 \quad [m]$$

or equivalently,

$\forall a \leq p - 1,$

$$a! \left\{ {m \atop a} \right\} \equiv 0 \quad [m]$$

Proof :

At first, we note that this criterion is compatible with the properties of Carmichael numbers : we know that, according to the Korselt's criterion [3], a Carmichael number is always square free. Besides, it has at least three prime factors.

Now, we have $\forall a \geq p$, $a! \equiv 0 \quad [m]$: indeed, since by hypothesis m is square free and its largest prime factor is p, all its prime factors are smaller than a and of exponent 1. Thus, their product m divides $a!$ and, a fortiori, $a!\left\{ {m \atop a} \right\}$. So, thanks to criterion C_2, there is no need to use congruences :

$$a!\left\{ {m \atop a} \right\} \equiv 0 \quad [m]$$

for all $a \geq p$.

According to lemma G, this result is equivalent to : $\forall a \leq p-1$,

$$a^m - a \equiv 0 \quad [m]$$

At the end of the day, we can state an even stronger result.

Criterion C_3 :

Let m be a composite square free integer such that :

$$m = p_1.p_2.p_3...p_k$$

Then, the following propositions are equivalent :

1. m is a Carmichael number.

2. $\forall j \in [1,k]$, $\forall a \leq p_j - 1$,
$$a^m - a \equiv 0 \quad [p_j]$$

3. $\forall j \in [1,k]$, $\forall a \leq p_j - 1$,
$$a!\left\{ {m \atop a} \right\} \equiv 0 \quad [p_j]$$

4. $\forall j \in [1,k]$, $\forall a \leq p_j - 1$,
$$\left\{ {m \atop a} \right\} \equiv 0 \quad [p_j]$$

Proof :

Again, it is easier to consider first the $a!\left\{ {m \atop a} \right\}$ numbers because of the factorial's properties. For each prime factor p_j of m, we have indeed :

$$\forall a \leq p_j - 1, \quad a! \left\{ {m \atop a} \right\} \equiv 0 \quad [p_j] \Leftrightarrow \forall a \in \mathbb{N}, \quad a! \left\{ {m \atop a} \right\} \equiv 0 \quad [p_j]$$

given that $\forall a \geq p_j$, $a! \equiv 0 \quad [p_j]$.

Besides :

$$\forall j \in [1,k], \forall a \in \mathbb{N}, \quad a! \left\{ {m \atop a} \right\} \equiv 0 \quad [p_j] \Leftrightarrow \forall a \in \mathbb{N}, \quad a! \left\{ {m \atop a} \right\} \equiv 0 \quad [m]$$

since m is square free with : $m = p_1.p_2.p_3...p_k$. According to criterion C_1, the last member of the equivalence above characterizes the Carmichael numbers.

Then, m is a Carmichael number if and only if $\forall j \in [1,k]$, we have : $\forall a \leq p_j - 1$,

$$a! \left\{ {m \atop a} \right\} \equiv 0 \quad [p_j]$$

This proves $(1) \Leftrightarrow (3)$. Besides, according to lemma G, proposition (3) is equivalent to (2).

At last, $\forall j \in [1,k]$, p_j is a prime number then, if $a < p_j$, $a!$ and p_j are relatively prime, which implies that p_j divides $a! \left\{ {m \atop a} \right\}$ if and only if p_j divides $\left\{ {m \atop a} \right\}$: we have proved that $(3) \Leftrightarrow (4)$.
Q.E.D.

Applications :

- The smallest Carmichael number with seven prime factors is [3] : $m = 5394826801 = 7 \times 13 \times 17 \times 23 \times 31 \times 67 \times 73$. Then, according to criterion C_2, m is a Carmichael number if and only if m divides all the $a^m - a$ for $a = 1, ..., a = p$, where $p = 73$ is the largest prime factor of m. No need in theory to check the congruences from $a = 1$ to $a = 5394826801$.

- In the same way, $m = 1436697831295441 = 11 \times 13 \times 19 \times 29 \times 31 \times 37 \times 41 \times 43 \times 71 \times 127$ is the smallest Carmichael number with ten prime factors. Then, congruence checks should be performed only up to $a = 127$ instead of $a = 1436697831295441$.

4 Conclusion

We started from the same combinatorial relation :

$$\sum_{i=0}^{n} (-1)^i C_n^i i^n = (-1)^n n!$$

that we slightly transformed to prove directly and generalize the Wilson's theorem, then to propose several simplified characterizations of the Carmichael numbers.

Références

[1] Comtet, L., *Analyse combinatoire*, PUF, 1970.

[2] Ruiz, S. M., "An algebraic identity leading to Wilson's theorem", *The Mathematical Gazette*, vol. 80, no. 489, 1996.

[3] Villemin, G., "Nombres de Carmichaël ou pseudo-premiers absolus", `http://villemin.gerard.free.fr/ThNbDemo/Carmicha.htm`

[4] Weisstein, Eric W. "Euler's Totient Theorem." From MathWorld–A Wolfram Web Resource. `http://mathworld.wolfram.com/EulersTotientTheorem.html`

[5] Weisstein, Eric W. "Finite Difference." From MathWorld–A Wolfram Web Resource. `http://mathworld.wolfram.com/FiniteDifference.html`