A GENERALIZATION OF THE KORSELT'S CRITERION

NESTED CARMICHAEL NUMBERS

By Renaud LIFCHITZ[1]

March 2002
first release (last update : March 31, 2002)

1 Introduction to Carmichael numbers :

1°) Definition : A positive composite integer n is called a Carmichael number if and only if for all integer b we have $b^n \equiv b\ [n]$.

2°) **Korselt's Criterion (1899)**

Theorem :

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.

2 The generalization :

1°) Definitions :
Let $E = \{C_1, C_2, ..., C_z\}$ be a set of coprime Carmichael numbers.
Let f be a function that returns the product of the elements of a given set.
Let F be the set of prime factors of $f(E)$.
Let $P(E)$ be the set of parts of E without $\{\emptyset\}$, and let $S \in P(E)$.
Let T be the set of prime factors of $f(S)$.
Let $m = lcm\,\{p_i - 1 \text{ for all } p_i \in F\}$
Let $g = gcd\,\{C_j - 1 \text{ for all } C_j \in E\}$

2°) Theorem :

$$\boxed{(\forall S \quad f(S) \text{ is a Carmichael number}) \Longleftrightarrow (m \mid g)}$$

[1]Student at University of PARIS VI (Jussieu) : **RenaudL@orange.fr**
See http ://ourworld.compuserve.com/homepages/hlifchitz/Renaud.html

3^o) Proof :

• Suppose $m \mid g$.
By definition of g, we have $g \mid C_j - 1 \quad \forall C_j \in E$
which is equivalent to $C_j \equiv 1\ [g] \quad \forall C_j \in E$
it implies $f(S) \equiv 1\ [g]\ \forall S$ because $f(S)$ is a product of elements of E
so $g \mid f(S) - 1 \quad \forall S \quad$ (I)
but by definition of m, we have $(p_i - 1 \mid m \ \ \forall p_i \in F)$ (II)
and by hypothesis : $m \mid g$ (III)
with (II),(III) and (I) $\Longrightarrow p_i - 1 \mid f(S) - 1 \quad \forall p_i \in F, \forall S$
$\Longrightarrow p_i - 1 \mid f(S) - 1 \quad \forall p_i \in T, \forall S$ because $S \in P(E) \Longrightarrow T \subseteq F$
By Korselt's criterion, $\forall S \ \ f(S)$ is a Carmichael number.

• Conversely, suppose ($\forall S \quad f(S)$ is a Carmichael number).
By Korselt's criterion :
$p_i - 1 \mid \left(\prod_{i \neq k} C_i\right) - 1 \quad \forall k, \forall p_i \mid \prod_{i \neq k} C_i$ (IV) because $\left(\prod_{i \neq k} C_i\right)$ is Carmichael
likewise, $p_i - 1 \mid \left(\prod_i C_i\right) - 1 \quad \forall k, \forall p_i \mid \prod_{i \neq k} C_i$ because $\left(\prod_i C_i\right)$ is Carmichael
it implies that $p_i - 1 \mid \left(\prod_i C_i\right) - \left(\prod_{i \neq k} C_i\right) \quad \forall k, \forall p_i \mid \prod_{i \neq k} C_i$
consequently, $p_i - 1 \mid \left(\left(\left(\prod_{i \neq k} C_i\right) - 1\right) + 1\right) . (C_k - 1) \quad \forall k, \forall p_i \mid \prod_{i \neq k} C_i$
(IV) implies $p_i - 1 \mid C_k - 1 \quad \forall k, \forall p_i \mid \prod_{i \neq k} C_i$ (V)
and of course, $p_i - 1 \mid C_k - 1 \quad \forall k, \forall p_i \mid C_k$ (VI) because C_k is Carmichael
(V)+(VI) $\Longrightarrow p_i - 1 \mid C_k - 1 \quad \forall C_k \in E, \forall p_i \in F$
$\Longrightarrow m \mid C_k - 1 \quad \forall C_k \in E$
$\Longrightarrow m \mid g$ $\square$

3 The concept of nested Carmichaels :

When $|S| = 1$, the previous theorem becomes :

$$C \text{ is a Carmichael number} \Longleftrightarrow lcm\,\{p_i - 1\} \mid C - 1$$

which is clearly equivalent to :

$$C \text{ is a Carmichael number} \Longleftrightarrow p_i - 1 \mid C - 1 \qquad \forall p_i \mid C$$

which is exactly the Korselt's criterion. But Korselt's criterion is only valid for a single Carmichael number. The above part gives a generalization for any number of Carmichael numbers. This leads us to the definition of a new concept : "a set of nested Carmichaels".

1^o) Definition : Using the definitions of the part 2, a set S is "a set of nested Carmichaels" if and only if $\forall\ S\ f(S)$ is a Carmichael number.

2^o) Example : One of the smallest set S of 2 elements is $S = \{C_1, C_2\}$ with $C_1 = 1729 = 7.13.19$ and $C_2 = 294409 = 37.73.109$. Thus, C_1, C_2, and $C_1.C_2$ are all Carmichael numbers.

A much more interesting set is for example $S = \{7207201, 230630401, 56951294401, 571019248801, 3278310235201, 3815902490401, 11943915984001, 129766580143201, 353830002926401, 831957935608801, 2210772268504801, 4513636250323201,$

$5514474572006401, 7571362807008001, 26830954437487201, 80222538033237601,$
$828430182206827201, 997651728495021601, 10229943908539555201, 28430757383895266401,$
$340866183402412668001, 474235364684225944801, 1254602952776990031415201,$
$12617108093511625126309286401\}$

Indeed, such a set of length $|S| = 24$ contains

$$\sum_{i=1}^{24} \binom{24}{i} = 2^{24} - 1 = 16\ 777\ 215$$

Carmichael numbers, which is quite huge compared with the 24 elements of S ! This set was found using a specific program, and the necessary conditions of the theorem. The decimal expansion of the 16 777 215 Carmichael numbers cannot fit in a CD (650 MB), even compressed, but one can easily recover them only using the 24 elements of S...

Conclusion : Thus, a nested set of Carmichael numbers provides a very efficient way to store $2^n - 1$ Carmichael numbers using only n numbers (which represents an exponential compression rate !) Could this be useful for future applications ?