A GENERALIZATION OF THE
KORSELT’S CRITERION

NESTED CARMICHAEL NUMBERS

By Renaud LIFCHITZ

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 $m = \text{lcm}\{p_i - 1 \text{ for all } p_i \in F\}$
Let $g = \gcd\{C_j - 1 \text{ for all } C_j \in E\}$

2°) Theorem :
$$(\forall S \ f(S) \text{ is a Carmichael number} \iff (m \ | \ g)$$

1 Student at University of PARIS VI (Jussieu) : RenaudL@orange.fr
See http://ourworld.compuserve.com/homepages/hilfchitz/Renaud.html
3°) Proof:

• Suppose \( m \mid g \).
By definition of \( g \), we have \( g \mid C_j - 1 \ \forall C_j \in E \)
which is equivalent to \( C_j \equiv 1 \mod g \ \forall C_j \in E \)
it implies \( f(S) \equiv 1 \mod g \ \forall S \) because \( f(S) \) is a product of elements of \( E \)
so \( g \mid f(S) - 1 \ \forall S \) (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) \( \implies p_i - 1 \mid f(S) - 1 \ \forall p_i \in F, \forall S \)
\( \implies p_i - 1 \mid f(S) - 1 \ \forall p_i \in T, \forall S \) because \( S \in P(E) \implies T \subseteq F \)
By Korselt’s criterion, \( \forall S \ f(S) \) is a Carmichael number.

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

3 The concept of nested Carmichaels:

When \(|S| = 1\), the previous theorem becomes :
\[ C \text{ is a Carmichael number } \iff \text{lcm } \{p_i - 1\} \mid C - 1 \]
which is clearly equivalent to :
\[ C \text{ is a Carmichael number } \iff p_i - 1 \mid C - 1 \ \forall p_i \mid C \]
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°) 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°) Example : One of the smallest set \( S \) of 2 elements is \( S = \{C_1, C_2\} \) with
\( C_1 = 1729 = 7 \cdot 13 \cdot 19 \) and \( C_2 = 294409 = 37 \cdot 73 \cdot 109 \). 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, 3273810253201, 381590249001, 1194391598401, 129766580143201, 353830002926401, 831957935608801, 221072268504801, 451363625032201, \}

2
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?