ON CARMICHAËL’S CONJECTURE

Florentin Smarandache
University of New Mexico
200 College Road
Gallup, NM 87301, USA
E-mail: smarand@unm.edu

Carmichaël’s conjecture is the following: “the equation \( \varphi(x) = n \) cannot have a unique solution, \((\forall)n \in \mathbb{N}\), where \( \varphi \) is the Euler’s function”. R. K. Guy presented in [1] some results on this conjecture; Carmichaël himself proved that, if \( n_0 \) does not verify his conjecture, then \( n_0 > 10^{37} \); V. L. Klee [2] improved to \( n_0 > 10^{400} \), and P. Masai & A. Valette increased to \( n_0 > 10^{1000} \). C. Pomerance [4] wrote on this subject too.

In this article we prove that the equation \( \varphi(x) = n \) admits a finite number of solutions, we find the general form of these solutions, also we prove that, if \( x_0 \) is the unique solution of this equation (for a \( n \in \mathbb{N} \)), then \( x_0 \) is a multiple of \( 2^2 \cdot 3^2 \cdot 7^2 \cdot 43^2 \) (and \( x_0 > 10^{10000} \) from [3]).

§1. Let \( x_0 \) be a solution of the equation \( \varphi(x) = n \). We consider \( n \) fixed. We’ll try to construct another solution \( y_0 \neq x_0 \).

The first method:
We decompose \( x_0 = a \cdot b \) with \( a, b \) integers such that \((a, b) = 1\).
we look for an \( a' \neq a \) such that \( \varphi(a') = \varphi(a) \) and \((a', b) = 1\); it results that \( y_0 = a' \cdot b \).

The second method:
Let’s consider \( x_0 = q_1^{\alpha_1} \cdots q_s^{\alpha_s} \), where all \( q_i \in \mathbb{N}^* \), and \( q_1, \ldots, q_s \) are distinct primes two by two; we look for an integer \( q \) such that \((q, x_0) = 1 \) and \( \varphi(q) \) divides \( x_0 / (q_1, \ldots, q_s) \); then \( y_0 = x_0 q / \varphi(q) \).

We immediately see that we can consider \( q \) as prime.

The author conjectures that for any integer \( x_0 \geq 2 \) it is possible to find, by means of one of these methods, a \( y_0 \neq x_0 \) such that \( \varphi(y_0) = \varphi(x_0) \).

Lemma 1. The equation \( \varphi(x) = n \) admits a finite number of solutions, \((\forall)n \in \mathbb{N}\).

Proof. The cases \( n = 0, 1 \) are trivial.
Let’s consider \( n \) to be fixed, \( n \geq 2 \). Let \( p_1 < p_2 < \ldots < p_s \leq n + 1 \) be the sequence of prime numbers. If \( x_0 \) is a solution of our equation (1) then \( x_0 \) has the form
\( x_0 = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \), with all \( \alpha_i \in \mathbb{N} \). Each \( \alpha_i \) is limited, because:
\((\forall)i \in \{1, 2, \ldots, s\}, (\exists) a_i \in \mathbb{N}: p_i^{\alpha_i} \geq n\).
Whence \( 0 \leq \alpha_i \leq a_i + 1 \), for all \( i \). Thus, we find a wide limitation for the number of solutions: 
\[
\prod_{i=1}^{s} (a_i + 2)
\]

**Lemma 2.** Any solution of this equation has the form (1) and (2):
\[
x_0 = n \cdot \left( \frac{p_1}{p_1 - 1} \right)^{e_1} \cdots \left( \frac{p_s}{p_s - 1} \right)^{e_s} \in \mathbb{Z},
\]
where, for \( 1 \leq i \leq s \), we have \( e_i = 0 \) if \( \alpha_i = 0 \), or \( e_i = 1 \) if \( \alpha_i \neq 0 \).

Of course, \( n = \varphi(x_0) = x_0 \left( \frac{p_1}{p_1 - 1} \right)^{e_1} \cdots \left( \frac{p_s}{p_s - 1} \right)^{e_s} \),
whence it results the second form of \( x_0 \).

From (2) we find another limitation for the number of the solutions: \( 2^s - 1 \) because each \( e_i \) has only two values, and at least one is not equal to zero.

§2. We suppose that \( x_0 \) is the unique solution of this equation.

**Lemma 3.** \( x_0 \) is a multiple of \( 2^2 \cdot 3^2 \cdot 7^2 \cdot 43^2 \).

**Proof.** We apply our second method.
Because \( \varphi(0) = \varphi(3) \) and \( \varphi(1) = \varphi(2) \) we take \( x_0 \geq 4 \).
If \( 2 \mid x_0 \) then there is \( y_0 = 2x_0 \neq x_0 \) such that \( \varphi(y_0) = \varphi(x_0) \), hence \( 2 \mid x_0 \); if \( 4 \mid x_0 \), then we can take \( y_0 = x_0 / 2 \).
If \( 3 \mid x_0 \) then \( y_0 = 3x_0 / 2 \), hence \( 3 \mid x_0 \); if \( 9 \mid x_0 \) then \( y_0 = 2x_0 / 3 \), hence \( 9 \mid x_0 \); whence \( 4 \cdot 9 \mid x_0 \).
If \( 7 \mid x_0 \) then \( y_0 = 7x_0 / 6 \), hence \( 7 \mid x_0 \); if \( 49 \mid x_0 \) then \( y_0 = 6x_0 / 7 \) hence \( 49 \mid x_0 \); whence \( 4 \cdot 9 \cdot 49 \mid x_0 \).
If \( 43 \mid x_0 \) then \( y_0 = 43x_0 / 42 \), hence \( 43 \mid x_0 \); if \( 43^2 \mid x_0 \) then \( y_0 = 42x_0 / 43 \), hence \( 43^2 \mid x_0 \); whence \( 2^2 \cdot 3^2 \cdot 7^2 \cdot 43^2 \mid x_0 \).
Thus \( x_0 = 2^{\gamma_1} \cdot 3^{\gamma_2} \cdot 7^{\gamma_3} \cdot 43^{\gamma_4} \cdot t \), with all \( \gamma_i \geq 2 \) and \( (t, 2^3 \cdot 7 \cdot 43) = 1 \) and \( x_0 > 10^{10000} \) because \( n_0 > 10^{10000} \).

§3. Let’s consider \( y_i \geq 3 \). If \( 5 \mid x_0 \) then \( 5x_0 / 4 = y_0 \), hence \( 5 \mid x_0 \); if \( 25 \mid x_0 \) then \( y_0 = 4x_0 / 5 \), whence \( 25 \mid x_0 \).
We construct the recurrent set \( M \) of prime numbers:
a) the elements \( 2, 3, 5 \in M \);
b) if the distinct odd elements \( e_1, \ldots, e_n \in M \) and \( b_m = 1 + 2^m \cdot e_1, \ldots, e_n \) is prime, with \( m = 1 \) or \( m = 2 \), then \( b_m \in M \);
c) any element belonging to \( M \) is obtained by the utilization (a finite number of times) of the rules a) or b) only.

The author conjectures that \( M \) is infinite, which solves this case, because it results that there is an infinite number of primes which divide \( x_0 \). This is absurd.

For example 2, 3, 5, 7, 11, 13, 23, 29, 31, 43, 47, 53, 61, … belong to \( M \).
The method from §3 could be continued as a tree (for \( \gamma_2 \geq 3 \) afterwards \( \gamma_3 \geq 3 \), etc.) but its ramifications are very complicated…

REFERENCES


[Published in “Gamma”, XXIV, Year VIII, No. 2, February 1986, pp. 13-14.]