International Journal of Applied Mathematics

Volume 35 No. 3 2022, 393-396
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
doi: http://dx.doi.org/10.12732/ijam.v35i3.3

A NOTE ON CARMICHAEL'S CONJECTURE

Antonio A. Andrade[1], Guilherme Z. Cundari[2 §]

[1,2] Department of Mathematics
São Paulo State University
São José do Rio Preto - SP, 15054-000, BRAZIL

Abstract: Euler's totient function (also known as Euler's φ-function or just Euler's function) was introduced by Leonhard Euler (1707-1783) in 1760, motivated by a problem proposed by Pierre of Fermat (1607-1665). Given a positive integer n, in this work, we present new results about the existence of a positive integer m such that $\varphi(m) = \varphi(n)$.

AMS Subject Classification: 11A41, 11A25, 11A99
Key Words: Euler function; prime number; Carmichael's conjecture

1. Introduction

Euler's totient function counts the positive integers up to a given integer n that are relatively prime to n. It is written using the Greek letter ϕ as $\phi(n)$ or $\varphi(n)$, and may also be called Euler's φ-function. In other words, it is the number of integers k in the range $1 \leq k < n$ for which the greatest common divisor $\gcd(n, k)$ is equal to 1.

The function $\varphi : \mathbb{N} \to \mathbb{N}$ that associates each $n \in \mathbb{N} - \{0\}$ to the number of elements of the set

$$\{k \in \mathbb{N} - \{0\} \ : \ 1 \leq k \leq n \quad \text{and} \quad \gcd(k, n) = 1\}$$

is called Euler's φ-function. For example, for $n = 8$, it follows that $\varphi(8) = 4$, since the numbers less than 8 and primes with 8 are 1, 3, 5, and 7.

Received: February 21, 2022

[§]Correspondence author

2. Carmichael's conjecture

In this section, initially, we briefly review the results that will be needed subsequently. Many of them will be assumed known to the reader, those interested in further details are referred to Ribenboim [1]. After, we present new results about the Carmichael's conjecture, that is, the existence of a positive integer m such that $\varphi(m) = \varphi(n)$ (Carmichael [2]).

Not every even integer $m > 1$ is a value of Euler's function, and that fact is not difficult to establish. For example, Schinzel showed in 1956 that, for every $k \geq 1$, $2 \cdot 7^k$ is not a value of Euler's function. In 1976, Mendelsohn showed that there exist infinitely many primes p such that, for every $k \geq 1$, $2^k p$ is not a value of the function φ. Concerning interesting values assumed by Euler's function, Erdös in 1946 proposed as a problem to show that for every $k \geq 1$ there exists n such that $\varphi(n) = k!$. A solution by Lambek was proposed in 1948; the same result was given later by Gupta in 1950.

An interesting question is: how often a value $\varphi(n)$ is assumed. If $m \geq 1$, let

$$A_\varphi(m) = \#\{n : \varphi(n) = m\}.$$

There are infinitely many even integers m for which $A_\varphi(m) = 0$. Furthermore, if $m = 2 \cdot 3^{6k+1}$, where $k \geq 1$, then $\varphi(n) = m$ exactly when $n = 3^{6k+2}$ or $n = 2 \cdot 3^{6k+2}$, and therefore, there are infinitely many integers m such that $A_\varphi(m) = 2$. Robert Carmichael first stated this conjecture in 1907, but as a theorem rather than as a conjecture. However, his proof was faulty, and in 1922, he retracted his claim and stated the conjecture as an open problem.

A conjecture that dominates the study of the valence of φ was proposed by Carmichael in 1922, i.e., A_φ does not assume the value 1. In other works, given $n > 1$, there exists $m > 1$, with $m \neq n$, such that $\varphi(m) = \varphi(n)$.

Proposition 1. *The conjecture holds for all odd positive integers.*

Proof. Let n be any positive odd. Since $\gcd(n, 2) = 1$, it follows that $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$. That is, for every odd n, $\varphi(n) = \varphi(2n)$. □

Now it remains for us to prove the validity for even numbers of the form $2n$, with n being any even.

Lemma 2. *The conjecture holds for all powers of* 2.

Proof. Let $n = 2^k$, with $k \in \mathbb{N}$ and $k \geq 2$ (the case $k = 1$ follows from the previous case), and $m = 3 \cdot 2^{k-1}$. Let us show that $\varphi(n) = \varphi(m)$. Since 2 is prime, it follows that $\varphi(2^k) = 2^{k-1}(2-1) = 2^{k-1} \cdot 1 = 2^{k-1}$, that is, $\varphi(2^k) = 2^{k-1}$. Now, as $\gcd(3, 2^{k-1}) = 1$, it follows that $\varphi(3 \cdot 2^{k-1}) = \varphi(3)\varphi(2^{k-1}) = 2 \cdot 2^{k-2} = 2^{k-1}$, that is, $\varphi(3 \cdot 2^{k-1}) = 2^{k-1}$. Therefore, $\varphi(2^k) = \varphi(3 \cdot 2^{k-1})$. □

Proposition 3. *The conjecture holds for all evens of the form* $2n$*, with* n *even and* $\gcd(n, 3) = 1$*, that is, that do not have the* 3 *in their factorization.*

Proof. Let $n_1 = 2^k \cdot p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ an integer in its factored form, $p_i \neq 3$ for all i, with $1 \leq i \leq r$, and $n_2 = 2^{k-1} \cdot 3 \cdot p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Let us show that $\varphi(n_1) = \varphi(n_2)$. Since all p_i are primes and different from each other, they are clearly co-prime, so we can use the multiplicative property of the function in all its factors, i.e.,

$$\begin{aligned} \varphi(n_1) &= \varphi(2^k)\varphi(p_1^{\alpha_1}) \ldots \varphi(p_r^{\alpha_r}) = 2^{k-1}\varphi(p_1^{\alpha_1}) \ldots \varphi(p_r^{\alpha_r}) \\ &= \varphi(2^{k-1} \cdot 3)\varphi(p_1^{\alpha_1}) \ldots \varphi(p_r^{\alpha_r}) \\ &\overset{*}{=} \varphi(2^{k-1} \cdot 3 \cdot p_1^{\alpha_1} \ldots p_r^{\alpha_r}) = \varphi(n_2). \end{aligned}$$

Therefore, $\varphi(n_1) = \varphi(n_2)$. Note that the equality $\overset{*}{=}$ is valid only because 3 is not in the factorization of n_1. □

Now we have reached a point where we can get around our problem of taking the 3 out of factorization, but we need to take some other number out, and to get that one we need to do this process again with no apparent end. This is because we will arrange the factors so that the φ of a prime comes up, and so originally it cannot be in factorization.

Example 4. Let $n_1 = 2^k \cdot 3^m \cdot p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ and $n_2 = 2^{k-1} \cdot 3^{m-1} \cdot 7 \cdot p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, with $k, m \geq 2$ and $p_i \neq 7$ for all i such that $1 \leq i \leq r$. Thus

$$\begin{aligned} \varphi(n_1) &= \varphi(2^k)\varphi(3^m)\varphi(p_1^{\alpha_1}) \ldots \varphi(p_r^{\alpha_r}) \\ &= 2^{k-1} \cdot 3^{m-1} \cdot 2 \cdot \varphi(p_1^{\alpha_1}) \ldots \varphi(p_r^{\alpha_r}) \\ &= 2^{k-2} \cdot 2 \cdot 3^{m-2} \cdot 3 \cdot 2 \cdot \varphi(p_1^{\alpha_1}) \ldots \varphi(p_r^{\alpha_r}) \\ &= 2^{k-2} \cdot 3^{m-2} \cdot 2 \cdot 3 \cdot 2 \cdot \varphi(p_1^{\alpha_1}) \ldots \varphi(p_r^{\alpha_r}) \\ &= 2^{k-2} \cdot 3^{m-2} \cdot 2 \cdot 6 \cdot \varphi(p_1^{\alpha_1}) \ldots \varphi(p_r^{\alpha_r}) \\ &= \varphi(2^{k-1})\varphi(3^{m-1})\varphi(7)\varphi(p_1^{\alpha_1}) \ldots \varphi(p_r^{\alpha_r}) \\ &\overset{**}{=} \varphi(2^{k-1} \cdot 3^{m-1} \cdot 7 \cdot p_1^{\alpha_1} \ldots p_r^{\alpha_r}) = \varphi(n_2). \end{aligned}$$

Note, again, that the equality $\overset{**}{=}$ is valid only because 7 is not in the factorization of n_1.

Now, analogously, we can prove for numbers that have both the 3 and the 7 in their factorization by guaranteeing the absence of another number, for example, 5, because we can separate 2^2 from the power of 2 that appears in $\varphi(n_1)$ and we write it as $\varphi(5)$, since $\varphi(5) = 4$.

Following the same logic, we can always get around our impediment if we manage to generate another prime from the product of previous ones plus 1, in other words, if there are infinitely many of these numbers, than Carmichael's conjecture is true. Notice that if any of these primes has exponent one in the factorization, then the problem will be solved, because this case is just the reciprocal of the previous examples, which means that our concern must be numbers that have in their factorization these primes with exponents greater or equal to 2. But we cannot guarantee that they will have exponents greater than 2, so the primes in the product we use to generate others must be only to the power of 1 or 2. This numbers are known as "Higgs primes", more specifically "Higgs primes for exponent 2", and are named after Denis Higgs. To give it a formal definition, a Higgs prime Hp_n for exponent 2 satisfies $\varphi(Hp_n)$ divides $\prod_{i=1}^{n-1} {Hp_i}^2$ and $Hp_n > Hp_{n-1}$.

It is not known if there are infinitely many Higgs primes for any exponent a greater than 1. It is also not difficult to observe that if Carmichael's conjecture is true, than there are infinitely many Higgs primes. A simple way to prove it is supposing that they are finite, and concluding, by the same logic seen before, that there are no numbers with the same φ of the number formed by the product of all Higgs primes to the power of 2, since there is no possible way to rearrange the numbers the way we did previously and generate another prime, change the power or take one of them out, which means Carmichael's conjecture would be false. In other words, we can conclude that Carmichael's conjecture is true if, and only if, there are infinitely many Higgs primes.

References

[1] P. Ribenboim, *The Little Book of Bigger Primes*, Springer Verlag, New York (1991).

[2] R.D. Carmichael, Note on Euler's φ-function, *Bull. Amer. Math. Soc.*, **28** (1922), 109-110.