Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 25, 2019, No. 1, 32–35
DOI: 10.7546/nntdm.2019.25.1.32-35

A note on Euler's totient function

József Sándor

Department of Mathematics, Babeş-Bolyai University
Str. Kogalniceanu 1, 400084 Cluj-Napoca, Romania
e-mail: `jsandor@math.ubblcuj.ro`

Received: 12 October 2018 **Accepted:** 24 February 2019

Abstract: We prove by elementary arguments that the inequalities $\varphi(2^k + 1) > 2^{k-1}$ and $\varphi(2^m + 1) < 2^{m-1}$ both have infinitely many solutions.
Keywords: Euler's totient, Primes, Fermat's little theorem, Quadratic residues.
2010 Mathematics Subject Classification: 11A07, 11A25, 11N37.

1 Introduction

The Euler totient function φ is defined as follows. For $n > 1$, put $\varphi(n)$ for the number of all $x \leq n$ such that $(x, n) = 1$. This function plays an important role in many fields of mathematics (see e.g. [5]). Put $\varphi(1) = 1$ and for $n > 1$, let $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ be the prime factorization of n. Then it is well-known that holds the following formula:

$$\varphi(n) = p_1^{\alpha_1} \dots p_r^{\alpha_r} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right), \tag{1}$$

or in another notation,

$$\frac{\varphi(n)}{n} = \prod_{q|n} \left(1 - \frac{1}{q}\right), \tag{2}$$

where q runs through all the prime divisors of n (see e.g. [1]). There exist many classical inequalities involving the function φ. The most known one is

$$\varphi(n) \leq n - 1 \text{ for all } n \geq 2 \tag{3}$$

with equality only for $n =$ prime. Also (see [1, 5]),

$$\varphi(mn) \leq m\varphi(n), \quad m, n \geq 1. \tag{4}$$

As a corollary to (4) we get the following:

If $a|b$, (i.e. a is a divisor of b), then

$$\frac{\varphi(b)}{b} \leq \frac{\varphi(a)}{a}. \tag{5}$$

Indeed, let $b = aq$. Then, by (4) we can write $\varphi(b) = \varphi(aq) \leq q\varphi(a) = \frac{b}{a}\varphi(a)$, implying relation (5).

By studying the properties of certain "composite functions" ([4], see also [2, 3]) we have encountered recently the following inequality:

$$\varphi(2^k + 1) > 2^{k-1}, \quad k \geq 1. \tag{6}$$

By checking this relation for some values (say $k \leq 10$), we get that (6) is true. But more surprising was that, by using a computer (e.g. Maple system), we find that relation (6) holds true also for all $k \leq 137(!)$.

By taking into account the complexity of numbers of type 2^k+1, probably, it would be difficult to get a counterexample to (6), by using direct computations.

Our aim in what follows is to show that (6) holds true for infinitely many k, but it is not true for other infinitely many values of k.

2 Main results

Theorem 1.

1) For sufficiently large prime numbers p *(i.e.* $p \geq p_0$*) one has*

$$\varphi(2^p + 1) > 2^{p-1}. \tag{7}$$

2) There are infinitely many numbers k *such that*

$$\varphi(2^k + 1) < 2^{k-1}. \tag{8}$$

Proof. Let $p_1 < p_2 < \cdots < p_n < \ldots$ be the set of all primes of the form $p \equiv 3 \pmod 8$. By Fermat's little theorem one has

$$p|2^{p-1} - 1 = (2^{(p-1)/2} - 1)(2^{(p-1)/2} + 1).$$

Remark that p cannot divide the first paranthese, since in that case, $\frac{p-1}{2}$ being odd, we would get that 2 is a quadratic residue $mod\, p$. It is well-known (see e.g. [1]) that this is not true for primes of the form $p \equiv 3 \pmod 8$. Therefore

$$p|2^{(p-1)/2} + 1. \tag{9}$$

Let us now define

$$k_0 = lcm\left[\frac{p_1 - 1}{2}, \ldots, \frac{p_m - 1}{2}\right], \tag{10}$$

(where lcm denotes the least common multiple). Then as k_0 is odd, $2^{k_0}+1 = 2^{\frac{M(p_1-1)}{2}}+1$ is divisible by $2^{(p_1-1)/2}+1$, which by (9) is divisible by p_1. The same can be repeated for all primes p_i $(i=\overline{1,m})$. Thus

$$p_1p_2\dots p_m|2^{k_0}+1. \tag{11}$$

Now, by inequality (5) one gets

$$\frac{\varphi(2^{k_0}+1)}{2^{k_0}+1} \le \frac{\varphi(p_1\dots p_m)}{p_1\dots p_m} = \left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_m}\right), \tag{12}$$

by (2).

It is well-known that $\lim_{m\to\infty}\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_m}\right)=0$ (which, essentially follows from the divergence of the series $\sum_{m\ge 1}\frac{1}{p_m}$); therefore for all $\varepsilon>0$ one can find $m\ge m_0$ such that $\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_m}\right)<\varepsilon$. For $\varepsilon=\frac{1}{4}$, we get from (12) that

$$\varphi(2^{k_0}+1)<(2^{k_0}+1)\cdot\frac{1}{4}<2^{k_0-1},\ \text{as } 2^{k_0}>1.$$

Put now $k=K\cdot k_0$, where K is an arbitrary odd number. Then it is immediate from above that, k also satisfies inequality (8). This finishes the proof of Part 2). □

Now, from the proof of Part 1) we need an auxiliary result:

Lemma 1.

$$\lim_{\substack{p\to\infty\\ p\ prime}}\frac{\varphi(2^p+1)}{2^p+1}=\frac{2}{3}. \tag{13}$$

Proof. If p is an odd prime, then 2^p+1 is divisible by 3, by a well-known divisibility criterion. By (5) we get

$$\frac{\varphi(2^p+1)}{2^p+1}\ge\frac{2}{3}\ \text{for all } p\ge 3. \tag{14}$$

On the other hand, all other prime factors of $M_p=2^p+1$ are $q\equiv 1 \pmod p$ (this follows by Fermat's little theorem), and the number of such prime is

$$O(\log M_p/\log\log M_p)$$

(see the results for $\omega(n)$ = number of distinct prime divisors of n, [1, 5]). Clearly,

$$O(\log M_p/\log\log M_p)=O(p/\log p). \tag{15}$$

Therefore, by relation (3) one has

$$\frac{\varphi(M_p)}{M_p}\ge\frac{2}{3}\left(1-\frac{1}{2p+1}\right)^{O(p/\log p)}, \tag{16}$$

since $q=2s+1\ge 2p+1$ ($s=1$ is impossible, since then q = even). But

$$\lim_{p\to\infty}\left(1-\frac{1}{2p+1}\right)^{O(p/\log p)}=1,$$

and relation (14) combined with (16) gives (13).

Now for the proof of (7) remark that, by (13), for all $\varepsilon > 0$ there is $p_0 \in \mathbb{N}$ such that for $p \geq p_0$ one has

$$\varphi(2^p + 1) > \left(\frac{2}{3} - \varepsilon\right)(2^p + 1).$$

Put $\varepsilon = \frac{1}{6}$. Then $\frac{2}{3} - \varepsilon = \frac{1}{2}$, and $\frac{1}{2}(2^p + 1) = 2^{p-1} + \frac{1}{2} > 2^{p-1}$, so finally, relation (7) follows for all sufficiently large primes p. □

3 Remarks

By more complicated arguments, it can be shown that (8) holds true for a positive proportion of values of k ([4], see also [2, 3]).

References

[1] Hardy, G. H. & Wright, E. N. (1964). *An Introduction to the Theory of Numbers*, Oxford University Press.

[2] Sándor, J. (1989). *On the composition of some arithmetic functions, I. Studia Univ. Babeş-Bolyai, Math.*, 34, 7–14.

[3] Sándor, J. (2005). *On the composition of some arithmetic functions, II. J. Ineq. Pure Appl. Math.*, 6 (2), Article No. 73.

[4] Sándor, J. (2005). *On the composition of some arithmetic functions, III.* (unpublished manuscript).

[5] Sándor, J. & Crstici, B. (2004). *Handbook of Number Theory II*, Springer.