Publ. Math. Debrecen
59 / 1-2 (2001), 9–16

A conjecture of Erdős concerning inequalities for the Euler totient function

By A. GRYTCZUK (Zielona Góra),
F. LUCA (Morelia) and M. WÓJTOWICZ (Zielona Góra)

Abstract. We partially confirm a conjecture of Erdős concerning inequalities between $\phi(n)$ and $\phi(n-\phi(n))$, where ϕ is the Euler totient function.

1. Introduction

For any positive integer n let $\phi(n)$ be the Euler ϕ function of n. Let $\varrho(M)$ denote the *density* (if it exists) of a nonempty subset M of the set of all positive integers $\mathbb{N}$, i.e.,

$$\varrho(M) = \lim_{n\to\infty} \frac{\#\{m \in M : m < n\}}{n};$$

the *lower density* of M is defined as

$$\varrho_*(M) = \liminf_{n\to\infty} \frac{\#\{m \in M : m < n\}}{n}.$$

We say that a property (P) defined on $\mathbb{N}$ holds for almost all n if $\rho(M_P)=1$, where $M_P = \{n \in \mathbb{N} : n \text{ satisfies } (P)\}$.

In [1] (see also **B42** in [3]), Erdős asks us to prove that $\phi(n) > \phi(n-\phi(n))$ for almost all n, but that $\phi(n) < \phi(n-\phi(n))$ for infinitely many n.

Mathematics Subject Classification: 11A25, 11L20, 11L26.
Key words and phrases: Euler function.
Work by the second author was supported by the Alexander von Humboldt Foundation.

Let us partition the set of all positive integers $\mathbb{N}$ in three pairwise disjoint classes, namely:

$$A = \{n \in \mathbb{N}^* : \phi(n) > \phi(n - \phi(n))\};$$

$$B = \{n \in \mathbb{N}^* : \phi(n) = \phi(n - \phi(n))\};$$

$$C = \{n \in \mathbb{N}^* : \phi(n) < \phi(n - \phi(n))\}.$$

Then the Erdős conjecture takes the form

(EC1) *we have* $\varrho(A) = 1$, *and*

(EC2) $\#(C) = \aleph_0$;

in particular, *the sets A and C are infinite*. It is easily seen that the set B is infinite because it contains the numbers of the form $n = 2^k 3$ and that the sets A and C are infinite follows from our theorems presented below. In Theorem 1 we partially confirm (EC1) by proving that $\rho_*(A) \geq 0.54$, while in Theorem 3 we prove a stronger version of (EC2) by showing that $\phi(n_k) + 2^k \leq \phi(n_k - \phi(n_k))$ for some infinite sequences of positive integers $(n_k)_{k=1}^{\infty}$. Theorem 2 completes Theorem 1 by indicating a "nice" infinite subset of A. It seems likely that the claim that C is infinite to be already known but we could not find any reference to this fact.

2. The results

Let A, B and C be the sets defined in previous section. We say that a number n satisfies relation (A) (or (B), or (C)) if $n \in A$ (or $n \in B$, or $n \in C$).

While we are not able to confirm (EC1), we can at least show that "more" integers satisfy inequality (A) than inequalities (B) and (C) together. That is, we have the following result.

Theorem 1. *We have* $\varrho_*(A) \geq 0.54$.

Proof. We begin with the following considerations:

(i) If n is odd and $\phi(n) \geq n/2$, then n satisfies (A);

(ii) If $n > 2$ is even and $\phi(n) > n/3$, then n satisfies (A).

To see why (i) holds, notice that if n is odd and $\phi(n) \geq n/2$, then the above inequality is, in fact, strict. Now,

$$\phi(n - \phi(n)) \leq n - \phi(n) < \phi(n),$$

so n satisfies (A).

Assume now that n satisfies (ii). Since $n > 2$, it follows that $\phi(n)$ is even. Since n is even as well, it follows that $n - \phi(n)$ is even. Since $\phi(k) \leq k/2$, whenever k is even, it follows that

$$\phi(n - \phi(n)) \leq \frac{n - \phi(n)}{2} < \phi(n),$$

where the last inequality follows from the fact that $\phi(n) > n/3$.

It now remains to "count" all positive integers satisfying either (i) or (ii). We use the method outlined in [2].

Let x be an arbitrary positive real number. Let

$$B_0(x) = \{n < x : n \text{ odd and } \phi(n) < n/2\}. \tag{1}$$

For any $s \geq 1$, let

$$B_s(x) = \{n < x : n = 2^s m \text{ with } m \text{ odd and } \phi(m) \leq 2m/3\}. \tag{2}$$

Notice that $B_s(x)$ is empty when $s > \log_2(x)$. Moreover, notice that if $n < x$ is such that n does not satisfy either (i) or (ii), then

$$n \in \bigcup_{0 \leq s \leq \log_2(x)} B_s(x). \tag{3}$$

We now bound the cardinality $b(x, s)$ of $B_s(x)$ in terms of s and x. Set

$$T(x, s) = \prod_{\substack{n<x \\ 2^s \| n}} \frac{\phi(n/2^s)}{n/2^s},$$

and let $c(i)$ be the function (over the nonnegative integers $\mathbb{N} \cup \{0\}$) defined by $c(0) = 2$ and $c(i) = 1.5$ for $i > 0$, then, by the definition of $B_s(x)$, we have

$$T(x, s) \leq c(s)^{-b(x,s)}. \tag{4}$$

Since $\phi(n)/n = \prod_{p|n}(1 - 1/p)$ and since for $n \in B_s(x)$ we have $n/2^s < x/2^s$, it follows that

$$T(x, s) \geq \prod_{3 \leq p < x} \left(1 - \frac{1}{p}\right)^{\frac{1}{2}\left(\frac{x}{2^s p} + 1\right)}. \tag{5}$$

From inequalities (4) and (5), we get

$$b(x,s)\log c(s) \le \frac{1}{2}\cdot\frac{x}{2^s}\Big(S_0 - \frac{\log 2}{2}\Big) + \frac{1}{2}S_1, \tag{6}$$

where

$$S_0 = \sum_{p\ge 2}\frac{1}{p}\log\Big(1+\frac{1}{p-1}\Big) < 0.58007$$

and

$$S_1 = \sum_{3\le p\le x}\log\Big(1+\frac{1}{p-1}\Big).$$

Since

$$\log\Big(1+\frac{1}{p-1}\Big) < \frac{1}{p-1}$$

and since

$$\sum_{3\le p\le x}\frac{1}{p-1} = O(\log\log x),$$

it follows that

$$b(x,s)\log c(s) < \frac{x}{2}\cdot\frac{1}{2^s}\Big(S_0 - \frac{\log 2}{2}\Big) + C\log\log x, \tag{7}$$

where C is a constant. When $s = 0$, we get

$$\frac{b(x,0)}{x} < \frac{1}{2\log 2}\Big(S_0 - \frac{\log 2}{2}\Big) + o(x). \tag{8}$$

For $s \ge 1$, we sum up inequalities (7) for all $s \le \log_2(x)$ and use the fact that

$$\sum_{s\ge 1}\frac{1}{2^s} = 1,$$

to get

$$\frac{1}{x}\sum_{s\ge 1} b(x,s) < \frac{1}{2\log 1.5}\Big(S_0 - \frac{\log 2}{2}\Big) + o(x). \tag{9}$$

Now let

$$b(x) = \sum_{s\ge 0} b(x,s).$$

From formulae (8) and (9), we have

$$\limsup_{x\to\infty} \frac{b(x)}{x} \le \frac{1}{2}\Big(\frac{1}{\log 2} + \frac{1}{\log 1.5}\Big)\Big(S_0 - \frac{\log 2}{2}\Big) < 0.45637.$$

This implies that the lower density of the set of all numbers satisfying either (i) or (ii) (and, hence, (A)), is at least

$$1 - 0.45637 > 0.54.$$

Theorem 1 is therefore completely proved. □

In the next theorem we show that, in the context of the above result, the set A is not only large, but it contains a "regular" infinite subset as well. We give two independent proofs of this fact, i.e., a combinatorial and an arithmetical one.

Theorem 2. *If $n > 2$ is such that the odd part of n is squarefull, then n satisfies inequality (A).*

First proof. Notice that since $n > 2$, it follows that $\phi(n)$ is even. Moreover, since the odd part of n is squarefull, it follows that every prime number dividing n (including also 2 if n is even) divides $\phi(n)$ as well. In particular, all primes dividing n divide also $n - \phi(n)$. Now notice that $\phi(n-\phi(n))$ counts the number of all numbers $< n-\phi(n)$ which are coprime to $n-\phi(n)$; in particular, to n. Hence, $\phi(n-\phi(n)) \le \phi(n)$. The inequality is strict because since $\phi(n) > 1$, it follows that $n - 1$ is a number which is coprime to n and is larger than $n - \phi(n)$ (hence, $n - 1$ is counted by $\phi(n)$ but not by $\phi(n - \phi(n))$). □

Second proof. Let $n = 2^\alpha \prod_{j=1}^r p_j^{\alpha_j}$, where p_j's are pairwise distinct odd primes, $\alpha_j \ge 2$, $r \ge 1$, and $\alpha \ge 0$. We shall consider the case $\alpha \ge 1$ and $r \ge 2$, since it can be checked directly that every number $n = 2^\alpha p^\beta$, with p odd prime, $\alpha \ge 1$ and $\beta \ge 2$, satisfies inequality (A), while for $\alpha = 0$ the proof is similar to the one presented below. We have

$$n - \phi(n) = 2^\alpha (x - y) \prod_{j=1}^r p_j^{\alpha_j - 1}, \tag{10}$$

where

$$x = \prod_{j=1}^r p_j \quad \text{and} \quad y = (1/2)\prod_{j=1}^r (p_j - 1). \tag{11}$$

Let S denote the (possibly empty) set $\{j \leq r : p_j$ divides $x-y\}$. From (11) we get

$$x - y = \prod_{j\in S} p_j^{\beta_j} \cdot \prod_{k=1}^{t} Q_k^{\gamma_k}, \tag{12}$$

where $\beta_j \geq 1$, $t \geq 0$, $\gamma_k \geq 1$, and where Q_k are odd primes with $Q_k \neq p_j$ for all indices $j \leq r$, $k \leq t$. Now, from (10), (11) and (12) we obtain

$$\begin{aligned}\phi(n-\phi(n)) &= 2^{\alpha-1}\prod_{j\in S} p_j^{\alpha_j+\beta_j-2}\prod_{j\notin S} p_j^{\alpha_j-2}\prod_{j=1}^{r}(p_j-1)\prod_{k=1}^{t} Q_k^{\gamma_k-1}(Q_k-1)\\ &= \frac{\phi(n)}{x}\prod_{j\in S} p_j^{\beta_j}\prod_{k=1}^{t} Q^{\gamma_k-1}(Q_k-1) < \phi(n)\frac{x-y}{x} < \phi(n).\end{aligned}$$

Theorem 2 is therefore proved. □

The last theorem deals with the problem (EC2) and inequality (C). We prove that a sharper inequality than Erdős conjectured holds for infinitely many n's.

Theorem 3. *Let m be an odd positive integer with $(3,m)=1$ and such that the number p defined by the rule*

$$p = 3m - \phi(m) \tag{13}$$

is prime. Then m is squarefree and for every positive integer k the number $n := 2^k 3m$ satisfies inequality

$$\phi(n-\phi(n)) \geq \phi(n) + 2^k. \tag{14}$$

Remark 1. The set of the solutions of equation (13) is nonempty. If $m = q$ is a prime number, then p is of the form $p = 2q+1$, i.e., it is a Sophie Germain's prime ([4], p. 261) with $q \geq 5$. Notice that in this case (14) is, in fact, an equality. If $m = q_1q_2$ with $q_1, q_2 \geq 5$ different primes, then p is of the form $p = 2q_1q_2 + q_1 + q_2 - 1$. It is easy to check that the least prime number p of this form is 191, obtained for $q_1 = 5$ and $q_2 = 17$.

Proof of Theorem 3. Let $m = p_1^{\alpha_1}\cdot\ldots\cdot p_r^{\alpha_r}$, where $p_1,\ldots,p_r$ are distinct primes, $r \geq 1$, and $\alpha_1,\ldots,\alpha_r \geq 1$. If m satisfies equality (13), then we easily obtain that $\alpha_1 = \cdots = \alpha_r = 1$, i.e., m is squarefree.

If k is a positive integer, then for the number $n = 2^k 3m$ we have

$$\phi(n) = 2^k \phi(m), \tag{15}$$

and hence $n - \phi(n) = 2^k(3m - \phi(m)) = 2^k p$. It follows that

$$\phi(n - \phi(n)) = 2^{k-1}(p - 1). \tag{16}$$

From (15) and (16) it follows that to prove inequality (14) it is enough to show that

$$p - 1 \geq 2(\phi(m) + 1). \tag{17}$$

This inequality follows easily from the obvious inequality $3(m - \phi(m)) \geq 3$ and from (13).

Theorem 3 is therefore completely proved. □

Remark 2. The set C contains other sequences of positive integers which do not arise as particular cases of Theorem 3. For example, when $n = 2^k \cdot 3 \cdot 5 \cdot 11$ one gets that

$$\phi(n) = 2^{k+3} \cdot 5, \tag{18}$$

and

$$\phi(n - \phi(n)) = \phi\big(2^k \cdot 3 \cdot 5 \cdot 11 - 2^{k+3} \cdot 5\big) = \phi\big(2^k \cdot 5 \cdot (33 - 8)\big) = 2^{k+1} \cdot 5^2. \tag{19}$$

From formulae (18) and (19), it is easily seen that $n \in C$. On the other hand, $n = 2^k \cdot 3 \cdot m$, where $m = 55$ does not satisfy condition (13).

Remark 3. It is clear that

$$\limsup_{n \to \infty} \frac{\phi(n) - \phi(n - \phi(n))}{n} = 1.$$

Indeed, it suffices to tend to infinity in the above expression through prime values of n. On the other hand, taking $n = 2^k 3m$, where m satisfies equality (13), and tending to infinity through the powers of 2, from Theorem 3 we get

$$\liminf_{n \to \infty} \frac{\phi(n) - \phi(n - \phi(n))}{n} \leq \frac{\phi(m)}{2m} + \frac{1}{6m} - \frac{1}{2}. \tag{20}$$

In particular, for $m = 5$ the right side of (20) equals $-1/15$. Can one find the exact value of the lim inf above?

Acknowledgements. We thank the referee for correcting several errors in previous versions of this paper as well as for pointing out the family given in Remark 2 above.

The second author would like to thank Professor Andreas Dress and his research group in Bielefeld for their hospitality during the period when this paper was written.

References

[1] P. Erdős, Proposed Problem P. 294, *Canad. Math. Bull.* **23** (1980), 505.

[2] A. Grytczuk, F. Luca and M. Wójtowicz, On a conjecture of Mąkowski and Schinzel concerning the composition of arithmetic functions σ and ϕ, *Colloquium Mathematicum* **86** (2000), 31–36.

[3] R. K. Guy, Unsolved Problems in Number Theory, *Springer-Verlag, New York, Heidelberg, Berlin*, 1994.

[4] P. Ribenboim, The Book of Prime Numbers Records, *Springer-Verlag, New York, Heidelberg, Berlin*, 1988.

A. GRYTCZUK and M. WÓJTOWICZ
INSTITUTE OF MATHEMATICS
T. KOTARBIŃSKI PEDAGOGICAL UNIVERSITY
65–069 ZIELONA GÓRA
POLAND

E-mail: agryt@lord.wsp.zgora.pl
mwojt@lord.wsp.zgora.pl

F. LUCA
INSTITUTO DE MATEMÁTICAS DE LA UNAM
CAMPUS MORELIA
AP. POSTAL 61–3 (XANGARI)
CP 58 089
MORELIA, MICHOACÁN
MÉXICO

E-mail: fluca@matmor.unam.mx

(Received September 29, 1999; revised June 20, 2000; galley proof received March 13, 2001)