On a Lehmer problem concerning Euler's totient function

By Aleksander GRYTCZUK*) and Marek WÓJTOWICZ**)

(Communicated by Heisuke HIRONAKA, M. J. A., Oct. 14, 2003)

Abstract: Let M be a positive integer with $M > 4$, and let φ denote Euler's totient function. If a positive integer n satisfies the Diophantine equation $(*)$ $M\varphi(n) = n - 1$, then the number of prime factors of n is much bigger than M. Moreover, the set of all squarefree integers which do not fulfil $(*)$ contains "nice" subsets.

Key words: Lehmer problem; Euler totient function.

Let φ denote Euler's totient function, and let M, n denote positive integers with $M \geq 2$. The present paper concerns the equation

$$(*) \qquad M\varphi(n) = n - 1$$

considered in 1932 by Lehmer [5]. Throughout this paper, for fixed M the symbol $\mathcal{L}_M$ stands for the (possibly empty) set of all *composite* solutions of $(*)$, and we put $\mathcal{L} = \bigcup_{M\geq 2} \mathcal{L}_M$. The letter n will always denote an element of $\mathcal{L}$. By $\mathcal{Q} = \{Q_1, Q_2, \ldots\}$ we denote the set of all primes with $Q_i < Q_{i+1}$, where $i = 1, 2, \ldots$.

Lehmer asked whether the set $\mathcal{L}$ is nonempty, and he proved that if $\mathcal{L} \neq \emptyset$ then every $n \in \mathcal{L}$ must be odd, squarefree, i.e.,

$$(1) \qquad n = p_1 p_2 \cdot \ldots \cdot p_r,$$

with $3 \leq p_1 < p_2 < \cdots < p_r$, $p_1, \ldots, p_r$ primes, and the number $\omega(n) := r$ is at least 7.

In this paper we assume that $\mathcal{L} \neq \emptyset$, and then we show that $\omega(n)$, for $n \in \mathcal{L}_M$, is much bigger than M, and that the set $\mathcal{L}' = \mathbf{SF} \setminus \mathcal{L}$, where $\mathbf{SF}$ denotes the set of all squarefree odd integers, contains "very regular" subsets (Theorems 1 and 2 below, respectively).

Since 1970, lower bounds for $\omega(n)$ have been improved by a number of authors. In 1970 Lieuwens [6] obtained $\omega(n) \geq 11$, what was extended in 1977 by Kishore [4] to

$$(2) \qquad \omega(n) \geq 13,$$

and in 1980 (by the use of a computer) by Cohen and Hagis [1] to $\omega(n) \geq 14$. The most amasing case is $3|n$: in 1988 Hagis [3] presented a computer-aided proof that then n must be huge, i.e.

$$(3) \qquad \omega(n) \geq 298\,848 \quad \text{and} \quad n > 10^{1\,937\,042},$$

strengthening earlier results of Lieuwens [6] and Wall [12] that

$$(3') \qquad \omega(n) \geq 213 \quad \text{and} \quad n > 5.5 \times 10^{570},$$

and Subbarao and Prasad [11]:

$$(3'') \qquad \omega(n) \geq 1850 \ \text{(partially by the use of a computer).}$$

In the same paper Hagis showed that n must be large enough, in general:

$$(4) \qquad \omega(n) \geq 1991 \quad \text{and} \quad n > 10^{8171} \quad \text{for } n \in \mathcal{L}_M \text{ with } M \geq 3.$$

One should mension here that in 1985 Prasad and Rangamma proved in elementary way that for $3|n$ with $n \in \mathcal{L}_M$ and $M > 4$ one has $\omega(n) \geq 5334$ ([8], Theorem 3).

As far as general results on bounds for n are concerned, in 1977 Pomerance [7] showed that

$$(5) \qquad n < r^{2^r}, \quad \text{where} \quad r = \omega(n),$$

what was improved in 1985 by Subbarao and Prasad [11] to $n < (r-1)^{2^{(r-1)}}$, and in 1980 Cohen and Hagis [1] obtained

$$(6) \qquad n > 10^{20}$$

(by (4), this result may be essential only for $M = 2$).

All the above-presented results concerning lower bounds for $\omega(n)$ does not depend explicitly on M. We show below that such a dependence does exist and that for large M's the value of $\omega(n)$, with $n \in$

2000 Mathematics Subject Classification. 11A25.

*) Institute of Mathematics, University of Zielona Góra, Podgórna 50, 65-246 Zielona Góra, Poland.

**) Instytut Matematyki, Akademia Bydgoska, Pl. Weyssenhoffa 11, 85-072 Bydgoszcz, Poland.

$\mathcal{L}_M$, rapidly tends to infinity as $M \to \infty$ exceeding (even for small M's) the gigantic bounds (3) and (4) obtained by Hagis.

Theorem 1. *Let $M \geq 4$, and let $n \in \mathcal{L}_M$ be of the form* (1).

(a) *If $p_1 = 3$ then $\omega(n) \geq 3049^{M/4} - 1509$.*

(b) *If $p_1 > 3$ then $\omega(n) \geq 143^{M/4} - 1$.*

Thus, if $p_1 = 3$ and $M \geq 7$, we have that $\omega(n) \geq 10^6$ and, by (7) below, $n > 10^{6 \cdot 10^6}$ (compare with the bounds in (3)). If $p_1 > 3$ and $M \geq 7$, then $\omega(n) \geq 5912$ and, by (7) below, $n > 10^{2 \cdot 10^5}$ (compare with the bounds in (4)).

The corollary below is an immediate consequence of Theorem 1 and Robin's inequality (see [9], Théorème 6) that for *every* positive integer n we have

$$n > \left(\frac{r \log r}{3}\right)^r, \tag{7}$$

where $r = \omega(n)$. Note that for $M \geq 4$ we have the following (rough, but more informative) bounds: $3049^{M/4} - 1509 > 6^M$, and $143^{M/4} - 1 > 3^M$.

Corollary. *Let $M \geq 4$, and let $n \in \mathcal{L}_M$ be of the form* (1).

(a) *If $p_1 = 3$ then $n > (cM6^M)^{6^M}$, where $c = 0.597\cdots = \log 6/3$.*

(b) *If $p_1 > 3$ then $n > (dM3^M)^{3^M}$, where $d = 0.366\ldots = \log 3/3$.*

The next theorem deals with the structure of the set $\mathcal{L}'$ defined above and it complements the result of Pomerance [7] that the number $\mathcal{L}(x)$ of all $n \in \mathcal{L}$ not exceeding x is $O(x^{1/2}(\log x)^{3/4})$.

Let $\mathcal{P} = \{P_1, P_2, \ldots\}$, where $P_i < P_{i+1}$ for all $i \geq 1$, denote the set of all *odd* primes.

Theorem 2. *For every integer $k \geq 2$ there exists an infinite subset $\mathcal{P}(k)$ of $\mathcal{P}$ such that*:

(i) *for every distinct primes $p_1, p_2, \ldots, p_k \in \mathcal{P}(k)$ the squarefree number $n = p_1 p_2 \cdots p_k$ does not fulfil equation $(*)$ (i.e., $n \in \mathcal{L}'$)*;

(ii) *$\mathcal{P}(k)$ is maximal with respect to inclusion.*

(Of course, since $\omega(n) \geq 14$ in general, we have that $\mathcal{P}(k) = \mathcal{P}$ for $k \leq 13$.)

The proof of Theorem 1. From $(*)$ we obtain that if $n = p_1 p_2 \cdots p_r \in \mathcal{L}_M$, then

$$\log M < \sum_{i=1}^{r} \log\left(1 + \frac{1}{p_i - 1}\right), \tag{8}$$

where $r = \omega(n)$. We shall apply below inequality (8) to obtain the bounds for $\omega(n)$.

Part (*a*). From $(*)$ it follows that $p_i \equiv 5 \pmod 6$, for $i \geq 2$. We define the set $\mathcal{A} := \{3\} \cup \{p \in \mathcal{P} : p \equiv 5 \pmod 6\} = \{a_1, a_2, \ldots\}$, where $a_j < a_{j+1}$ for $j = 1, 2, \ldots$. Put

$$\alpha(k) = \sum_{i=1}^{k} \log\left(1 + \frac{1}{a_i - 1}\right),$$

where $k \geq 14$. From (8) we obtain

$$\log M < \alpha(r). \tag{9}$$

Let k_0 be the least integer k with $\log 4 \leq \alpha(k)$ (i.e., $\alpha(k_0) \geq \log 4$ and $\alpha(k_0 - 1) < \log 4$). Since $\alpha(1539) = 1.38625\cdots < \log 4 = 1.3862943\cdots < 1.3862948\cdots = \alpha(1540)$, we obtain that $k_0 = 1540$. Now from (9) it follows that for $n \in \mathcal{L}_M$ with $M \geq 4$ we have $\omega(n) = r \geq 1540$.

Since $a_{1540} = Q_{3050}$, $a_i \geq Q_{1510+i}$ for $i \geq 1540$, from (9) we obtain

$$\begin{aligned} \log M &< \alpha(1539) + \sum_{i=1540}^{r} \log\left(1 + \frac{1}{a_i - 1}\right) \\ &< \log 4 + \sum_{i=1540}^{r} \frac{1}{Q_{1510+i} - 1} \\ &< \log 4 + \int_{1539}^{r} \frac{\mathrm{d}x}{(1510 + x)\log(1510 + x)}, \end{aligned}$$

as

$$Q_m > m \log m + 1, \quad \text{for} \quad m > 20; \tag{10}$$

(this follows from Rosser's inequality $Q_m \geq m(\log m + \log(\log m) - 1.0072629)$ for $m \geq 2$; see [10], cf. [9], p. 368). Hence $\log M < \log 4 + \log(\log(r + 1510)) - \log(\log(3049))$, which follows that $\omega(n) = r \geq (3049)^{M/4} - 1509$ indeed.

Part (*b*). We have in (8) that $p_1 \geq 5 = Q_3$. Put

$$\beta(k) = \sum_{i=1}^{k} \log\left(1 + \frac{1}{Q_{i+2} - 1}\right),$$

where $k \geq 14$. Now from (8) we obtain

$$\log M < \beta(r). \tag{9'}$$

Since $\beta(141) = 1.3851\cdots < \log 4 < 1.3863\cdots = \beta(142)$, from (9′) it follows that for $n \in \mathcal{L}_M$ with $M \geq 4$ we have $\omega(n) = r \geq 142$, and hence (by (10) again)

$$\log M < \beta(141) + \sum_{142}^{r} \log\left(1 + \frac{1}{Q_{i+2} - 1}\right)$$
$$< \log 4 + \sum_{142}^{r} \frac{1}{Q_{i+2} - 1}$$
$$< \log 4 + \log(\log(r+2)) - \log(\log(143)),$$

i.e., $\omega(n) = r \geq (143)^{M/4} - 1$, as claimed. □

The proof of Theorem 2. For X a nonempty subset of the set $\mathbf{N}$ of all positive integers and $k \in \mathbf{N}$ the symbol $[X]^k$ denotes the set of all k-element subsets of $\mathbf{N}$.

Fix an integer $k \geq 2$, and consider the function $f : [\mathbf{N}]^k \to \{0, 1\}$ of the form: $f(\{i_1, \dots, i_k\}) = 0$ iff the number $n := P_{i_1} P_{i_2} \cdots P_{i_k}$ fulfils equation $(*)$. By the Ramsey theorem (see [2]), there exists an infinite subset $\mathbf{N}(k)$ of $\mathbf{N}$ such that $f([\mathbf{N}(k)]^k) = \{0\}$ or $f([\mathbf{N}(k)]^k) = \{1\}$; equivalently, there exists an infinite subset $\mathcal{P}(k)$ of $\mathcal{P}$ such that the following alternative holds:

$$(*)_1 \qquad P_{i_1} P_{i_2} \cdots P_{i_k} \in \mathcal{L}, \quad \text{or}$$

$$(*)_2 \qquad P_{i_1} P_{i_2} \cdots P_{i_k} \notin \mathcal{L},$$

for all pairwise distinct $P_{i_1}, \dots, P_{i_k} \in \mathcal{P}(k)$. From (5) it follows that for every k the number $\#\{n \in \mathcal{P} : \omega(n) \leq k\}$ is finite, and thus the case $(*)_1$ is impossible. Hence case $(*)_2$ takes place, which implies that the set $\mathcal{P}(k)$ fulfils condition (i) of Theorem 2. The existence of a maximal (with respect to inclusion) set $\mathcal{P}(k)$ follows easily from Zorn's Lemma (applied in the proof of the Ramsey theorem). □

References

[1] Cohen, G. L., and Hagis, P. Jr.: On the number of prime factors of n if $\varphi(n) \mid n-1$. Nieuw Arch. Wisk. (3), **28**, 177–185 (1980).

[2] Graham, R. L., Rothschild, B. L., and Spencer, J. H.: Ramsey Theory. John Wiley & Sons, Inc., New York (1980).

[3] Hagis, P. Jr.: On the equation $M \cdot \varphi(n) = n - 1$. Nieuw Arch. Wisk. (4), **6**, 225–261 (1988).

[4] Kishore, M.: On the number of distinct prime factors of n for which $\varphi(n) \mid n-1$. Nieuw Arch. Wisk. (3), **25**, 48–53 (1997).

[5] Lehmer, D. H.: On Euler's totient function. Bull. Amer. Math. Soc., **38**, 745–751 (1932).

[6] Lieuwens, E.: Do there exist composite M for which $k\varphi(M) = M - 1$ holds? Nieuw Arch. Wisk. (3), **18**, 165–169 (1970).

[7] Pomerance, C.: On composite n for which $\varphi(n) | n-1$. II. Pacific J. Math., **69**, 177–186 (1977).

[8] Siva Rama Prasad, V., and Rangamma, M.: On composite n satisfying a problem of Lehmer. Indian J. Pure Appl. Math., **16**, 1244–1248 (1985).

[9] Robin, G.: Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n. Acta Arith., **42**, 367–389 (1983).

[10] Rosser, J. B.: The n-th prime is greater than $n \log n$. Proc. London Math. Soc., **45**, 21–44 (1938).

[11] Subbarao, M. V., and Siva Rama Prasad, V.: Some analogues of a Lehmer problem on the totient function. Rocky Mountain J. Math., **15**, 609–620 (1985).

[12] Wall, D. W.: Conditions for $\varphi(N)$ to properly divide $N - 1$. A Collection of Manuscripts Related to the Fibonacci Sequence (eds. Hoggatt, V. E., and Bicknell-Johnson, M.), 18th Anniv. Vol., Fibonacci Assoc., Santa Clara, pp. 205–208 (1980).