Available online at www.sciencedirect.com
ScienceDirect
C. R. Acad. Sci. Paris, Ser. I 346 (2008) 727–728
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Number Theory

The structure of the set of numbers with the Lehmer property

Marek Wójtowicz, Marta Skonieczna

Instytut Matematyki, Uniwersytet Kazimierza Wielkiego, Pl. Weyssenhoffa 11, 85-072 Bydgoszcz, Poland

Received 7 January 2008; accepted after revision 24 April 2008

Available online 6 June 2008

Presented by Jean-Pierre Serre

Abstract

Let φ be the Euler totient function, and let k, r be fixed integers with $k \geqslant 1$ and $|r| \geqslant 1$. A positive integer n has the *Lehmer property* if it is composite and $\varphi(n)$ divides $n-1$. We give a short proof that the set $\mathcal{L}(k,r)$ – of numbers n with the Lehmer property that fulfil the extra condition $\varphi(n)^k \equiv r \pmod n$ – is finite. This is an extension of a result obtained recently by Deaconescu. ***To cite this article: M. Wójtowicz, M. Skonieczna, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

Résumé

L'ensemble des entiers ayant la propriété de Lehmer. Soit φ la fonction indicatrice d'Euler, et soient k, r des entiers fixés tels que $k \geqslant 1$ et $|r| \geqslant 1$. Un entier strictement positif n a la *propriété de Lehmer* s'il est composé et si $\varphi(n)$ divise $n-1$. On donne une courte preuve du fait que l'ensemble $\mathcal{L}(k,r)$ – des nombres n possédant la propriété de Lehmer et qui vérifient la condition supplémentaire suivante $\varphi(n)^k \equiv r \pmod n$ – est fini. Ceci est une extension d'un résultat obtenu récemment par Deaconescu. ***Pour citer cet article : M. Wójtowicz, M. Skonieczna, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

Throughout this Note φ stands for Euler's totient function, $\mathbf{N}$ denotes the set of positive integers, $M \in \mathbf{N}$ with $M \geqslant 2$, and $\mathcal{L}_M$ denotes the (possibly empty) set of solutions to the equation

$$M \cdot \varphi(n) = n - 1. \tag{$*$}$$

Notice that $\varphi(n) = n-1$ if n is prime. In 1932 Lehmer [5] asked whether the set $\mathcal{L} := \bigcup_{M=2}^{\infty} \mathcal{L}_M$ is nonempty. Following Luca [6], the elements of $\mathcal{L}$ will be referred to as *the numbers with the Lehmer property*.

Although Lehmer's problem is still open, there are many results on the members of $\mathcal{L}$ proven under the assumption $\mathcal{L} \neq \emptyset$, e.g., Lehmer has proved that every $n \in \mathcal{L}$ is odd, squarefree, and the number $\omega(n)$ of prime factors of n is $\geqslant 7$ (for more recent results in this direction see [3] and the references given therein; cf. [1,4]).

Let $\mathcal{L}(k,r)$ denote the set consisting of numbers with the Lehmer property that fulfil the congruence

$$\varphi(n)^k \equiv r \pmod n, \tag{1}$$

where k, r are integers with $k \geqslant 1$ and $|r| \geqslant 1$. In 2006 Deaconescu proved that

E-mail addresses: mwojt@ukw.edu.pl (M. Wójtowicz), mcz@ukw.edu.pl (M. Skonieczna).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2008.05.002

– for every $r \geqslant 1$ the set $\mathcal{L}(2, r)$ is finite, and
– for every $k \geqslant 2$ the set $\mathcal{L}(k, 1)$ is finite

([2, Theorems 1.1 and 1.2], plus remarks on p. 2).

In the theorem below we extend Deaconescu results and we give a short proof, based heavily on the following estimate of the numbers $n_M := \min \mathcal{L}_M$ obtained in [3, Corollary]:

$$n_M > (M \cdot 3^{M-1})^{3^M} \quad \text{for all } M \geqslant 8. \tag{2}$$

For this purpose, we define a sequence $(a_M)_{M=2}^{\infty}$ which tends rapidly to ∞ as follows: $a_2 = 10^{20} + 1$, $a_3 = \cdots = a_7 = 10^{8170} + 1$, and $a_M = (M \cdot 3^{M-1})^{3^M} + 1$ for $M \geqslant 8$. The symbol $\langle a, b\rangle_{\mathbf{N}}$ will denote the set $\{n \in \mathbf{N}\colon a \leqslant n \leqslant b\}$.

Theorem. *For every pair k, r of integers with $k \geqslant 1$ and $|r| \geqslant 1$ the set $\mathcal{L}(k, r)$ is finite. More exactly, this set is included in the finite set*

$$\mathcal{B}(k, r) := \bigcup_{M=2}^{\infty} \langle a_M, |r| \cdot M^k + 1\rangle_{\mathbf{N}}$$

(here $\langle a_M, |r| \cdot M^k + 1\rangle_{\mathbf{N}} = \emptyset$ for all but a finite number of M's).

From the inclusion $\mathcal{L}(k, r) \subset \mathcal{B}(k, r)$ one can evaluate the cardinality of $\mathcal{L}(k, r)$. For example, let us consider an extreme case. It is easy to check that for $k \leqslant 10$ and $|r| \leqslant 10^{16}$ (and for other cases listed below) we have $a_M > |r| \cdot M^k + 1$ for all $M \geqslant 2$, whence $\mathcal{B}(k, r) = \emptyset$. Thus from the theorem we immediately obtain

Corollary. *If $a_M > |r| \cdot M^k + 1$ for all $M \geqslant 2$, then $\mathcal{L}(k, r) = \emptyset$. In particular, this is so for the cases $k \leqslant 10$ and $|r| \leqslant 10^{16}$, $k \leqslant 30$ and $|r| \leqslant 10^{10}$, and $k \leqslant 50$ and $|r| \leqslant 10^4$.*

Proof of the Theorem. Assume $\mathcal{L}(k, r) \neq \emptyset$, and fix $n \in \mathcal{L}(k, r)$. Then $n \in \mathcal{L}_M$ for some M, and from $(*)$ we obtain $M^k \cdot \varphi(n)^k \equiv (-1)^k \pmod n$. Moreover, (1) implies that $M^k \cdot \varphi(n)^k \equiv r \cdot M^k \pmod n$. Hence n divides $r \cdot M^k + (-1)^{k+1}$, and so

$$n \leqslant |r| \cdot M^k + 1. \tag{3}$$

Further, we obviously have $n \geqslant n_M$, and since $n_2 \geqslant 10^{20} + 1 = a_2$ (Cohen and Hagis [1]), $n_M \geqslant 10^{8170} + 1 = a_M$ for $3 \leqslant M \leqslant 7$ (Hagis [4]), and $n_M \geqslant a_M$ for $M \geqslant 8$ (by (2) above), we get $n \geqslant a_M$ in any case. Combining the latter inequality with (3) we obtain $n \in \langle a_M, |r| \cdot M^k + 1\rangle_{\mathbf{N}}$; this proves the required inclusion $\mathcal{L}(k, r) \subset \mathcal{B}(k, r)$.

Moreover, since $\lim_{M\to\infty} \frac{a_M}{|r| \cdot M^k + 1} = \infty$, the sets $\langle a_M, |r| \cdot M^k + 1\rangle_{\mathbf{N}}$ are empty for almost all M's.

References

[1] G.L. Cohen, P. Hagis Jr., On the number of prime factors of n if $\varphi(n)|n - 1$, Nieuw Arch. Wisk. (3) 28 (1980) 177–185.
[2] M. Deaconescu, On the equation $m - 1 = a\varphi(n)$, Integers: Electronic Journal of Combinatorial Number Theory 6 (2006), Paper A06.
[3] A. Grytczuk, M. Wójtowicz, On a Lehmer problem concerning Euler's totient function, Proc. Japan Acad. Ser. A 79 (2003) 136–138.
[4] P. Hagis Jr., On the equation $M \cdot \varphi(n) = n - 1$, Nieuw Arch. Wisk. (4) 6 (1988) 225–261.
[5] D.H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc. 38 (1932) 745–751.
[6] F. Luca, Fibonacci numbers with the Lehmer property, Bull. Pol. Acad. Sci. Math. 55 (2007) 7–15.