Available online at www.sciencedirect.com
ScienceDirect
C. R. Acad. Sci. Paris, Ser. I 347 (2009) 1111–1114
COMPTES RENDUS MATHEMATIQUE

Number Theory

Appendix to the Note "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 21 July 2008; accepted after revision 17 July 2009

Available online 19 September 2009

Presented by Jean-Pierre Serre

Abstract

Let φ denote the Euler totient function, and let P be a monic polynomial with integer coefficients and positive degree. Combining the techniques of proof from our previous paper and that of a recent paper by Hernández and Luca we generalize the following result of Hernández and Luca: the set of composite positive integers n such that $\varphi(n)|n-1$ and $P(\varphi(n)) \equiv 0 \pmod{n}$ is finite. The generalization is of the quantitative type, and applies also to the so-called *unitary analogue of the Lehmer problem* (studied earlier by Subbarao and Siva Rama Prasad). ***To cite this article: M. Wójtowicz, M. Skonieczna, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***

Résumé

Appendice à l'article : « Structure de l'ensemble des entiers possèdant la propriété de Lehmer ». Soit φ la fonction indicatrice d'Euler, et P un polynôme unitaire à coefficients entiers et de degré strictement positif. En combinant les techniques de démonstration de notre précédent article et celles d'un article récent de Hernández et Luca, nous généralisons le résultat suivant de Hernández et Luca : l'ensemble des entiers n strictement positifs composés tels que $\varphi(n)|n-1$ et $P(\varphi(n)) \equiv 0 \pmod{n}$, est fini. La généralisation est quantitative, et s'applique aussi à l'analogue unitaire du problème de Lehmer (antérieurement étudié par Subbarao et Siva Rama Prasad). ***Pour citer cet article : M. Wójtowicz, M. Skonieczna, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***

1. Introduction

Throughout this Note φ stands for Euler's totient function, $\mathbf{Z}$ and $\mathbf{N}$ denote the sets of integers and positive integers, respectively, $k, M \in \mathbf{N}$ with $M \geqslant 2$, and $r \in \mathbf{Z} \setminus \{0\}$. By $\mathcal{L}_M$ we denote the (possibly empty) set of composite solutions to the Lehmer equation,

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

DOI of original article: 10.1016/j.crma.2008.05.002.
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.2009.07.019

In 1932 Lehmer [5] asked whether the set $\mathcal{L} := \bigcup_{M=2}^{\infty} \mathcal{L}_M$ is not empty. This question remains still open (see, e.g., [3, Problem B37]); and (under the hypothesis $\mathcal{L} \neq \emptyset$) the structure of $\mathcal{L}$ was studied in a number of papers (see [2,4,12] and the references given therein).

In 2006 Deaconescu [1] considered equation (1_M) with a constraint, and its generalizations were studied in the papers [4,12] as follows. If $P \in \mathbf{Z}[X]$ is a monic non-constant polynomial, then $\mathcal{L}(P)$ denotes the subset of $\mathcal{L}$ consisting of elements that fulfill the extra condition,

$$P\big(\varphi(n)\big) \equiv 0 \pmod{n}, \tag{2}$$

and we put $\mathcal{L}(k,r)$ for $P(X) = X^k - r$. In our previous paper [12] we gave an efficient proof that the set $\mathcal{L}(k,r)$ is finite, with an application to the case $\mathcal{L}(k,r) = \emptyset$ (in the proof we used lower estimations of the numbers $n_M := \min \mathcal{L}_M$).

Recently, Hernández and Luca [4] presented an independent proof of a more general result: *the set $\mathcal{L}(P)$ is finite* (a part of their proof is based on the Rosser–Schoenfeld inequality $n/\varphi(n) \leqslant e^{\gamma} \cdot \log_2 n \cdot D_n$, where $D_n = 1 + \frac{2.50637}{e^{\gamma} \cdot (\log_2 n)^2}$ and $n \geqslant 3$; see [8, Theorem 15], cf. [6, p. 114]).

In this Note we show that, combining our technique of proof [12] and that of Hernández and Luca [4], and using the above-mentioned estimations of n_M's, one obtains (see Theorem 1) an essential strengthening of the Hernández–Luca theorem as follows. Firstly, we extend the constraint (2) to *a sequence* $\mathcal{F} = (P_M)_{M=2}^{\infty}$ of polynomials, each polynomial P_M corresponding to Eq. (1_M). Secondly, we define a subset $\mathcal{L}(\mathcal{F})$ of $\mathcal{L}$ determined by the new constraint for $\mathcal{F}$. Then we indicate the cases for which $\mathcal{L}(\mathcal{F})$ is finite or empty. As an application we obtain the following generalization of our [12, Corollary]: *if $P(X) = \sum_{j=0}^{k} b_j X^j$ is a monic non-constant polynomial in $\mathbf{Z}[X]$ then the inequality $\sum_{j=0}^{k} |b_j| 2^{k-j} \leqslant 10^{20}$ implies the set $\mathcal{L}(P)$ is empty*.

By a recent result of Skonieczna [10], our method works also for the so-called *unitary analogue of the Lehmer problem*, studied by Subbarao and Siva Rama Prasad [11]: it deals with the existence of a composite solution $n \in \mathbf{N}$ to the equation

$$M \cdot \varphi^*(n) = n - 1, \tag{3}$$

for some M, where φ^* is the unitary analogue of φ (i.e., $\varphi^*(n)$ counts the number of all $m \in \mathbf{N}$ such that $m \leqslant n$ and $(m,n)^* = 1$, where $(m,n)^*$ is the greatest divisor ℓ of m which is also a *unitary divisor of n*: ℓ and n/ℓ are coprime):

$$\varphi^*(n) = n \prod_{p^{\alpha} \| n} \left(1 - \frac{1}{p^{\alpha}}\right).$$

We use notations similar to those of [12]. Thus $(a_M)_{M=2}^{\infty}$ is the sequence of the form $a_2 = 10^{20} + 1$, $a_3 = \cdots = a_7 = 10^{8170} + 1$, and $a_M = (M \cdot 3^{M-1})^{3^M} + 1$ for $M \geqslant 8$. The symbol $\langle a, b \rangle_{\mathbf{N}}$ denotes the set $\{n \in \mathbf{N}\colon\ a \leqslant n \leqslant b\}$, and we recall that $n_M := \min \mathcal{L}_M$, $M = 2, 3, \ldots$, with the convention that $\min \emptyset = +\infty$.

For a sequence $\mathcal{F} = (P_M)_{M=2}^{\infty}$ of monic non-constant polynomials in $\mathbf{Z}[X]$, we let $\mathcal{L}_M(\mathcal{F})$ to denote the subset of $\mathcal{L}_M$ consisting of its elements n that fulfill the constraint

$$P_M\big(\varphi(n)\big) \equiv 0 \pmod{n}, \tag{4}$$

and we let:

$$\mathcal{L}(\mathcal{F}) = \bigcup_{M=2}^{\infty} \mathcal{L}_M(\mathcal{F}).$$

When $P_M = P$ for all M's, we simply write $\mathcal{L}(P)$ instead of $\mathcal{L}(\mathcal{F})$. Notice that then condition (4) becomes $P(\varphi(n)) \equiv 0 \pmod{n}$ (studied by Hernández and Luca [4]), and we do not need consider it for separate M's.

For a polynomial P_M of degree $k = k_M \geqslant 1$ and of the form $P_M(X) = \sum_{j=0}^{k} b_j^{(M)} X^j$, we define the number c_M by the formula

$$c_M := \sum_{j=0}^{k} \big|b_j^{(M)}\big| M^{k-j}, \quad M = 2, 3, \ldots.$$

Notice that if the sequence $\mathcal{F}$ is constant, then $c_M = c_2$ for all M's.

2. The main result

Now we can present a generalization of the main results of [4] and [12]; it is stated in the form of our [12, Theorem].

Theorem 1. *With the notations as above, the set $\mathcal{L}(\mathcal{F})$ is included in the set*

$$\mathcal{B}(\mathcal{F}) := \bigcup_{M=2}^{\infty} \langle a_M, c_M \rangle_{\mathbf{N}},$$

and it is

(i) *finite, whenever* $\limsup_{M\to\infty} \frac{c_M}{a_M} < 1$,
(ii) *empty, whenever* $c_M < a_M$ *for all* M*'s.*

In particular, the set $\mathcal{L}(\mathcal{F})$ is finite if the sequence $\mathcal{F}$ takes a finite number of values, and $\mathcal{L}(\mathcal{F})$ is empty for $c_2 \leqslant 10^{20}$.

We shall indicate the main step in the proof of Theorem 1 leaving the remaining details to the reader. Let a polynomial P_M of degree k be fixed, and choose $n \in \mathcal{L}_M(\mathcal{F})$. By the trick that condition (4) implies $M^k \cdot P_M(\varphi(n)) \equiv 0 \pmod{n}$ we obtain $n \leqslant c_M$ (see [4, p. 2]). Hence, by the estimation $n \geqslant a_M$ (see [12, proof of the theorem]), $n \in \langle a_M, c_M \rangle_{\mathbf{N}}$.

The above method of proof allows us to settle a similar subcase of the unitary analogue of the Lehmer problem mentioned in the Introduction. Let us put:

$$\mathcal{S}^*_M := \big\{ n \in \mathbf{N} \colon\ n \text{ fulfills Eq. (3)} \big\},$$

and $\mathcal{S}^* := \bigcup_{M=2}^{\infty} \mathcal{S}^*_M$. (From now on we assume we act on non-empty sets, if necessary.) The unitary analogue of the Lehmer problem is thus equivalent to the statement that *the set $\mathcal{S}^*$ is not empty*. Further, let $\mathcal{S}^*_M(\mathcal{F})$ denote the subset of $\mathcal{S}^*_M$ consisting of the elements n that fulfill the constraint

$$P_M\big(\varphi^*(n)\big) \equiv 0 \pmod{n}, \tag{4a}$$

and set $S^*(\mathcal{F}) := \bigcup_{M=2}^{\infty} \mathcal{S}^*_M(\mathcal{F})$ (and if $P_M = P$ for all M's, we write $S^*(P)$ instead of $\mathcal{S}^*(\mathcal{F})$). As we shall see below, the sets $\mathcal{L}(\mathcal{F})$ and $\mathcal{S}^*(\mathcal{F})$ are finite simultaneously. For this purpose, let us consider a sequence $(a^*_M)_{M=2}^{\infty}$ tending rapidly to ∞ of the form: $a^*_2 = 10^{10} + 1$, $a^*_3 = 10^{52} + 1$, and $a^*_M = (M \cdot 3^{M-1})^{3^M} + 1$ for $M \geqslant 4$ (this sequence corresponds to the sequence $(a_M)_{M=2}^{\infty}$ defined in Section 1 for φ). We shall need the following estimations of the numbers $n^*_M := \min \mathcal{S}^*_M$ (and these numbers correspond to the numbers $n_M = \min \mathcal{L}_M$; see [12, p. 728]):

$$n^*_M \geqslant a^*_M \quad \text{for all } M \geqslant 2.$$

The case $M \geqslant 4$ follows from [10, Corollary 1.2]. For the cases $M = 2$ and $M = 3$ we apply the Robin's inequality [7, Théorème 6]:

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

where $r = \omega(n)$ is the number of distinct prime factors of arbitrary $n \in \mathbf{N}$. We have $\omega(n) \geqslant 11$ for all $n \in \mathcal{S}^*$ (hence for $n \in \mathcal{S}^*_2$), and $\omega(n) \geqslant 33$ for $n \in \mathcal{S}_3$ (see [9,11]). This gives us $n^*_2 \geqslant a^*_2$ and $n^*_3 \geqslant a^*_3$.

Now we can mimic the proof of Theorem 1 to obtain the following result.

Theorem 1a. *With the notations as above, the set $\mathcal{S}^*(\mathcal{F})$ is included in the set*

$$\mathcal{B}^*(\mathcal{F}) := \bigcup_{M=2}^{\infty} \langle a^*_M, c_M \rangle_{\mathbf{N}},$$

and it is

(i) *finite, whenever* $\limsup_{M\to\infty} \frac{c_M}{a^*_M} < 1$,

(ii) *empty, whenever* $c_M < a_M^*$ *for all* M*'s.*

In particular, if $P \in \mathbf{Z}[X]$ *is a monic polynomial of positive degree, then the set* $\mathcal{S}^*(P)$ *is finite, and it is empty for* $c_2 < 10^{10}$.

Remarks. (1) Since the numbers a_M and a_M^* coincide for $M \geqslant 8$, *the sets* $\mathcal{L}(\mathcal{F})$ *and* $\mathcal{S}^*(\mathcal{F})$ *are finite simultaneously*.

(2) It was proved by Lehmer [5] that every $n \in \mathcal{L}$ is square-free, whence $\varphi(n) = \varphi^*(n)$ for such n's. Therefore $\mathcal{L}_M \subset \mathcal{S}_M^*$ for all $M \geqslant 2$, and hence $\mathcal{L} \subset \mathcal{S}^*$. It obviously follows that *the finiteness of* $\mathcal{S}^*$ *implies the finiteness of* $\mathcal{L}$, and we see that the study of *the unitary analogue* of the Lehmer problem may lead to a solution of the Lehmer problem.

References

[1] M. Deaconescu, On the equation $m - 1 = a\varphi(n)$, Integers: Electronic Journal of Combinatorial Number Theory 6 (2006), Paper A06.
[2] A. Grytczuk, M. Wójtowicz, On a Lehmer problem concerning Euler's totient function, Proc. Japan Acad. Ser. A 79 (2003) 136–138.
[3] R. Guy, Unsolved Problems in Number Theory, Springer-Verlag, New York, 2004.
[4] S.H. Hernández, F. Luca, A note on Deaconescu's result concerning Lehmer's problem, Integers: Electronic Journal of Combinatorial Number Theory 8 (2008), Paper A12.
[5] D.H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc. 38 (1932) 745–751.
[6] W.J. LeVeque, Topics in Number Theory, vol. I, Dower Publications Inc., New York, 2002.
[7] G. Robin, Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valuers de la fonction $\omega(n)$ nombre de diviseurs premiers de n, Acta Arith. 42 (1983) 367–389.
[8] J.B. Rosser, L. Schoenfeld, Approximation formulas for some functions of prime numbers, Illinois J. Math. 6 (1962) 64–94.
[9] V. Siva Rama Prasad, U. Dixit, Inequalities related to the unitary analogue of Lehmer problem, J. Inequal. Pure Appl. Math. 7 (2006), Article 142.
[10] M. Skonieczna, Some results on the unitary analogue of the Lehmer problem, J. Inequal. Pure Appl. Math. 9 (2008), Article 55.
[11] M.V. Subbarao, V. Siva Rama Prasad, Some analogues of a Lehmer problem on the totient function, Rocky Mountain J. Math. 15 (1985) 609–619.
[12] M. Wójtowicz, M. Skonieczna, The structure of the set of numbers with the Lehmer property, C. R. Acad. Sci. Paris Ser. I 346 (2008) 727–728.