INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8 (2008), #A12

A NOTE ON DEACONESCU'S RESULT CONCERNING LEHMER'S PROBLEM

Santos Hernández Hernández[1]
Unidad Académica de Matemáticas, UAZ, Ap. Postal 612, C.P. 98000, Zacatecas, Zacatecas
shh@mate.reduaz.mx

Florian Luca
Instituto de Matemáticas, UNAM, Ap. Postal 61-3 (Xangari), C.P. 58 089, Morelia, Michoacán, MEXICO
fluca@matmor.unam.mx

Received: 11/7/07, Accepted: 2/13/08, Published: 3/24/08

Abstract

Let $\phi(n)$ be the Euler function of n. We prove that there are at most finitely many composite integers n such that $\phi(n) \mid n-1$ and $P(\phi(n)) \equiv 0 \pmod{n}$, where $P(X) \in \mathbb{Z}[X]$ is any monic non-constant polynomial.

1. Introduction and the Result

Let $\phi(n)$ be the Euler function of n. In [3], D. H. Lehmer conjectured that $\phi(n) \mid n-1$ if an only if n is prime. This is still an open problem. Several partial results can be found in [1], [6] and [8]. In [5], F. Luca has shown that there is no composite Fibonacci number n such that $\phi(n) \mid n-1$. Several partial results on Lehmer's problem with up to dated references can be found in the recent monograph [7].

Recently, Deaconescu (see [2]) has proved the following results:

1. Let $r \geq 2$ be a fixed integer. Then there are only finitely many n such that $\phi(n) \mid n-1$ and $\phi(n)^2 \equiv r \pmod{n}$.
2. Let $k \geq 3$ be a fixed integer. Then, there are only finitely many composite n such that $\phi(n) \mid n-1$ and $\phi(n)^k \equiv 1 \pmod{n}$.

[1]Partly supported by grant PROMEP/103.5/07/2573

In this note, we prove the following result.

Theorem 1. *Let $P(X) \in \mathbb{Z}[X]$ be a monic non-constant polynomial. Then there are at most finitely many composite integers n such that $\phi(n) \mid n-1$ and $P(\phi(n)) \equiv 0 \pmod{n}$.*

Our theorem implies Deaconescu's results by taking $P(X) = X^2 - r$ and $P(X) = X^k - 1$, respectively.

2. Proof of the Theorem 1

In what follows, we use the Vinogradov symbols $\gg$ and $\ll$ with their usual meanings. Let

$$P(X) = a_0 X^d + a_1 X^{d-1} + \cdots + a_d \in \mathbb{Z}[X]$$

with $a_0 = 1$ and $d \geq 1$ and write

$$n - 1 = k\phi(n), \quad \text{where} \quad k \geq 2. \tag{1}$$

It is known that $\phi(n) \gg n/\log\log n$ (see [4] Vol. I, pag. 114). Thus,

$$k \ll \log\log n. \tag{2}$$

Since $P(\phi(n)) \equiv 0 \pmod{n}$ we have that $k^d P(\phi(n)) \equiv 0 \pmod{n}$. Thus, by (1), we get

$$a_0(-1)^d + a_1 k(-1)^{d-1} + \cdots + a_d k^d \equiv 0 \pmod{n}.$$

Let A denote the left hand of the above congruence. Now, we distinguish two cases:

Case 1: $A \neq 0$. Then, from the above congruence and (2), we have that

$$n \leq |A| < \left(\sum_{j=o}^{n} |a_j|\right) k^d \ll (\log\log n)^d,$$

which implies $n \ll 1$, as we want.

Case 2: $A = 0$. Then, $a_0(-1)^d + a_1 k(-1)^{d-1} + \cdots + a_d k^d = 0$ or

$$a_0 \left(\frac{-1}{k}\right)^d + a_1 \left(\frac{-1}{k}\right)^{d-1} + \cdots + a_d = 0,$$

or $P(-1/k) = 0$. Since $a_0 = 1$, we get that $-1/k$ is both an algebraic integer and a rational number, which is impossible since $k \geq 2$.

More generally, our argument implies that if $P(X) \in \mathbb{Z}[X]$ is a nonconstant polynomial such that the congruence $P(\phi(n)) \equiv 0 \pmod{n}$ has infinitely many composite solutions n, then there exists an integer $k \geq 2$ with $P(-1/k) = 0$. Furthermore, all but finitely many of the composite n satisfying the above congruence satisfy also $n - 1 = k\phi(n)$ for some $k \geq 2$ such that $-1/k$ is a root of $P(X)$.

Acknowledgment We thank the referee for valuable comments that improved the presentation of this paper.

References

[1] W. D. Banks, F. Luca, Composite integers n for which $\phi(n) \mid n-1$, *Acta Math. Sinica* **23** (2007), 1915–1918.

[2] M. Deaconescu, On the equation $m-1 = a\phi(m)$, *Integers: Elec. Jour. of Comb. Number theory* **6** (2006), #A06.

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

[4] W. J. LeVeque, *Topics in number theory, Vol. I, II*, Dover Pubications Inc., New York, 2002.

[5] F. Luca, Fibonacci numbers with the Lehmer property, *Bull. Pol. Acad. Sci. Math.* **55** (2007), 7-15.

[6] C. Pomerance, On composite n for which $\phi(n) \mid n-1$, II, *Pacific J. Math.* **69** (1977), 177–186.

[7] J. Sándor, B. Crstici, *Handbook of number theory. II*, Kluwer Academic Publishers, Dordrecht, 2004.

[8] Z. Shan, On composite n for which $\phi(n) \mid n-1$, *J. China Univ. Sci. Tech.* **15** (1985), 109–112.