Generalizing the Lehmer’s totient problem

Marius Tărnăuceanu

October 18, 2021

Abstract

An important unsolved question in number theory is the Lehmer’s totient problem that asks whether there exists any composite number $n$ such that $\varphi(n) \mid n - 1$, where $\varphi$ is the Euler’s totient function. It is known that if any such $n$ exists, it must be odd, square-free, greater than $10^{30}$, and divisible by at least 15 distinct primes. Such a number must be also a Carmichael number.

In this short note, we discuss a group-theoretical analogous problem involving the function that counts the number of automorphisms of a finite group. Another way to generalize the Lehmer’s totient problem is also proposed.

MSC 2020: Primary 20D60, 11A25; Secondary 20D99, 11A99.

Key words: Lehmer’s totient problem, Euler’s totient function, finite group, group automorphism, exponent of a group.

1 Introduction

The Euler’s totient function $\varphi$ is one of the most famous functions in number theory. Recall that the totient $\varphi(n)$ of a positive integer $n$ is defined to be the number of positive integers less than or equal to $n$ that are coprime to $n$. In algebra this function is important mainly because it gives the order of the group of units in the ring $(\mathbb{Z}_n, +)$. Also, $\varphi(n)$ can be seen as the number of generators or as the number of automorphisms of the cyclic group $(\mathbb{Z}_n, +)$.

Lehmer’s totient problem [6] asks whether the well-known property ”$\varphi(n) = n - 1$ $\iff$ $n$ is a prime” can be generalized to ”$\varphi(n) \mid n - 1$ $\iff$ $n$ is a prime”. This problem has been studied by many mathematicians (see e.g. [2, 4, 6, 7]).
but up to now no counterexample has been found. Such a counterexample is often called a Lehmer number.

We observe that an integer \( n \geq 2 \) is a prime or a Lehmer number if and only if
\[
|G| - 1 \equiv 0 \pmod{|\text{Aut}(G)|},
\]
where \( G \) a cyclic group of order \( n \). This fact suggests us to consider arbitrary finite groups \( G \) which satisfy the relation (1). Their description is given by the following theorem.

**Theorem 1.1.** A finite group \( G \) satisfies the relation (1) if and only if it is cyclic and its order is a prime or a Lehmer number.

Finally, we indicate another way to extend the Lehmer’s totient problem via group theory.

**Open problem.** Determine the finite groups \( G \) satisfying
\[
|G| - 1 \equiv 0 \pmod{\varphi(G)},
\]
where
\[
\varphi(G) = |\{a \in G \mid o(a) = \exp(G)\}|
\]
is the generalization of the Euler’s totient function studied in [8].

Note that since \( \varphi(\mathbb{Z}_n) = \varphi(n) \) for all \( n \in \mathbb{N}^* \), cyclic groups of prime or Lehmer order will be solutions of (2).

**2 Proof of Theorem 1.1**

First of all, we recall the well-known formula for the number of automorphisms of a finite abelian \( p \)-group (see e.g. [1, 5]).

**Theorem 2.1.** Let \( G = \prod_{i=1}^{k} \mathbb{Z}_{p^{n_i}} \) be a finite abelian group, where \( 1 \leq n_1 \leq n_2 \leq \ldots \leq n_k \). Then
\[
|\text{Aut}(G)| = \prod_{i=1}^{k} (p^{n_i} - p^{i-1}) \prod_{u=1}^{k} p^{n_u(k-a_u)} \prod_{v=1}^{k} p^{(n_v-1)(k-b_v+1)},
\]
where
\[
a_r = \max\{s \mid n_s = n_r\} \quad \text{and} \quad b_r = \min\{s \mid n_s = n_r\}, \quad r = 1, 2, \ldots, k.
\]
By using Theorem 2.1, we easily get the following corollary.

**Corollary 2.2.** Let $G$ be a finite abelian $p$-group. If $p 
mid |\text{Aut}(G)|$, then $G \cong \mathbb{Z}_p$.

*Proof.* Under the notation in Theorem 2.1, we infer that $n_1 = n_2 = \cdots = n_k = 1$ and $a_1 = a_2 = \cdots = a_k = k$. Then the first product in the right side of (3) is $\prod_{i=1}^{k} (p^k - p^{i-1})$. Obviously, this is not divisible by $p$ if and only if $k = 1$. Thus $G \cong \mathbb{Z}_p$, as desired. \hfill $\Box$

We are now able to prove our main result.

**Proof of Theorem 1.1.** Let $G$ be a finite group satisfying (1).

We first prove that $G$ is abelian. If not, then $Z(G) \neq G$ and so there exists a prime $p$ dividing $|G/Z(G)|$. Since $G/Z(G)$ can be embedded in $\text{Aut}(G)$, it follows that $p$ divides $|\text{Aut}(G)|$. Consequently, $p \mid |G| - 1$, contradicting the fact that $p \mid |G|$. Thus $G$ is abelian.

Let $G = \prod_{i=1}^{m} G_i$, where $G_i$ is a finite abelian $p_i$-group, $i = 1, 2, \ldots, m$. Since

$$|\text{Aut}(G)| = \prod_{i=1}^{m} |\text{Aut}(G_i)| \text{ and } |G| = \prod_{i=1}^{m} |G_i|,$$

by (1) we infer that $p_i \nmid |\text{Aut}(G_i)|$ for each $i$. Then Corollary 2.2 implies $G_i \cong \mathbb{Z}_{p_i}$ and therefore

$$G \cong \prod_{i=1}^{m} \mathbb{Z}_{p_i} \cong \mathbb{Z}_{p_1 p_2 \cdots p_m}$$

is cyclic. Moreover, (1) becomes $|G| - 1 \equiv 0 \pmod{\varphi(|G|)}$, i.e. $|G|$ is a prime or a Lehmer number. This completes the proof. \hfill $\Box$

**References**

[1] J.N.S. Bidwell, M.J. Curran and D.J. McCaughan, *Automorphisms of direct products of finite groups*, Arch. Math. **86** (2006), 481-489.

[2] P. Burcsi, S. Czirbusz and G. Farkas, *Computational investigation of Lehmer’s totient problem*, Annales Univ. Sci. Budapest., Sect. Comp. **35** (2011), 43-49.
[3] A. Grytczuk and M. Wójtowicz, *On a Lehmer problem concerning Euler’s totient function*, Proc. Japan Acad. Ser. A Math. Sci. 79 (2003), 136-138.

[4] P. Hagis, *On the equation $M\varphi(n) = n - 1$*, Nieuw Arch. Wiskd. IV Series. 6 (1988), 255-261.

[5] C.J. Hillar and D.L. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly 114 (2007), 917-923.

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

[7] F. Luca and C. Pomerance, *On composite integers $n$ for which $\varphi(n) \mid n - 1$*, Bol. Soc. Mat. Mexicana. 17 (2011), 13-21.

[8] M. Tărnăuceanu, *A generalization of the Euler’s totient function*, Asian-Eur. J. Math. 8 (2015), article ID 1550087.

Marius Tărnăuceanu  
Faculty of Mathematics  
“Al.I. Cuza” University  
Iași, Romania  
e-mail: tarnauc@uaic.ro