Elemente der Mathematik 79 (2024), 77–79
DOI 10.4171/EM/492

Short note Generalizing Lehmer's totient problem

Marius Tărnăuceanu

Abstract. An important unsolved question in number theory is Lehmer's totient problem that asks whether there exists any composite number n such that $\varphi(n) \mid n-1$, where φ is the Euler's totient function. It is known that if any such n exists, it must be odd, square-free, greater that 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 Lehmer's totient problem is also proposed.

1 Introduction

Euler's totient function φ 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 $(\mathbb{Z}_n, +, \cdot)$. 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

$$\varphi(n) = n-1 \iff n \text{ is a prime}$$

can be generalized to

$$\varphi(n) \mid n-1 \iff n \text{ is a prime.}$$

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

$$|G| - 1 \equiv 0 \pmod{|\mathrm{Aut}(G)|}, \tag{1}$$

where G a cyclic group of order n. Here $|G|$ denotes the order of G, that is the number of elements of G, and $\mathrm{Aut}(G)$ denotes the automorphism group of G, that is the group of all bijective homomorphisms from G to itself. We recall that a cyclic group is a group generated by a single element. We also recall that a cyclic group of order n is isomorphic to $\mathbb{Z}_n$, the group of integers modulo n. Our observation follows from the fact that $|\mathrm{Aut}(\mathbb{Z}_n)| = \varphi(n)$.

This suggests us to consider *arbitrary* finite groups G which satisfy relation (1). Their description is given by the following theorem.

Theorem 1.1. *A finite group G satisfies 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 Lehmer's totient problem via group theory.

Open problem. Determine the finite groups G satisfying

$$|G| - 1 \equiv 0 \ (\mathrm{mod}\ \varphi(G)), \tag{2}$$

where $\varphi(G) = |\{a \in G \mid o(a) = \exp(G)\}|$ is the generalization of the Euler's totient function studied in [8]. Here $o(a)$ denotes the order of a, that is the smallest positive integer m such that $a^m = 1$, and $\exp(G)$ denotes the exponent of G, that is the least common multiple of the orders of all elements in G. Since $\exp(\mathbb{Z}_n) = n$ and the group $\mathbb{Z}_n$ has $\varphi(n)$ elements of order n, it follows that $\varphi(\mathbb{Z}_n) = \varphi(n)$. Then cyclic groups of prime or Lehmer order are solutions of (2), and thus this problem generalizes the classical Lehmer conjecture.

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]). Given a prime number p, we recall that a p-group is a group in which the order of every element is a power of p.

Theorem 2.1. *Let $G \cong \prod_{i=1}^{k} \mathbb{Z}_{p^{n_i}}$ be a finite abelian p-group with $1 \le n_1 \le n_2 \le \cdots \le n_k$. Then*

$$|\mathrm{Aut}(G)| = \prod_{i=1}^{k}(p^{a_i} - p^{i-1}) \prod_{u=1}^{k} p^{n_u(k-a_u)} \prod_{v=1}^{k} p^{(n_v-1)(k-b_v+1)}, \tag{3}$$

where

$$a_r = \max\{s \mid n_s = n_r\} \quad \textit{and} \quad b_r = \min\{s \mid n_s = n_r\}, \quad r = 1, 2, \ldots, k.$$

By using Theorem 2.1, we easily get the following corollary.

Corollary 2.2. *Let G be a finite abelian p-group. If $p \nmid |\mathrm{Aut}(G)|$, then $G \cong \mathbb{Z}_p$, i.e. G is isomorphic to $\mathbb{Z}_p$.*

Proof. Under the notation in Theorem 2.1, we infer that $k = 1$. Indeed, if $k \ge 2$, then p divides $\prod_{i=1}^{k}(p^{a_i} - p^{i-1})$, and so p divides $|\mathrm{Aut}(G)|$, a contradiction. Then $G \cong \mathbb{Z}_{p^{n_1}}$, and (3) becomes

$$|\mathrm{Aut}(G)| = \varphi(p^{n_1}) = (p-1)p^{n_1-1}.$$

Clearly, the hypothesis $p \nmid |\mathrm{Aut}(G)|$ implies $n_1 = 1$, and therefore we have $G \cong \mathbb{Z}_p$, as desired. ∎

We are now able to prove our main result.

Proof of Theorem 1.1. Let G be a finite group satisfying (1), and let $Z(G)$ be the center of G, i.e. $Z(G) = \{a \in G \mid ab = ba \text{ for all } b \in G\}$.

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 $\mathrm{Aut}(G)$, it follows that p divides $|\mathrm{Aut}(G)|$. Consequently, $p \mid |G|-1$, contradicting the fact that $p \mid |G|$. Thus G is abelian.

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

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

by (1), we infer that $p_i \nmid |\mathrm{Aut}(G_i)|$ 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. Note that the above second group isomorphism holds by the well-known Chinese remainder theorem. Moreover, (1) becomes $|G| - 1 \equiv 0 \pmod{\varphi(|G|)}$, i.e. $|G|$ is a prime or a Lehmer number. This completes the proof. ∎

Acknowledgments. The author is grateful to the reviewer for remarks which improve the previous version of the paper.

References

[1] J. N. S. Bidwell, M. J. Curran, and D. J. McCaughan, Automorphisms of direct products of finite groups. *Arch. Math. (Basel)* **86** (2006), no. 6, 481–489

[2] P. Burcsi, S. Czirbusz, and G. Farkas, Computational investigation of Lehmer's totient problem. *Ann. Univ. Sci. Budapest. Sect. Comput.* **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), no. 8, 136–138

[4] P. Hagis, Jr., On the equation $M \cdot \phi(n) = n - 1$. *Nieuw Arch. Wisk. (4)* **6** (1988), no. 3, 255–261

[5] C. J. Hillar and D. L. Rhea, Automorphisms of finite abelian groups. *Amer. Math. Monthly* **114** (2007), no. 10, 917–923

[6] D. H. Lehmer, On Euler's totient function. *Bull. Amer. Math. Soc.* **38** (1932), no. 10, 745–751

[7] F. Luca and C. Pomerance, On composite integers n for which $\phi(n) \mid n - 1$. *Bol. Soc. Mat. Mexicana (3)* **17** (2011), no. 1, 13–21

[8] M. Tărnăuceanu, A generalization of the Euler's totient function. *Asian-Eur. J. Math.* **8** (2015), no. 4, 1550087, 13

Marius Tărnăuceanu
Faculty of Mathematics
"Al. I. Cuza" University
Iaşi, Romania
tarnauc@uaic.ro