Annales Univ. Sci. Budapest., Sect. Comp. 35 (2011) 43–49

COMPUTATIONAL INVESTIGATION OF LEHMER'S TOTIENT PROBLEM

P. Burcsi (Budapest, Hungary)
S. Czirbusz (Budapest, Hungary)
G. Farkas (Budapest, Hungary)

Dedicated to Professor Antal Járai on his 60th birthday

Abstract. Let N be a composite number for which $k \cdot \varphi(N) = N - 1$. We show that if $3 \mid N$ then $\omega(N) \geq 40\ 000\ 000$ and $N > 10^{360\ 000\ 000}$.

1. Introduction

In this paper we study a famous unanswered question, the so-called "Lehmer's Totient Problem", which was first studied by Lehmer in 1932 [1]. Lehmer asked whether there is such a composite integer N for which the equation

$$k \cdot \varphi(N) = N - 1 \tag{1}$$

holds, where φ is the Euler totient function. Then we say that N is a Lehmer number and k is the Lehmer index of N. Let us denote the set of Lehmer numbers by L. Lehmer conjectured that L is empty.

Let us consider the equation (1) in the form

$$1 = N - k \cdot \varphi(N), \tag{2}$$

from which some interesting facts follow immediately. We know that $\varphi(N)$ is always even, if $N > 1$. Thus if N is even, then $N - k \cdot \varphi(N)$ cannot be 1. Also

we can observe easily that if N is not squarefree then N has a prime factor p_i for which $p_i \mid \varphi(N)$. In this case if N is a Lehmer number, then $p_i \mid 1$ would be valid which is impossible, so we get the following assertion.

Remark 1. If N is a Lehmer number, then $2 \nmid N$ and N is square-free.

Hereafter we write a Lehmer number N in the form

$$N = p_1 p_2 \dots p_n, \text{ where } 3 \le p_1 < p_2 < \dots < p_n \tag{3}$$

and $p_1, p_2, \dots p_n$ are different prime numbers.

A composite number N is called *Carmichael number* if

$$a^{N-1} \equiv 1 \pmod{N}$$

is valid for all $a \in \mathbb{Z}$, where $(a, N) = 1$. The *Carmichael function* for N is defined as the smallest positive integer $\lambda(N)$ such that

$$a^{\lambda(N)} \equiv 1 \pmod{N}$$

for every integer a that is both coprime to and smaller than N. As a matter of fact $\lambda(N)$ is the exponent of $\mathbb{Z}_N^*$, the multiplicative group of residues modulo N, i. e. $\lambda(N)$ is the least common multiple of the orders of the elements of $\mathbb{Z}_N^*$. Since the order of $\mathbb{Z}_N^*$ is $\varphi(N)$ we have $\lambda(N) \mid \varphi(N)$. Thus if $\varphi(N) \mid N - 1$, then $\lambda(N) \mid N - 1$. Finally we get that $a^{N-1} \equiv 1 \pmod{N}$ for all elements of $\mathbb{Z}_N^*$, which implies the next assertion.

Remark 2. Every Lehmer number is a Carmichael number.

The next observation is important for the computational investigation of the Lehmer conjecture.

Remark 3. Let $3 \le p_1 < p_2 < \dots < p_n$ are different prime numbers. If $N = p_1 p_2 \dots p_n p_{n+1}$ is a Lehmer number, then

$$p_i \nmid p_{n+1} - 1, \text{ where } 1 \le i \le n.$$

This assertion follows directly from (2). Subbarao and Siva Rama Prasad proved the following statement in [2].

Remark 4. If N is a Lehmer number and $3 \mid N$, then

$$k \equiv 1 \pmod{3}.$$

2. Previous achievements

Although the Lehmer totient problem has not yet solved, a lot of results are published concerning it. Let us denote the number of distinct prime factors of N by $\omega(N)$. Lehmer showed that if $N \in L$, than $\omega(N) \geq 7$. Improving this result Lieuwens [3] proved in 1970 that $\omega(N) \geq 11$. In 1977 Kishore [4] showed that $\omega(N) \geq 13$, and his result was increased to 14 by Cohen and Hagis [5] in 1980 using a computational method. Nowadays the best lower bound of $\omega(N)$ is 15 reached by John Renze [6] in 2004, and R. Pinch gave a computational proof of the assertion:

$$N > 10^{30}.$$

Let us suppose that $p_1 = 3$. In this case Lieuwens shoved in [3] that

$$\omega(N) \geq 212 \text{ and } N > 5.5 \cdot 10^{570}.$$

This result was improved by Subbarao and Siva Rama Prasad in [2]:

$$\omega(N) \geq 1850.$$

In 1988 Hagis [7] proved by computer the following inequalities:

$$\omega(N) \geq 298\,848 \text{ and } n > 10^{1\ 937\ 042}. \tag{4}$$

We also mention two interesting pure mathematical results: Banks and Luca proved in [8] that the number of composite integers $N < x$ for which $\varphi(N) \mid N - 1$ is at most

$$O\left(x^{1/2}(\log\log x)^{1/2}\right).$$

Subbarao and Siva Rama Prasad showed in [2] that

$$N < (\omega(N) - 1)^{2^{(\omega(N)-1)}}.$$

3. Results

We focus on the case where $p_1 = 3$. With computational methods, we improve the results in (4) on $\omega(N)$ and N mentioned above.

We need some notations. Let $p_1 < p_2 < \ldots < p_m$ be a sequence of prime numbers. Hereafter we call this sequence a *G-sequence* if the numbers fulfill the conditions in (3). Now let r be a positive real number and $\underline{p} = p_1, \ldots, p_m$ be a G-sequence. We define the following value:

$$\begin{aligned}\min\omega(\underline{p}, r) \quad = \quad & \inf\{\omega(N) | N = p_1 p_2 \cdots p_m p_{m+1} \cdots p_n, \text{where} \\ & p_1 < \ldots < p_n \text{ is a G-sequence} \\ & \text{and the Lehmer index of N is at least } r\}.\end{aligned}$$

We define $\min N(\underline{p}, r)$ similarly, but for the infinum of N rather than $\omega(N)$. Clearly, if we set $r = 4$, these values give lower bounds for $\omega(N)$ and N if N is a Lehmer number with $3 \mid N$, since it follows from (4) that the Lehmer index of such a number is at least 4.

Unfortunately, it seems infeasible to calculate these values exactly. The greedy algorithm of choosing $p_{m+1}, \ldots, p_n$ such that we always select the smallest prime that keeps the G-sequence property might fail if r is large enough. We illustrate the intuition behind this with an example: Let $m = 1$ and $p_1 = 3$. The smallest possible value for p_2 is 5. Now if we want to extend the sequence, we will have to look for primes that are incongruent to 1 modulo 3 and 5, giving a set of 3 possible residue classes modulo 15, loosely speaking, a 3/8 fraction of all subsequent primes. If we choose $p_2 = 11$ instead, we get 9 possible residues modulo 33, a 9/20 fraction of primes, which is larger. So choosing 5 increases the Lehmer index faster, but this advantage might turn over when n becomes large, since there are more primes to choose from.

However, it is possible to give *lower bounds* with the simple greedy algorithm of choosing the minimal possible value for $p_m, \ldots, p_n$, if we only require $p_i \nmid p_j - 1$ to hold for $i < j$ with $i \leq m$. Such a sequence will be called a G_m-sequence. The estimates obtained this way are denoted by $\operatorname{est}\omega(\underline{p}, r)$ and $\operatorname{est} N(\underline{p}, r)$. We have

$$\min\omega(\underline{p}, r) \geq \operatorname{est}\omega(\underline{p}, r)$$

and also

$$\min\omega(\underline{p}, r) \geq \min \operatorname{est}\omega(\left[\underline{p}, p_{m+1}\right], r) \ , \tag{5}$$

where the minimum is taken over all p_{m+1} such that $\underline{p}, p_{m+1}$ is a G_{m+1}-sequence. The same is true for the estimates of N. Unfortunately, there are infinitely many possible p_{m+1} values, so in this form the estimate is still ineffective. Therefore we investigate the special case of G_m sequences when we add the extra condition that p_{m+1} is at least q. This will be written as $\operatorname{est}\omega([\underline{p}, q+], r)$. Note that we denote the extension of a sequence by brackets.

The algorithm is relatively simple to implement. The main idea was to transform the problem to an additive setting: instead of calculating the Lehmer

index directly, we calculate the sum of the logarithms of the $\frac{p_i}{p_i-1}$, and then account for the -1 in the numerator of the Lehmer index. The logarithms of the mentioned fractions were pre-stored in a table using fixed point representation. The rounding errors and the slight imprecision caused by the -1 in the numerator of the Lehmer-index are also considered, so we found that the 64-bit fixed point representation never caused problems.

We summarize the results in the Table 1 where the estimates correspond to nodes in a rooted tree. The root is 3, and each node of the tree represents a G-sequence $p_1, \ldots, p_m$ or a sequence $p_1, \ldots, p_m, q+$. Part of this infinite tree is shown in Figure 1. The table shows the values of $\operatorname{est}\omega(\underline{p}, 4)$, $\operatorname{est}N(\underline{p}, 4)$, and the lower bounds coming from inequality (5), where the minimum was taken over the descendants shown in the tree.

Sequence $\underline{p}$	$\operatorname{est}\omega$	$\log_{10}(\operatorname{est}N)$	bound for $\min\omega$	bound for $\min N$
[3]	1540	6082	$4.0 \cdot 10^7$	$10^{3.6 \cdot 10^8}$
[3, 5]	$4.9 \cdot 10^6$	$3.9 \cdot 10^7$	$4.0 \cdot 10^7$	$10^{3.6 \cdot 10^8}$
[3, 11]	$1.6 \cdot 10^7$	$1.3 \cdot 10^8$	$8.1 \cdot 10^7$	$10^{7.4 \cdot 10^8}$
[3, 17]	$4.8 \cdot 10^7$	$4.3 \cdot 10^8$	$8.4 \cdot 10^7$	$10^{7.6 \cdot 10^8}$
[3, 23]	$> 8.7 \cdot 10^7$	$> 7.9 \cdot 10^8$	$8.7 \cdot 10^7$	$10^{7.9 \cdot 10^8}$
[3, 29+]	$> 8.9 \cdot 10^7$	$> 8.1 \cdot 10^8$		
[3, 5, 17]	$4.0 \cdot 10^7$	$3.6 \cdot 10^8$		
[3, 5, 23]	$> 7.5 \cdot 10^7$	$> 6.8 \cdot 10^8$		
[3, 5, 29+]	$> 7.6 \cdot 10^7$	$> 7.0 \cdot 10^8$		
[3, 11, 17]	$> 8.1 \cdot 10^7$	$> 7.4 \cdot 10^8$		
[3, 11, 29]	$> 8.3 \cdot 10^7$	$> 7.5 \cdot 10^8$		
[3, 11, 41+]	$> 8.4 \cdot 10^7$	$> 7.7 \cdot 10^8$		
[3, 17, 23]	$> 8.4 \cdot 10^7$	$> 7.6 \cdot 10^8$		
[3, 17, 29+]	$> 8.6 \cdot 10^7$	$> 7.8 \cdot 10^8$		
[3, 23, 29]	$> 8.7 \cdot 10^7$	$> 7.9 \cdot 10^8$		
[3, 23, 41+]	$> 8.7 \cdot 10^7$	$> 7.9 \cdot 10^8$		

Table 1. This table shows our main results. For each sequence we show the estimates that were output by the program, and the estimates obtained by looking at the sequence's displayed descendants - only shown for nodes with children.

4. Further work

The efficiency of the programs can be further enhanced by parallel processing several G-sequences at a time. This can be achieved by "batch sieving"

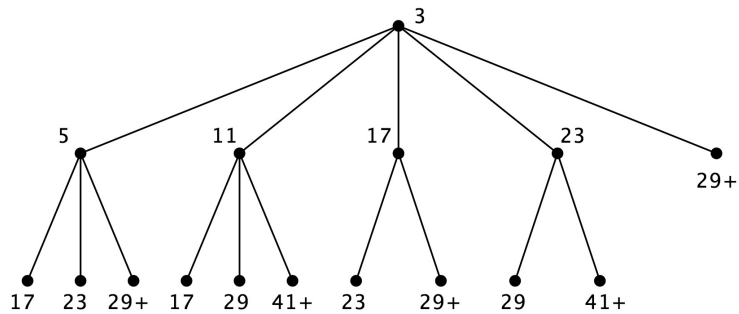

Figure 1. This figure shows part of the infinite tree of G-sequences.

that is calculating the logarithms of primes in an interval and registering which of the examined G-sequences can be extended by the sieved prime. This method will probably further improve the above results. New bounds will be published on the project's home page:

`http://compalg.inf.elte.hu/tanszek/projects.php`

Acknowledgment

The Project is supported by the European Union and co-financed by the European Social Fund (grant agreement no. TAMOP 4.2.1/B-09/1/KMR-2010-0003). Also we are greatly indebted to Prof. Antal Járai for his scientific consultations.

References

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

[2] **Subbarao, M.V. and V. Siva Rama Prasad,**, Some analogues of a Lehmer problem on the totient function, *Rocky Mountain Journal of Mathematics,* **15(2)** (1985), 187–202.

[3] **Lieuwens, E.,** Do there exists composite M for which $k\varphi(M) = M - 1$ holds?, *Nieuw Arch. Wisk.,* **18** (1970), 165–169.

[4] **Kishore, M.,** On the number of distinct prime factors of n for which $\varphi(n) \mid n - 1$, *Nieuw Arch. Wisk.,* **25** (1977), 48–53.

[5] **Cohen, G.L. and P. Jr. Hagis,** On the number of prime factors of n for which $\varphi(n) \mid n - 1$, *Nieuw Arch. Wisk.,* **28** (1980), 177–185.

[6] **Renze, J.,** Computational evidence for Lehmer's totient conjecture, *Published electronically at*
`http://library.wolfram.com/ infocenter/MathSource/5483/`, 2004.

[7] **Hagis, P. Jr.,** On the equation $M\varphi(n) = n - 1$, *Nieuw Arch. Wisk.,* **6** (1988), 225–261.

[8] **Banks, W.D. and F. Luca,** Composite integers n for which $\varphi(n) \mid n-1$, *Acta Mathematica Sinica, English Series*, **23** (2007), 1915–1918.

P. Burcsi, S. Czirbusz and G. Farkas
Department of Computer Algebra
Eötvös Loránd University
H-1117 Budapest, Hungary
`bupe@compalg.inf.elte.hu`
`czirbusz@gmail.com`
`farkasg@compalg.inf.elte.hu`