A note on Lehmer's Totient Problem

Richard G.E. Pinch

2 Eldon Road, Cheltenham, Glos GL52 6TU, U.K. rgep@chalcedon.demon.co.uk

Introduction

Lehmer's Totient Problem asks whether there is an integer n such that $\phi(n)$ divides $n-1$. We give a computational proof that there is no such n less than 10^{30} and that the number of prime factors of such a number must be at least 15.

Lehmer's Totient Problem

Lehmer's Totient Problem asks whether there is a composite integer N with $\phi(N)$ dividing $N-1$. We call such an N a *Lehmer number* and define the *Lehmer index* of N to be the ratio $\frac{N-1}{\phi(N)}$.

A *Carmichael number* N is a composite number N with the property that for every b prime to N we have $b^{N-1} \equiv 1 \mod N$. Equivalently the exponent $\lambda(N)$ of the multiplicative group $(\mathbb{Z}/N)^*$ must divide $N-1$. It follows that a Carmichael number N must be square-free, with at least three prime factors, and that $p-1|N-1$ for every prime p dividing N: conversely, any such N must be a Carmichael number.

Since the exponent $\lambda(N)$ of the multiplicative group divides its order $\phi(N)$, a Lehmer number must be a Carmichael number.

For background on Carmichael numbers and details of previous computations we refer to our previous paper [5] and to other posters at this conference.

No example of a Lehmer number is known. In this note we show that there is no Lehmer number less than 10^{30} and give an independent proof that a Lehmer number must have at least 15 prime factors.

Bounds on Lehmer numbers

Lieuwens [4] shows that a Lehmer number divisible by 3 must have index at least 4 and hence must have at least 212 prime factors and exceed $5 \cdot 10^{570}$.

Kishore [3] showed that a Lehmer number of index at least 3 must have at least 33 prime factors and hence exceed $2 \cdot 10^{56}$.

Cohen and Hagis [2] show that a Lehmer number divisible by 5 and of index 2 must have at least 15 prime factors.

Theorem 1. *There are no Lehmer numbers less than* 10^{30}.

Theorem 2. *A Lehmer number of index 3 must have at least 200 prime factors: it must exceed* $1.24 \cdot 10^{518}$.

Theorem 3. *A Lehmer number of index 4 must have at least 1000 prime factors: it must exceed* $2.68 \cdot 10^{3396}$.

Carmichael numbers with large Lehmer index

We define the *Lehmer index* of a Carmichael number N to be the quotient $(N-1)/\phi(N)$. A Lehmer number is thus a Carmichael number with integer Lehmer index.

We define a *C-sequence* to be a sequence of primes (p_i) such that no $p_i - 1$ is divisible by any term p_j. The prime divisors of a Carmichael number form a C-sequence. We may identify a C-sequence with the product of its terms and thus talk of its Lehmer index.

We extend a C-sequence $(p_i)_{i=1}^{d}$ by the *greedy algorithm* by taking p_{d+1} to be the smallest prime $> p_d$ such that the extended sequence retains the C-sequence property. We call such a sequence a *G-sequence*.

The G-sequence starting at 3 begins 3, 5, 17, 23, 29, 53, 83, 89, 113, 149, 173, 197, 257. This sequence after 4 terms has Lemher index $5865/2816 > 2$. The G-sequence starting at 3 and extending for 153903 terms, ending with 10853963, has Lehmer index > 3.

The back-tracking algorithm described in [5] proceeds by listing all C-sequences of given length with bounded product.

There are only finitely many Carmichael numbers with given index

We fix parameters r, I and ℓ and aim to list all Carmichael numbers $N > M$ with r prime factors and index at most I. Since the index of such a Carmichael number is at least 2^{r-1} we see that for given I there are only finitely many values of r which can occur.

Theorem 4. *For given d and $\ell > 1$, there are only finitely many C-sequences of length d with Lehmer index ℓ.*

The proof gives an algorithm for computing the sets $C(p,d,t)$ by recursion.

We were not able to find the smallest value of d such that $C(3,d,1/3)$ was non-empty but the greedy algorithm yields a sequence of length 153903, ending with 10853963. Lieuwens [4] conjectured that there was no such sequence, and that the Lehmer index of a C-sequence is bounded above. A heuristic argument suggests that this is false, that is, that the Lehmer index of a C-sequence is unbounded.

We were not able to find the smallest value of d such that $C(5,d,1/3)$ was non-empty but the set is empty when $d \leq 199$ and the greedy algorithm yields a sequence of length 100470, ending with 5160959.

A proof that $\omega(N) \geq 15$

The results of Hagis etc cited above show that we need only consider the case of Lehmer numbers of index 2 with smallest prime factor 5.

We define the *Euler index* of n to be $e(N) = N/\phi(N) = \prod_{p|N} \frac{p}{p-1}$. As before, we define the Euler index of a C-sequence (p_i) to be the Euler index of the product.

Since a Lehmer number must exceed 10^{30}, we have $\ell(N) < e(N) < \left(1+\frac{1}{10^{30}}\right)\ell(N)$.

It is sufficient to show that there is no C-sequence of length 14 beginning with 5, for which the Euler index lies in the interval $\left(2, 2+\frac{2}{10^{30}}\right)$, and which defines a Lehmer number of index 2.

A heuristic for the Lehmer index

Define a *K-number* to be a number n such that n is coprime to $\phi(n)$. The question of distribtion of K-numbers was considered by Erdos [1] who showed that the number of such $n \leq x$ is asymptotically $e^{-\gamma}x/\log\log\log x$. Clearly every Carmichael number is a K-number. The argument of Alford, Granville and Pomerance can be extended to show that there are infinitely many Carmichael numbers divisible by any given K-number.

There is a heuristic argument uggestinghow that the Lehmer index of a K-number n can be unbounded: that is, that $E(n) = n/\phi(n)$ can be arbitrarily large for K-numbers n.

ℓ	N	factors
2.14055	64075459460541239985	$3 \cdot 5 \cdot 17 \cdot 29 \cdot 53 \cdot 113 \cdot 173 \cdot 389 \cdot 4463 \cdot 4817$
2.14083	101817952350880305	$3 \cdot 5 \cdot 17 \cdot 23 \cdot 89 \cdot 113 \cdot 149 \cdot 3257 \cdot 3557$
2.17348	1177908521713261185	$3 \cdot 5 \cdot 17 \cdot 23 \cdot 29 \cdot 197 \cdot 617 \cdot 1217 \cdot 46817$
2.23494	171800042106877185	$3 \cdot 5 \cdot 17 \cdot 23 \cdot 29 \cdot 53 \cdot 89 \cdot 197 \cdot 1086989$

Carmichael numbers up to 10^{20} with Lehmer index greater than 2.14

References

[1] Pál Erdős, *Some asymptotic formulae in number theory*, J. Indian Math. Soc. **12** (1948), 75–78.

[2] Cohen G.L. and P. Hagis jr, *On the number of prime factors of n if* $\phi(n)|n-1$, Nieuw Arch. Wisk. (3) **28** (1980), 177–185.

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

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

[5] Richard G.E. Pinch, *The Carmichael numbers up to* 10^{15}, Math. Comp. **61** (1993), 381–391, Lehmer memorial issue.