A NOTE ON LEHMER'S TOTIENT PROBLEM (ABSTRACT)

RICHARD G.E. PINCH

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 $\frac{N-1}{\phi(N)}$.

No example of a Lehmer number is known. In this note we show that there is no Lehmer number less than 10^{28}, and that a Lehmer number must have at least 15 prime divisors.

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.

Lieuwens [3] 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 5.10^{570}. Kishore [2] showed that a Lehmer number of index at least 3 must have at least 33 prime factors and hence exceed 2.10^{56}. Cohen and Hagis [1] show that a Lehmer number divisible by 5 and of index 2 must have at least 13 prime factors.

To establish the lower bound of 10^{28}, it is sufficient to compute all the Carmichael numbers in this range with at least 14 prime factors, the smallest of which is at most 5. There are no such Carmichael numbers with more than 16 prime factors so the computation is reasonably small. We used the same back-tracking technique as described in [4] to find suitable sequences of possible prime factors.

To establish that there is no Lehmer number with 14 prime factors, necessarily of index 3 and with 5 as least prime factor, we used a recursive search over all permissible sequences with *Euler index* $\prod_p (1-1/p)$ in the interval $[2, 2+10^{-28}]$ and showed that none corresponds to a Lehmer number.

We were not able to find the smallest value of d such that there is a sequence of d primes with Lehmer index ≥ 3, but the greedy algorithm yields a sequence of length 153903, ending with 10853977. Lieuwens [3] conjectured that there was no such sequence, and that the Lehmer index is bounded above. We indicate a heuristic to suggest that this is false, that is, that the Lehmer index is unbounded.

References

1. G.L. Cohen and P. Hagis jr, *On the number of prime factors of n if $\phi(n) \mid (n-1)$*, Nieuw Arch. Wiskd., III. Ser. **28** (1980), 177–185.
2. M. Kishore, *On the number of distinct prime factors of n for which $\phi(n)|(n-1)$*, Nieuw Arch. Wisk. **25** (1977), 48–53.
3. E. Lieuwens, *Do there exist composite numbers for which $k\phi(M) == M - 1a$ holds?*, Nieuw. Arch. Wisk. **18** (1970), 165–169.
4. Richard G.E. Pinch, *The Carmichael numbers up to* 10^{15}, Math. Comp. **61** (1993), 381–391, Lehmer memorial issue.

2 Eldon Road, Cheltenham, Glos GL52 6TU, U.K.
E-mail address: rgep@chalcedon.demon.co.uk

Date: 01 May 2006.