COLLOQUIUM MATHEMATICUM

VOL. 86 2000 NO. 1

INFINITE FAMILIES OF NONCOTOTIENTS

BY

A. FLAMMENKAMP AND F. LUCA (BIELEFELD)

Abstract. For any positive integer n let $\phi(n)$ be the Euler function of n. A positive integer n is called a noncototient if the equation $x - \phi(x) = n$ has no solution x. In this note, we give a sufficient condition on a positive integer k such that the geometrical progression $(2^m k)_{m\geq 1}$ consists entirely of noncototients. We then use computations to detect seven such positive integers k.

For any positive integer n let $\phi(n)$ be the Euler ϕ function of n. A positive integer n is called a *noncototient* if the equation $x-\phi(x) = n$ has no solution. For example, $n = 10, 26, 34, 50, 52, 58, 86, 100$ are all noncototients. Sierpiński and Erdős (see **B36** in [3]) conjectured that there are infinitely many noncototients.

An affirmative answer to the above conjecture was given by Browkin and Schinzel in [1]. In the above mentioned paper, they showed that $2^n \cdot 509203$ is a noncototient for all positive integers n. Their proof used the number 509203 in an essential way. In this work, we extend the result of [1] by giving a general method for finding numbers k such that $2^n k$ is a noncototient for all positive integers n. As a corollary of our method, we have the following:

THEOREM. *Let $m \geq 1$ be a positive integer. Then each of the numbers $n=2^m k$, where $k\in\{509203, 2554843, 9203917, 9545351, 10645867, 11942443, 65484763\}$, is a noncototient.*

The following proposition provides the theoretical background for our Theorem.

PROPOSITION. *Let k be a positive integer satisfying the following four conditions*:

(i) *k is an odd prime.*

(ii) *k is not a Mersenne prime.*

2000 *Mathematics Subject Classification*: 11A25, 11L20, 11L26.

Work by the second author was supported by the Alexander von Humboldt Foundation.

(iii) *The number* $2^t k - 1$ *is composite for all integers* $t \geq 1$.
(iv) *The number* $2k$ *is a noncototient.*

Then the number $2^m k$ *is a noncototient for all positive integers* m.

Proof. Assume that $2^m k$ is a cototient for some $m \geq 1$. Write

$$x - \phi(x) = 2^m k. \tag{1}$$

Clearly, $x > 2$. In particular, $\phi(x)$ is even. From equation (1), it follows that x is even.

Write $x = 2^\alpha y$ where y is odd. If $y = 1$, we get

$$2^m k = x - \phi(x) = 2^\alpha - 2^{\alpha-1} = 2^{\alpha-1},$$

which is impossible. So, $y > 1$. We distinguish two cases:

Case 1: *y is squarefree.* If $y = p$ is prime, we get

$$2^m k = x - \phi(x) = 2^\alpha p - 2^{\alpha-1}(p-1) = 2^{\alpha-1}(p+1).$$

It now follows that $m \geq \alpha - 1$ and $p = 2^t k - 1$, where $t = m - \alpha + 1$. This contradicts condition (iii).

Assume now that $y = p_1 \dots p_s$, where $p_1 < \dots < p_s$ are odd primes and $s \geq 2$. We get

$$2^m k = 2^\alpha p_1 \dots p_s - 2^{\alpha-1}(p_1 - 1) \dots (p_s - 1).$$

It now follows that $m \geq \alpha - 1$ and

$$2p_1 \dots p_s - (p_1 - 1) \dots (p_s - 1) = 2^t k, \tag{2}$$

where $t = m - \alpha + 1$. Since $s \geq 2$, the product $(p_1 - 1) \dots (p_s - 1)$ is a multiple of 4. Since $2p_1 \dots p_s$ is a multiple of 2 but not of 4, from equation (2) it follows that $t = 1$. Now, if we set $z = 2p_1 \dots p_s$, equation (2) becomes

$$z - \phi(z) = 2k,$$

which contradicts condition (iv).

Case 2: *y is not squarefree.* Let $p^\beta \| y$ for some odd prime p and some $\beta > 1$. Since $p^{\beta-1} \mid \phi(x)$, it follows that

$$p^{\beta-1} \mid (x - \phi(x)) = 2^m k.$$

Since p is odd and k is prime, it follows that $p = k$ and $\beta = 2$. Now write $y = k^2 z$ for some odd squarefree integer z such that $k \nmid z$. If $z = 1$, we get

$$2^m k = x - \phi(x) = 2^\alpha k^2 - 2^{\alpha-1} k(k-1) = 2^{\alpha-1} k(k+1). \tag{3}$$

Equation (3) implies that $m \geq \alpha - 1$ and $k + 1 = 2^t$, where $t = m - \alpha + 1$. This contradicts (ii).

Assume now that $z > 1$. Write $z = p_1 \dots p_s$ for some odd primes $p_1 < \dots < \dots < p_s$. We get

$$2^m k = 2^\alpha k^2 p_1 \dots p_s - 2^{\alpha-1} k(k-1)(p_1 - 1) \dots (p_s - 1),$$

or

$$2kp_1 \dots p_s - (k-1)(p_1-1)\dots(p_s-1) = 2^t. \tag{4}$$

Since $s > 1$, the product $(k-1)(p_1-1)\dots(p_s-1)$ is a multiple of 4. Since $2kp_1 \dots p_s$ is even but is not a multiple of 4, it follows that $t = 1$. If we write $w = 2kp_1 \dots p_s$, equation (4) becomes

$$w - \phi(w) = 2. \tag{5}$$

The only solution of (5) is $w = 4$, which is impossible since w is a multiple of k.

The Proposition is therefore completely proved.

Proof of the Theorem. It suffices to construct numbers k with properties (i)–(iv) of the above Proposition. We first look at (iii). The first one to prove the existence of infinitely many positive integers k fulfilling (iii) was H. Riesel [4]. Since then, such numbers have been called *Riesel numbers*. The smallest Riesel number known is $k = 509203$ and it is conjectured (see [6]) that this is the smallest Riesel number. Four years later, W. Sierpiński (see [5]) showed that there exist infinitely many positive integers k such that $2^m k + 1$ is composite for all $m \geq 1$. The proofs of both Riesel's result and Sierpiński's result rely on an idea from a 1950 paper of Erdős (see [2]).

In what follows, we shall explain this idea in the case of the existence of Riesel numbers.

Suppose that $(a_i, m_i)_{i=1}^s$ is a *covering system of congruences*, that is, every positive integer n satisfies at least one congruence $n \equiv a_i \pmod{m_i}$ for some $i = 1, \dots, s$. Moreover, assume that the moduli m_i are chosen in such a way that $\prod_{i=1}^s (2^{m_i} - 1)$ is divisible by at least s distinct primes. By Hall's theorem, one can exhibit a set of s different primes p_i for $i = 1, \dots, s$ such that $p_i \mid (2^{m_i} - 1)$. Hence, in order to assure that a positive integer k fulfills (iii), it suffices to choose k such that

$$2^{a_i} k - 1 \equiv 0 \pmod{p_i}. \tag{6}$$

Indeed, if condition (6) is satisfied, then $2^m k - 1$ is always divisible by some p_i, hence it can never be prime. The fact that the system of congruences (6) is solvable is an immediate consequence of the Chinese Remainder Lemma. Moreover, the Chinese Remainder Lemma guarantees that all solutions of the system of congruences (6) form an arithmetical progression with first term k_0 and difference $\prod_{i=1}^s p_i$. Clearly, k_0 is coprime to $\prod_{i=1}^s p_i$. In particular, by Dirichlet's theorem, one can find infinitely many k's fulfilling both conditions (iii) and (i). From density arguments, it follows that most of the primes fulfilling (i) and (iii) are not Mersenne primes. The only condition that is left to check is therefore (iv).

A few words about computations. If one starts with the covering system of congruences $(0,2)$, $(0,3)$, $(1,4)$, $(3,8)$, $(7,12)$, $(23,24)$, then one can choose the six primes p_i to be $\{3,7,5,17,13,241\}$, resulting in the following system of congruences for k:

$$k \equiv 1 \pmod 3, \qquad k \equiv 1 \pmod 7, \qquad 2k \equiv 1 \pmod 5,$$
$$8k \equiv 1 \pmod{17}, \quad 2^7 k \equiv 1 \pmod{13}, \quad 2^{23} k \equiv 1 \pmod{241}.$$

This leads to the arithmetical progression for k with first term $k_0 = 509203$ and difference $3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$. A quick computer check revealed that 509203 satisfies conditions (i), (ii) and (iv) as well. Condition (iv) needed 2 sec of CPU-time. The next number in the above progression which satisfies conditions (i), (ii) and (iv) is 65484763. Condition (iv) now needed 40 min of CPU-time.

The other 5 values of k claimed by the Theorem were found choosing other systems of covering congruences.

Finally, a few words about checking for condition (iv). Suppose that $2k$ is a cototient. If x is a solution of

$$x - \phi(x) = 2k, \tag{7}$$

then, since $\phi(x)$ is even, it follows that x is even as well. Moreover, it is easy to see that x is squarefree. Since $\phi(x) \le x/2$ whenever x is even, any solution of (7) satisfies $x \le 4k$. Since the largest value of k tested satisfies

$$x \le 4k \le 4 \cdot 65484763 < \prod_{i=1}^{10} q_i = Q,$$

where $q_1, \dots, q_{10}$ are the first 10 primes, it follows that

$$\phi(x) > \frac{\phi(Q)}{Q} \cdot x > 0.163588x$$

in the tested range. Hence, if x satisfies equation (7), then

$$2k = x - \phi(x) < (1 - 0.163588)x,$$

or $x > 2.39k$. To summarize, in order to check (iv), we wrote a computer program which checked that equation (7) has no even squarefree solution in the interval $[2.39k, 4k]$ for every Riesel number k satisfying conditions (i) and (ii).

The Theorem is therefore proved.

REMARK. It is interesting to point out that all the known noncototients are even. To see why this is not coincidental, assume that y is an odd noncototient. If $y - 1$ can be written as a sum of two distinct primes p and q, then

$$pq - \phi(pq) = y,$$

which contradicts the fact that y is a noncototient. Since $y-1$ is even, Goldbach's conjecture asserts that $y-1$ can be written as a sum of two primes, at least when $y \geq 5$ (notice that 1 and 3 are not noncototients). Of course, in Goldbach's conjecture one allows the two primes to be equal. However, a conjecture of Hardy and Littlewood asserts that every large enough even number (probably larger than 12) can be written as a sum of two primes in more than one way. In particular, it can be written as a sum of two distinct primes. Thus, it seems reasonable to conjecture that, in fact, there are no odd noncototients. Notice also that since

$$p^k - \phi(p^k) = p^{k-1},$$

for all $k \geq 1$ and all prime numbers p, it follows that a noncototient can never be a power of a prime.

We also point out that the authors of [1] asked for the lower density of the set of noncototients. The above heuristic reasoning seems to indicate that the upper density of this set is at most 0.5.

Acknowledgements. We thank Marek Wójtowicz for pointing out to us reference [1].

We also thank Professor Andreas Dress and his research group in Bielefeld for their hospitality during the period when this paper was written.

REFERENCES

[1] J. Browkin and A. Schinzel, *On integers not of the form $n-\phi(n)$*, Colloq. Math. 68 (1995), 55–58.

[2] P. Erdős, *On integers of the form 2^k+p and related problems*, Summa Brasil. Math. 2 (1950), 113–123.

[3] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, 1994.

[4] H. Riesel, *Nøgra stora primtal* [Some large primes], Elementa 39 (1956), 258–260 (in Swedish).

[5] W. Sierpiński, *Sur un problème concernant les nombres $k \cdot 2^n + 1$*, Elem. Math. 15 (1960), 73–74; Corrigendum, ibid. 17 (1962), 85.

[6] *The Riesel Problem*, http://vamri.xray.ufl.edu/proths/rieselprob.html.

FSP Mathematisierung
Universität Bielefeld
Postfach 10 01 31
33 501 Bielefeld, Germany
E-mail: achim@uni-bielefeld.de
fluca@mathematik.uni-bielefeld.de

Received 2 July 1999 (3786)