COLLOQUIUM MATHEMATICUM

VOL. LXVIII 1995 FASC. 1

ON INTEGERS NOT OF THE FORM $n - \varphi(n)$

BY

J. BROWKIN AND A. SCHINZEL (WARSZAWA)

W. Sierpiński asked in 1959 (see [4], pp. 200–201, cf. [2]) whether there exist infinitely many positive integers not of the form $n-\varphi(n)$, where φ is the Euler function. We answer this question in the affirmative by proving

THEOREM. *None of the numbers* $2^k \cdot 509203$ $(k = 1, 2, \ldots)$ *is of the form* $n - \varphi(n)$.

LEMMA 1. *The number* 1018406 *is not of the form* $n - \varphi(n)$.

Proof. Suppose that

$$1018406 = n - \varphi(n) \tag{1}$$

and let

$$n = \prod_{i=1}^{j} q_i^{\alpha_i} \quad (q_1 < q_2 < \ldots < q_j \text{ primes}). \tag{2}$$

If for any $i \le j$ we have $\alpha_i > 1$ it follows that $q_i \mid 2 \cdot 509203$, and since 509203 is a prime, either $q_i = 2$ or $q_i = 509203$. In the former case $n - \varphi(n) \equiv 0 \not\equiv 1018406 \pmod 4$, in the latter case $n - \varphi(n) > 1018406$, hence

$$\alpha_i = 1 \quad (1 \le i \le j). \tag{3}$$

Since $n > 2$ we have $\varphi(n) \equiv 0 \pmod 2$, hence $n \equiv 0 \pmod 2$. However, $n/2$ cannot be a prime since 1018405 is composite. Hence $\varphi(n) \equiv 0 \pmod 4$ and $n \equiv 2 \pmod 4$. Moreover, $n \equiv 1 \pmod 3$ would imply $\varphi(n) \equiv n - 1018406 \equiv 2 \pmod 3$, which is impossible, since

$$\varphi(n) \equiv \begin{cases} 0 \pmod 3 & \text{if at least one } q_i \equiv 1 \pmod 3, \\ 1 \pmod 3 & \text{otherwise.} \end{cases}$$

Hence $n \equiv 2 \pmod{12}$ or $n \equiv 6 \pmod{12}$ and

$$n - \varphi(n) > \frac{1}{2} n. \tag{4}$$

1991 *Mathematics Subject Classification*: Primary 11A25.

Let p_i denote the ith prime and consider first the case $n = 12k + 2$. We have $q_1 = 2$, $q_i \geq p_{i+1}$ $(i \geq 2)$. Since

$$\prod_{i=2}^{7} p_{i+1} > 1018406, \tag{5}$$

it follows from (1)–(4) that $j \leq 6$ and

$$\frac{1}{2}\prod_{i=2}^{6}\left(1-\frac{1}{p_{i+1}}\right) \leq \frac{\varphi(n)}{n} \leq \begin{cases} 2/5 & \text{if } n \equiv 0 \pmod 5, \\ 1/2 & \text{otherwise.} \end{cases}$$

Hence if $n = 12k + 2$ satisfies (1) we have either $116381 < k < 141446$ or $141446 \leq k < 169735$ and $k \not\equiv 4 \pmod 5$.

Consider now $n = 12k + 6$. Here $q_1 = 2$, $q_2 = 3$, $q_i \geq p_i$. By (1)–(5), $j \leq 7$ and

$$\prod_{i=1}^{7}\left(1-\frac{1}{p_i}\right) \leq \frac{\varphi(n)}{n} \leq \frac{1}{3}.$$

Hence if $n = 12k + 6$ satisfies (1) we have

$$103561 < k < 127301.$$

The computation performed on the computer SUN/SPARC of the Institute of Applied Mathematics and Mechanics of the University of Warsaw using the program GP/PARI has shown that no n corresponding to k in the indicated ranges satisfies (1).

LEMMA 2. *All the numbers* $2^k \cdot 509203 - 1$ $(k = 1, 2, \ldots)$ *are composite.*

Proof. We have

$$509203 \equiv 2^{a_i} \pmod{q_i},$$

where $\langle q_i, a_i\rangle$ is given by $\langle 3, 0\rangle$, $\langle 5, 3\rangle$, $\langle 7, 1\rangle$, $\langle 13, 5\rangle$, $\langle 17, 1\rangle$ and $\langle 241, 21\rangle$ for $i = 1, 2, \ldots, 6$, respectively. Now, 2 belongs mod q_i to the exponent m_i, where $m_i =$ $2, 4, 3, 12, 8$ and 24 for $i = 1, 2, \ldots, 6$, respectively.

It is easy to verify that every integer n satisfies one of the congruences

$$n \equiv -a_i \pmod{m_i} \quad (1 \leq i \leq 6).$$

If $k \equiv -a_j \pmod{m_j}$ we have

$$2^k \cdot 509203 \equiv 2^{a_j - a_j} \equiv 1 \pmod{q_j},$$

and since $2^k \cdot 509203 - 1 > q_j$ the number $2^k \cdot 509203 - 1$ is composite.

Remark 1. Lemma 2 was proved by H. Riesel, already in 1956 (see [3], Anhang).

The following problem, implicit in [1], suggests itself.

PROBLEM 1. What is the least positive integer n such that all integers $2^k n - 1$ $(k = 1, 2, \dots)$ are composite?

Proof of the theorem. We shall prove that $n - \varphi(n) \neq 2^k \cdot 509203$ by induction on k. For $k = 1$ this holds by virtue of Lemma 1. Assume that this holds with k replaced by $k - 1$ $(k \geq 2)$ and that

$$n - \varphi(n) = 2^k \cdot 509203. \tag{6}$$

If $\varphi(n) \equiv 0 \pmod 4$ we have $n \equiv 0 \pmod 4$ and

$$\frac{n}{2} - \varphi\left(\frac{n}{2}\right) = 2^{k-1} \cdot 509203,$$

contrary to the inductive assumption. Thus $\varphi(n) \equiv 2 \pmod 4$ and $n = 2p^\alpha$, where p is an odd prime. From (6) we obtain

$$p^{\alpha-1}(p+1) = 2^k \cdot 509203.$$

By Lemma 2, $\alpha = 1$ is impossible. If $\alpha > 1$ we have

$$p \mid 2^k \cdot 509203,$$

and since 509203 is a prime, $p = 509203$, $\alpha = 2$ and

$$509204 = 2^k,$$

which is impossible. The inductive proof is complete.

Remark 2. D. H. Lehmer on the request of one of us has kindly computed the table of all numbers not of the form $n - \varphi(n)$ up to 50 000. This table and its prolongation up to 100 000 seems to indicate that the numbers not of the form $n - \varphi(n)$ have a positive density, about 1/10.

This suggests

PROBLEM 2. Have the integers not of the form $n - \varphi(n)$ a positive lower density?

Added in proof ((November 1994). A computation performed by A. Odlyzko has shown that there are 561 850 positive integers less than 5 000 000 not of the form $n - \varphi(n)$.

REFERENCES

[1] A. Aigner, *Folgen der Art $ar^n + b$, welche nur teilbare Zahlen liefern*, Math. Nachr. 23 (1961), 259–264.

[2] P. Erdős, *Über die Zahlen der Form $\sigma(n) - n$ und $n - \varphi(n)$*, Elem. Math. 28 (1973), 83–86.

[3] W. Keller, *Woher kommen die größten derzeit bekannten Primzahlen?*, Mitt. Math. Ges. Hamburg 12 (1991), 211–229.
[4] W. Sierpiński, *Number Theory*, Part II, PWN, Warszawa, 1959 (in Polish).

INSTITUTE OF MATHEMATICS
UNIVERSITY OF WARSAW
BANACHA 2
02-097 WARSZAWA, POLAND
E-mail: BRO@PLEARN.BITNET

MATHEMATICAL INSTITUTE
POLISH ACADEMY OF SCIENCES
ŚNIADECKICH 8
P.O. BOX 137
00-950 WARSZAWA, POLAND
E-mail: SCHINZEL@IMPAN.IMPAN.GOV.PL

Reçu par la Rédaction le 11.4.1994