MATHEMATICS OF COMPUTATION
VOLUME 46, NUMBER 174
APRIL 1986, PAGES 715–716

On the Congruence $2^{n-k} \equiv 1 \pmod{n}$

By Mok-Kong Shen

Abstract. It is shown that there are infinitely many positive integers k such that the congruence $2^{n-k} \equiv 1 \pmod{n}$ has infinitely many solutions n.

LEMMA. *If* m *satisfies the congruence*

$$b^{m-s} \equiv 1 \pmod{m} \tag{1}$$

then $n = b^m - 1$ *satisfies the congruence*

$$b^{n-t} \equiv 1 \pmod{n} \tag{2}$$

where $t = b^s - 1$.

Proof. $n - t = b^m - b^s = b^s(b^{m-s} - 1)$. Hence by (1) we have $m \mid (n - t)$, from which (2) follows.

Rotkiewicz [1] has recently proved that the congruence $2^{n-2} \equiv 1 \pmod{n}$ has infinitely many solutions. Using the above lemma, which is a generalization of a result of Malo [2], the following extension is immediate:

THEOREM. *Each of the congruences*

$$2^{n-k_i} \equiv 1 \pmod{n} \qquad (i = 0, 1, 2, \ldots), \tag{3}$$

where $k_0 = 2$, $k_{i+1} = 2^{k_i} - 1$, *has infinitely many solutions* n.

It remains an open question whether the congruence $2^{n-k} \equiv 1 \pmod{n}$ has infinitely many solutions n for all positive integers k.

It may be noted that our lemma, while useful in proving the theorem, is quite impractical for numerical computations. For instance, using a digital computer, the author found the following solutions of $2^{n-2} \equiv 1 \pmod{n}$ in the interval $[3, 10^6]$, which Rotkiewicz asked for in [1]:

$$20737 = 89 \cdot 233, \qquad 93527 = 7 \cdot 31 \cdot 431,$$
$$228727 = 127 \cdot 1801, \qquad 373457 = 7 \cdot 31 \cdot 1721,$$
$$540857 = 31 \cdot 73 \cdot 239.$$

Received December 5, 1984; revised April 22, 1985.
1980 *Mathematics Subject Classification*. Primary 10A15.

If one were to use the lemma to derive from them solutions of $2^{n-3} \equiv 1 \pmod{n}$, one would have obtained numbers having 6043 digits or more, while the least nontrivial solution in this case is modestly $n = 9$.

Postfach 340238
D-8000 Munich 34,
West Germany

1. A. Rotkiewicz, "On the congruence $2^{n-2} \equiv 1 \pmod{n}$," *Math. Comp.*, v. 43, 1984, pp. 271–272.
2. L. E. Dickson, *History of the Theory of Numbers*, Vol. 1, Chelsea, New York, 1971, p. 93.