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

(1) \[ b^{m-s} \equiv 1 \pmod{m} \]

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

(2) \[ b^{n-t} \equiv 1 \pmod{n} \]

where $t = b^s - 1$.

Proof. $n - t = b^m - b^s = b^s(b^{m-s} - 1)$. Hence by (1) we have $m | (n - t)$, 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

(3) \[ 2^{n-k_i} \equiv 1 \pmod{n} \quad (i = 0, 1, 2, \ldots) \]

where $k_0 = 2$, $k_{i+1} = 2k_i - 1$, 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]:

\[
\begin{align*}
20737 &= 89 \cdot 233, \\
93527 &= 7 \cdot 31 \cdot 431, \\
228727 &= 127 \cdot 1801, \\
373457 &= 7 \cdot 31 \cdot 1721, \\
540857 &= 31 \cdot 73 \cdot 239.
\end{align*}
\]
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