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

By A. Rotkiewicz

Abstract. There exist infinitely many positive integers $n$ such that $2^{n-2} \equiv 1 \pmod{n}$.

In the monograph [5] I proposed the following problem (problem 18, p. 138): Let $a, k > 1$ be fixed positive integers. Do there exist infinitely many composite $n$ such that $n \mid a^{n-k} - 1$?

Put $a = 2, k = 2$ in the above problem. Since by Fermat’s theorem $2^{p-1} \equiv 1 \pmod{p}$ for odd primes $p$, if $2^{n-2} \equiv 1 \pmod{n}$ and $n > 2$, $n$ must be composite. R. Matuszewski and P. Rudnicki (with the aid of the computer K-202 in Warsaw) checked that below 4208 such integers do not exist.

The following theorem holds:

**Theorem T.** There exist infinitely many positive integers $n$ such that $2^{n-2} \equiv 1 \pmod{n}$.

**Proof.** D. H. and Emma Lehmer ([1, p. 96] and [2, p. 139, F 10]) found the smallest (and still the only known) value $n > 1$ for which $2^n \equiv 3 \pmod{n}$. It is $n = 4700063497 = 19 \cdot 47 \cdot 5263229$.

First we remark that if $2^m \equiv 3 \pmod{m}$, then $n = 2^m - 1$ satisfies the congruence $2^{n-2} \equiv 1 \pmod{n}$. Indeed if $(2^m - 3)/m$ is a positive integer, then from the congruence $2^m \equiv 1 \pmod{2^m - 1}$ it follows that $(2^m)^{(2^m-3)/m} \equiv 1 \pmod{2^m - 1}$, $2^{2^m-3} \equiv 1 \pmod{2^m - 1}$ and $2^{n-2} \equiv 1 \pmod{n}$ for $n = 2^m - 1$. Thus $2^{n-2} \equiv 1 \pmod{n}$ for $n = 2^{n_0} - 1$, where $n_0 = 4700063497$.

Suppose now that $2^{n-2} \equiv 1 \pmod{n}$, and $n > 8$. Let $p$ be a primitive factor of the number $2^{n-2} - 1$ (a prime factor of $2^n - 1$ is said to be primitive if it does not divide any of the numbers $2^m - 1$ for $m = 1, 2, \ldots, n - 1$). By a theorem of K. Zsigmondy [7] such a prime factor exists for any $n > 6$ and is of the form $nt + 1$).

Now we shall show that $n_1 = np$ is also a solution of the congruence $2^{n_1-2} \equiv 1 \pmod{n_1}$.

We have $p = 2(n - 2)k + 1$, where $k$ is a positive integer and $p > 2n - 3 > n$ and $(p, n) = 1$. Thus

$$np - 2 = n[2(n - 2)k + 1] - 2 = (n - 2)(2nk + 1).$$
Hence $2^{n-2} - 1 | 2^{np-2} - 1$, and since

$$2^{n-2} \equiv 1 \pmod{n}, \quad 2^{p-2} \equiv 1 \pmod{p}, \quad (p, n) = 1,$$

we have $np | 2^{np-2} - 1$ and $n_1 = np$ satisfies the congruence $2^{n_1-2} \equiv 1 \pmod{n_1}$.

This completes the proof of our theorem.

In our proof we use the number $n = 2^{n_0} - 1$, where $n_0 = 470063497$. Thus $n$ has more than $1.4 \cdot 10^9$ digits and this raises the following question:

What is the smallest solution of $2^{n-2} \equiv 1 \pmod{n}$ with $n > 2$? From every solution of the congruence $2^m \equiv 3 \pmod{m}$ we can get a solution of the congruence $2^{n-2} \equiv 1 \pmod{n}$, but we do not know whether the converse is true. This leaves the problem:

Do there exist infinitely many natural numbers $n$ such that $2^n \equiv 3 \pmod{n}$?

An old conjecture of R. L. Graham [1, p. 96] asserts that for all $k \neq 1$, there are infinitely many $n$ such that $2^n \equiv k \pmod{n}$.

Remarks. I proved [6] that for every prime $p$ and every positive integer $a$ not divisible by $p$ there exist infinitely many natural numbers $n$ such that

$$p | n \quad \text{and} \quad n | a^{n-1} - 1$$

(so-called pseudoprimes to base $a$ which are divisible by a prime $p$).

The following problem arises:

For what primes $p$ does there exist a natural number $n$ such that $n | 2^{n-2} - 1$ and $p | n$?

Numbers $n > 3$ for which $n | a^{n-3} - 1$ holds for $(a, n) = 1$ have been considered by D. C. Morrow [4], who has called them $D$ numbers.

It is easy to see that every number of the form $n = 3p$, where $p$ is a prime $\geq 3$, is a $D$ number. A. Makowski [3] has proved that for any number $k \geq 2$ there exist infinitely many composite natural numbers $n$ such that the relation $n | a^{n-k} - 1$ holds for any integer $a$ with $(a, n) = 1$.

A. Makowski remarked also that one can prove in a similar way, as in Theorem T, that if $a^n \equiv k \pmod{n}$, then $a^{s-(k-1)} \equiv 1 \pmod{s}$ for $s = a^n - 1$.