Solutions of the congruence $2^{n-2} \equiv 1 \pmod{n}$ up to 10^{11}

Matti K. Sinisalo

Department of Mathematics
University of Oulu
Finland

Preprint
April, 1991

Abstract. All solutions of the congruence $2^{n-2} \equiv 1 \pmod{n}$ up to 10^{11} have been presented. Theoretical results and computing methods used have been described. More generally, it is shown that these methods can be used to find solutions for congruence $2^{f(n)} \equiv 1 \pmod{n}$, where f is a function $\mathbf{Z}^+ \to \mathbf{Z}$ having some quite general properties.

1 INTRODUCTION

In last years several authors ([3], [4], [6]) have proved, that congruence

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

and some of its generalisations have infinitely many solutions.

Anyway, only five least solutions have been published so far by Mok-Kong Shen ([4]) in 1986.

The aim of this paper is to show, that these solutions can be quite effectively computed and to present first solutions for further investigations.

2 THEORETICAL BACKGROUND

Let us start with some general results.vfil

In the following examinations we suppose that a and n are integers > 1.

Congruence $a^x \equiv 1 \pmod{n}$ has a trivial solution $x = 0$. It can be easily shown that this congruence has solutions $x > 0$ if and only if $\gcd(a, n) = 1$ and then $x > 0$ is a solution if and only if $\mathrm{ord}(a, n)|x$ (where $\mathrm{ord}(a, n)$ is the order of a modulo n ie. the least positive integer m for which $a^m \equiv 1 \pmod{n}$).

When the condition $\gcd(a, n) = 1$ is satisfied it follows from Euler's Theorem that a has unique inverse modulo n, say $\bar{a}$ ($\equiv a^{\varphi(n)-1} \pmod{n}$, where φ is Euler's totient function, $\bar{a}$ can be computed by this or by Euclidean algorithm), and we can define negative powers of a modulo n such that $a^x \equiv \bar{a}^{-x} \pmod{n}$. Again it can be shown that $x < 0$ is a solution of congruence $a^x \equiv 1 \pmod{n}$ if and only if $\mathrm{ord}(a, n)|x$.

LEMMA 1. Let f be a function $\mathbf{Z}^+ \to \mathbf{Z}$ such that for every odd integer x $f(x)$ is also odd. Let n be a solution of $2^{f(n)} \equiv 1 \pmod{n}$. Then either
1) $f(n) = 0$ or
2) n is odd and for every $q > 1$, such that $q|n$, $\mathrm{ord}(2, q)$ is odd.

Proof. If $f(n) = 0$ then the congruence is trivially true. Let us suppose that $f(n) \neq 0$.

Congruence $2^x \equiv 1 \pmod{n}$ has nontrivial solutions x if and only if $\gcd(2, n) = 1$, hence n is odd. But then $f(n)$ must also be odd.

From conditions $q|n$ and $2^{f(n)} \equiv 1 \pmod{n}$ it follows that $2^{f(n)} \equiv 1 \pmod{q}$ and $\mathrm{ord}(2, q)|f(n)$. Hence $\mathrm{ord}(2, q)$ must be odd. QED

By this simple lemma we can quite efficiently decrease the number of possilities to be checked. For example, a solution n of congruence (1) can't be divisable by primes $2, 3, 5, 11, 13, 17, 19, ...$ and so on. The only possible prime factor < 20 is 7.

Let us now suppose, that f in lemma 1 is a polynomial function say

$$f(x) = \sum_{k=0}^{m} c_k x^k, \quad c_k \in \mathbf{Z} \quad \forall k = 0, ..., m.$$

When $x \equiv 1 \pmod 2$ we have

$$f(x) \equiv \sum_{k=0}^{m} c_k, \quad (\text{mod } 2).$$

Hence necessary and sufficient condition for f having the property in lemma 1 is that the sum of the coefficients of f is odd. Function $f(x) = x-2$ in congruence (1) satisfies clearly this condition.

Now we know something about possible prime factors of n, but which of these factors can be quadratic in n?

LEMMA 2. Let $x \in \mathbf{Z}$, $\gcd(a, n) = 1$ and $a^x \equiv 1 \pmod n$. If $p > 1$ is a prime for which $p^m | n$, $m > 1$, and $p \nmid x$ then p has the property that $\text{ord}(a, p^m) | (p-1)$.

Proof. We have $p^m | n$ and $a^x \equiv 1 \pmod n$. Hence $a^x \equiv 1 \pmod{p^m}$ and $\text{ord}(a, p^m) | x$.

By the theorem of Euler we have $\text{ord}(a, p^m) | \varphi(p^m)$ ie. $\text{ord}(a, p^m) | p^{m-1}(p-1)$. Let us suppose, that $p | \text{ord}(a, p^m)$. Then we have $p | x$ which is a contradiction. Hence we have $\text{ord}(a, p^m) | (p-1)$. QED

By Fermat's little theorem we know, that $p | (a^{p-1} - 1)$ for every a such that $p \nmid a$. Hence $(a^{p-1} - 1)/p$ (which is called Fermat's quotient) is an integer for every a for which $p \nmid a$. Condition $\text{ord}(a, p^2) | (p-1)$ means that $p | (a^{p-1} - 1)/p$.

Prime numbers p for which this condition is satisfied are generally quite rare. When $a = 2$ these numbers are called Wieferich's numbers and when $a = 3$ they are called Mirimanoff's numbers.

These numbers have many interesting and important properties. Wieferich has shown that if the first case of Fermat conjecture has a counterexample, the exponent in this counterexample is a Wieferich number. Mirimanoff has shown the same for Mirimanoff's numbers. (see [2] p. 263, [5] p. 33, [8], [10], [11])

Only two Wieferich numbers are known. These numbers are 1093 ja 3511. By using a computer it has been shown, that there are no other Wieferich primes on the interval $[2, 6 \cdot 10^9]$ (Lehmer [8] 1981).

The orders of number 2 modulo 1093 and 3511 are 364 ja 1755. Hence by Lemma 1 number 1093 can't be a divisor of any solution of congruence (1) and we have only 3511 left.

LEMMA 3. Let $\gcd(a, n) = 1$ and $f : \mathbf{Z}^+ \to \mathbf{Z}$ be such function that if $q > 1$ is any quadratic prime factor of $x \in \mathbf{Z}^+$, then $q \nmid f(x)$. Let $a^{f(n)} \equiv 1 \pmod n$ and $p > 1$ be a quadratic prime factor of n. Then $\text{ord}(a, p^2) | (p-1)$.

Proof. This is a direct consequence of Lemma 2. QED

LEMMA 4. Let $\gcd(a,n)=1$, $f:\mathbf{Z}^+\to\mathbf{Z}$ be polynomial

$$f(x)=\sum_{k=0}^{m}c_kx^k,\quad c_k\in\mathbf{Z},\qquad \text{for all } k=0,...,m,$$

and $a^{f(n)}\equiv 1 \pmod n$. If $p>1$ is a quadratic prime factor off n and $f(n)\neq 0$, then
1) $p|c_0$
or
2) $\mathrm{ord}(a,p^2)|(p-1)$.

Proof. Let us suppose that $p\not|c_0$. Then we have $p\not|f(n)$. By Lemma 3 we have $\mathrm{ord}(a,p^2)|(p-1)$. QED

Let us now turn to congruence (1).

First off all we can see that congruence (1) has trivial solution $n=2$. Let us suppose from now on, that $n\geq 3$.

LEMMA 5. Let $n=pq$ be a solution of the congruence (1) where p is a prime (>2) and q an integer >2. Then $p|(2^{q-2}-1)$ and as a consequence $\mathrm{ord}(2,p)|(q-2)$.

Proof. From the congruence (1) it follows, that $p|(2^{pq-2}-1)$. Hence $p|(2^{(p-1)q+(q-2)}-1$ and $\mathrm{ord}(2,p)|(p-1)q+(q-2)$ On the other side by the Theorem of Euler we know that $\mathrm{ord}(2,p)|(p-1)$. Necessarily $p|(2^{q-2}-1)$. QED

LEMMA 6. Let n be a solution of congruence (1). Then n is not a power of an odd prime number.

Proof. Let $n=p^m$, where $m\geq 1$ is an integer. Using Lemma 5 $m-1$ times we get $\mathrm{ord}(2,p)|(p-2)$. By this and the Theorem of Euler we get $\mathrm{ord}(2,p)|((p-1)-(p-2))$ and $\mathrm{ord}(2,p)=1$, but this is a contradiction. QED

LEMMA 7. Let $n>2$ be a solution of congruence (1) and q any divisor of n. Then $q\equiv\pm 1 \pmod 8$. If q is a prime, then $q\equiv\pm 1,7 \pmod{24}$.

Proof. Let p be some prime factor of n. Clearly $p>2$. Congruence (1) can be written in the form $2^{n-1}\equiv 2 \pmod n$, from which we can conclude, that $(2^{(n-1)/2})^2\equiv 2 \pmod p$. Hence number 2 is a quadratic residue modulo p.

For the Legendre symbol we have then $(\frac{2}{p}) = 1$. On the other side, from a well-known result (see Rosen [7]) it follows that $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$. Hence we get $(-1)^{(p^2-1)/8} = 1$. Necessarily $(p^2-1)/8 = 2k$, where $k \in \mathbf{Z}$. So $p^2 = 16k+1$. But this can only happen, when $p \equiv 1, 7, 9, 15 \pmod{16}$, and $p \equiv \pm 1 \pmod 8$.

From this result it can be clearly seen that the similar result holds for every divisor q of n, and so for n itself, too.

For every $q|n$ we now have $q \equiv \pm 1, 7, 9 \pmod{24}$. But if $q \equiv \pm 9 \pmod{24}$ then $3|q$ and q can't be prime ($\mathrm{ord}(2,3) = 2$ is even). QED

LEMMA 8. Let n be a solution of congruence (1) and $p > 2$ a prime factor of n ie. $n = ap^m$, where a is an integer, $m \geq 1$, $p^{m+1} \not| n$. Then there exists an integer k, for which $n = ((\mathrm{ord}(2,p^m)+2) + k(2\mathrm{ord}(2,p^m)))p^m$.

Proof. From the congruence (1) we get $2^{ap^m-2} \equiv 1 \pmod{p^m}$ and so necessarily $\mathrm{ord}(2,p^m)|(ap^m-2)$ and $\mathrm{ord}(2,p^m)|a((p-1)+1)^m - 2$. By Lemma 2 we know that $\mathrm{ord}(2,p^m)|p-1$ and hence we get $\mathrm{ord}(2,p^m)|(a-2)$ ie. $a = k_1\mathrm{ord}(2,p^m)+2$ for some integer k_1. For $n = (k_1\mathrm{ord}(2,p^m)+2)p^m$ to be odd we must have k_1 odd. So $k_1 = 2k+1$ for some integer k and finally we get $n = ((2k+1)\mathrm{ord}(2,p^m) + 2)p^m = ((\mathrm{ord}(2,p^m)+2) + k(2\mathrm{ord}(2,p^m)))p^m$. QED

We can now easily conclude that there doesn't exist any solution $n \leq 10^{11}$ for congruence (1) having quadratic divisors. By Lemma 8 we know that if n is such a solution, then n is of the form $n = ((1755+2) + k(2 \cdot 1755))3511^2 = 21,658,751,597 + k \cdot 43,268,194,710$, where k is an integer ≥ 0. The only possibilities for n to be $\leq 10^{11}$ are $k = 0$ and $k = 1$, but these are not solutions.

THEOREM 1. Let n be a solution of the congruence (1), $p_1, p_2, ..., p_m$ be distinct odd primes, $\epsilon_1, \epsilon_2, ..., \epsilon_m$ integers ≥ 1, $P = p_1^{\epsilon_1}p_2^{\epsilon_2}\cdots p_m^{\epsilon_m}$, $L = \mathrm{lcm}(\mathrm{ord}(2,p_1^{\epsilon_1}), ..., \mathrm{ord}(2,p_m^{\epsilon_m}))$ and $P|n$.

Then
1) for all $i, j \in \{1, ..., m\}$ $p_i \not| \mathrm{ord}(2, p_j^{\epsilon_j})$,
2) there exists an integer h, unique modulo L, such that $hP \equiv 2 \pmod L$ and
3) there exists an integer k such that $n = (h + kL)P$.

Proof. 1) Let us suppose that $p_i|\mathrm{ord}(2,p_j^{\epsilon_j})$ for some $1 \leq i, j \leq m$. From the congruence (1) it follows that $p_j^{\epsilon_j}|(2^{n-2}-1)$. Hence $\mathrm{ord}(2,p_j^{\epsilon_j})|(n-2)$ and so we have $p_i|(n-2)$. But we have also $p_i|n$ and at least we get $p_i|(n-(n-2))$ or $p_i|2$. This is a contradiction.

2) From 1) it follows that $\gcd(P, L) = 1$. Hence there exists integers a, b such that $1 = aL + bP$. Multiplying by 2 and taking congruence modulo L we get $2 \equiv (2b)P \pmod{L}$. Hence we only have to select h such that $h \equiv 2b \pmod{L}$.

Let $h_1P \equiv h_2P \equiv 2 \pmod{L}$. Then $(h_1 - h_2)P \equiv 0 \pmod{L}$. But $\gcd(P, L) = 1$, hence $h_1 \equiv h_2 \pmod{L}$.

3) From congruence (1) it follows that n must satisfy the congruences

$$\begin{cases} n \equiv 0 & (\text{mod } P) \\ n \equiv 2 & (\text{mod } L).QED \end{cases}$$

One solution for these congruences is hP. From the Chinese Remainder Theorem it follows that this solution is unique modulo PL ($\gcd(P, L) = 1$). Hence n must be of the form $hP + k(PL) = (h + kL)P$, where $k \in \mathbb{Z}$. QED

3 COMPUTATIONAL PROCESS

The method used to compute the solutions of congruence (1) up to $M = 10^{11}$ had three steps:

1) Finding all solutions n of (1) having a prime factor p on interval $[\alpha, \beta]$, where α and β are some integers satisfying $\alpha < \sqrt{M} < \beta$.

This step was based on Lemma 8 and quite big amount of computing time. The prime numbers were checked from $2,000$ to $84,600,000$.

2) Finding all solutions n of (1) having a composite divisor $q < 1200 = \gamma$ and only one prime factor more ($n = qp$, p prime).

This step was based on Lemma 5 and the tables of factorizations of Mersenne type numbers in source Brillhart et al. [9]. For every q all prime factors p of $2^{q-2} - 1$ having $p \leq M/q$ were checked.

3) Finding all solutions n of (1) having all its prime factors $\leq \delta$ for some δ.

This step was easily done by a small Fortran which combined possible prime factors.

When step 1) has been executed, the solutions n which haven't been found have either a) all its prime factors $< \alpha$ or b) exactly one prime factor $> \beta$. Solutions having property a) can be found in step 3) when $\delta > \alpha$. Solutions which have property b) can be found in step 2) if $M/\beta < \gamma$.

4 SOLUTIONS

By using the method described above I have found the following solutions of congruence (1) on the interval $[3, 10^{11}]$.

$$S_1 = 20,737 = 89 \cdot 233$$
$$S_2 = 93,527 = 7 \cdot 31 \cdot 431$$
$$S_3 = 228,727 = 127 \cdot 1,801$$
$$S_4 = 373,457 = 7 \cdot 31 \cdot 1,721$$
$$S_5 = 540,857 = 31 \cdot 73 \cdot 239$$
$$S_6 = 2,231,327 = 7 \cdot 151 \cdot 2,111$$
$$S_7 = 11,232,137 = 7 \cdot 31 \cdot 191 \cdot 271$$
$$S_8 = 15,088,847 = 31 \cdot 233 \cdot 2,089$$
$$S_9 = 15,235,703 = 7 \cdot 79 \cdot 27,551$$
$$S_{10} = 24,601,943 = 79 \cdot 239 \cdot 1,303$$
$$S_{11} = 43,092,527 = 71 \cdot 337 \cdot 1,801$$
$$S_{12} = 49,891,487 = 47 \cdot 71 \cdot 14,951$$
$$S_{13} = 66,171,767 = 89 \cdot 233 \cdot 3,191$$
$$S_{14} = 71,429,177 = 31 \cdot 1,103 \cdot 2,089$$
$$S_{15} = 137,134,727 = 127 \cdot 151 \cdot 7,151$$
$$S_{16} = 207,426,737 = 7 \cdot 151 \cdot 311 \cdot 631$$
$$S_{17} = 209,402,327 = 23 \cdot 199 \cdot 45,751$$
$$S_{18} = 269,165,561 = 7 \cdot 79 \cdot 233 \cdot 2,089$$
$$S_{19} = 302,357,057 = 23 \cdot 463 \cdot 28,393$$
$$S_{20} = 383,696,711 = 89 \cdot 233 \cdot 18,503$$
$$S_{21} = 513,013,327 = 31 \cdot 3,257 \cdot 5,081$$
$$S_{22} = 1,145,222,057 = 7 \cdot 31 \cdot 191 \cdot 27,631$$
$$S_{23} = 1,198,235,777 = 31 \cdot 2,089 \cdot 18,503$$
$$S_{24} = 1,200,963,953 = 7 \cdot 73 \cdot 89 \cdot 26,407$$
$$S_{25} = 1,210,344,599 = 73 \cdot 337 \cdot 49,199$$

$$S_{26} = 1,336,271,543 = 89 \cdot 233 \cdot 64,439$$
$$S_{27} = 1,530,206,537 = 23 \cdot 79 \cdot 842,161$$
$$S_{28} = 1,654,163,777 = 7 \cdot 151 \cdot 431 \cdot 3,631$$
$$S_{29} = 2,247,340,097 = 23 \cdot 79 \cdot 151 \cdot 8,191$$
$$S_{30} = 2,383,604,687 = 71 \cdot 73 \cdot 199 \cdot 2,311$$
$$S_{31} = 2,745,926,897 = 7 \cdot 31 \cdot 1,831 \cdot 6,911$$
$$S_{32} = 3,067,561,177 = 71 \cdot 1,151 \cdot 37,537$$
$$S_{33} = 3,444,456,017 = 73 \cdot 89 \cdot 151 \cdot 3,511$$
$$S_{34} = 3,543,720,833 = 73 \cdot 48,544,121$$
$$S_{35} = 3,567,496,337 = 31 \cdot 4,177 \cdot 27,551$$
$$S_{36} = 3,638,049,527 = 7 \cdot 271 \cdot 601 \cdot 3,191$$
$$S_{37} = 4,135,367,777 = 23 \cdot 127 \cdot 337 \cdot 4,201$$
$$S_{38} = 4,343,487,407 = 7 \cdot 31 \cdot 431 \cdot 46,441$$
$$S_{39} = 4,404,655,367 = 7 \cdot 31 \cdot 3,191 \cdot 6,361$$
$$S_{40} = 5,056,376,807 = 191 \cdot 271 \cdot 97,687$$
$$S_{41} = 5,108,079,407 = 23 \cdot 79 \cdot 881 \cdot 3,191$$
$$S_{42} = 5,793,119,327 = 31 \cdot 73 \cdot 239 \cdot 10,711$$
$$S_{43} = 6,008,364,727 = 23 \cdot 31 \cdot 1801 \cdot 4,679$$
$$S_{44} = 6,629,012,777 = 127 \cdot 631 \cdot 82,721$$
$$S_{45} = 6,876,643,727 = 31 \cdot 71 \cdot 73 \cdot 127 \cdot 337$$
$$S_{46} = 7,650,778,457 = 7 \cdot 151 \cdot 631 \cdot 11,471$$
$$S_{47} = 8,143,707,497 = 23 \cdot 3,319 \cdot 106,681$$
$$S_{48} = 8,369,326,319 = 23 \cdot 607 \cdot 599,479$$
$$S_{49} = 8,605,878,287 = 31 \cdot 863 \cdot 321,679$$
$$S_{50} = 9,039,241,577 = 151 \cdot 487 \cdot 122,921$$
$$S_{51} = 9,046,381,577 = 127 \cdot 1,801 \cdot 39,551$$
$$S_{52} = 10,702,466,777 = 79 \cdot 463 \cdot 292,601$$
$$S_{53} = 10,915,386,649 = 233 \cdot 727 \cdot 64,439$$
$$S_{54} = 12,193,861,799 = 7 \cdot 79 \cdot 4,177 \cdot 5,279$$
$$S_{55} = 12,299,106,503 = 23 \cdot 73 \cdot 103 \cdot 71,119$$

$$S_{56} = 13,985,638,127 = 31 \cdot 13,367 \cdot 33,751$$
$$S_{57} = 17,312,443,631 = 7 \cdot 103 \cdot 503 \cdot 47,737$$
$$S_{58} = 17,343,716,537 = 7 \cdot 31 \cdot 1,721 \cdot 46,441$$
$$S_{59} = 17,554,812,167 = 73 \cdot 881 \cdot 272,959$$
$$S_{60} = 19,414,922,177 = 7 \cdot 89 \cdot 199 \cdot 156,601$$
$$S_{61} = 22,869,186,617 = 73 \cdot 89 \cdot 151 \cdot 23,311$$
$$S_{62} = 23,155,375,817 = 7 \cdot 31 \cdot 73 \cdot 79 \cdot 18,503$$
$$S_{63} = 25,367,354,777 = 31 \cdot 71 \cdot 127 \cdot 151 \cdot 601$$
$$S_{64} = 25,494,650,777 = 191 \cdot 199 \cdot 631 \cdot 1,063$$
$$S_{65} = 26,508,475,007 = 7 \cdot 31 \cdot 233 \cdot 524,287$$
$$S_{66} = 27,823,040,777 = 7 \cdot 47 \cdot 223 \cdot 601 \cdot 631$$
$$S_{67} = 31,109,707,127 = 337 \cdot 751 \cdot 122,921$$
$$S_{68} = 32,024,538,119 = 7 \cdot 73 \cdot 89 \cdot 704,161$$
$$S_{69} = 35,802,513,623 = 47 \cdot 10,711 \cdot 71,119$$
$$S_{70} = 35,879,030,327 = 7 \cdot 311 \cdot 1,801 \cdot 9,151$$
$$S_{71} = 42,245,251,127 = 23 \cdot 71 \cdot 89 \cdot 290,671$$
$$S_{72} = 47,909,079,407 = 7 \cdot 73 \cdot 89 \cdot 991 \cdot 1,063$$
$$S_{73} = 51,416,714,351 = 199 \cdot 431 \cdot 599,479$$
$$S_{74} = 51,563,126,617 = 127 \cdot 1,871 \cdot 217,001$$
$$S_{75} = 55,837,893,377 = 7 \cdot 31 \cdot 73 \cdot 271 \cdot 13,007$$
$$S_{76} = 63,731,873,207 = 23 \cdot 71 \cdot 73 \cdot 89 \cdot 6,007$$
$$S_{77} = 64,999,529,399 = 7 \cdot 89 \cdot 199 \cdot 524,287$$
$$S_{78} = 72,236,945,497 = 89 \cdot 233 \cdot 3,483,481$$
$$S_{79} = 74,605,302,977 = 337 \cdot 1,801 \cdot 122,921$$
$$S_{80} = 75,049,066,127 = 7 \cdot 31 \cdot 47 \cdot 73 \cdot 100,801$$
$$S_{81} = 78,625,368,857 = 7 \cdot 151 \cdot 3,191 \cdot 23,311$$
$$S_{82} = 78,943,150,127 = 271 \cdot 337 \cdot 751 \cdot 1,151$$
$$S_{83} = 82,597,478,537 = 7 \cdot 23 \cdot 79 \cdot 991 \cdot 6,553$$
$$S_{84} = 83,072,478,127 = 127 \cdot 22,751 \cdot 28,751$$
$$S_{85} = 83,266,672,777 = 89 \cdot 167 \cdot 881 \cdot 6,359$$
$$S_{86} = 90,578,716,697 = 7 \cdot 31 \cdot 271 \cdot 631 \cdot 2,441$$
$$S_{87} = 94,437,919,487 = 911 \cdot 4,447 \cdot 23,311$$
$$S_{88} = 97,019,792,537 = 31 \cdot 431 \cdot 1,609 \cdot 4,513$$

The first 5 solutions have been found by Mok-Kong Shen [4]. Solution $S_{34} = 73 \cdot 48,544,121$ has been found by McDaniel [1].

5 REMARKS

We have concluded above, that solutions n of (1) having a quadratic prime factors are quite rare. One can ask, if there exists any such solutions at all. Answer to this question is yes, since I have found the following solution satisfying this condition:

$$n = 39,992,485,447,538,478,857 = 71 \cdot 199 \cdot 263 \cdot 881 \cdot 991 \cdot 3,511^2.$$

Factorizing this $n - 2$ gives us

$$n - 2 = 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 131 \cdot 337 \cdot 216,245,789.$$

The orders of number 2 modulo divisors 71, 199, 263, 881, 991 and $3,511^2$ of n are $35 = 5 \cdot 7$, $99 = 3^2 \cdot 11$, 131, $55 = 5 \cdot 11$, $495 = 3^2 \cdot 5 \cdot 11$ and $1755 = 3^3 \cdot 5 \cdot 13$ correspondingly. Clearly they all divide $n - 2$.

Some open promblems remain:

1) For every p having the order of number 2 modulo p odd there exists a solution n of congruence (1) having $p|n$?

The least primes having the order of number 2 odd are 7, 23, 31, 47, 71, 73, 79, 89, 103, 127, 151, 167, 191, 199, 223, 233, 239, 263, 271, 311, 337 and so on. These all have corresponding solution in the list of solutions above (263 in counterexample above) first one without such a solution being 359.

2) Can these solutions and lemmas be used to find some heuristical formulas for the statistical distribution of the solutions?

The computational results presented here were obtained by using a Morse AT-computer and Microsoft Fortran interpreter. The factorizations of solutions were made by Derive calculator program. The computing time needed was some hundred hours.

6 References

[1] Wayne L. McDaniel: Some Pseudoprimes and Related Numbers Having Special Forms, Mathematics of Computation, vol 53 (187), pp. 407-409, 1989.

[2] Paolo Ribenboim: The book of Prime Number Records, Springer-Verlag, New York, Berlin, London, 1988.

[3] Peter Kiss, Bui Minh Phong: On a Problem of A. Rotkiewicz, Mathematics of Computation, vol 48 (178), pp. 751-755, 1988.

[4] Mok-Kong Shen: On the Congruence $2^{n-k} \equiv 1 \pmod{n}$, Mathematics of Computation, vol 46 (174), pp. 715-716, 1986.

[5] Wladyslaw Narkiewicz: Classical Problems in Number Theory, Polish Scientific Publishers, Warszawa, 1986.

[6] A. Rotkiewicz: On the Congruence $2^{n-2} \equiv 1 \pmod{n}$, Mathematics of Computation, vol 43 (164), pp. 271-272, 1984.

[7] Kenneth H. Rosen: Elementary Number Theory and Its Applications, Addison Wesley Publishing Company, publaddr London, 1984.

[8] D. H. Lehmer: On Fermat's Quotient, Base Two, Mathematics of Computation, vol 36 (153), pp. 289-290, 1981.

[9] Brillhart, Lehmer, Selfridge, Tuckerman, Wagstaff: Contemporary Mathematics, Vol 22, Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 7, 10, 11, 12$ up to high powers, American Mathematical Society, Providence, Rhode Island, 1980.

[10] Wells Johnson: On the p-divisibility of the Fermat Quotients, Mathematics of Computation, vol 32 (141), pp. 297-301, 1978.

[11] Wells Johnson: On the nonvanishing of Fermat quotients (mod p), J. Reine Angew. Math, vol 292, pp. 196-200, 1977.