ON EVEN PSEUDOPRIMES

A. Rotkiewicz
Institute of Mathematics, Polish Academy of Sciences
ul. Śniadeckich 8, 00-950 Warszawa, Poland

K. Ziemak
Technical University in Białystok
ul. Wiejska 45, Białystok, Poland
(*Submitted July 1993*)

A composite number n is called a pseudoprime if $n|2^n-2$. Until 1950 only odd pseudoprimes were known. So far, little is known about even pseudoprimes. D. H. Lehmer (see Erdös [5]) found the first even pseudoprime: $161038=2\cdot 73\cdot 1103$. In 1951 Beeger [2] showed the existence of infinitely many even pseudoprimes and found the following three even pseudoprimes: $2\cdot 23\cdot 31\cdot 151$, $2\cdot 23\cdot 31\cdot 1801$, and $2\cdot 23\cdot 31\cdot 100801$. Later Maciąg (see Sierpiński [9], p. 131) found the following two other even pseudoprimes:

$$2\cdot 73\cdot 1103\cdot 2089 \text{ and } \frac{2(2^{23}-1)(2^{29}-1)}{47}=2\cdot 233\cdot 1103\cdot 2089\cdot 178481.$$

The first-named author in his book [8] put forward the following problems: Does there exist a pseudoprime of the form 2^n-2? (problem #22) and: Do there exist infinitely many even pseudoprime numbers which are the products of three primes? (problem #51).

In 1989 McDaniel [4] gave an example of a pseudoprime which is itself of the form $2^n-2=2(2^{pq}-1)$ by showing that $2^{\mathcal{N}}-2$ is a pseudoprime if $\mathcal{N}=465794=2\cdot 7^4\cdot 97$, $p=37$, and $q=12589$.

In connection with the second problem, McDaniel [4] found the following even pseudoprimes: $2\cdot 178481\cdot 154565233$ and $2\cdot 1087\cdot 164511353$.

In 1965 (see [7], [6]) the first-named author proved the following two theorems:

1. The number pq, where p and q are different primes is a pseudoprime if and only if the number $(2^p-1)(2^q-1)$ is a pseudoprime.
2. For every prime number p $(7<p\neq 13)$, there exists a prime q such that $(2^p-1)(2^q-1)$ is a pseudoprime. For p = 2, 3, 5, 7, and 13, there is no prime q for which $(2^p-1)(2^q-1)$ is a pseudoprime.

If the number $2(2^p-1)$, where p is a prime, is a pseudoprime, then $2^p-1|2^{2^{p+1}-3}-1$; hence, $2^{p+1}\equiv 3 \pmod p$, which is impossible. McDaniel [4] showed that, if n satisfies the congruence $2^{n+1}\equiv 3 \pmod n$, then $2(2^n-1)$ is an even pseudoprime for $n=p_1p_2$ if $2^{p_1+1}\equiv 3 \pmod{p_2}$ and $2^{p_2+1}\equiv 3 \pmod{p_1}$. Here we shall prove the following theorem.

Theorem: Let p and q be primes and d be a divisor of $(2^p-1)(2^q-1)$. If d is coprime to p and q and not divisible by either 2^p-1 or 2^q-1, then $\frac{2(2^p-1)(2^q-1)}{d}$ is an even pseudoprime if and only if $\frac{2(2^{pq}-1)}{d}$ is an even pseudoprime.

Proof: Let $M = (2^p - 1)(2^q - 1)$, $N = 2^{pq} - 1$, where p and q are distinct primes. Suppose d is a divisor of M that is coprime to pq and which is divisible by neither $2^p - 1$ nor $2^q - 1$. First note that $M \equiv N \pmod{pq}$. Indeed, $M \equiv 2^q - 1 \equiv N \pmod{p}$ and, similarly, $M \equiv N \pmod{q}$, so that the assertion follows. Next let $\ell(m)$ denote the exponent to which 2 belongs modulo the odd natural number m, so that $2m$ is an even pseudoprime if and only if $\ell(m) \mid 2m-1$. Now it is easy to see that, if d has the stated properties, then $\ell(\frac{M}{d}) = \ell(\frac{N}{d}) = pq$. Thus, $\frac{2M}{d}$ is an even pseudoprime if and only if $pq \mid \frac{2M}{d} - 1$ if and only if $pq \mid \frac{2N}{d} -$ [since $M \equiv N \pmod{pq}$ and $(pq, d) = 1$] if and only if $\frac{2N}{d}$ is an even pseudoprime. Q.E.D.

Example: Since 47 is coprime to $23 \cdot 29$, from Maciąg's pseudoprime $\frac{2(2^{23}-1)(2^{29}-1)}{47}$, by the Theorem, we get the pseudoprime $\frac{2^{668}-2}{47}$.

For $d = 1$, we get the following corollary from the Theorem.

Corollary: The number $2(2^p - 1)(2^q - 1)$ is a pseudoprime if and only if the number $2(2^{pq} - 1)$ is a pseudoprime.

Example: By the Corollary, from McDaniel's [4] pseudoprime $2(2^{37 \cdot 12589} - 1)$, we get the pseudoprime $2(2^{37} - 1)(2^{12589} - 1)$.

Using the method presented in the paper of McDaniel [4] and the tables in [3], we found the following 24 even pseudoprimes with 3, 4, 5, 6, 7, and 8 prime factors:

$2 \cdot 311 \cdot 79903$, $2 \cdot 1319 \cdot 288313$, $2 \cdot 4721 \cdot 459463$, $2 \cdot 7 \cdot 359 \cdot 601$, $2 \cdot 23 \cdot 271 \cdot 631$,
$2 \cdot 31 \cdot 233 \cdot 631$, $2 \cdot 127 \cdot 199 \cdot 3191$, $2 \cdot 127 \cdot 599 \cdot 1289$, $2 \cdot 73 \cdot 631 \cdot 3191$, $2 \cdot 7 \cdot 191 \cdot 153649$,
$2 \cdot 47 \cdot 311 \cdot 68449$, $2 \cdot 7 \cdot 79 \cdot 7555991$, $2 \cdot 151 \cdot 383 \cdot 201961$, $2 \cdot 73 \cdot 271 \cdot 2940521$,
$2 \cdot 89 \cdot 337 \cdot 11492353$, $2 \cdot 23 \cdot 31 \cdot 151 \cdot 991$, $2 \cdot 73 \cdot 631 \cdot 991 \cdot 3191$,
$2 \cdot 233 \cdot 1103 \cdot 2089 \cdot 12007 \cdot 178481$, $2 \cdot 233 \cdot 1103 \cdot 2089 \cdot 178481 \cdot 458897$,
$2 \cdot 233 \cdot 1103 \cdot 2089 \cdot 178481 \cdot 88039999$, $2 \cdot 233 \cdot 1103 \cdot 2089 \cdot 12007 \cdot 178481 \cdot 458897$,
$2 \cdot 233 \cdot 1103 \cdot 2089 \cdot 12007 \cdot 178481 \cdot 88039999$, $2 \cdot 233 \cdot 1103 \cdot 2089 \cdot 178481 \cdot 458897 \cdot 88039999$,
$2 \cdot 233 \cdot 1103 \cdot 2089 \cdot 12007 \cdot 178481 \cdot 458897 \cdot 88039999$.

Beeger's [2] proof of the existence of an infinite number of even pseudoprimes has been based on the fact that, for every even pseudoprime $a_1 = 2n$, there exists a prime p such that $a_2 = pa_1$ is also a pseudoprime. We shall repeat it shortly. By a theorem of Bang [1], it follows that there exists a prime p (called a primitive prime factor of $2^{2n-1} - 1$) for which holds $2^{2n-1} \equiv 1 \pmod{p}$, $2^x \not\equiv 1 \pmod{p}$, $1 \le x < 2n-1$, and $p \equiv 1 \pmod{2(2n-1)}$, which leads to the fact that pa_1 is a pseudoprime. We can take instead of a primitive prime factor of $2^{2n-1} - 1$ any other factor of the same number that is $\equiv 1 \pmod{2(2n-1)}$ and coprime with a_1 if it exists. So the infinite sequence $a_1, a_2, \ldots$, has the property $2 < a_1 \mid (a_i, a_j)$ for $i \ne j$. Thus, the following problem arises:

1. Does there exist an infinite sequence $a_1, a_2, \ldots$ of even pseudoprimes such that $(a_i, a_j) = 2$ for every $i \ne j$?

It is easy to see that if the problem #51 mentioned at the beginning of the present paper has an affirmative answer then there is a positive answer to problem 1, but problem 1 seems to be easier.

We also do not know the answer to the following question:

2. Does there exist an integer n such that n and $n+1$ are pseudoprimes?

It would be of interest to investigate the case of n even or odd separately.

REFERENCES

1. A. S. Bang. "Taltheoretiske Undersøgelser." *Tidskrift f. Math.* ser. 5, **4** (1886):70-80 and 130-37.
2. N. G. W. H. Beeger. "On Even Numbers m Dividing $2^m - 2$." *Amer. Math. Monthly* **58** (1951):553-55.
3. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, & S. S. Wagstaff, Jr. "Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ Up to High Powers." *Contemp. Math.* **22** (1983), Amer. Math. Soc., Providence, RI.
4. W. L. McDaniel. "Some Pseudoprimes and Related Numbers Having Special Forms." *Math. Comp.* **53** (1989):407-09.
5. P. Erdös. "On Almost Primes." *Amer. Math. Monthly* **57** (1950):404-07.
6. A. Rotkiewicz. "Sur les nombres premiers p et q tels que $pq | 2^{pq} - 2$." *Rendiconti del Circolo Matematico di Palermo* **11** (1962):280-82.
7. A. Rotkiewicz. "Sur les nombres pseudopremiers de la forme $M_p M_q$." *Elemente der Mathematik* **20** (1965):108-09.
8. A. Rotkiewicz. *Pseudoprime Numbers and Their Generalizations.* MR 48#8373. Student Association of Faculty of Sciences, University of Novi Sad, 1972.
9. W. Sierpiński. *Arytmetyka Teoretyczna.* Warszawa, 1953, PWN.

AMS Classification Number: 11A07

❖❖❖