MATHEMATICS OF COMPUTATION
VOLUME 53, NUMBER 187
JULY 1989, PAGES 407-409

Some Pseudoprimes and Related Numbers Having Special Forms

By Wayne L. McDaniel

Abstract. We give an example of a pseudoprime which is itself of the form $2^n - 2$, answering a question posed by A. Rotkiewicz, show that Lehmer's example of an even pseudoprime having three prime factors is not unique, and answer a question of Benkoski concerning the solutions of $2^{n-2} \equiv 1 \pmod n$.

1. Introduction. The following theorem is a slightly more general form of a result which has been applied to the discovery of pseudoprimes (that is, of composite integers n such that $n \mid (2^n - 2)$) for many years (see Dickson [3, v. I, pp. 91–95]).

THEOREM 1. *Let u be any integer, $n = p_1 p_2 \cdots p_s$ with $p_1, \ldots, p_s$ distinct primes, a be any integer such that $(a, n) = 1$, and e_i be the order of a modulo p_i for $1 \le i \le s$. If r_i is the least nonnegative integer such that $a^{r_i} \equiv u \pmod{p_i}$, then*

$$a^{cn-k} \equiv u \pmod n$$

if and only if $e_i \mid (cn/p_i - k - r_i)$ for $i = 1, 2, \ldots, s$.

Proof. The convergence $a^{cn-k} \equiv u \pmod n$ holds if and only if, for each i, $a^{cn-k-r_i} \equiv 1 \pmod{p_i}$, which holds precisely if $e_i \mid (cn - k - r_i)$ for each i. But

$$cn - k - r_i = \frac{cn}{p_i}(p_i - 1) + \left(\frac{cn}{p_i} - k - r_i\right).$$

The computation involved in the application of this theorem to our problem is quite straightforward, requiring only a programmable hand-held calculator (we used a Casio fx-4000P), and, on occasion, the tables [2].

2. Applications. We now apply Theorem 1 to three distinct problems.

Application 1. In his book *Pseudoprime Numbers and Their Generalizations* [9], Rotkiewicz asks (problem #22) if there exists a pseudoprime of the form $2^N - 2$. We find a pseudoprime of this form by first applying Theorem 1 to the congruence $2^{p_1 p_2 + 1} \equiv 3 \pmod{p_1 p_2}$ (i.e., $c = 1$, $k = -1$, $a = 2$, $u = 3$). Letting r_1 assume the values $2, 4, 6, \ldots$, we find that when $r_1 = 26$, then $37 \mid (2^{26} - 3)$. Choosing $p_1 = 37$ and $r_2 = p_1 + 1$ assures that for any positive integer $e_2, e_2 \mid (n/p_2 - k - r_2)$. Upon examining the divisors of $2^{r_2} - 3$, it is found that the divisor $p_2 = 12589$ satisfies the condition $(p_1 - 1) \mid (n/p_1 - k - r_1)$. It follows from the theorem that $2^{n+1} \equiv 3$

Received March 24, 1988; revised September 6, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11A07.
Key words and phrases. Pseudoprime.

$(\mathrm{mod}\, n)$ for $n = p_1p_2$. Indeed,

$$2^{n+1} - 3 \equiv 2^{p_1p_2+1} - 3 \equiv \begin{cases} 2^{37+1} - 3 \equiv 0 \ (\mathrm{mod}\, 12589), \\ 2^{12589+1} - 3 \equiv 2^{36\cdot 349} \cdot 2^{26} - 3 \equiv 0 \ (\mathrm{mod}\, 37). \end{cases}$$

Let $N = 37 \cdot 12589 + 1 = 465794$ and $m = 2^N - 2$. Now,

$$\begin{aligned}(N-1) \mid (2^N - 3) &\Rightarrow (2^{N-1} - 1) \mid (2^{2^N-3} - 1) \\ &\Rightarrow (2^N - 2) \mid (2^{2^N-2} - 2) \Rightarrow 2^m \equiv 2 \ (\mathrm{mod}\, m).\end{aligned}$$

We believe, but have not shown, that $N = 465794$ is the smallest integer such that $2^N - 2$ is a pseudoprime.

Application 2. In [9, problem 51], Rotkiewicz asks whether there exist infinitely many even pseudoprimes which are the product of three primes. The only known example is $161038 = 2 \cdot 73 \cdot 1103$, found by D. H. Lehmer (see Erdös [4]). While answering Rotkiewicz's question would appear to be quite difficult, it is *not* difficult to show that there are at least three solutions.

We apply Theorem 1 to the congruence $2^{2p_1p_2-1} \equiv 1 \ (\mathrm{mod}\, p_1p_2)$ (i.e., $c = 2$, $k = 1$, $u = 1$), proceeding by letting e_1 assume the values $3, 5, 7, \ldots.$ We readily find that $e_1 = 23$ and $e_1 = 41$ lead, respectively, to the two solutions $N_1 = 2 \cdot 178481 \cdot 154565233$ and $N_2 = 2 \cdot 1087 \cdot 164511353$. Verification, using the tables [2] is immediate (2 belongs to 23 modulo 178481, to 1119 modulo 154565233, to 543 modulo 1087 and to 41 modulo 164511353). Hence, N_1 and N_2 are even pseudoprimes having exactly three prime factors.

Application 3. S. J. Benkoski observes, in his review [1] of Mok-Kong Shen's paper "On the congruence $2^{n-k} \equiv 1 \ (\mathrm{mod}\, n)$" [11], that Shen's five solutions n of $2^{n-2} \equiv 1 \ (\mathrm{mod}\, n)$ are each congruent to 7 modulo 10, and asks whether there is a solution whose last digit is not 7.

Applying Theorem 1 to $2^{p_1p_2-2} \equiv 1 \ (\mathrm{mod}\, p_1p_2)$, we find that, for $e_1 = 9$, $p_1 \mid (2^{e_1} - 1)$ for $p_1 = 73$; letting $e_2 = 71$ assures that $e_2 \mid (p_1 - 2)$. From the tables [2], we find that $p_2 = 48544121$ is a prime divisor of $2^{71} - 1$ and $e_1 \mid (p_2 - 2)$. Hence, $n = 73 \cdot 48544121$ is a solution of $2^{n-2} \equiv 1 \ (\mathrm{mod}\, n)$ which is not congruent to 7 modulo 10.

Two other, larger, solutions of $2^{n-2} \equiv 1 \ (\mathrm{mod}\, n)$ which are not congruent to 7 modulo 10 are, in fact, known. Rotkiewicz [10] showed that if m satisfies the congruence $2^m \equiv 3 \ (\mathrm{mod}\, m)$, then $n = 2^m - 1$ is a solution of $2^{n-2} \equiv 1 \ (\mathrm{mod}\, n)$; the only known solution $m = 4700063497$ (found by Lehmer [5, p. 96]) of $2^m \equiv 3 \ (\mathrm{mod}\, m)$ gives a solution n congruent to 1 modulo 10 of $2^{n-2} \equiv 1 \ (\mathrm{mod}\, n)$. The referee of this paper has informed us that Professor Mingzhi Zhang has noted the above example and has given the following additional example: $n = p_1p_2$ where $p_1 = 524287$ and $p_2 = 13264529$ ($p_1 = 2^{19} - 1$ and $p_2 \mid 2^{47} - 1$) [12].

Benkoski's question is interesting because it leads to the following more general observation which implies the existence of infinitely many solutions n of $2^{n-2} \equiv 1 \ (\mathrm{mod}\, n)$ which are congruent to 7 modulo 10. We note, prior to stating the theorem, that $a^{n-k} \equiv 1 \ (\mathrm{mod}\, n)$ has been shown to have infinitely many solutions for all pairs of positive integers a and k [6], [7] (for $a = k = 2$, see [10], and for k negative, [8]).

THEOREM 2. *If* $a^{n-k} \equiv 1 \pmod{n}$ *has a solution* $n = n_0 > 2k - 1$ *such that* $n_0 \equiv k \pmod 5$, *then the congruence has infinitely many solutions congruent to* n_0 *modulo* 10 (*and hence, also, congruent to* $k \pmod 5$).

Proof. Let $n = n_0$ satisfy the hypothesis of the theorem. Rotkiewicz showed ([9, Theorem 31]) that if p is any primitive prime divisor of $a^{n_0-k} - 1$ and n_0 is composite (this restriction was recently removed by McDaniel [8]) with $n_0 > 2k-1$, then pn_0 is also a solution (p is a primitive prime divisor of $a^N - 1$ if $p \mid (a^N - 1)$ and $p \nmid (a^m - 1)$ for $1 \leq m < N$; it is well known that a primitive divisor has the form $jN + 1$). Thus, p has the form $p = j(n_0 - k) + 1$ and is clearly congruent to $1 \pmod{10}$ since $j(n_0 - k)$ is even and divisible by 5. Hence, if $n_1 = pn_0$, then $n_1 \equiv n_0 \pmod{10}$. The theorem follows.

Department of Mathematics and Computer Science
University of Missouri–St. Louis
St. Louis, Missouri 63121

1. S. J. BENKOSKI, Review of "On the congruence $2^{n-k} \equiv 1 \pmod{n}$." MR 87e:11005.

2. 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., vol. 22, Amer. Math. Soc., Providence, R.I., 1983.

3. L. E. DICKSON, *History of the Theory of Numbers*, Chelsea, New York, 1952.

4. P. ERDÖS, "On almost primes," *Amer. Math. Monthly*, v. 57, 1950, pp. 404–407.

5. P. ERDÖS & R. L. GRAHAM, *Old and New Problems and Results in Combinatorial Number Theory*, Monographies de L'Enseignement Mathématique, No. 28, Genève, 1980.

6. P. KISS & B. M. PHONG, "On a problem of A. Rotkiewicz," *Math. Comp.*, v. 48, 1987, pp. 751–755.

7. W. L. MCDANIEL, "The generalized pseudoprime congruence $a^{n-k} \equiv b^{n-k} \pmod{n}$," *C. R. Math. Rep. Acad. Sci. Canada*, vol. 9 (2), 1987, pp. 143–147.

8. W. L. MCDANIEL, "The existence of solutions of the generalized pseudoprime congruence $a^{f(n)} \equiv b^{f(n)} \pmod{n}$." (To appear.)

9. A. ROTKIEWICZ, *Pseudoprime Numbers and Their Generalizations*, Student Association of the Faculty of Sciences, Univ. of Novi Sad, 1972.

10. A. ROTKIEWICZ, "On the congruence $2^{n-2} \equiv 1 \pmod{n}$," *Math. Comp.*, v. 43, 1984, pp. 271–272.

11. M.-K. SHEN, "On the congruence $2^{n-k} \equiv 1 \pmod{n}$," *Math. Comp.*, v. 46, 1986, pp. 715–716.

12. M. ZHANG (unpublished result).